

# Fortinet

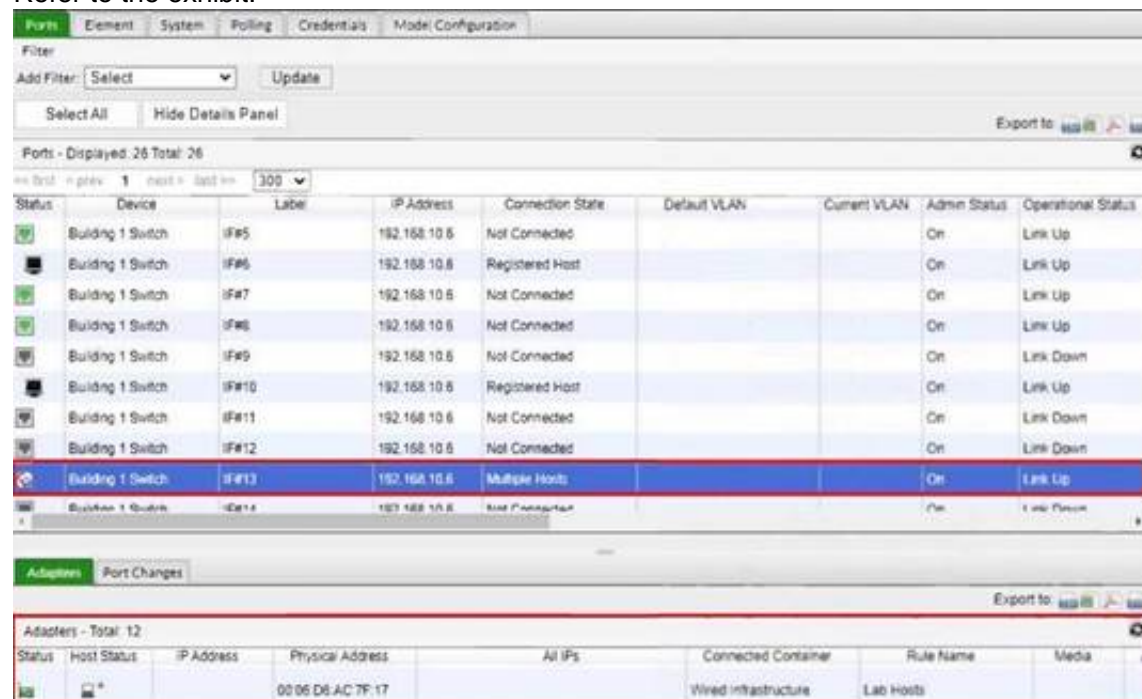
## Exam Questions NSE6\_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2



## NEW QUESTION 1

Refer to the exhibit.



Status	Device	Label	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Status
	Building 1 Switch	IF#5	192.168.10.5	Not Connected			On	Link Up
	Building 1 Switch	IF#6	192.168.10.6	Registered Host			On	Link Up
	Building 1 Switch	IF#7	192.168.10.6	Not Connected			On	Link Up
	Building 1 Switch	IF#8	192.168.10.6	Not Connected			On	Link Up
	Building 1 Switch	IF#9	192.168.10.6	Not Connected			On	Link Down
	Building 1 Switch	IF#10	192.168.10.6	Registered Host			On	Link Up
	Building 1 Switch	IF#11	192.168.10.6	Not Connected			On	Link Down
	Building 1 Switch	IF#12	192.168.10.6	Not Connected			On	Link Down
	Building 1 Switch	IF#13	192.168.10.6	Multiple Hosts			On	Link Up

Status	Host Status	IP Address	Physical Address	All IPs	Connected Container	Rule Name	Media
			00:06:D6:AC:7F:17		Wired Infrastructure	Lab Hosts	

What would happen if the highlighted port with connected hosts was placed in both the Forced Registration and Forced Remediation port groups?

- A. Multiple enforcement groups could not contain the same port.
- B. Only the higher ranked enforcement group would be applied.
- C. Both types of enforcement would be applied.
- D. Enforcement would be applied only to rogue hosts.

**Answer: B**

### Explanation:

In systems like FortiNAC, when a port is designated to be in multiple enforcement groups, it is common for only the higher-priority or higher-ranked group's policies to be applied. This is to prevent conflicting enforcement actions from being attempted on the same port. Although the specific details of the priority or ranking system are not provided in the extracted references, the principle of hierarchical policy enforcement suggests that only the policies of the higher-ranked group would be applied to the port.

References

? FortiNAC documentation would typically outline this behavior in sections discussing port group enforcement or policy application.

## NEW QUESTION 2

Which two things must be done to allow FortiNAC to process incoming syslog messages from an unknown vendor? (Choose two.)

- A. A security event parser must be created for the device.
- B. The device sending the messages must be modeled in the Network Inventory view.
- C. The device must be added as a patch management server.
- D. The device must be added as a log receiver.

**Answer: AB**

### Explanation:

To allow FortiNAC to process incoming syslog messages from an unknown vendor, two steps must be taken:

? Creation of a customized event parser: This enables FortiNAC to parse and integrate syslog messages from any vendor or device, as long as the messages are in CSV, CEF, or Tag/Value format.

? Modeling the device in the Topology view: Any device that sends syslog messages to FortiNAC must be modeled in this view. FortiNAC will not process syslog or trap messages unless the source address belongs to a device modeled in the topology.

References

? FortiNAC 7.2 Study Guide, pages 428 and 399

## NEW QUESTION 3

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 4

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

- A. Configure them only after you configure linkup and linkdown traps.
- B. Configure them on all ports on the switch.

- C. Configure them only on ports set as 802 1g trunks.
- D. Configure them on all ports except uplink ports.

**Answer:** C

**Explanation:**

In general, for network switches supporting MAC notification traps, it's advisable to configure these traps on all ports except uplink ports. Uplink ports are used for connecting to other switches or network infrastructure devices and typically don't need MAC notification traps, which are more relevant for end-device connectivity monitoring.

The study guide specifies that MAC notification traps should not be configured on interfaces that are uplinks. They are the preferred method for learning and updating Layer 2 information and should be used whenever available, but not on uplink interfaces.

**NEW QUESTION 5**

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 6**

While troubleshooting a network connectivity issue, an administrator determines that a device was being automatically provisioned to an incorrect VLAN. Where would the administrator look to determine when and why FortiNAC made the network access change?

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

**Answer:** C

**NEW QUESTION 7**

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 at-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 8**

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 9**

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 10**

View the output.

```
yans.CampusManager INFO :: 2021-07-15 11:37:58:137 :: masterLoaderPID = 10285 nexusLoaderPID = 10372  
yans.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendToNetwork verb Start Processes standbyenabled true inControl true controlServer true  
yans.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendToNetwork() servers = {192.168.10.10, 192.168.10.110, ,  
yans.CampusManager INFO :: 2021-07-15 11:37:58:137 :: skip sending verb to 192.168.10.10.  
yans.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendPacket() 192.168.10.10 verb Start Processes retval = null  
yans.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. Failover from the primary server to the secondary server is in progress.

**Answer:** A

**NEW QUESTION 10**

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 13**

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](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 18**

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 21**

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 23**

.....

## 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](#)**