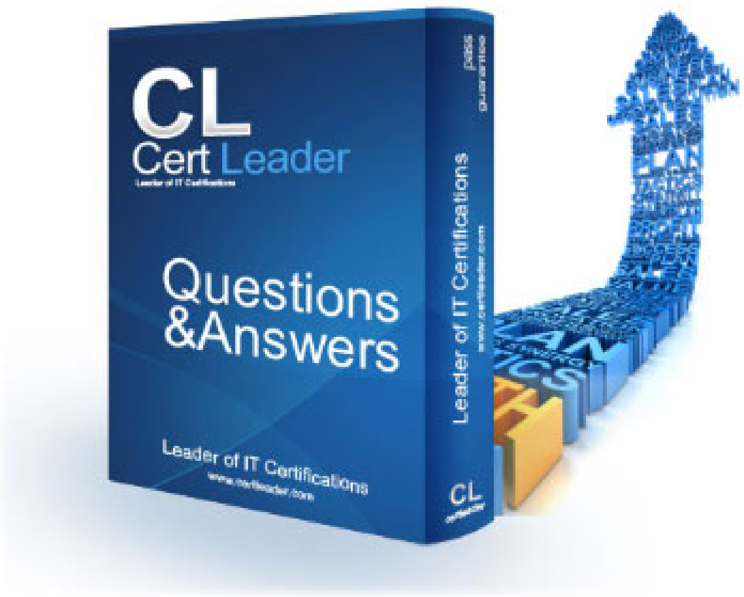
NSE6_FNC-7.2 Dumps

Fortinet NSE 6 - FortiNAC 7.2

https://www.certleader.com/NSE6_FNC-7.2-dumps.html



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 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 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

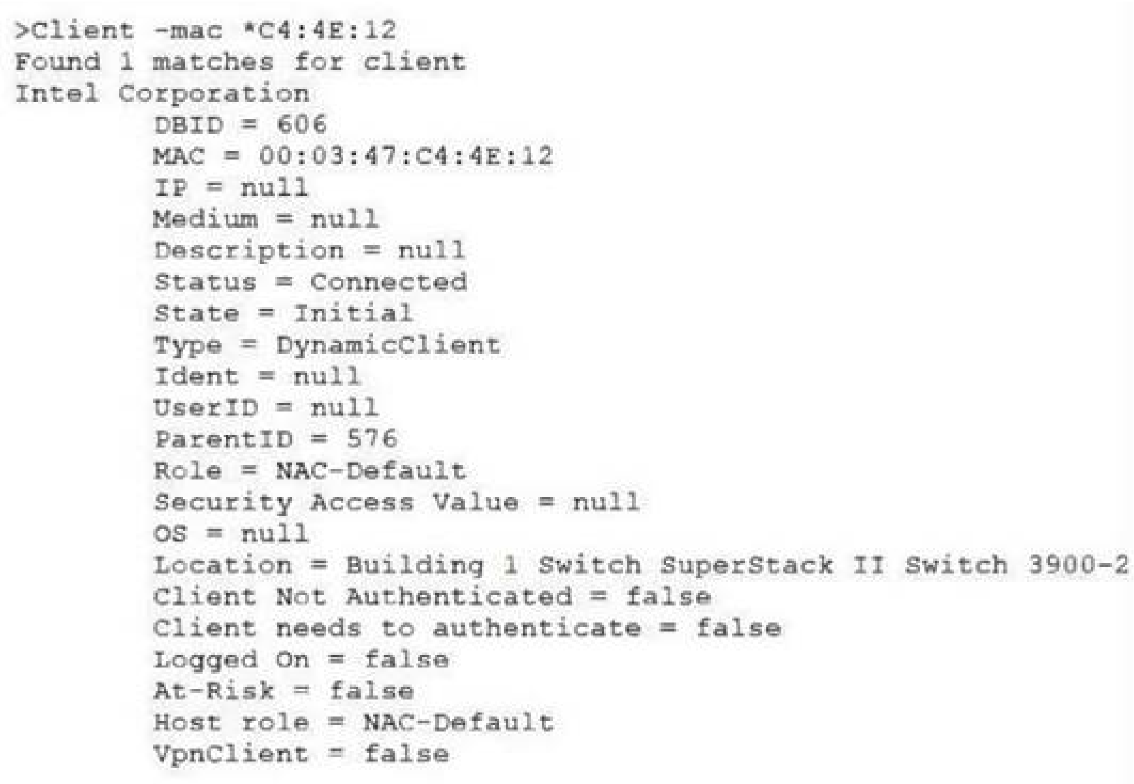
Answer: B

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
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 7
By default, if after a successful Layer 2 poll, more than 20 endpoints are seen connected on a single switch port simultaneously, what happens to the port?

A. The port becomes a threshold uplink
B. The port is disabled
C. The port is added to the Forced Registration group
D. The port is switched into the Dead-End VLAN

Answer: A

Explanation:
If more than 20 endpoints are seen connected on a single switch port simultaneously after a successful Layer 2 poll, the port is designated as an uplink. FortiNAC will ignore all physical addresses learned on an uplink port and will not perform any control operations on it

NEW QUESTION 8
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 9
Where should you configure MAC notification traps on a supported switch?

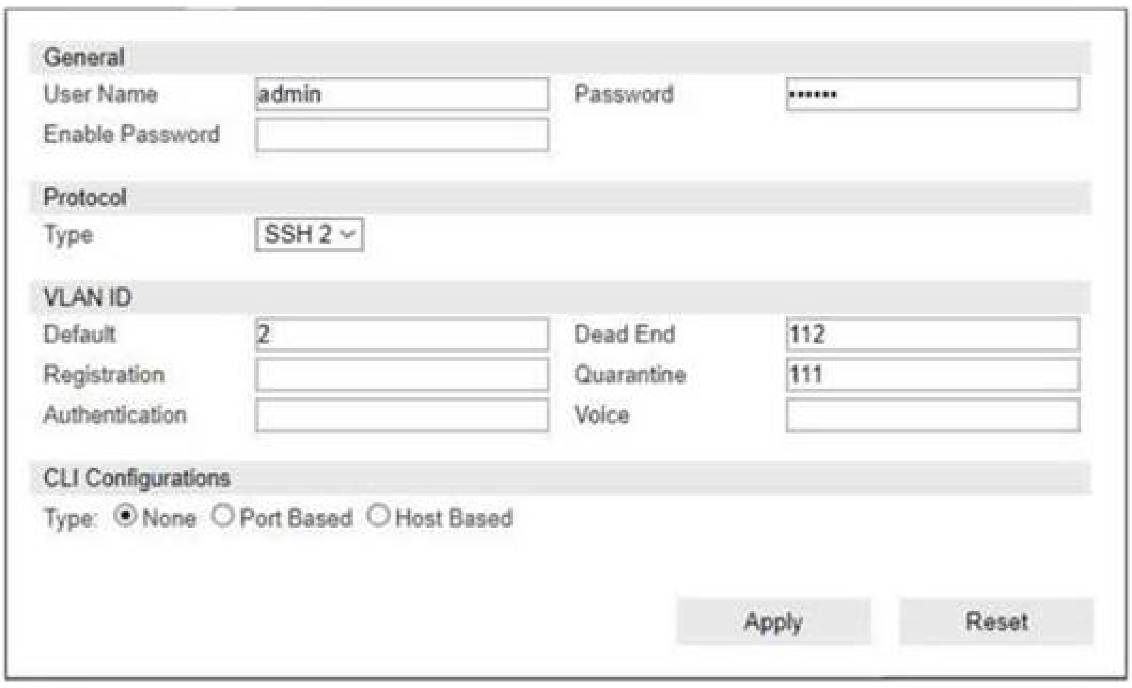
A. Configure them only after you configure linkup and linkdown traps.
B. Configure them on all ports on the switch.
C. Configure them only on ports set as 802 1g trunks.
D. Configure them on all ports except uplink ports.

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 10
Refer to the exhibit.



General

User Name	admin	Password	••••••
Enable Password			

Protocol

Type	SSH 2

VLAN ID

Default	2	Dead End	112
Registration		Quarantine	111
Authentication		Voice	

CLI Configurations

Type: ● None ○ Port Based ○ Host Based

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 10
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 14
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 17
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 22
Which two methods can be used to gather a list of installed applications and application details from a host? (Choose two.)

A. Agent technology
B. Portal page on-boarding options
C. MDM integration
D. Application layer traffic inspection

Answer: AC

Explanation:
To gather a list of installed applications and application details from a host, two methods can be used:
? Agent technology: FortiNAC uses agent technology to collect all installed applications on an endpoint.
? Integration with MDMs (Mobile Device Management systems): MDMs that support application gathering can be integrated with FortiNAC to collect application information.
References
? FortiNAC 7.2 Study Guide, page 302

NEW QUESTION 25
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 30
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 32
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 37
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 38
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 41
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 42
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 43
When FortiNAC passes a firewall tag to FortiGate, what determines the value that is passed?

A. Security rule
B. Device profiling rule
C. RADIUS group attribute
D. Logical network

Answer: B

NEW QUESTION 46
During the on-boarding process through the captive portal, what are two reasons why a host that successfully registered would remain stuck in the Registration VLAN? (Choose two.)

A. The wrong agent is installed.
B. The port default VLAN is the same as the Registration VLAN.
C. Bridging is enabled on the host.
D. There is another unregistered host on the same port.

Answer: BD

NEW QUESTION 47
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 51
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 55
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 58
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 62
......