



Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

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 5

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 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

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 8

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 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 connecting endpoints are evaluated against all enabled device profiling rules?

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

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 10

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 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 17





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 21

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 24

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 28

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 32

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 37

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 38

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 41

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-chnages-made-to-group-policy-objects.html>

NEW QUESTION 44

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 49

.....

Relate Links

100% Pass Your NSE6_FNC-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE6_FNC-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>