Wireless Network Design Best Practices

Summary

WirelessTrakker is a powerful networking tool that can be configured in a wire variety of ways. This article will help guide you in making the appropriate decisions for your network and usage case.

Applies To

WirelessTrakker

More Information

WirelessTrakker supports several different ways to validate users on your wireless network, as well as multiple networks allowing different levels of access. Making smart and planned decisions on the layout and design of the wireless network is important to minimize the amount of problems you as an administrator will have to deal with, while maximizing the usefulness of your network without giving up security controls.

Wireless Access Control

First, you must decide how secure you want the wireless network to be. If you want the network to be truly open, then the decision is easy. Create one SSID with no encryption or access controls, and allow it to access anything on your network. This clearly has some drawbacks. For example, anyone with a wireless device can get on your network and look for things to hack into. With a wide variety of network scanning tools available, this is a fairly easy thing to do.

If you want to control access to your network, then you have another decision to make: how to control access. WirelessTrakker supports both "Shared Key WPA2" and "Enterprize WPA2". (In this article, we will always talk about WPA2, and not WPA or WEP. For information on these security measures, see Wireless Encryption & Authentication Methods). With "Shared Key WPA2", the network has a key / password that the user must enter to join the wireless network. Everything on that wireless network uses the same key. With "Enterprize WPA2", each user authenticates to the wireless network with their own unique username and password. This adds accountability to the network, along with tighter access controls. In a Shared Key situation, most users end up needing to know the key to connect to the network. The more people that know the key, the higher the likelihood of the key being compromised. Additionally, it's good practice to change the key every so

often, so you then have to tell everyone the new key. While Shared Key is slightly easier for the end user, it is less secure then Enterprize WPA2. WirelessTrakker supports several different authentication methods / user databases for Enterprize mode. It can use a database on the appliance itself that you can manage users on, it can use a database on a remote SecureSchool appliance that is already setup, or it can use your Microsoft Windows Active Directory.

Wired Network Access Limits

Once you decide on how to control access to the wireless networks (SSIDs), you then decide what the wireless network(s) have access to. WirelessTrakker's firewall can limit which SSIDs/subnets can access different wired resources. Typically you want to minimally allow access to SecureSchool (or whatever proxy or filtering device you have) so that wireless users can access the Internet. You may also want to allow wireless users to access certain wired devices, like print servers or some file servers. These limits depend on who your target audience is for the particular SSID/subnet. If the wireless SSID is accessed only by staff computers, you can probably trust them to allow access to your entire wired network. If the wireless SSID can be accessed by anyone, then you probably will only want to allow access to your Internet proxy/filter.

Putting It All Together

Using the ideas above, we would recommend starting with the following ideas and modifying them as they suit your needs and security policies / requirements.

- Create an SSID for your staff that is controlled with Enterprize WPA2. Allow this network to get to whatever resources the staff needs to do their job: printers, Internet proxy/filter, file servers, web servers, etc.
- Create an SSID for your students. If your students are allowed to bring in their own wireless devices or use "wireless laptop carts", this is a good idea. If your students do not need wireless access, you can skip this. The best situation would be to control access using Enterprize WPA2, with each student using their own login. Using this method allows the administrators to see what student connected to the wireless network and at what time from what device. Limit the resources this network is allow to get to to the bare minimum that is required for their designed use. For example, the Internet proxy/filter. If they need to access their home folders or a file server, you may want to consider creating a file server that houses only student folders and allow access to only that server to minimize your network exposure.
- Create an open guest network that allows only access to the Internet. This network can run without any key, or with a key that you must provide to any guests.

Additionally, for wireless networks that use Enterprize WPA2, WirelessTrakker can notify the SecureSchool Enhanced iPad, iPod, Android add-on feature that user X is at IP address Y, and filter that user according to whatever filterset they are supposed to be in.