Exam NSE6_FNC_AD-7.6 Lab Questions - Pass Guaranteed NSE6_FNC_AD-7.6 - Fortinet NSE 6 - FortiNAC-F 7.6 Administrator First-grade Valid Study Materials

Many clients worry that after they our NSE6_FNC_AD-7.6 exam simulation they may fail in the test and waste their money and energy. There are no needs to worry about that situation because our study materials boost high passing rate and hit rate and the possibility to fail in the NSE6_FNC_AD-7.6 test is very little. Just consider that our pass rate of the NSE6_FNC_AD-7.6 study guide is high as 98% to 100%, which is unique in the market. And you will get the best pass percentage with our NSE6_FNC_AD-7.6 learning questions.

Fortinet NSE6_FNC_AD-7.6 Exam Syllabus Topics:

Section	Objectives
Topic 1: Concepts and Initial Configuration	- Explain isolation networks and the configuration wizard - Model and organize infrastructure devices
Topic 2: Deployment and Provisioning	- Configure FortiNAC-F security policies - Configure security automation - Configure access control on FortiNAC-F - Configure and monitor high availability (HA)
Topic 3: Integration	- Integrate with third-party devices using Syslog and SNMP traps - Configure mobile device management (MDM) integration - Configure and use FortiNAC-F Manager
Topic 4: Network Visibility and Monitoring	- Use logging options - Manage guests and contractors - Troubleshoot network devices and device status - Configure device profiling

>> Exam NSE6_FNC_AD-7.6 Lab Questions <<

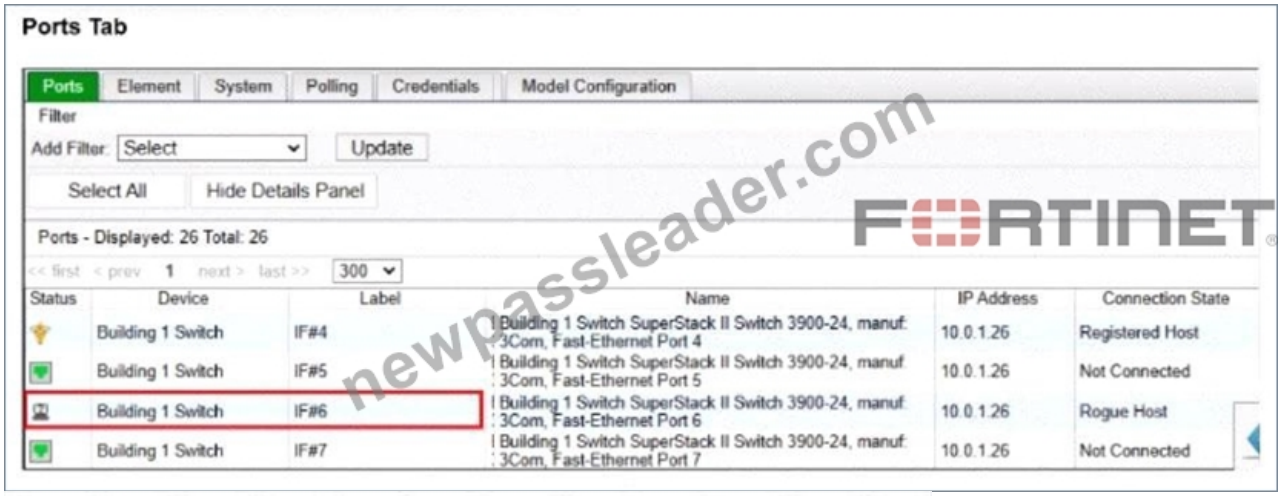
Fortinet NSE6_FNC_AD-7.6 PDF Questions - Accessible On Any Device

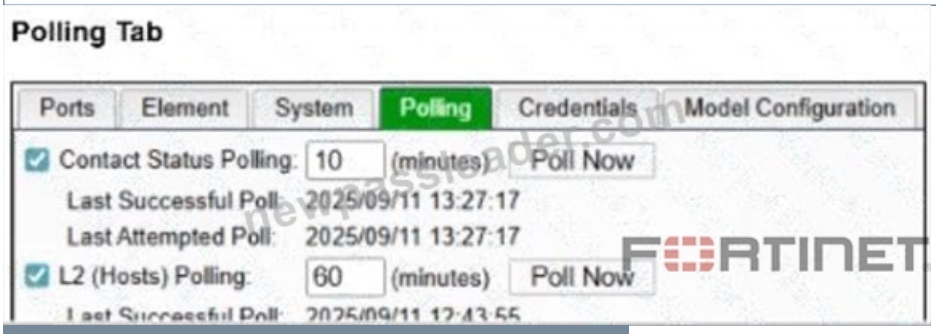
Our NSE6_FNC_AD-7.6 quiz torrent can provide you with a free trial version, thus helping you have a deeper understanding about our NSE6_FNC_AD-7.6 test prep and estimating whether this kind of study material is suitable to you or not before purchasing. With the help of our trial version, you will have a closer understanding about our NSE6_FNC_AD-7.6 exam torrent from different aspects, ranging from choice of three different versions available on our test platform to our after-sales service. Otherwise you may

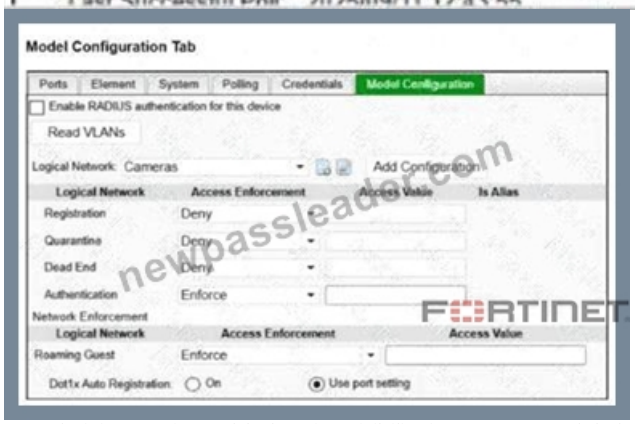
still be skeptical and unintelligible about our NSE6_FNC_AD-7.6 Test Prep. So as you see, we are the corporation with ethical code and willing to build mutual trust between our customers.

Fortinet NSE 6 - FortiNAC-F 7.6 Administrator Sample Questions (Q26-Q31):

NEW QUESTION # 26
Refer to the exhibits.







An administrator is troubleshooting visibility issues on a modeled switch The switch is configured to use link traps and to provision hosts based on network access policies. The administrator is seeing hosts on ports with no hosts connected and not seeing hosts on ports where hosts are known to be connected.
What is the most likely cause?

- A. The switch cannot be contacted by FortiNAC-F
- B. The host has uninstalled the FortiNAC-F agent.
- C. The logical networks are set to deny.
- D. The credentials are incorrect.

Answer: A

Explanation:
The correct answer is C . In a link-trap-based wired deployment, the switch sends a linkUp or linkDown SNMP trap to FortiNAC-F, but that trap does not contain the endpoint MAC address. After receiving the link trap, FortiNAC-F must contact the switch and

perform a Layer 2 poll to read the forwarding table and determine which MAC address was added or removed on the port. The FortiNAC-F study guide states that link traps trigger FortiNAC-F to perform a Layer 2 poll to update its awareness of devices connected to the edge device, and the wired link-trap workflow specifically shows FortiNAC-F performing a Layer 2 poll before locating the host record and provisioning access.
The symptoms in the exhibit are classic stale Layer 2 visibility: FortiNAC-F still shows a rogue host on a port where no host is connected, while also failing to show hosts on ports where endpoints are actually connected.
That means FortiNAC-F is not successfully refreshing the switch MAC table information. Since link traps depend on FortiNAC-F being able to poll the switch after the trap, a contact failure with the modeled switch is the most likely cause.
Option A is wrong because logical network settings affect access enforcement, not whether FortiNAC-F can see current MAC-to-port mappings. Option B is wrong because the FortiNAC-F agent is not required for basic switch-port visibility; Layer 2 visibility comes from switch polling, MAC notification traps, or RADIUS. Option D is tempting, but the broader failure shown here is not merely a policy or endpoint-side issue-it is that FortiNAC-F cannot obtain current Layer 2 data from the switch. In practice, you would still verify SNMP/CLI credentials while troubleshooting, but the best answer to the symptom pattern is that FortiNAC-F cannot contact/query the switch successfully.

NEW QUESTION # 27
A network administrator is troubleshooting a network access issue for a specific host. The administrator suspects the host is being assigned a different network access policy than expected.
Where would the administrator look to identify which network access policy, if any, is being applied to a particular host?

- A. The Policy Logs view
- B. The Connections view
- C. The Port Properties view of the hosts port
- D. The Policy Details view for the host

Answer: D

Explanation:
When troubleshooting network access in FortiNAC-F, it is often necessary to verify exactly why a host has been granted a specific level of access. Since FortiNAC-F evaluates policies from the top down and assigns access based on the first match, an administrator needs a clear way to see the results of this evaluation for a specific live endpoint.
The Policy Details (C) view is the designated tool for this purpose. By navigating to the Hosts > Hosts (or Adapter View) in the Administration UI, an administrator can search for the specific MAC address or IP of the host in question. Right-clicking on the host record reveals a context menu from which Policy Details can be selected. This view provides a real-time "look" into the policy engine's decision for that specific host, showing the Network Access Policy that was matched, the User/Host Profile that triggered the match, and the resulting Network Access Configuration (VLAN/ACL) currently applied.

NEW QUESTION # 28
When creating a device profiling rule, what is an advantage of modeling the endpoint as a device in the inventory view?

- A. The devices can be associated with a logged on user.
- B. The devices will have connection logs.
- C. The devices can have scheduled connection status polling.
- D. The device will have historic connection logs.

Answer: C

Explanation:
The correct answer is B . When a device profiling rule classifies an endpoint, the Register as setting can place the device in the host view, the topology/inventory view, or both. The study guide explains that if the profiled endpoint is registered into the topology view, the administrator must select a topology container.
The advantage of modeling the endpoint as a device in the inventory view is that it can be treated as a pingable device , where FortiNAC-F can use Contact Status settings. The guide explains that a modeled pingable device has contact status controls that allow polling to be enabled or disabled, the polling interval to be set, and the last successful and last attempted poll to be displayed.
Option A and option C are not the best answers because connection logs are associated with host connection tracking, not the key advantage of placing a profiled endpoint into inventory as a modeled device. Option D is wrong because user association applies more naturally to hosts or BYOD ownership workflows; it is not the main benefit of inventory modeling. The tested benefit is scheduled reachability monitoring through contact status polling.

NEW QUESTION # 29
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. The isolation network type is Layer 2.
- B. There is a direct cable link between FortiNAC-F devices.
- C. The isolation network type is layer 3.
- D. The primary and secondary administrative interfaces are on the same subnet.

Answer: D

Explanation:
In a1+1 High Availability (HA)deployment, FortiNAC-F supports two primary methods for management access: individual IP addresses or aShared IP Address(also known as a Virtual IP or VIP). The Shared IP option is part of aLayer 2 HAdesign, 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, thePrimary 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 theUse Shared IP Addresscheckbox 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 # 30
While discovering network infrastructure devices, a switch appears in the inventory topology with a question mark (?) on the icon. What would cause this?

- A. A read-only SNMP community siring was used.
- B. The SNMP ObjectlD is not recognized by FortiNAC-F.
- C. The wrong SNMP community string was entered during discovery.
- D. SNMP is not enabled on the switch.

Answer: B

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."

NEW QUESTION # 31
.....

Perhaps it was because of the work that there was not enough time to learn, or because the lack of the right method of learning led

to a lot of time still failing to pass the NSE6_FNC_AD-7.6 examination. Whether you are the first or the second or even more taking Fortinet examination, our NSE6_FNC_AD-7.6 Exam Prep not only can help you to save much time and energy but also can help you pass the exam. In the other words, passing the exam once will no longer be a dream.

Valid NSE6_FNC_AD-7.6 Study Materials: https://www.newpassleader.com/Fortinet/NSE6_FNC_AD-7.6-exam-preparation-materials.html