Switch to WPA / WPA2-Enterprise encryption

In this article, we will show you two very different modes of accessing a protected Wi-Fi network.

Network administration **- Every Wi-Fi network in an enterprise needs to use the Enterprise mode of WPA or WPA2 encryption. In this article, we will show you how to switch from Personal (PSK) mode to Enterprise (RADIUS) mode.**

Certainly many of you know, encryption of Wired Equivalent Privacy (WEP) is a code that is no longer safe today. The security standard for the first wireless LAN, developed by IEEE, has emerged as a vulnerability that allows attackers to crack.
In 2003, the Wi-Fi Association released another security standard called Wi-Fi Protected Access. Although the first version (WPA), which uses TKIP / RC4 encryption, gave the attackers some disappointment, it was still not considered safe.

In the second version (WPA2), released in mid-2004, security has improved quite well with the implementation of IEEE 802.11i security standards and CCMP / AES encryption.

In this article, I will show you two very different modes of accessing a protected Wi-Fi network (Wi-Fi Protected Access) and show you how to switch from Personal mode to Enterprise mode.

Let's start!

Two modes of WPA / WPA2: Personal (PSK) and Enterprise

Both versions of Wi-Fi Protected Access (WPA / WPA2) can be executed in two modes:

1. **Personal mode or Pre-Shared Key (PSK)** : This mode is suitable for most home networks - not suitable for corporate networks. You can define encryption passwords on wireless routers and other access points (APs). The password must then be entered by the user when connecting to a Wi-Fi network.

   Although this mode seems very easy to enforce, it cannot guarantee enterprise network security. Unlike the Enterprise mode, wireless access is not separate or centrally managed. A password is applied to all users. If the global password needs to be changed, it must be changed on all APs and computers. This will cause a lot of difficulties when you need to change; for example, when an employee leaves the company or, when a computer is stolen or compromised.

   Unlike the Enterprise mode, encrypted passwords are stored on computers. However, anyone on the computer - whether it's an employee or a criminal - can connect to the network and can recover the encrypted password.

- **Enterprise mode (EAP / RADIUS):** This mode provides the necessary security for wireless networks in enterprise environments. Although complicated in settings, this security mode provides centralized and discriminatory control of Wi-Fi network access. Users are assigned login information that they need to enter when connecting to the network, which can be changed or revoked by administrators at any time.

  Users do not need to care about actual encryption keys. They are created safely and assigned on each user session in the background after a user enters their login credentials. This will prevent someone from recovering the network key from computers.

Introducing 802.1X authentication and RADIUS servers

The authentication method is used to verify user (and server) information on WPA / WPA2-Enterprise networks defined by the IEEE 802.1X standard. This method of authentication requires an external server, still called Remote Authentication Server In User Service (RADIUS) or Authentication, Authorization, and Accounting (AAA), used for a variety of network protocols and environment containing ISP.

A RADIUS server needs to understand the Extensible Authentication Protocol (EAP) language and can communicate with wireless APs, referring to RADIUS clients or authentication suites. The RADIUS server will essentially serve as an intermediary between APs and user data. Since then APs can communicate directly with the 802.1X client, also referred to as an 802.1X Supplicant, on a user's computer or device.

Verify 802.1X not based on port. This means that when someone tries to connect to a protected enterprise network, communication will be allowed through a virtual port to transmit the login information. If the authentication process is successful, the encryption keys will be sent securely and users will now be given full access.

See page 2

Authentication server (Authentication)

There are several ways you can get an 802.1X authentication server:

- **FreeRADIUS:** This is one of the most popular AAA servers in the world. Although it is a free, open source project, this server has a lot of advanced points. It is available for different platforms, including Linux, Mac OS X, and Windows. By default, you change these settings in the configuration file.
- **Windows Server:** If you have a Windows Server set up, you can use an Internet Authentication Service (IAS) available in Windows Server 2003 or Network Policy Server (NPS) in Windows Server 2008.
- **Outsourced Services:** Hosting services, such as AuthenticateMyWiFi, are one of the good ways for those who do not want to invest much money or time in setting up a RADIUS server, with multiple offices, or without Deep technical expertise. These services can provide additional functionality for traditional RADIUS servers.

  For example, APs are not directly connected to the Internet; they can be placed behind NAT routers or gateways, allowing you to assign a unique secret to each AP. These services also have control panels on the web, so users can easily configure authentication settings.

Other advantages of EAP

The mind behind 802.1X authentication is the Extensible Authentication Protocol (EAP). There are many other advantages of EAP. Which features in each organization should be used is entirely dependent on the level of security desired, as well as some degree of complexity and server / client specifications.

These are the most common types:

- **PEAP (Protected EAP):** This is one of the most popular and easy to implement EAP methods. It can authenticate users through the username and password they enter when connecting to the network.

  The authentication server can also be validated during PEAP authentication when an SSl certificate is installed on the server. This type is supported by default in Windows.
- **TLS (Transport Layer Security)** : Is one of the most secure types of security, but quite complex in implementation and maintenance. The server and client validation process needs to be done via SSL certificates. Instead of having to provide a username and password when connecting, user devices or computers must be loaded SSL certificate files into its 802.1X client.

  Administrators can control the Certificate Authority (CA) and manage client certificates, which allows them to have more control, but also require more administrative time.

- **TTLS (Tunneled TLS):** An improved version of TLS, which does not require client-side security certificates, has reduced the complexity of network management. However, this EAP type does not have native support in Windows; it needs a third client like SecureW2.

Your next steps

From what I have shown you above, you probably know the 802.1X authentication mechanism that makes WPA / WPA2-Enterprise encryption a way to secure corporate Wi-Fi networks. . Also, you know that to implement them, we need to have an authentication server and PEAP, TLS, and TTLS are common EAP types.

Here are some tips that can help you with the next steps:

1. Find and select a RADIUS server or outsource service.
2. Set up a RADIUS server with EAP, AP and user settings.
3. Configure APs with encryption information and RADIUS server.
4. Windows configuration (or other operating system) with encryption settings and 802.1X.
5. Finally, connect to your protected Enterprise network!