



**Fortinet**

## **Exam Questions NSE6\_FNC-7.2**

Fortinet NSE 6 - FortiNAC 7.2

#### NEW QUESTION 1

Where do you look to determine when and why the FortiNAC made an automated network access change?

- A. The Event view
- B. The Port Changes view
- C. The Connections view
- D. The Admin Auditing view

**Answer:** B

#### Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/536166/viewing-event-logs>

Study Guide p. 356: Any time FortiNAC changes network access for an endpoint, the change is documented on the Port Changes view. This provides an administrator with valuable information when validating control configurations and enforcement.

#### NEW QUESTION 2

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 3

When configuring isolation networks in the configuration wizard, why does a Layer 3 network type allow for more than one DHCP scope for each isolation network type?

- A. There can be more than one isolation network of each type.
- B. Any scopes beyond the first scope are used if the Initial scope runs out of IP addresses.
- C. Configuring more than one DHCP scope allows for DHCP server redundancy.
- D. The Layer 3 network type allows for one scope for each possible host status.

**Answer:** A

#### NEW QUESTION 4

View the command and output shown in the exhibit.

```
>Client -mac *C4:4E:12
Found 1 matches for client
Intel Corporation
    DBID = 606
    MAC = 00:03:47:C4:4E:12
    IP = null
    Medium = null
    Description = null
    Status = Connected
    State = Initial
    Type = DynamicClient
    Ident = null
    UserID = null
    ParentID = 576
    Role = NAC-Default
    Security Access Value = null
    OS = null
    Location = Building 1 Switch SuperStack II Switch 3900-2
    Client Not Authenticated = false
    Client needs to authenticate = false
    Logged On = false
    At-Risk = false
    Host role = NAC-Default
    VpnClient = false
```

What is the current state of this host?

- A. Rogue
- B. Registered
- C. Not authenticated
- D. At-Risk

**Answer:** A

#### Explanation:

The exhibit's command and output detail various attributes for a specific host, including the MAC address, connection status, and various other parameters. The status "Connected" and state "Initial" indicate that the host has been detected on the network but has not yet completed any authentication process. The lines "Client Not Authenticated = true" and "Client needs to authenticate = false" suggest that the host has not yet been authenticated. Therefore, the current state of the

host is "Not authenticated," since there is a clear indication that the authentication process has not been completed for this host.

#### NEW QUESTION 5

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 6

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 7

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 8

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 9

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 10

Which three communication methods are used by FortiNAC to gather information from and control, infrastructure devices? (Choose three.)

- A. CLI

- B. SMTP
- C. SNMP
- D. FTP
- E. RADIUS

**Answer:** ACE

**Explanation:**

FortiNAC Study Guide 7.2 | Page 11

FortiNAC uses various methods to communicate with infrastructure devices such as SNMP for discovery and ongoing management, SSH or Telnet through the CLI for tasks related to the infrastructure, and RADIUS for handling specific types of requests

**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 14**

Which two methods can be used to gather a list of installed applications and application details from a host? (Choose two.)

- A. Agent technology
- B. Portal page on-boarding options
- C. MDM integration
- D. Application layer traffic inspection

**Answer:** AC

**Explanation:**

To gather a list of installed applications and application details from a host, two methods can be used:

? Agent technology: FortiNAC uses agent technology to collect all installed applications on an endpoint.

? Integration with MDMs (Mobile Device Management systems): MDMs that support application gathering can be integrated with FortiNAC to collect application information.

References

? FortiNAC 7.2 Study Guide, page 302

**NEW QUESTION 18**

When FortiNAC is managing VPN clients connecting through FortiGate. why must the clients run a FortiNAC agent?

- A. To collect user authentication details
- B. To meet the client security profile rule for scanning connecting clients
- C. To collect the client IP address and MAC address
- D. To transparently update the client IP address upon successful authentication

**Answer:** B

**NEW QUESTION 23**

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 25**

Refer to the exhibit.

Add Guest/Contractor Template

Required Fields

Data Fields

Note

Template Name:

Engineer-Contractor

Visitor Type:

Contractor

Role:

Use a unique Role based on this template name

Select Role: Accounting Contractor

Security & Access Value:

Eng-Contractor

Username Format:

Email

Send Email

Send SMS

Password Length:

6

Password Exclusions:

I!@#\$%^&\*()\_~`{|}~<>?~=:[]

Use Mobile-Friendly Exclusions

Reauthentication Period:

(hours)

Authentication Method:

Local

Account Duration:

(hours)

Login Availability:

Always

URL for Acceptable Use Policy (optional)

Resolve URL

IP Address of URL

Portal Version 1 Settings

OK

Cancel

When a contractor account is created using this template, what value will be set in the accounts Rote field?

- A. Accounting Contractor
- B. Eng-Contractor
- C. Engineer-Contractor
- D. Conti actor

Answer: C

NEW QUESTION 30

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 34

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 35

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 39

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 43

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

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

**Answer: ABE**

#### Explanation:

A. Manual Polling: This is when an administrator or network operator initiates a poll manually to gather information or check the status of the network devices. This can be done for immediate troubleshooting or assessment.

\* B. Scheduled Poll Timings: Network management systems often have the capability to schedule regular polls of devices to check their status or monitor their performance. These scheduled polls can be set at regular intervals (such as every few minutes, hours, or daily) depending on the requirements of the network.

\* E. Linkup and Linkdown Traps: SNMP (Simple Network Management Protocol) traps, like Linkup and Linkdown, are automated notifications sent from network devices to a management system. A Linkup trap indicates that a particular interface has become active (up), while a Linkdown trap indicates that an interface has become inactive (down). These traps can trigger Layer 2 polling to ascertain the current status of network interfaces and devices.

#### NEW QUESTION 45

Where do you look to determine which network access policy, if any is being applied to a particular host?

- A. The Policy Details view for the host
- B. The Connections view
- C. The Port Properties view of the hosts port
- D. The Policy Logs view

**Answer: A**

#### Explanation:

To determine which network access policy is applied to a particular host, you should look at the Policy Details window. This window provides information about the types of policies applied (such as Network Access, Authentication, Supplicant, etc.), including the profile name, policy name, configuration name, and any settings that make up the configuration.

FortiNAC p 382: "Under Network Access Settings - Policy Name - Name of the Network Access Policy that currently applies to the host."

#### NEW QUESTION 47

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 48

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 49**

Where are logical network values defined?

- A. In the model configuration view of each infrastructure device
- B. In the port properties view of each port
- C. On the profiled devices view
- D. In the security and access field of each host record

**Answer:** A

**Explanation:**

In FortiNAC, logical networks are an integral part of device management and network segmentation. These logical networks are defined and appear within the model configuration of each infrastructure device that is modeled in the topology tree. The configuration allows for the assignment of unique names and, optionally, descriptions to each logical network, thereby clarifying their purpose or use within the network infrastructure.  
References: FortiNAC 7.2 Study Guide, Logical Networks Security Fabric and Firewall Tags section.

**NEW QUESTION 54**

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 59**

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 60**

View the command and output.

```
>hsIsSlaveActive Host FortiNAC-Secondary  
  
Host fortinac-primary  
  
SQL version 5.6.31,  
  
Slave is active
```

What is the state of database replication?

- A. Secondary to primary synchronization failed.
- B. Primary to secondary synchronization failed.
- C. Secondary to primary synchronization was successful.
- D. Primary to secondary database synchronization was successful.

**Answer:** D

**Explanation:**

The command and output shown in the exhibit indicate that the host FortiNAC-Secondary is referencing FortiNAC-Primary, and it states "Slave is active." In database replication terminology within a high availability setup, the term "Slave is active" typically means that the secondary server (slave) is actively receiving

data from the primary server (master). This implies that the synchronization process from the primary to the secondary database has been successful and is currently active.

References

? FortiNAC 7.2 Study Guide, Security Policies section

#### NEW QUESTION 63

What capability do logical networks provide?

- A. Point of access-base autopopulation of device groups'
- B. Interactive topology view diagrams
- C. Application of different access values from a single access policy
- D. IVLAN -based inventory reporting

**Answer:** C

#### Explanation:

Logical Networks allow you to create fewer Network Access Policies than before. (FortiNAC - What's new in FortiNAC 7.2)

Logical networks in FortiNAC decouple a policy from a specific access value, allowing for the application of different access values from a single access policy.

This is done based on the point of connection, significantly reducing the number of network access policies needed and simplifying network access policy management

#### NEW QUESTION 65

.....



## 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](#)**