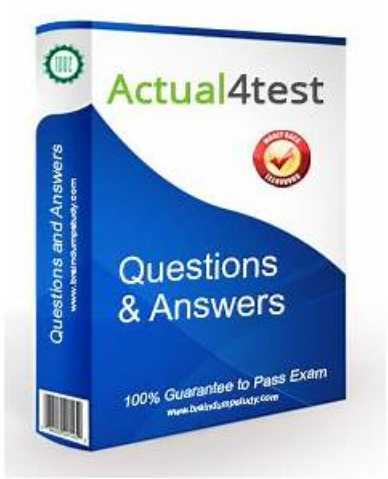
NSE5_FNC_AD_7.6 Real Test Preparation Materials - NSE5_FNC_AD_7.6 Guide Torrent - Itexamguide



This document of NSE5_FNC_AD_7.6 exam questions is very convenient. Furthermore, the Fortinet NSE5_FNC_AD_7.6 PDF questions collection is printable which enables you to study without any smart device. This can be helpful since many applicants prefer off-screen study. All these features of Fortinet NSE5_FNC_AD_7.6 Pdf Format are just to facilitate your preparation for the NSE5_FNC_AD_7.6 examination.

In today's society, many enterprises require their employees to have a professional NSE5_FNC_AD_7.6 certification. It is true that related skills serve as common tools frequently used all over the world, so we can realize that how important an NSE5_FNC_AD_7.6 certification is, also understand the importance of having a good knowledge of it. The rigorous world force us to develop ourselves, thus we can't let the opportunities slip away. Being more suitable for our customers the NSE5_FNC_AD_7.6 Torrent question complied by our company can help you improve your competitiveness in job seeking, and NSE5_FNC_AD_7.6 exam training can help you update with times simultaneously.

>> Simulation NSE5_FNC_AD_7.6 Questions <<

New Launch Fortinet NSE5_FNC_AD_7.6 Exam Questions Are Out: Download And Prepare

We are committed to using Itexamguide Fortinet NSE5_FNC_AD_7.6 Exam Training materials, we can ensure that you pass the exam on your first attempt. If you are ready to take the exam, and then use our Itexamguide Fortinet NSE5_FNC_AD_7.6 exam training materials, we guarantee that you can pass it. If you do not pass the exam, we can give you a refund of the full cost of the materials purchased, or free to send you another product of same value.

Fortinet NSE5_FNC_AD_7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
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	• 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.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q25-Q30):

NEW QUESTION # 25
When creating a user or host profile, which three criteria can you apply? (Choose three.)

- A. Host or user group memberships
- B. An applied access policy
- C. Adapter current VLAN
- D. Location
- E. Host or user attributes

Answer: A,D,E

Explanation:
The User/Host Profile is the primary mechanism in FortiNAC-F for identifying and categorizing endpoints to determine their level of network access. According to the FortiNAC-F Administration Guide, a profile is built using a combination of criteria that define "Who" is connecting, "What" device they are using, and "Where" they are located on the network.
The three main categories of criteria available in the configuration are:
Host or User Attributes (B): This includes specific details such as the host's operating system, the user's role (e.g., Employee, Contractor), or custom attributes assigned to the record.
Host or User Group Memberships (A): Profiles can be configured to match endpoints that are members of specific internal FortiNAC groups or synchronized directory groups (like LDAP or Active Directory groups). This allows for broad policy application based on organizational structure.
Location (E): The "Where" component allows administrators to restrict a profile match to specific physical or logical areas of the network, such as a particular switch, a group of ports, or a specific SSID.
Criteria like an "applied access policy" (D) are the outcome of a profile match rather than a criterion used to define the profile itself. Similarly, the "Adapter current VLAN" (C) is a dynamic state that changes based on enforcement and is not a standard static identifier used for profile matching.
"User/Host Profiles are used to identify the hosts and users to which a policy will apply. Profiles are created by selecting various criteria in the Who/What (Attributes and Groups) and Where (Locations) sections. Attributes can include Host Role, User Role, and OS. Group memberships allow matching based on internal or directory-based groups. Location criteria allow for filtering based on the device or port where the host is connected." - FortiNAC-F Administration Guide: User/Host Profile Configuration.

NEW QUESTION # 26
When FortiNAC-F is managing VPN clients connecting through FortiGate, why must the clients run a FortiNAC-F agent?

- A. To collect the client IP address and MAC address
- B. To collect user authentication details
- C. To validate the endpoint policy compliance
- D. To transparently update The client IP address upon successful authentication

Answer: A

Explanation:
When FortiNAC-F manages VPN clients through a FortiGate, the agent plays a fundamental role in device identification that standard network protocols cannot provide on their own. In a standard VPN connection, the FortiGate establishes a Layer 3 tunnel and assigns a virtual IP address to the client. While the FortiGate sends a syslog message to FortiNAC-F containing the username and this assigned IP address, it typically does not provide the hardware (MAC) address of the remote endpoint's physical or virtual adapter.
FortiNAC-F relies on the MAC address as the primary unique identifier for all host records in its database. Without the MAC address, FortiNAC-F cannot correlate the incoming VPN session with an existing host record to apply specific policies or track the device's history. By running either a Persistent or Dissolvable Agent, the endpoint retrieves its own MAC address and communicates it directly to the FortiNAC-F service interface. This allows the "IP to MAC" mapping to occur. Once FortiNAC-F has both the IP and the MAC, it can successfully identify the device, verify its status, and send the appropriate FSSO tags or group information back to the FortiGate to lift network restrictions.
Furthermore, while the agent can also perform compliance checks (Option D), the architectural requirement for the agent in a managed VPN environment is primarily driven by the need for session data correlation-specifically the collection of the IP and MAC address pairing.
"Session Data Components: * User ID (collected via RADIUS, syslog and API from the FortiGate). * Remote IP address for the remote user connection (collected via syslog and API from the FortiGate and from the FortiNAC agent). * Device IP and MAC address (collected via FortiNAC agent). ... The Agent is used to provide the MAC address of the connecting VPN user (IP to MAC)." - FortiNAC-F FortiGate VPN Integration Guide: How it Works Section.

NEW QUESTION # 27
A healthcare organization is integrating FortiNAC-F with its existing MDM. Communication is failing between the systems.
What could be a probable cause?

- A. SSH communication is failing
- B. SOAP API communication is failing
- C. REST API communication is failing
- D. Security Fabric traffic is failing

Answer: C

Explanation:
The integration between FortiNAC-F and Mobile Device Management (MDM) platforms (such as Microsoft Intune, VMware Workspace ONE, or Jamf) is a critical component for providing visibility into mobile assets that do not connect directly to the managed infrastructure via standard wired or wireless protocols.
According to the FortiNAC-F MDM Integration Guide, the communication between the FortiNAC-F appliance and the MDM server is handled through REST API calls. FortiNAC-F acts as an API client, periodically polling the MDM server to retrieve device metadata, compliance status, and ownership information. If communication is failing, it is most likely because the API credentials (Client ID/Secret) are incorrect, the MDM's API endpoint is unreachable from the FortiNAC-F service port, or the SSL certificate presented by the MDM is not trusted by the FortiNAC-F root store.
While SSH (B) is used for switch CLI management and the Security Fabric (A) uses proprietary protocols for FortiGate synchronization, neither is the primary vehicle for MDM data exchange. SOAP API (D) is an older protocol that has been largely replaced by REST in modern FortiNAC integrations.
"FortiNAC integrates with MDM systems by utilizing REST API communication to query the MDM database for device information. To establish this link, administrators must configure the MDM Service Connector with the appropriate API URL and authentication credentials. If the 'Test Connection' fails, verify that the FortiNAC can reach the MDM provider via the REST API port (usually HTTPS 443)." - FortiNAC-F Administration Guide: MDM Integration and Troubleshooting.

NEW QUESTION # 28
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 identify who added the ports to the groups?

(Selected)

- A. The Admin Auditing view
- B. The Port Changes view
- C. The Event Management view
- D. The Security Events view

Answer: A

Explanation:
In FortiNAC-F, accountability and forensic tracking of configuration changes are managed through the Admin Auditing functionality. When an administrator performs an action that modifies the system state-such as creating a policy, changing a device's status, or adding a switch port to an Enforcement Group-the system generates an audit record. This record is essential for troubleshooting scenarios where unauthorized or accidental configuration changes have occurred, leading to unintended network behavior.
The Admin Auditing view (found under Logs > Admin Auditing) provides a comprehensive log of the "Who, What, and When" for every administrative session. Each entry includes the username of the administrator, the source IP address from which they accessed the FortiNAC-F console, a precise timestamp, and a detailed description of the modification. In the scenario described, where ports have been incorrectly added to enforcement groups, the Admin Auditing view allows a supervisor to filter by the specific "Port" or "Group" object to identify exactly which administrator executed the command.
In contrast, the Event Management view (B) is designed to monitor system and network events, such as RADIUS authentications, host connections, and SNMP trap arrivals. While it tracks system activity, it does not typically log the manual configuration changes performed by admins. The Port Changes view (C) tracks the operational history of a port (such as VLAN assignment changes and host movements) but does not attribute the administrative assignment of the port to a group. Finally, the Security Events view (D) is dedicated to alerts triggered by security rules and external threat feeds.
"Admin Auditing displays a record of all modifications made to the FortiNAC-F system by an administrator. This view includes the administrator's name, the date and time of the change, and a description of the action taken. It is the primary resource for determining which administrative user performed a specific configuration change, such as modifying port group memberships or altering policy settings." - FortiNAC-F Administration Guide: Logging and Auditing Section.

NEW QUESTION # 29
In which three ways would deploying a FortiNAC-F Manager into a large environment consisting of several FortiNAC-F CAs simplify management? (Choose three.)

- A. Global version control
- B. Global visibility
- C. Global authentication security policies
- D. Pooled licenses
- E. Global infrastructure device inventory

Answer: A,B,D

Explanation:
The FortiNAC-F Manager (FortiNAC-M) is designed as a centralized management platform for large-scale distributed environments where multiple FortiNAC-F Control and Application (CA) appliances are deployed across different sites. According to the FortiNAC-F Manager Administration Guide, the deployment of a Manager simplifies administrative overhead in three specific ways:
First, it provides Global Version Control (B). The Manager serves as a central repository for firmware and software updates, allowing administrators to push specific versions to all managed CAs simultaneously, ensuring consistency across the entire fabric.
Second, it enables Pooled Licenses (D). Instead of purchasing and managing individual licenses for every CA, licenses are centralized on the Manager. The Manager then distributes these licenses to the CAs as needed based on their host counts. This "floating" license model optimizes cost and prevents individual sites from running out of capacity while others have excess. Third, it offers Global Visibility (E). The Manager aggregates host and device data from every managed CA into a single console. This "single pane of glass" allows an administrator to search for a specific MAC address or user across the entire global organization without logging into individual servers.
While the Manager can assist with configuration templates, authentication security policies (C) and infrastructure modeling (A) are still predominantly managed at the local CA level to ensure site-specific logic and performance.
"The FortiNAC Manager provides a central management console for multiple FortiNAC-F servers (CAs). Key benefits include: * License Management: Licenses are pooled on the Manager and allocated to managed CAs as needed. * Software Management: Firmware updates can be centrally managed and pushed to all CAs from the Manager. * Centralized Monitoring: Provides a global view of all hosts, adapters, and events across the entire managed environment." - FortiNAC-F Manager Administration Guide:

Overview and Benefits.

NEW QUESTION # 30

......

If you buy our NSE5_FNC_AD_7.6 exam questions, then you will find that Our NSE5_FNC_AD_7.6 actual exam has covered all the knowledge that must be mastered in the exam. You just should take the time to study NSE5_FNC_AD_7.6 preparation materials seriously, no need to refer to other materials, which can fully save your precious time. To keep up with the changes of the exam syllabus, our NSE5_FNC_AD_7.6 Practice Engine are continually updated to ensure that they can serve you continuously.

New NSE5_FNC_AD_7.6 Exam Testking: https://www.itexamguide.com/NSE5_FNC_AD_7.6_braindumps.html