Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

NEW QUESTION 1
Which two policy types can be created on a FortiNAC Control Manager? (Choose two.)

A. Authentication
B. Network Access
C. Endpoint Compliance
D. Supplicant EasvConnect

Answer: AB

Explanation:
Network Access policies as a common type of policy in FortiNAC, used to dynamically provision access to connecting endpoints. While Authentication is typically a policy type in network access control systems like FortiNAC

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
Which three are components of a security rule? (Choose three.)

A. Methods
B. Security String
C. Trigger
D. User or host profile
E. Action

Answer: CDE

Explanation:
Components of a security rule in FortiNAC include:
? Trigger: The condition or event that initiates the evaluation of the rule.
? User or Host Profile: A requirement that can be added to a rule to specify the user or host profile that must be matched.
? Action: The activities or responses that FortiNAC performs when the rule is matched.
References
? FortiNAC 7.2 Study Guide, page 419

NEW QUESTION 4
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 5
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 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
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
In an isolation VLAN which three services does FortiNAC supply? (Choose three.)

A. NTP
B. DHCP
C. Web
D. DNS
E. ISMTP

Answer: BCD

Explanation:
In an isolation VLAN, FortiNAC supplies DHCP and DNS services. The guide specifies that FortiNAC has a DHCP scope defined for a particular VLAN and should be the only DHCP server available to hosts on that VLAN. Additionally, hosts on the VLAN would get a DNS server configuration of the FortiNAC IP for that VLAN

NEW QUESTION 8
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 9
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 10
Which system group will force at-risk hosts into the quarantine network, based on point of connection?

A. Physical Address Filtering
B. Forced Quarantine
C. Forced Isolation
D. Forced Remediation

Answer:

D

Explanation:
Forced Quarantine, study guide 7.2 pag 245 and 248

NEW QUESTION 10
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 14
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 17
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 21
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 22
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.

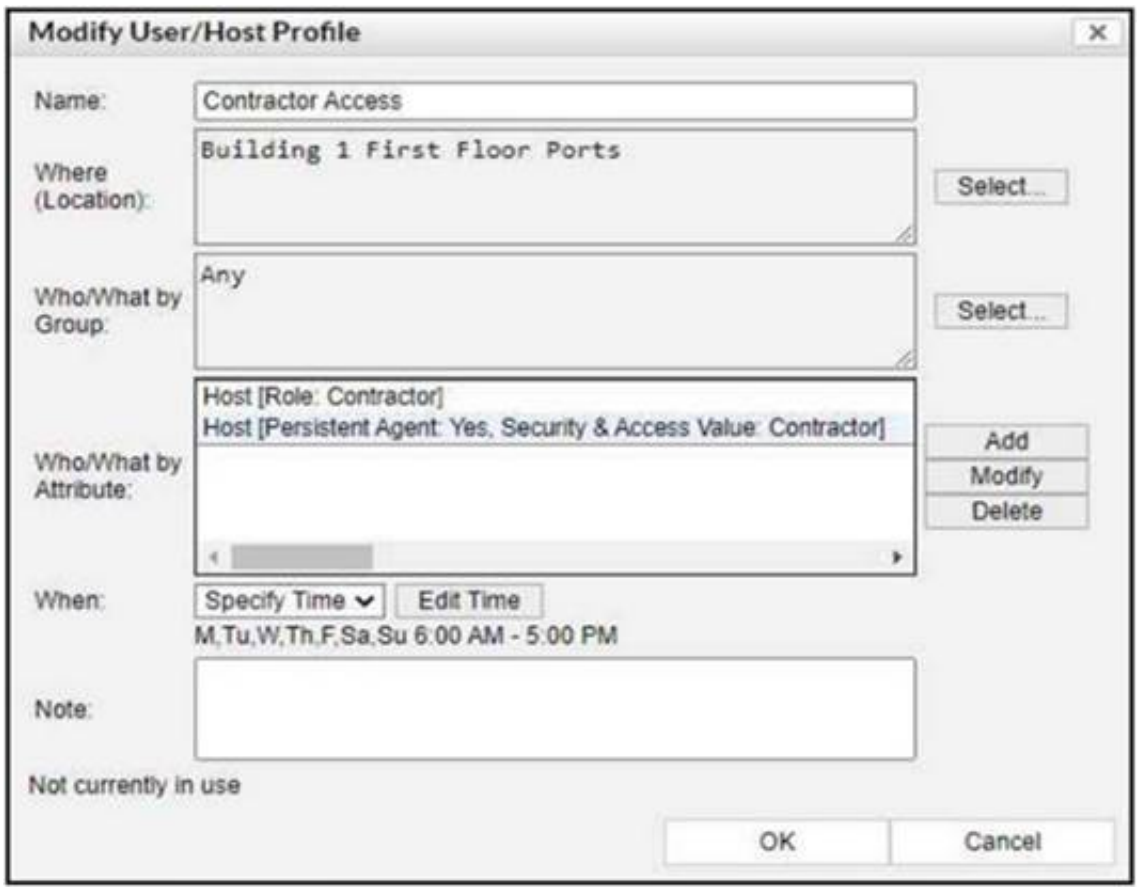
NEW QUESTION 25
With enforcement for network access policies and at-risk hosts enabled, what will happen if a host matches a network access policy and has a state of "at risk"?

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 28
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 32
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 37
.....

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