Robert Carpenter
github.com/robertmcarpenter
Sat January 18th 2025

Lab 8.6.7: Wireless Intrusion Protection Configuration on a Ruckus WLAN AP Controller

From TestOut CompTIA Security+ Course

In this lab I will be configuring the Wireless Intrusion Protection System (WIPS) on a Ruckus WLAN AP Zone Controller.

The scenario for this lab is as follows:

"You are a network technician for a small corporate network. You would like to enable Wireless Intrusion Prevention on the wireless controller. You are already logged in as WxAdmin.

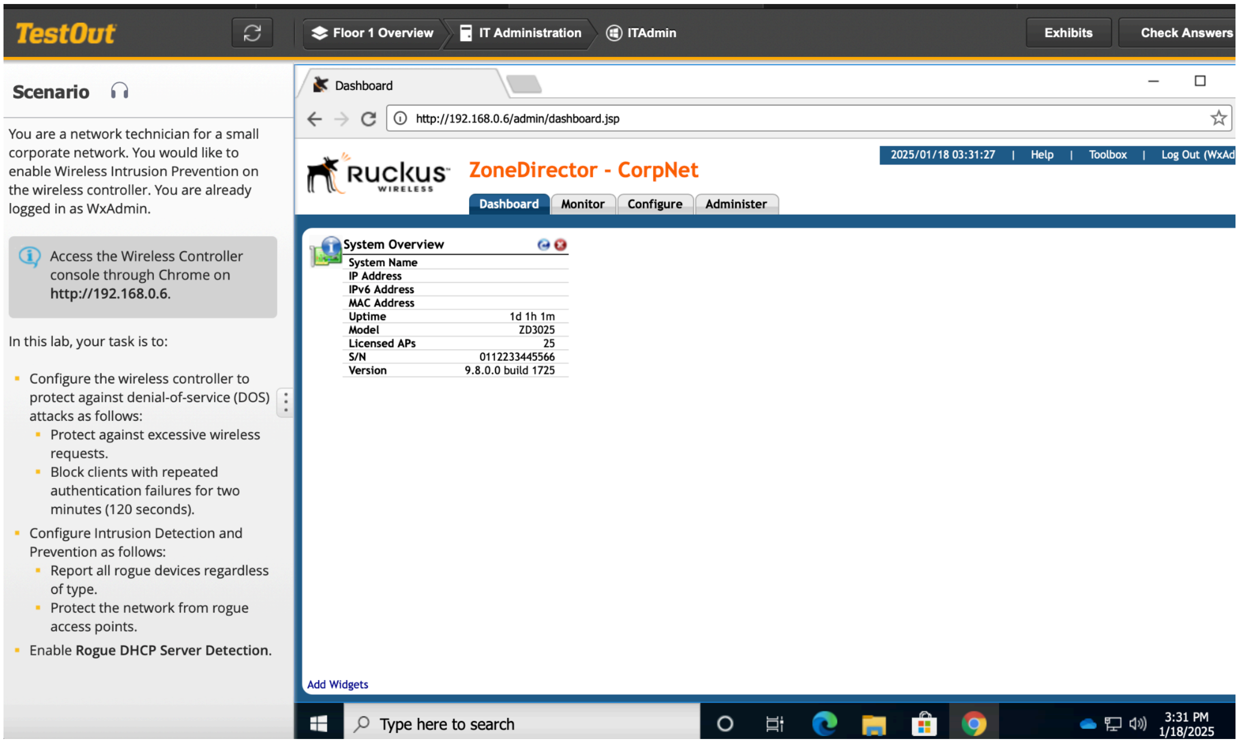
Access the Wireless Controller console through Chrome on http://192.168.0.6.

In this lab, your task is to:

- **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."**

To start I will navigate to the Ruckus Web Portal @ **192.168.0.6**. The Lab states that we are pre-authenticated as the user **WxAdmin**.

Robert Carpenter
github.com/robertmcarpenter
Sat January 18th 2025



Scenario

You are a network technician for a small corporate network. You would like to enable Wireless Intrusion Prevention on the wireless controller. You are already logged in as WxAdmin.

Access the Wireless Controller console through Chrome on **http://192.168.0.6.**

In this lab, your task is to:

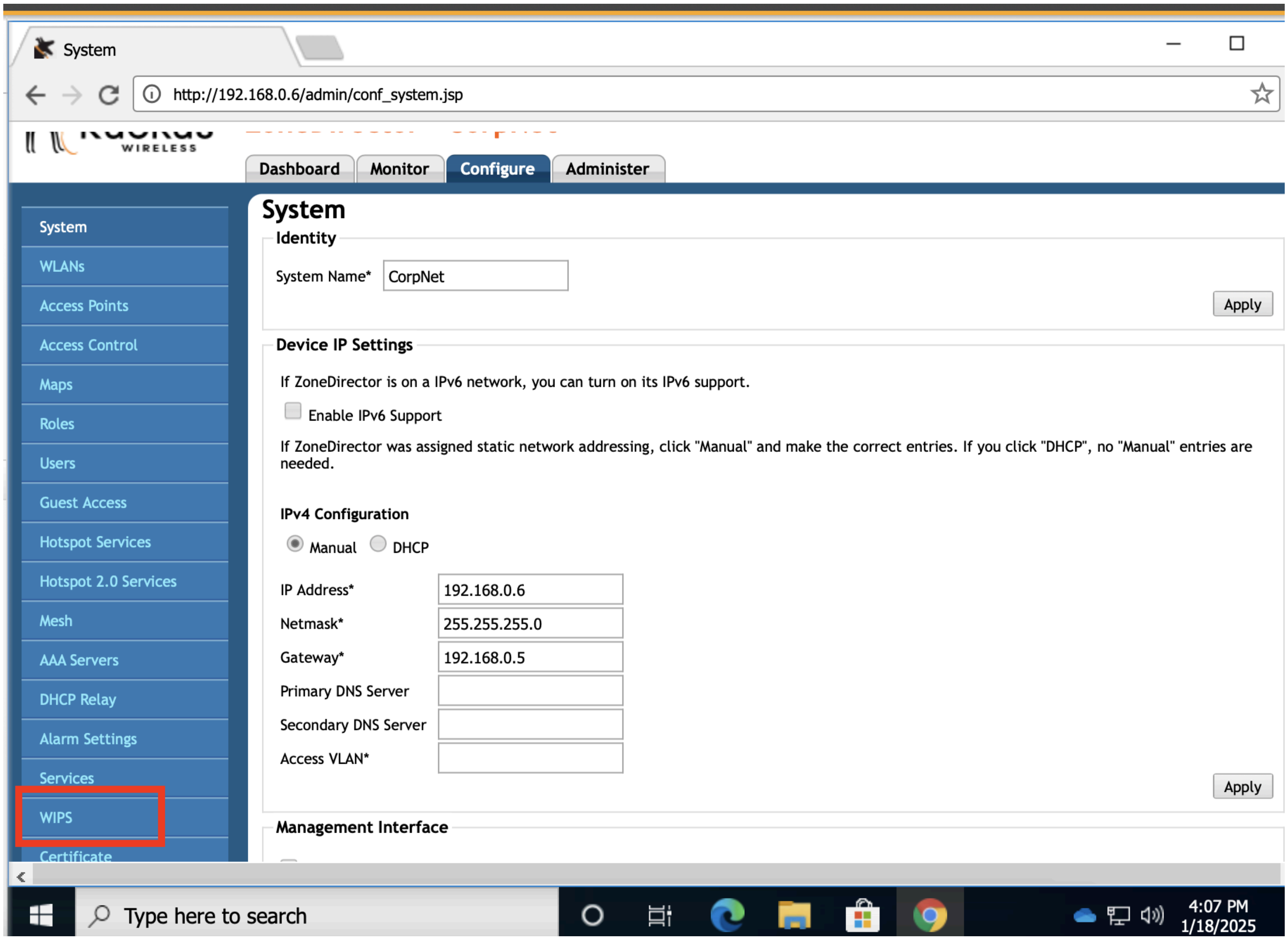
- Configure the wireless controller to protect against denial-of-service (DOS) attacks as follows:
  - Protect against excessive wireless requests.
  - Block clients with repeated authentication failures for two minutes (120 seconds).
- Configure Intrusion Detection and Prevention as follows:
  - Report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

System Overview

System Name	
IP Address	
IPv6 Address	
MAC Address	
Uptime	1d 1h 1m
Model	ZD3025
Licensed APs	25
S/N	0112233445566
Version	9.8.0.0 build 1725

To get to the **Wireless Intrusion Prevention System** configuration settings I’ll navigate on the top menu bar to the **Configure** Master Menu. Once there I will head to the left menu panel and select **WIPS:**

Robert Carpenter
github.com/robertmcarpenter
Sat January 18th 2025



System

Identity

System Name* CorpNet

Apply

Device IP Settings

If ZoneDirector is on a IPv6 network, you can turn on its IPv6 support.

□ Enable IPv6 Support

If ZoneDirector was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP", no "Manual" entries are needed.

IPv4 Configuration

● Manual ○ DHCP

IP Address*	192.168.0.6
Netmask*	255.255.255.0
Gateway*	192.168.0.5
Primary DNS Server	
Secondary DNS Server	
Access VLAN*	

Apply

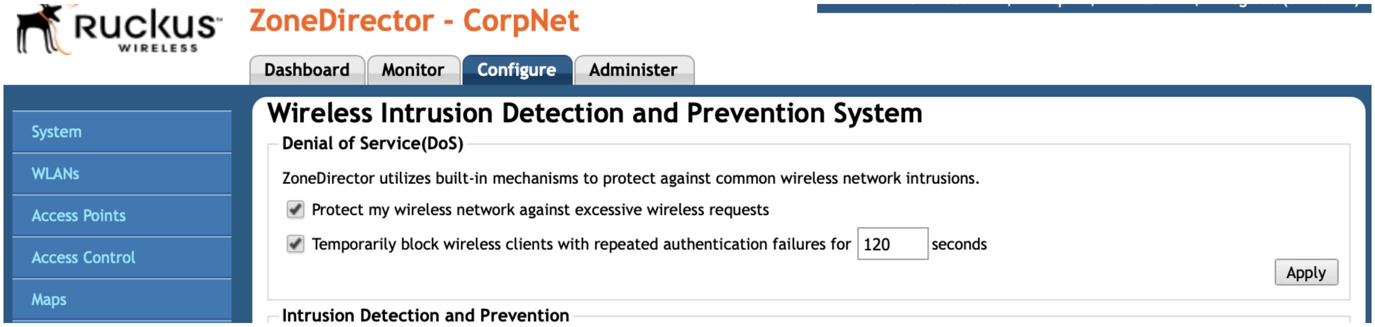
Management Interface

Once I'm on the menu for **WIPS,** my first task is to enable DOS Attacks Protection. This is when an attacker is able to send packets against a WiFi Network and De Authenticate all Users off it (provided their Wifi Adapter has a strong enough signal in the vicinity of the target SSID). The Lab states:

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).**

On the **WIPS** configuration page I can scroll down to enable these:



Wireless Intrusion Detection and Prevention System

Denial of Service(DoS)

ZoneDirector utilizes built-in mechanisms to protect against common wireless network intrusions.

☑ Protect my wireless network against excessive wireless requests

☑ Temporarily block wireless clients with repeated authentication failures for 120 seconds

Apply

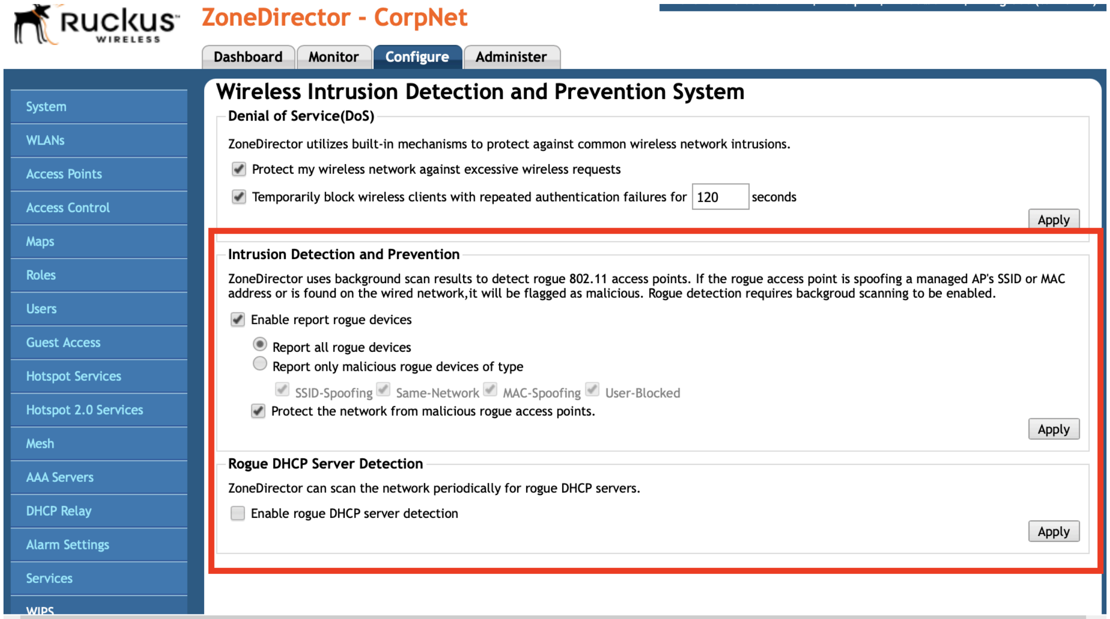
Intrusion Detection and Prevention

Once those are enabled I will hit the **Apply** button. After that applies, I’ll move on to the next part of the lab which is:

- **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.**

Both tasks can be done from within the same place in the Ruckus Web Portal Configurator.

Within the same **WIPS** submenu where I completed the last task , I’ll scroll down to the **Intrusion Detection and Prevention** subsection (highlighted below in Red).



Wireless Intrusion Detection and Prevention System

Denial of Service(DoS)

ZoneDirector utilizes built-in mechanisms to protect against common wireless network intrusions.

☑ Protect my wireless network against excessive wireless requests

☑ Temporarily block wireless clients with repeated authentication failures for 120 seconds

Apply

Intrusion Detection and Prevention

ZoneDirector uses background scan results to detect rogue 802.11 access points. If the rogue access point is spoofing a managed AP's SSID or MAC address or is found on the wired network,it will be flagged as malicious. Rogue detection requires backgroud scanning to be enabled.

☑ Enable report rogue devices

● Report all rogue devices

○ Report only malicious rogue devices of type

☑ SSID-Spoofing ☑ Same-Network ☑ MAC-Spoofing ☑ User-Blocked

☑ Protect the network from malicious rogue access points.

Apply

Rogue DHCP Server Detection

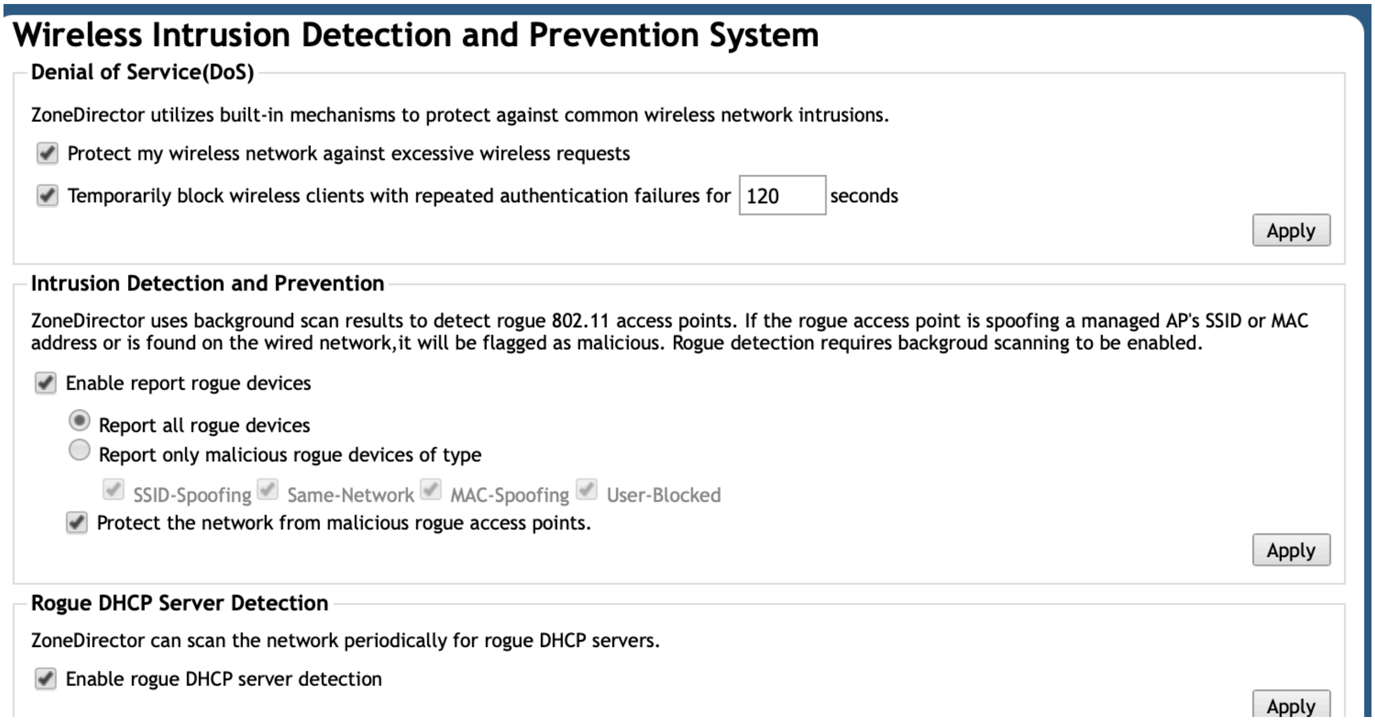
ZoneDirector can scan the network periodically for rogue DHCP servers.

☐ Enable rogue DHCP server detection

Apply

Robert Carpenter
github.com/robertmcarpenter
Sat January 18th 2025

Once all the settings have been configured it will look like this:



Wireless Intrusion Detection and Prevention System

Denial of Service(DoS)

ZoneDirector utilizes built-in mechanisms to protect against common wireless network intrusions.

☑ Protect my wireless network against excessive wireless requests

☑ Temporarily block wireless clients with repeated authentication failures for 120 seconds

Intrusion Detection and Prevention

ZoneDirector uses background scan results to detect rogue 802.11 access points. If the rogue access point is spoofing a managed AP's SSID or MAC address or is found on the wired network,it will be flagged as malicious. Rogue detection requires backgroud scanning to be enabled.

☑ Enable report rogue devices

● Report all rogue devices
○ Report only malicious rogue devices of type

☑ SSID-Spoofing ☑ Same-Network ☑ MAC-Spoofing ☑ User-Blocked

☑ Protect the network from malicious rogue access points.

Rogue DHCP Server Detection

ZoneDirector can scan the network periodically for rogue DHCP servers.

☑ Enable rogue DHCP server detection

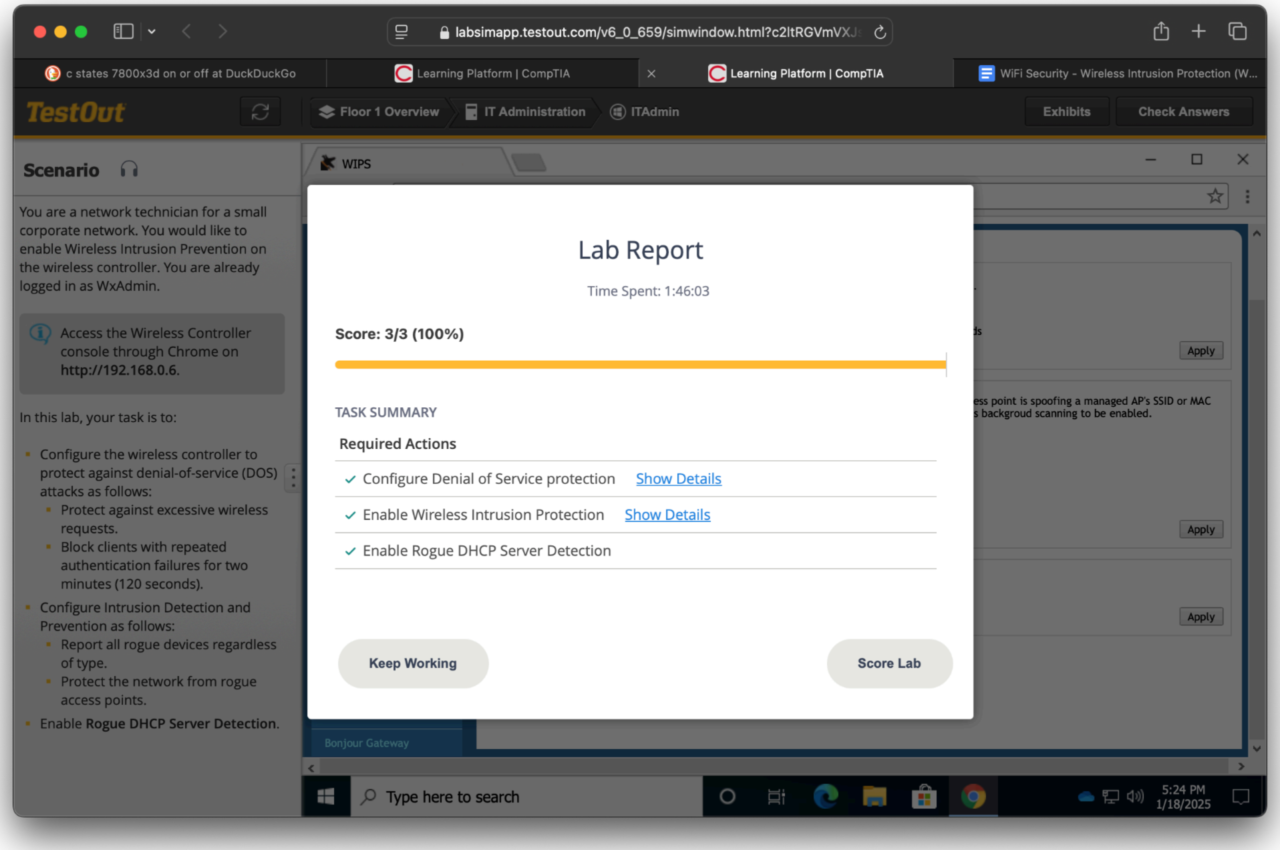
I will hit **Apply** on all 3 sections just to make sure everything is properly pushed out to our APs.

At this point I have completed all tasks for this lab, which again is:

- **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**

This now concludes this lab!

Robert Carpenter
github.com/robertmcarpenter
Sat January 18th 2025


labsimapp.testout.com/v6_0_659/simwindow.html?c2ltRGVmVXJ
c states 7800x3d on or off at DuckDuckGo
Learning Platform | CompTIA
Learning Platform | CompTIA
WiFi Security - Wireless Intrusion Protection (W...
TestOut
Floor 1 Overview
IT Administration
ITAdmin
Exhibits
Check Answers
WIPS
Apply
Apply
Apply
Bonjour Gateway
Type here to search
5:24 PM
1/18/2025

Scenario

You are a network technician for a small corporate network. You would like to enable Wireless Intrusion Prevention on the wireless controller. You are already logged in as WxAdmin.

Access the Wireless Controller console through Chrome on **http://192.168.0.6.**

In this lab, your task is to:

- 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.**

ess point is spoofing a managed AP's SSID or MAC
s backgroud scanning to be enabled.

Lab Report

Time Spent: 1:46:03

Score: 3/3 (100%)

TASK SUMMARY

Required Actions

- ✓ Configure Denial of Service protection Show Details
- ✓ Enable Wireless Intrusion Protection Show Details
- ✓ Enable Rogue DHCP Server Detection

Keep Working

Score Lab