



Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

NEW QUESTION 1

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 2

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 3

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 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

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 6

Which two are required for endpoint compliance monitors? (Choose two.)

- A. Custom scan
- B. ZTNA agent
- C. Persistent agent
- D. MDM integration

Answer: AC

NEW QUESTION 7

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

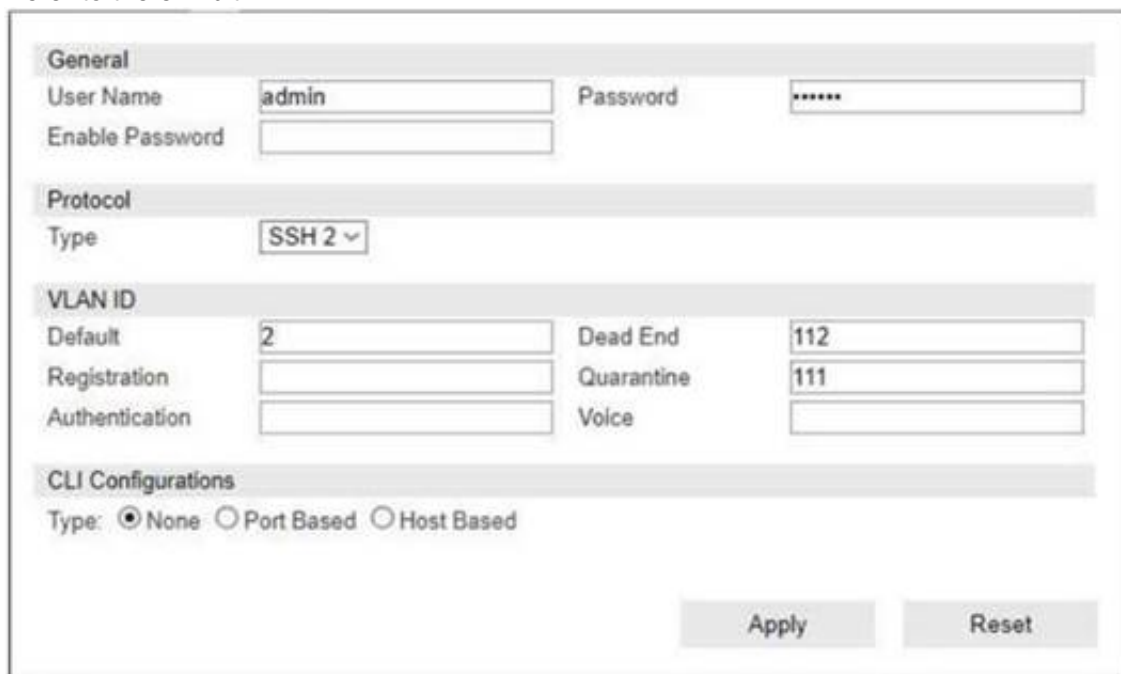
Explanation:

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 8

Refer to the exhibit.



If you are forcing the registration of unknown (rogue) hosts, and an unknown (rogue) host connects to a port on the switch, what occurs?

- A. The host is moved to VLAN 111.
- B. The host is moved to a default isolation VLAN.
- C. No VLAN change is performed.
- D. The host is disabled.

Answer: A

Explanation:

The exhibit shows a configuration panel where VLAN IDs are specified for different states, such as Default, Registration, and Authentication. When forcing the

registration of unknown (rogue) hosts, if an unknown host connects to a port on the switch, the FortiNAC system will move the host to the VLAN designated for Registration. In the exhibit, the VLAN ID for Registration is set to 111, hence the host would be moved to VLAN 111 to undergo the registration process.

NEW QUESTION 9

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 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 10

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 13

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 16

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 20

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 24

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 27

Two FortiNAC devices have been configured in an HA configuration. After five failed heartbeats between the primary device and secondary device, the primary device fail to ping the designated gateway. What happens next?

- A. The primary device continues to operate as the in-control device and changes the status of secondary device to contact lost.
- B. The primary device changes its designation to secondary, and the secondary device changes to primary.
- C. The primary device shuts down NAC processes and changes to a management down status.
- D. The primary device waits 3 minutes and attempts to re-establish the HA heartbeat before attempting a second ping of the gateway.

Answer: C

NEW QUESTION 29

An administrator is configuring FortiNAC to manage FortiGate VPN users. As part of the configuration, the administrator must configure a few FortiGate firewall policies.

What is the purpose of the FortiGate firewall policy that applies to unauthorized VPN clients?

- A. To deny access to only the production DNS server
- B. To allow access to only the FortiNAC VPN interface
- C. To allow access to only the production DNS server
- D. To deny access to only the FortiNAC VPN interface

Answer: B

NEW QUESTION 34

View the output.

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

Answer: A

NEW QUESTION 38

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 42

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 45

.....

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](#)