Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

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.

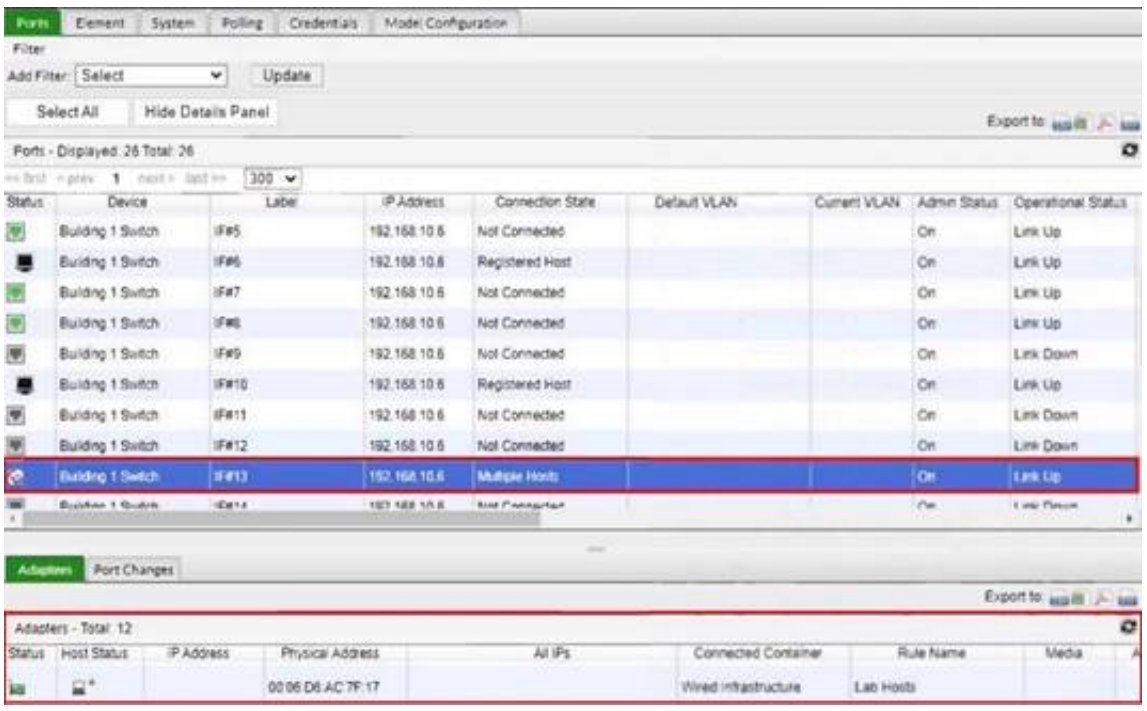
NEW QUESTION 2
Which two policy types can be created on a FortiNAC Control Manager? (Choose two.)

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
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 4
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 5
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

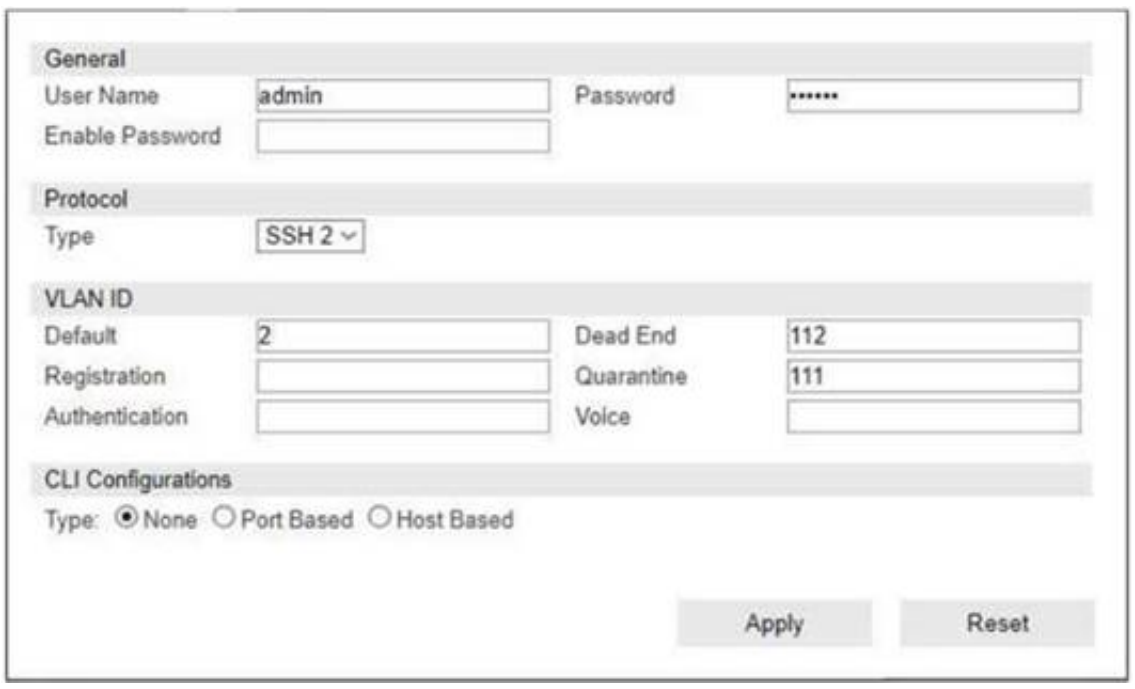
NEW QUESTION 6
Which three are components of a security rule? (Choose three.)

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 7
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 8
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 9
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 10
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 10
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 13
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 17
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 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 al-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 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 26
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 31
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 or 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 34
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

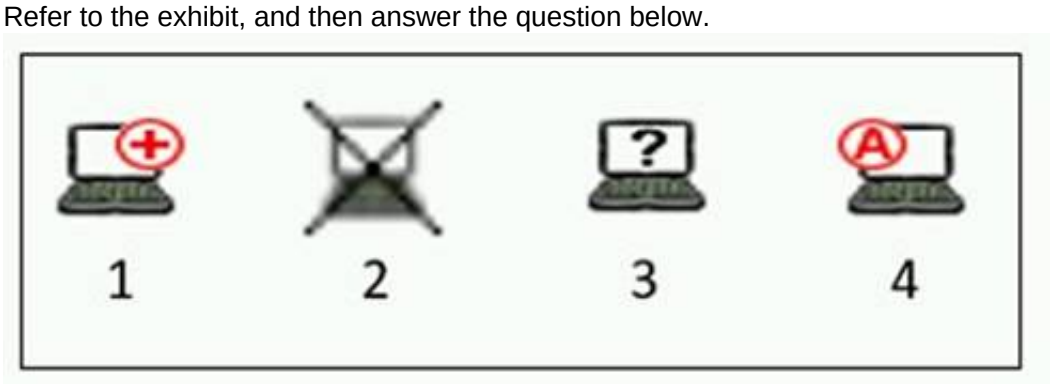
Answer: B

NEW QUESTION 39
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 44
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 48
When you create a user or host profile; which three criteria can you use? (Choose three.)

A. An applied access policy
B. Administrative group membership
C. Location
D. Host or user group memberships
E. Host or user attributes

Answer: CDE

Explanation:
Fortinac-admin-operations, P. 391

NEW QUESTION 52
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 55
.....

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