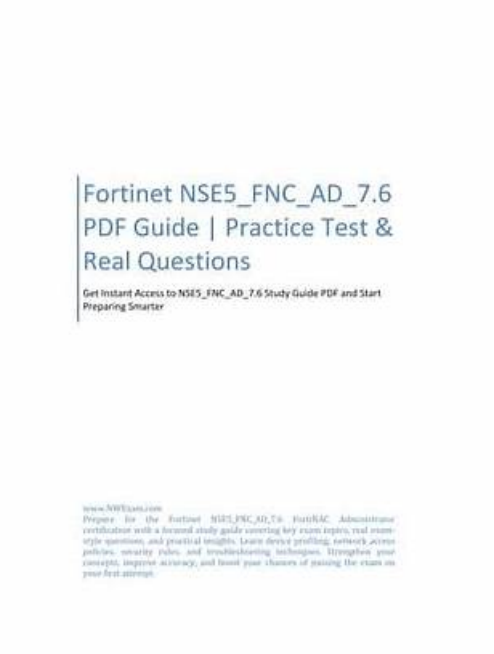
Brain NSE5_FNC_AD_7.6 Exam & Valid NSE5_FNC_AD_7.6 Exam Simulator



However, when asked whether the NSE5_FNC_AD_7.6 latest dumps are reliable, costumers may be confused. For us, we strongly recommend the NSE5_FNC_AD_7.6 exam questions compiled by our company, here goes the reason. On one hand, our NSE5_FNC_AD_7.6 test material owns the best quality. When it comes to the study materials selling in the market, qualities are patchy. But our Fortinet test material has been recognized by multitude of customers, which possess of the top-class quality, can help you pass exam successfully. On the other hand, our NSE5_FNC_AD_7.6 Latest Dumps are designed by the most experienced experts, thus it can not only teach you knowledge, but also show you the method of learning in the most brief and efficient ways.

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	• 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 3	• 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 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.

100% Pass Quiz 2026 Fortinet High Pass-Rate NSE5_FNC_AD_7.6: Brain Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Exam

TestPassKing certification training exam for NSE5_FNC_AD_7.6 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development. TestPassKing NSE5_FNC_AD_7.6 certification training exam material including the examination question and the answer, complete by our senior lecturers and the NSE5_FNC_AD_7.6 product experts, included the current newest NSE5_FNC_AD_7.6 examination questions.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q60-Q65):

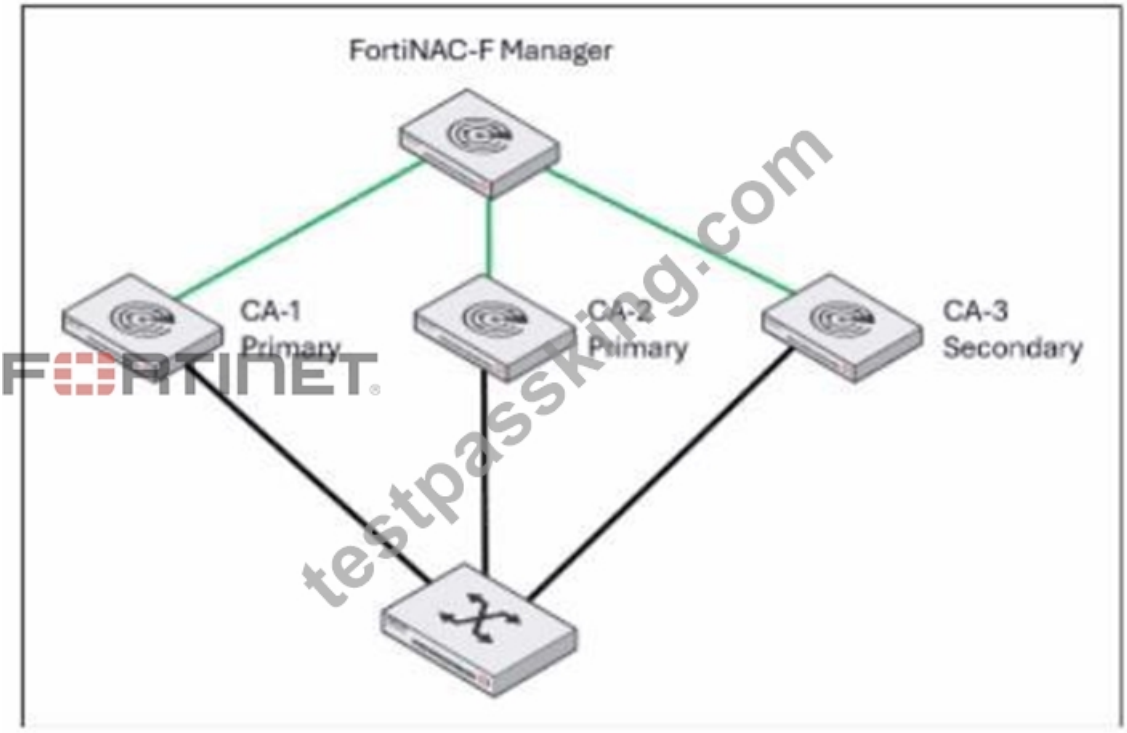
NEW QUESTION # 60
While deploying FortiNAC-F devices in a 1+1 HA configuration, the administrator has chosen to use the shared IP address option. Which condition must be met for this type of deployment?

- A. There is a direct cable link between FortiNAC-F devices.
- B. The primary and secondary administrative interfaces are on the same subnet.
- C. The isolation network type is layer 3.
- D. The isolation network type is Layer 2.

Answer: B

Explanation:
In a 1+1 High Availability (HA) deployment, FortiNAC-F supports two primary methods for management access: individual IP addresses or a Shared IP Address (also known as a Virtual IP or VIP). The Shared IP option is part of a Layer 2 HA design, which simplifies administration by providing a single URL or IP that always points to whichever appliance is currently in the "Active" or "In Control" state.
For a Shared IP configuration to function correctly, the Primary and Secondary administrative interfaces (port1) must be on the same subnet. This requirement exists because the Shared IP is a logical address that is dynamically assigned to the physical interface of the active unit. Since only one unit can own the IP at a time, both units must reside on the same broadcast domain (Layer 2) to ensure that ARP requests for the Shared IP are correctly answered and that the gateway remains reachable regardless of which unit is active. If the appliances were on different subnets (a Layer 3 HA design), a shared IP could not be used because it cannot "float" across different network segments; instead, administrators would need to manage each unit via its unique physical IP or use a FortiNAC Manager.
"For L2 HA configurations, click the Use Shared IP Address checkbox and enter the Shared IP Address information... If your Primary and Secondary Servers are not in the same subnet, do not use a shared IP address. The shared IP address moves between appliances during a failover and recovery and requires both units to reside on the same network." - FortiNAC-F High Availability Reference Manual: Shared IP Configuration.

NEW QUESTION # 61
Refer to the exhibit.
A FortiNAC-F N+1 HA configuration is shown.



What will occur if CA-2 fails?

- A. CA-3 will be promoted to a primary and share management responsibilities with CA-1.
- B. CA-1 and CA-3 will operate as a 1+1 HA cluster with CA-3 acting as a hot standby.
- C. CA-3 will continue to operate as a secondary in an N+1 HA configuration.
- D. CA-3 will be promoted to a primary and FortiNAC-F manager will load balance between CA-1 and CA-3.

Answer: C

Explanation:
In anN+1 High Availability (HA)configuration, a single secondary Control and Application (CA) server provides backup for multiple primary CA servers. The FortiNAC-F Manager (FortiNAC-M) acts as the centralized orchestrator for this cluster, monitoring the health of all participating nodes.
According to theFortiNAC-F 7.6.0 N+1 Failover Reference Manual, when a primary CA (such asCA-2in the exhibit) fails, the secondary CA (CA-3) is automatically promoted by the Manager to take over the specific workload and database functions of that failed primary. Crucially, the documentation specifies that even after this promotion, the system architecture maintains its N+1 logic. The secondary CA effectively " assumes the identity " of the failed primary while continuing to operate within the N+1 framework established by the Manager.
It doesnotmerge with CA-1 to form a traditional 1+1 active/passive cluster (A), nor does it engage in load balancing (D), as FortiNAC-F HA is designed for redundancy and failover rather than active traffic distribution. Furthermore, CA-3 does not " share " management with CA-1 (C); it independently handles the tasks originally assigned to CA-2. Throughout this failover state, the Manager continues to oversee the group, and CA-3 remains the designated secondary unit currently acting in a primary capacity for the downed node until CA-2 is restored.
" In an N+1 Failover Group, theSecondary CAis designed to take over the functionality ofany single failed primary componentwithin the group. The FortiNAC Manager monitors the primaries and initiates the failover to the secondary... Once failover occurs, the secondary continues to operate as the backup unit for the failed primary while remaining part of the managed N+1 HA configuration. " -FortiNAC-F 7.6.0 N+1 Failover Reference Manual: Failover Behavior Section.

NEW QUESTION # 62
How can an administrator configure FortiNAC-F to normalize incoming syslog event levels across vendors?

- A. Configure the vendor OUI settings.
- B. Configure severity mappings.
- C. Configure event to alarm mappings.
- D. Configure the security rule settings.

Answer: B

Explanation:
FortiNAC-F serves as a central manager for security events originating from a diverse ecosystem of third-party security appliances, such as FortiGate, Check Point, and Cisco. Each vendor utilizes its own internal scale for severity levels within syslog messages (e.g., Check Point uses a 1-5 scale, while others may use 0-7). To provide a consistent response regardless of the source, FortiNAC-F uses Severity Mappings to normalize these incoming values.
According to the FortiNAC-F Administration Guide, severity mappings allow the administrator to translate vendor-specific threat levels into standardized FortiNAC Security Levels (such as High, Medium, or Low Violation). When a syslog message arrives, the parser extracts the vendor's severity code, and the system immediately references the Security Event Severity Level Mappings table to determine how that event should be categorized internally. This normalization is vital because it allows a single Security Alarm to be configured to respond to any "High Violation" event, whether it was reported as a "Critical" by one vendor or a "Level 5" by another. Without these mappings, the administrator would have to create separate, redundant security rules for every vendor to account for their different naming conventions and numerical scales.
"Each vendor defines its own severity levels for syslog messages. The following table shows the equivalent FortiNAC security level... To normalize these events, configure the Severity Level Mappings found in the device integration guides. This allows FortiNAC to generate a consistent security event that can then trigger an alarm regardless of the reporting vendor's specific terminology." - FortiNAC-F Administration Guide: Vendor Severity Levels and Syslog Management.

NEW QUESTION # 63
An administrator wants to use FortiNAC-F to prevent internal engineers from accessing specific websites as defined in web filter categories on FortiGate. In addition to a security trigger and associated action, which configuration must also be defined on FortiNAC-F?

- A. A user/host profile
- B. A profiling method
- C. A compliance policy
- D. A firewall policy

Answer: A

Explanation:
The correct answer is C . FortiNAC-F security automation does not rely only on a trigger and action. After a security alert is received and the security trigger is satisfied, FortiNAC-F can also evaluate an associated user
/host profile before generating the security alarm and executing the action. The study guide explains that user
/host profiles are the same profiles used by security policies and are used in security rules to leverage "who, what, where, and when" visibility information. This is exactly what the question requires: the rule must apply specifically to internal engineers , not every user who triggers the FortiGate web-filter category event.
A compliance policy is wrong because compliance policies evaluate endpoint health, posture, scans, or agent results; they do not scope FortiGate web-filter-triggered automation to a user population. A firewall policy is configured on FortiGate, not as the FortiNAC-F-side matching condition in the security rule. A profiling method is also wrong because profiling methods classify rogue or unknown devices, such as printers, cameras, or phones; they do not identify internal engineers for a security automation workflow. The user/host profile is the correct FortiNAC-F object because it lets the same FortiGate security trigger produce a different response depending on the matched user, host, group, location, or ownership context.

NEW QUESTION # 64
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 Security Events view
- B. The Port Changes view
- C. The Event Management view
- D. The Admin Auditing view

Answer: D

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 # 65
.....

Since different people have different preferences, we have prepared three kinds of different versions of our NSE5_FNC_AD_7.6 practice test: PDF, Online App and software. Last but not least, our customers can accumulate exam experience as well as improving their exam skills in the mock exam. And your success is 100 guaranteed for our pass rate of NSE5_FNC_AD_7.6 Exam Questions is as high as 99% to 100%. And We have put substantial amount of money and effort into upgrading the quality of our NSE5_FNC_AD_7.6 Exam Preparation materials.

NSE5_FNC_AD_7.6 Dumps Demo

- scalar.usc.edu, writeablog.net, www.fundable.com, www.callcentersindia.co.in, notefolio.net, blogfreely.net, fortunetelleroracle.com, learn.csisafety.com.au, wibki.com, www.slideshare.net, Disposable vapes