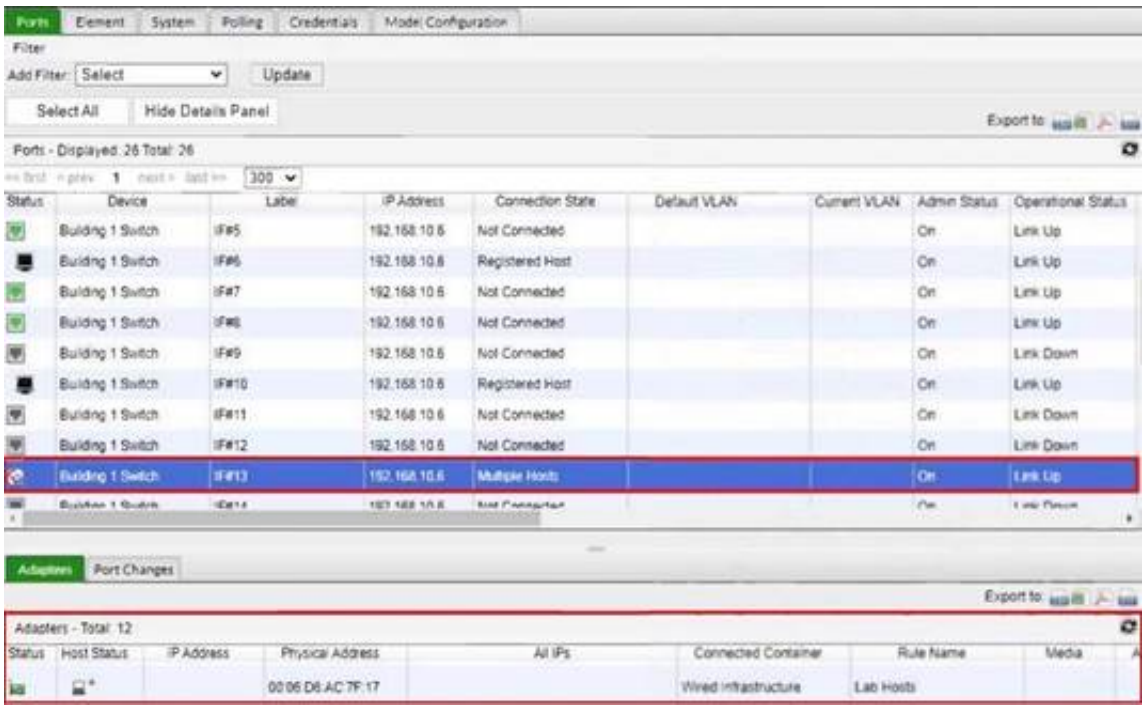
Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

NEW QUESTION 1
Refer to the exhibit.



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 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
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 4
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 5
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 6
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

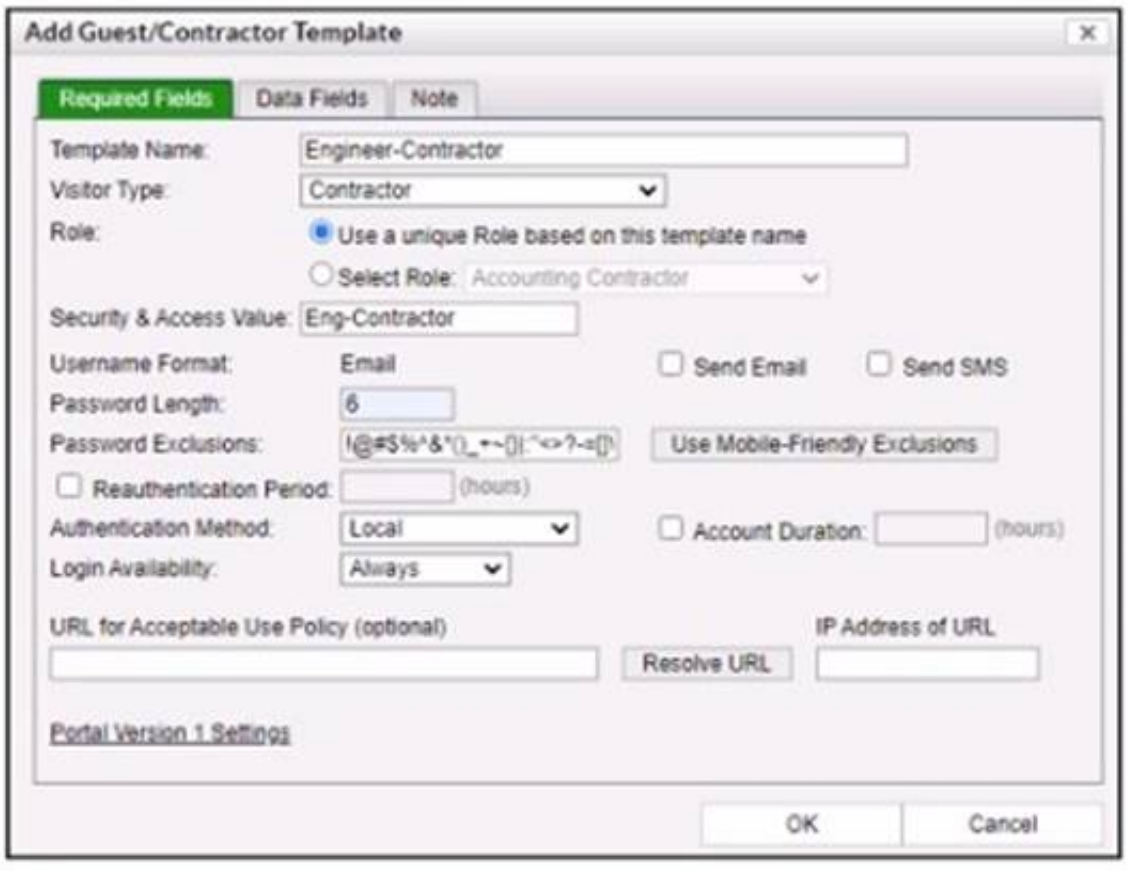
NEW QUESTION 7
What causes a host's state to change to "at risk"?

A. The host has failed an endpoint compliance policy or admin scan.
B. The logged on user is not found in the Active Directory.
C. The host has been administratively disabled.
D. The host is not in the Registered Hosts group.

Answer: A

Explanation:
Failure – Indicates that the host has failed the scan. This option can also be set manually. When the status is set to Failure the host is marked "At Risk" for the selected scan.
Reference: https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/241168/host-health-and-scanning
p. 244 of the Study Guide, "A state of at-risk indicates the host has failed a scan. This could be a compliance scan or an administrative scan."

NEW QUESTION 8
Refer to the exhibit.



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

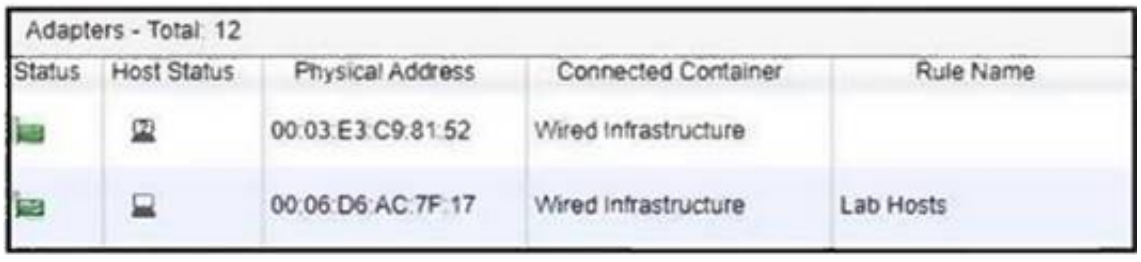
NEW QUESTION 9
Which devices would be evaluated by device profiling rules?

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 10
Refer to the exhibit.



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
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 14
Which two device classification options can register a device automatically and transparently to the end user? (Choose two.)

A. Dissolvable agent
B. DotlxAuto Registration
C. Device importing
D. MDM integration
E. Captive portal

Answer: BD

Explanation:
The FortiNAC 7.2 Study Guide does not explicitly mention Dot1x Auto Registration and MDM integration as the specific device classification options for automatic and transparent registration to the end user. However, based on the general functioning of FortiNAC, Dot1x Auto Registration and MDM integration are typically used for such purposes. The guide discusses automatic device registration in the context of profiling rules

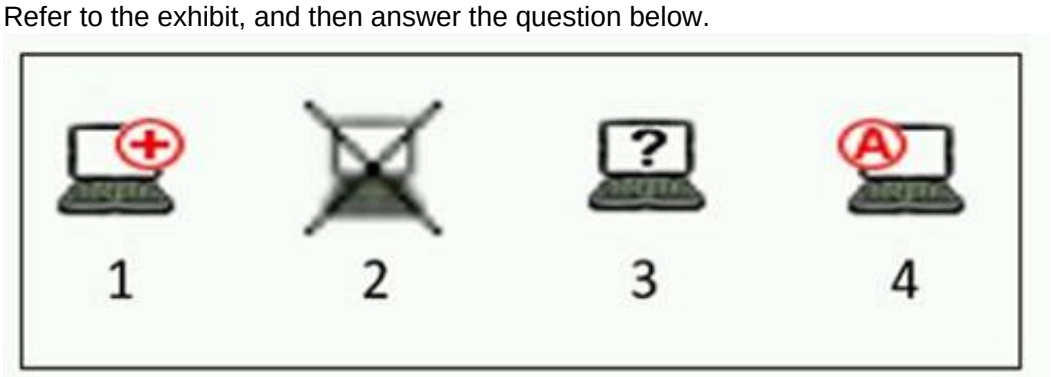
NEW QUESTION 19
What agent is required in order to detect an added USB drive?

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 21
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 23
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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