Lab Report

Your Performance

Your Score: 0 of 3 (0%)

Pass Status: Not Passed

Elapsed Time: 1 minute 2 seconds

Required Score: 100%

Task Summary

✖ Configure Denial of Service protection   Hide Details

> ➖ Protect against excessive wireless requests
>
> ➖ Block clients with repeated authentication failures
>
> ➖ Block clients for two minutes (120 seconds)

✖ Enable Wireless Intrusion Protection   Hide Details

> ➖ Enable Rogue Device Reporting
>
> ➖ Report all rogue devices regardless of type
>
> ➖ Protect the network from rogue access points

✖ Enable Rogue DHCP Server Detection

Explanation

In this lab, you perform the following tasks:

- Configure the wireless controller to protect against denial of service (DOS) attacks as follows:
    - Protect against excessive wireless requests.
    - Block clients with repeated authentication failures for two minutes (120 seconds).
- Configure Intrusion Detection and Prevention as follows:
    - Report all rogue devices regardless of type.
    - Protect the network from rogue access points.
- Enable rogue DHCP server detection.

Enable Wireless Intrusion Prevention on the wireless controller as follows:

1. Select the **Configure** tab.
2. From the left menu, select **WIPS**.
3. Configure Denial of Service protection as follows:
    - a. Select **Protect my wireless network against excessive wireless requests**.
    - b. Select **Temporarily block wireless clients with repeated authentication failures**.
    - c. Enter the *threshold* in seconds.
    - d. On the right, click **Apply**.

4. Configure Intrusion Detection and Prevention as follows:
    - a. Select **Enable report rogue devices**.
    - b. Select **Report all rogue devices**.
    - c. Select **Protect the network from malicious rogue access points**.
    - d. On the right, click **Apply**.
5. Select **Enable rogue DHCP server detection**; then click **Apply**.