Reliable Fortinet NSE7_LED-7.0 Exam Topics, Training NSE7_LED-7.0 Kit

BTW, DOWNLOAD part of DumpsQuestion NSE7_LED-7.0 dumps from Cloud Storage: https://drive.google.com/open?id=1BVqjtwu85wDlcPv_51QKmacbgVkOjjBi

Our NSE7_LED-7.0 test torrent is of high quality, mainly reflected in the pass rate. As for our NSE7_LED-7.0 study tool, we guarantee our learning materials have a higher passing rate than that of other agency. Our NSE7_LED-7.0 test torrent is carefully compiled by industry experts based on the examination questions and industry trends in the past few years. More importantly, we will promptly update our NSE7_LED-7.0 exam materials based on the changes of the times and then send it to you timely. 99% of people who use our learning materials have passed the exam and successfully passed their certificates, which undoubtedly show that the passing rate of our NSE7_LED-7.0 Test Torrent is 99%. If you fail the exam, we promise to give you a full refund in the shortest possible time. So our product is a good choice for you. Choosing our NSE7_LED-7.0 study tool can help you learn better. You will gain a lot and lay a solid foundation for success.

Fortinet NSE 7 - LAN Edge 7.0 Exam, also known as the Fortinet NSE7_LED-7.0 Exam, is a certification exam offered by Fortinet. NSE7_LED-7.0 exam is designed to test the knowledge and skills of IT professionals who are responsible for managing and securing LAN edge networks. NSE7_LED-7.0 Exam covers topics such as network design, firewall policies, VPNs, advanced threat protection, and more.

>> Reliable Fortinet NSE7_LED-7.0 Exam Topics <<

100% Pass Quiz 2026 Fortinet High Hit-Rate NSE7_LED-7.0: Reliable Fortinet NSE 7 - LAN Edge 7.0 Exam Topics

In a busy world, managing your time is increasingly important. If you don't want to waste much time on preparing for your exam, NSE7_LED-7.0 exam braindumps files will be a shortcut for you. Good exam materials make you twice the result with half the effort. Our NSE7_LED-7.0 Exam Braindumps cover many questions and answers of the real test so that you can be familiar with the real test question. When you attend NSE7_LED-7.0 exam, it is easy for you to keep good mood and control your finishing time.

The NSE7_LED-7.0 exam is designed for professionals who have a deep understanding of the Fortinet Security Fabric and have experience in deploying and managing Fortinet solutions in LAN Edge environments. NSE7_LED-7.0 Exam Tests the candidate's skills in securing LAN Edge networks, including access control, authentication, VPN, and security policies.

Fortinet NSE 7 - LAN Edge 7.0 Sample Questions (Q50-Q55):

NEW QUESTION # 50

Which CLI command should an administrator use to view the certificate verification process in real time?

- A. diagnose debug application radiusd -1
- B. diagnose debug application foauthd -1
- C. diagnose debug application fnbamd -1
- D. diagnose debug application authd -1

Answer: D

Explanation:
According to the FortiOS CLI Reference Guide, "The diagnose debug application foauthd command enables debugging of certificate verification process in real time." Therefore, option A is true because it describes the CLI command that an administrator should use to view the certificate verification process in real time. Option B is false because diagnose debug application radiusd -1 enables debugging of RADIUS authentication process, not certificate verification process. Option C is false because diagnose debug application authd -1 enables debugging of authentication daemon process, not certificate verification process. Option D is false because diagnose debug application fnbamd -1 enables debugging of FSSO daemon process, not certificate verification process.

NEW QUESTION # 51
When you configure a FortiAP wireless interface for auto TX power control which statement describes how it configures its transmission power"?

- A. Every 30 seconds FortiGate measures the signal strength of adjacent AP interfaces It will adjust its own AP power to match the adjacent AP signal strength
- B. Every 30 seconds FortiGate measures the signal strength of the weakest associated client The AP will then configure its radio power to match the detected signal strength of the client
- C. Every 30 seconds the AP will measure the signal strength of the AP using the client The AP will adjust its signal strength up or down until the AP signal is detected at -70 dBm
- D. Every 30 seconds FortiGate measures the signal strength of adjacent FortiAP interfaces It will adjust the adjacent AP power to be detectable at -70 dBm

Answer: D

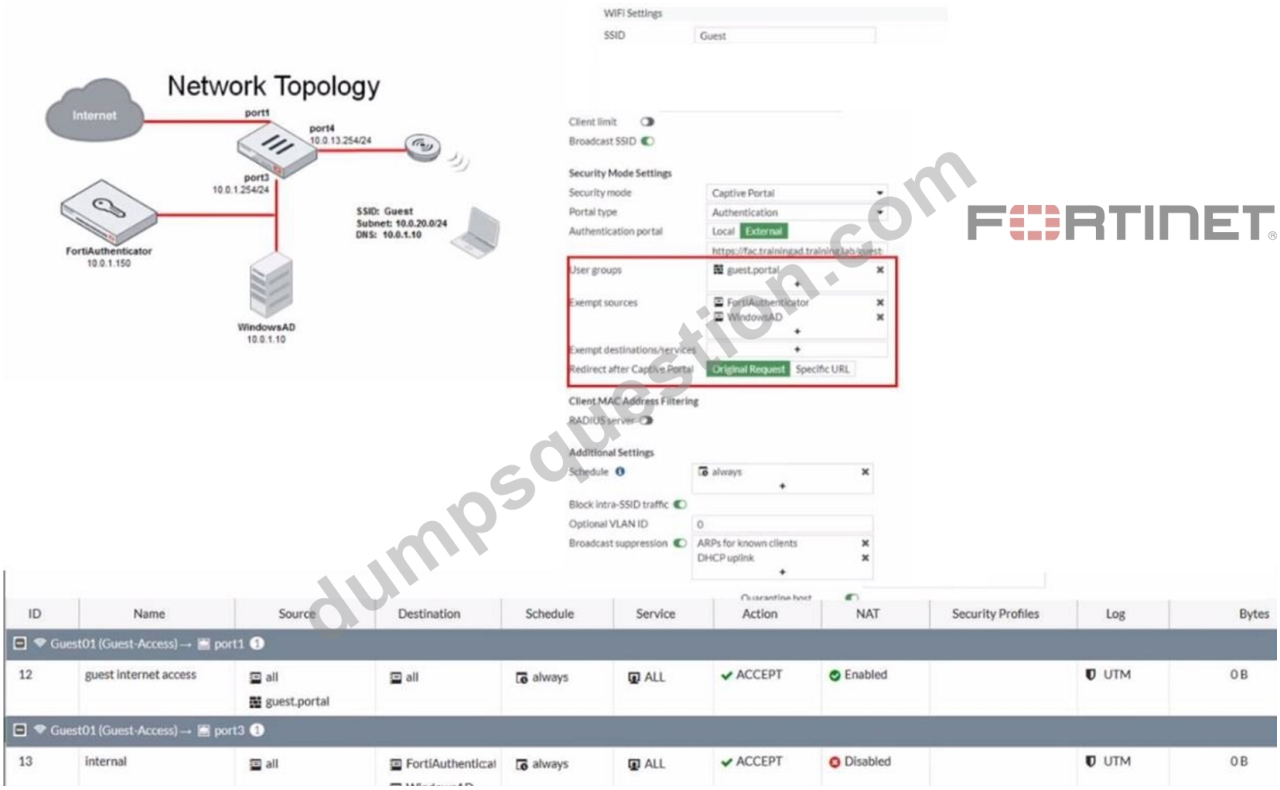
NEW QUESTION # 52
A wireless network in a school provides guest access using a captive portal to allow unregistered users to self- register and access the network The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS) Which two changes must the administrator make to enforce HTTPS authentication"? (Choose two >

- A. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator
- B. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection
- C. Enable HTTP redirect in the user authentication settings
- D. Create a new SSID with the HTTPS captive portal URL

Answer: A,C

Explanation:
According to the FortiGate Administration Guide, "To enable HTTPS authentication, you must enable HTTP redirect in the user authentication settings. This redirects HTTP requests to HTTPS. You must also update the captive portal URL to use HTTPS on both FortiGate and FortiAuthenticator." Therefore, options B and D are true because they describe the changes that the administrator must make to enforce HTTPS authentication for the captive portal. Option A is false because creating a new SSID with the HTTPS captive portal URL is not required, as the existing SSID can be updated with the new URL. Option C is false because disabling HTTP administrative access on the guest SSID will not enforce HTTPS connection, but rather block HTTP connection.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-secure-authentication-HTTPS-on-a- FortiGate/ta-p/192486

NEW QUESTION # 53
Exhibit.



Refer to the exhibit showing a network topology and SSID settings.
FortiGate is configured to use an external captive portal However wireless users are not able to see the captive portal login page
Which configuration change should the administrator make to fix the problem?

- A. Enable NAT in the firewall policy with the ID 13.
- B. Add the FortiAuthenticator and WindowsAD address objects as exempt destinations services
- C. Enable the captive-portal-exempt option in the firewall policy with the ID 12
- D. Remove the guest.portal user group in the firewall policy with the ID 12

Answer: B

Explanation:
According to the exhibit, the network topology and SSID settings show that FortiGate is configured to use an external captive portal hosted on FortiAuthenticator, which is connected to a Windows AD server for user authentication. However, wireless users are not able to see the captive portal login page, which means that they are not redirected to the external captive portal URL. Therefore, option B is true because adding the FortiAuthenticator and WindowsAD address objects as exempt destinations services will allow the wireless users to access the external captive portal URL without being blocked by the firewall policy. Option A is false because enabling NAT in the firewall policy with the ID 13 will not affect the redirection to the external captive portal URL, but rather the source IP address of the wireless traffic. Option C is false because enabling the captive-portal-exempt option in the firewall policy with the ID 12 will bypass the captive portal authentication for the wireless users, which is not the desired outcome. Option D is false because removing the guest.portal user group in the firewall policy with the ID 12 will prevent the wireless users from being authenticated by FortiGate, which is required for accessing the external captive portal.

NEW QUESTION # 54
Which two statements about FortiSwitchmanager are true1? (Choose two)

- A. If the administrator makes any changes on FortiSwitch manager they must also install those changes on FortiGate so that those changes are applied on the managed switches
- B. Any switch discovered or authorized on FortiGate must be added manually on FortiSwitch manager
- C. FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes
- D. Per-device management is the default management mode on FortiManager

Answer: A,C

Explanation:
Explanation

According to the FortiManager Administration Guide1, "FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes." Therefore, option B is true because it describes how FortiManager gets the information about the managed switches. According to the same guide2,
"If you make any changes in this module, you must install them on your managed device so that they are applied on your managed switches." Therefore, option C is true because it describes what the administrator must do after making any changes on FortiSwitch manager. Option A is false because central management is the default management mode on FortiManager, not per-device management. Option D is false because anyswitch discovered or authorized on FortiGate will be automatically added on FortiSwitch manager, not manually.
1: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager 2: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager#fortisw

NEW QUESTION # 55
.....