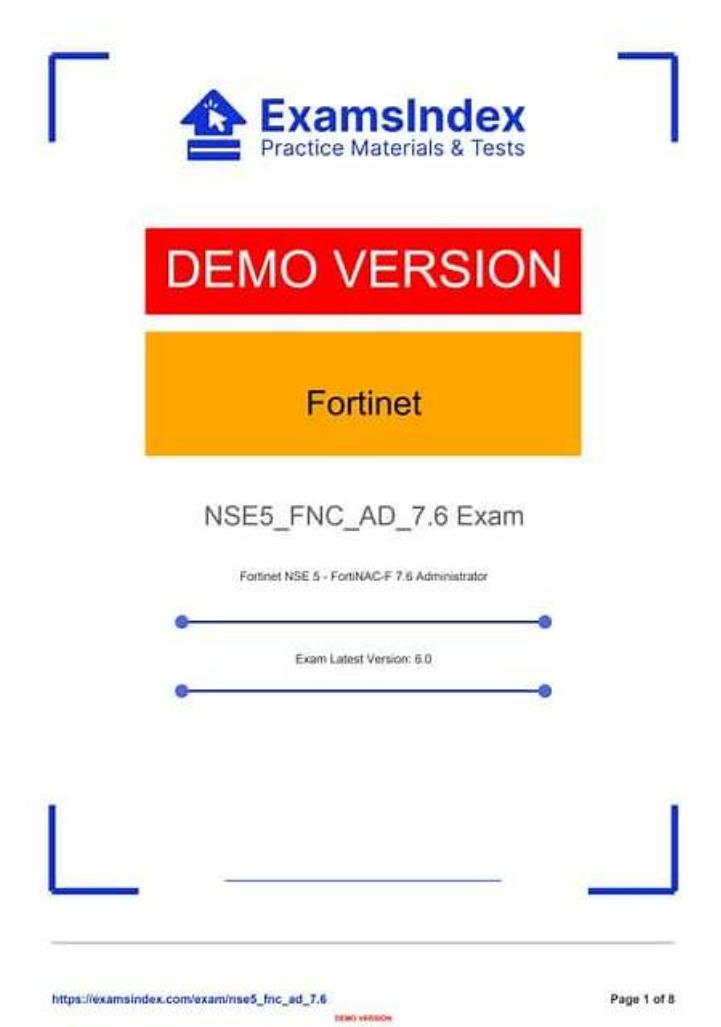
NSE5_FNC_AD_7.6 Reliable Braindumps Free - Valid NSE5_FNC_AD_7.6 Exam Answers



P.S. Free & New NSE5_FNC_AD_7.6 dumps are available on Google Drive shared by ExamTorrent: https://drive.google.com/open?id=1l7zHFya5X1jiZ6VyVWOJs3PHez7F7HfC

You can learn our NSE5_FNC_AD_7.6 test prep in the laptops or your cellphone and study easily and pleasantly as we have different types, or you can print our PDF version to prepare your exam which can be printed into papers and is convenient to make notes. Studying our NSE5_FNC_AD_7.6 exam preparation doesn't take you much time and if you stick to learning you will finally pass the exam successfully. Believe us because the NSE5_FNC_AD_7.6 Test Prep are the most useful and efficient, and the NSE5_FNC_AD_7.6 exam preparation will make you master the important information and the focus to pass the NSE5_FNC_AD_7.6 exam.

Fortinet NSE5_FNC_AD_7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Integration: This domain addresses connecting FortiNAC-F with other systems using Syslog and SNMP traps, managing multiple instances through FortiNAC-F Manager, and integrating Mobile Device Management for extending access control to mobile devices.

Topic 2	• Deployment and Provisioning: This domain focuses on configuring security automation for automatic event responses, implementing access control policies, setting up high availability for system redundancy, and creating security policies to enforce network security requirements.
Topic 3	• Network Visibility and Monitoring: This domain covers managing guest and contractor access, utilizing logging options for tracking network events, configuring device profiling for automatic device identification and classification, and troubleshooting network device connection issues.
Topic 4	• Concepts and Initial Configuration: This domain covers organizing infrastructure devices within FortiNAC-F and understanding isolation networks for quarantining non-compliant devices. It includes using the configuration wizard for initial system setup and deployment.

Valid Fortinet NSE5_FNC_AD_7.6 Exam Answers, Reliable NSE5_FNC_AD_7.6 Guide Files

Our company abides by the industry norm all the time. By virtue of the help from professional experts, who are conversant with the regular exam questions of our latest real dumps. The Fortinet NSE 5 - FortiNAC-F 7.6 Administrator exam dumps have summarized some types of questions in the qualification examination, so that users will not be confused when they take part in the exam, to have no emphatic answers. It can be said that the template of these questions can be completely applied. The user only needs to write out the routine and step points of the NSE5_FNC_AD_7.6 test material, so that we can get good results in the exams.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q24-Q29):

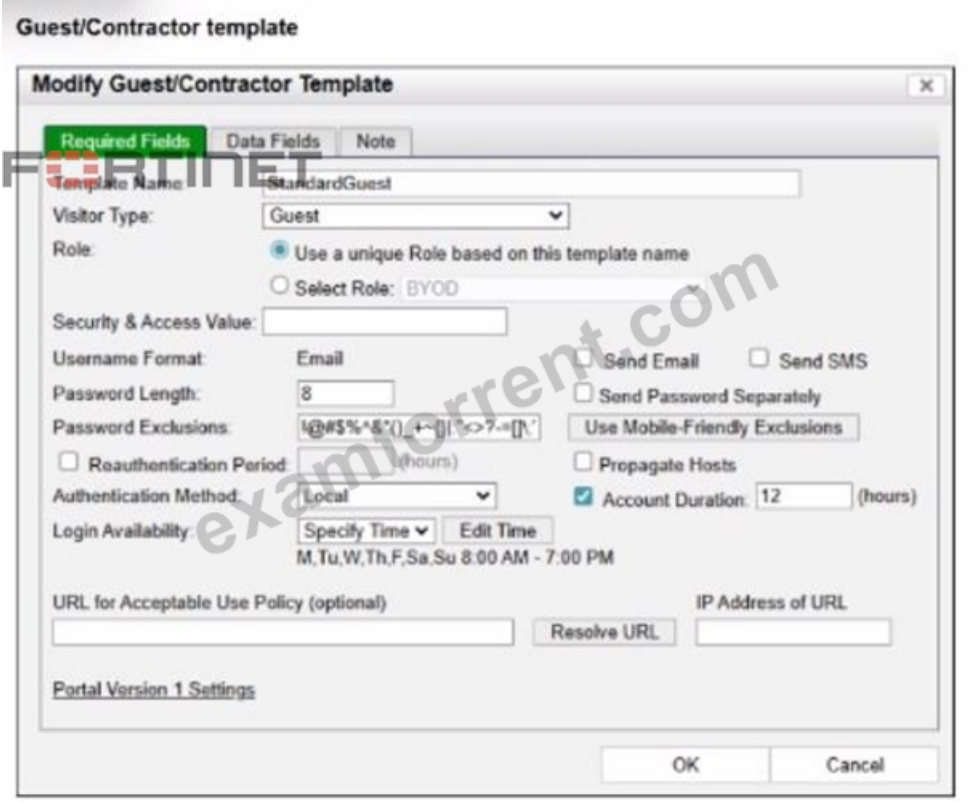
NEW QUESTION # 24
An administrator wants FortiNAC-F to return a group of user-defined RADIUS attributes in RADIUS responses.
Which condition must be true to achieve this?

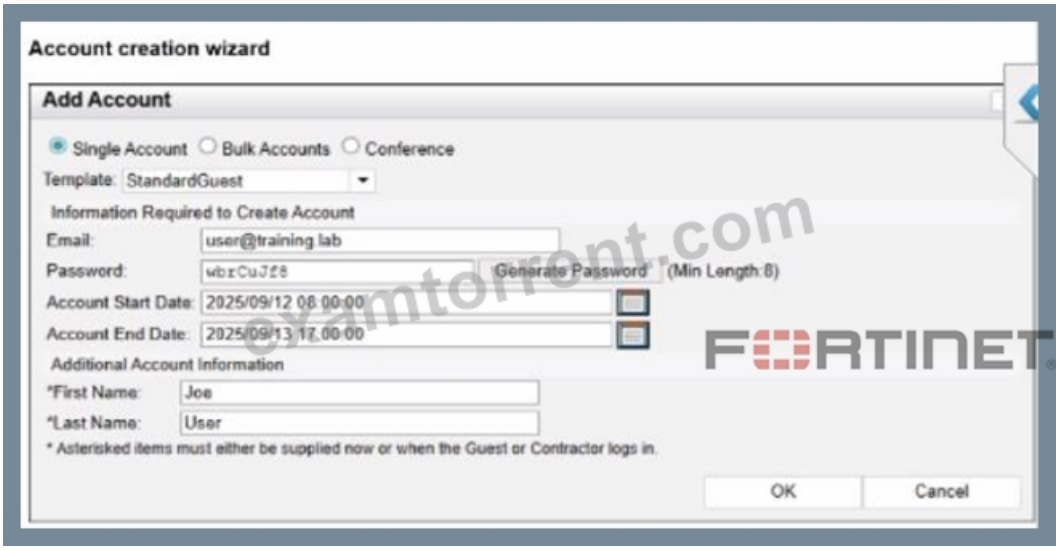
- A. Inbound RADIUS requests must contain the Calling-Station-ID attribute.
- B. RADIUS accounting must be enabled on the FortiNAC-F RADIUS server configuration.
- C. The requesting device must support RFC 5176.
- D. The device models in the inventory view must be configured for proxy-based authentication.

Answer: A

Explanation:
In FortiNAC-F, the RADIUS Attribute Groups feature allows administrators to return customized RADIUS attributes (such as specific VLAN IDs, filter IDs, or vendor-specific attributes) in an Access-Accept packet sent back to a network device. This is particularly useful for supporting "Generic RADIUS" devices that are not natively supported but can be managed using standard AVPairs.
According to the FortiNAC-F Generic RADIUS Wired Cookbook and the RADIUS Attribute Groups section of the Administration Guide, there is one critical prerequisite for this feature to function: the inbound RADIUS request must contain the Calling-Station-ID attribute. The Calling-Station-ID typically contains the MAC address of the connecting endpoint. Because FortiNAC-F is a host-centric system, it uses the MAC address as the unique identifier to look up the host record, evaluate the associated Network Access Policy, and determine which Logical Network (and thus which Attribute Group) should be applied. If the incoming request lacks this attribute, FortiNAC-F cannot reliably identify the host and, as a safety mechanism, will not include any user-defined RADIUS attributes in the response. This ensures that unauthorized or unidentifiable devices do not receive privileged access through misapplied attributes.
"Configure a set of attributes that must be included in the RADIUS Access-Accept packet returned by FortiNAC... Requirement: Inbound RADIUS request must contain Calling-Station-Id. Otherwise, FortiNAC will not include the RADIUS attributes. This attribute is used to identify the host and its current state within the FortiNAC database." - FortiNAC-F 7.6.0 Generic RADIUS Wired Cookbook: Configure RADIUS Attribute Groups.

NEW QUESTION # 25
Refer to the exhibits.





Based on the given configurations and settings, on which date and time would a guest account created at 8:00 AM on 2025/09/12 expire?

- A. 2025/09/13 at 17:00:00
- B. 2025/09/12 at 17:00:00
- C. 2025/09/12 at 8:00 PM
- D. 2025/09/12 at 7:00 PM

Answer: A

Explanation:
Questio ns no: 22
Verified Answe r: D
Comprehensive and Detailed 250 to 300 words each Explanation with Exact Matched Extract from FortiNAC-F Administrator library and documentation for current versions (including F 7.2, 7.4, and 7.6) documents:
In FortiNAC-F, the expiration of a guest or contractor account is determined by the configuration settings within the Account Creation Wizard and the associated Guest/Contractor Template. While a template can define a default "Account Duration" (as seen

in the 12-hour setting in the second exhibit), the Account Creation Wizard allows an administrator to manually specify or override the start and end parameters for a specific user session.
According to the FortiNAC-F Administration Guide regarding guest management, the Account End Date field in the creation wizard is the definitive timestamp for when the account object will be disabled or deleted from the system. In the provided exhibit (Account Creation Wizard), the administrator has explicitly set the Account Start Date to 2025/09/12 08:00:00 and the Account End Date to 2025/09/13 17:00:00.
Even though the template indicates an "Account Duration" of 12 hours, this value typically serves as a pre-populated default. When a manual date and time are entered into the wizard, those specific values take precedence for that individual account. The account will remain active and valid until 5:00 PM (17:00:00) on the following day, 2025/09/13. It is also important to note the "Login Availability" from the template (8:00 AM - 7:00 PM); while the account exists until the 13th at 17:00:00, the user would only be able to authenticate during the active hours defined by the login schedule on both days.
"When creating an account, the administrator can select a template to provide default settings. However, specific values such as the Account End Date can be modified within the Account Creation Wizard. The date and time specified in the 'Account End Date' field determines the absolute expiration of the account. Once this time is reached, the account is moved to an expired state and the user's network access is revoked." - FortiNAC-F Administration Guide: Guest and Contractor Account Management.

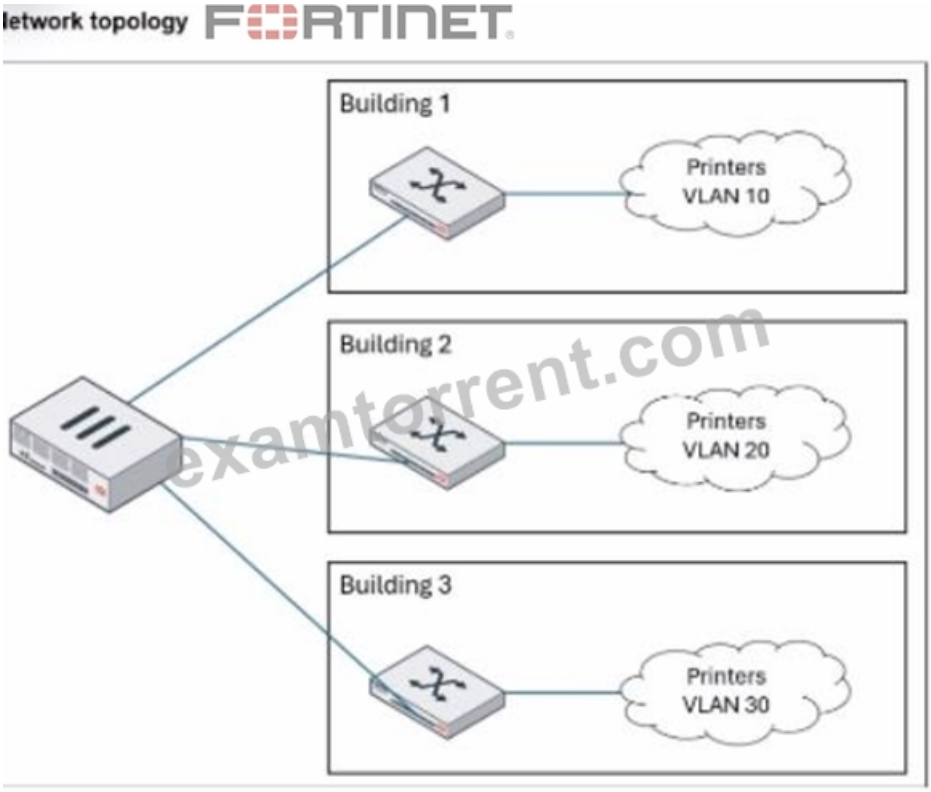
NEW QUESTION # 26
When creating a device profiling rule, what are two advantages of registering the device in the host view? (Choose two.)

- A. The devices can be managed as a generic SNMP device.
- B. The devices can be polled for connection status.
- C. The devices can be associated with a user.
- D. The devices will have connection logs.

Answer: C,D

Explanation:
In FortiNAC-F, the Device Profiler is a rule-based engine that evaluates unknown "rogue" devices and classifies them based on fingerprints and behavior. When a profiling rule matches a device, the administrator can configure the rule to automatically register that device. The registration process can place the device record in two primary locations: the Topology View (as a device) or the Host View (as a registered host).
According to the FortiNAC-F Administration Guide, registering a device in the Host View provides significant advantages for identity management and historical tracking. First, the devices can be associated with a user (C). In the FortiNAC database architecture, the Host View is the primary repository for endpoint identity; placing a profiled device here allows the system to link that hardware (MAC address) to a specific user account, whether that user is an employee, guest, or a system-level "owner". This association is essential for Role-Based Access Control (RBAC) and for tracking accountability across the network fabric.
Second, devices registered in the Host View will have connection logs (B). FortiNAC-F maintains a detailed operational history for all host records, including every instance of the device connecting to or disconnecting from a port, its IP address assignments, and the specific policies applied during each session. These logs are invaluable for troubleshooting connectivity issues and for security forensic audits, as they provide a clear timeline of the device's lifecycle on the network. In contrast, devices managed only in the Topology View are typically treated as infrastructure components where the focus is on device availability rather than individual session history.
"Devices that are registered and associated with a user are placed in the Host View and removed from the Profiled Devices window... Placing a device in the Host View allows for the tracking of connection history and the association of the device with a specific identity or user record within the FortiNAC database." - FortiNAC-F Administration Guide: Device Profiler How it Works.

NEW QUESTION # 27
Refer to the exhibit.



An administrator wants to use FortiNAC-F to automatically provision printers throughout their organization. Each building uses its own local VLAN for printers.
Which FortiNAC-F feature would allow this to be accomplished with a single network access policy?

- A. Dynamic host groups
- B. Device profiling rules
- C. Preferred VLAN designations
- D. Logical networks

Answer: D

Explanation:
The FortiNAC-F Logical Network feature is specifically designed to provide an abstraction layer between high-level security policies and the underlying physical network infrastructure. In large-scale deployments where different physical locations (like Building 1, 2, and 3 in the exhibit) use different local VLAN IDs for the same type of device (e.g., VLAN 10, 20, and 30 for printers), managing separate policies for each building would create significant administrative overhead.
By using a Logical Network, an administrator can create a single entity-for example, a logical network named "Printers"-and use it as the "Access Value" in a single Network Access Policy. The mapping of this logical label to a specific physical VLAN occurs at the Model Configuration level for each network device. When a printer connects to a switch in Building 1, FortiNAC-F evaluates the policy, identifies that the printer should be in the "Printers" logical network, and checks the Model Configuration for that specific switch to see which VLAN ID is mapped to that label (VLAN 10). If the same printer moves to Building 3, the same single policy applies, but FortiNAC-F provisions it to VLAN 30 based on the local mapping for that building's switch.
This architectural approach ensures that policies remain consistent and easy to manage regardless of the complexity or variations in the local network topology.
"Logical Networks provide a way to define a network access requirement once and apply it across many different network devices that may use different VLAN IDs for that access... Each managed device can use different VLAN IDs for the same Logical Network label. You can define the Logical Networks based on requirements and then associate the network to a VLAN ID when the managed device is configured in the Model Configuration." - FortiNAC-F IoT Deployment Guide: Define the Logical Networks.

NEW QUESTION # 28
While discovering network infrastructure devices, a switch appears in the inventory topology with a question mark (?) on the icon.
What would cause this?

- A. The SNMP ObjectID is not recognized by FortiNAC-F.
- B. SNMP is not enabled on the switch.

- C. The wrong SNMP community string was entered during discovery.
- D. A read-only SNMP community siring was used.

Answer: A

Explanation:
In FortiNAC-F, the Inventory topology uses specific icons to represent the status and model of discovered network infrastructure. When a switch or other network device is discovered via SNMP, FortiNAC-F retrieves its System ObjectID (sysObjectID) to identify the specific make and model. This OID is then compared against the internal database of supported device mappings.
A question mark (?) icon appearing on a discovered switch indicates that while the discovery process successfully communicated with the device (meaning SNMP credentials were correct), the SNMP ObjectID is not recognized or mapped in the current version of FortiNAC-F. This essentially means the device is "unsupported" by the current software out-of-the-box. Because the OID is unknown, FortiNAC-F does not know which CLI or SNMP command set to use for critical functions like L2 polling (host visibility) or VLAN switching (enforcement). To resolve this, an administrator can manually "Set Device Mapping" to a similar existing model or a "Generic SNMP Device" if only basic L3 visibility is required.
"Discovered devices displaying a '?' icon indicate the currently running version does not have a mapping for that device's System OID (device is not supported). Device mappings are used to manage the device by performing functions such as L2/L3 Polling, Reading, and Switching VLANs." - Fortinet Technical Tip: Options for devices unable to be modeled in Inventory.

NEW QUESTION # 29
.....

□NSE5_FNC_AD_7.6 Reliable Test Materials

- keybookmarks.com, bookmarkick.com, alexiakwtr026763.theideasblog.com, hamzaagnc938269.wiki-jp.com, www.stes.tyc.edu.tw, jasonxoax892467.blogcudinti.com, freshbookmarking.com, www.stes.tyc.edu.tw, delilahpkxe734682.59bloggers.com, donnaacrt594646.blogoxo.com, Disposable vapes

P.S. Free 2026 Fortinet NSE5_FNC_AD_7.6 dumps are available on Google Drive shared by ExamTorrent: https://drive.google.com/open?id=1l7zHFya5X1jiZ6VyVWOJs3PHez7F7HfC