Deploy WPA2-Enterprise wireless security in small businesses

In this article we will show you some of the issues that are needed when setting up WPA2-Enterprise wireless security.

In this article we will discuss some of the issues you need to know when setting up WPA2-Enterprise wireless security . The information contained in this article contains tips to help you understand, install and manage wireless security issues in small businesses.

When setting up a wireless network, you will probably find that there are two different Wi-Fi Protected Access (WPA) security modes, WPA and WPA2.

It can be said that *Personal* mode is the easiest setting mode, this is the still-known mode of Pre-Shared Key (PSK). It does not require anything other than the Wireless Router, AP access points and the use of passwords for all users or devices.

Another mode is *Enterprise* , which is the mode that businesses and organizations should use, it is also known as RADIUS, 802.1X, 802.11i or EAP. This mode provides more effective security solutions, better key management and supports other business functions such as VLAN and NAP. However, this mode requires an additional authentication server, Remote Authentication Dial In User Service (RADIUS) server, to manage the user's 802.1X authentication.

In this article we will share some information and tips to help you understand, install and manage Enterprise wireless security in small businesses - even run a non-domain network without Windows Server.

Advantages of Enterprise mode

The Enterprise mode allows users to log on to the wireless network with a name and password or a digital certificate. Both types of certificates can be changed or revoked at any time on the server when the wireless device is lost or stolen. In contrast, when using Personal mode, the password needs to be changed manually on all APs and wireless devices.

Because the Enterprise mode provides users with a unique and dynamic encryption key, it can prevent viewing of information theft among users on the network. When using Personal mode, successful connected users can see the traffic of other users - be it passwords, emails, or other sensitive data.

Dynamic keys enhance the power of WPA (TKIP) and WPA2 (AES) encryption. Personal mode is more likely to be revealed for brute-force dictionary attacks. This explains why when using Personal mode, creating long and complex passwords is very important.

Server options

If a small business has Windows Server, you can use the Internet Authenticate Service (IAS) or Network Policy Server (NPS) feature for the RADIUS server.

However, there are many other options, some suitable for the lack of domains:

- Buy and use APs with an attached RADIUS server. Examples include HP ProCurve 530 and NWA-3500 or NWA3166 ZyXEL. If it's a simple wireless setup, you can just use one server and many cheap APs to increase coverage.
- Create your own router / gateway with the attached RADIUS server, such as RouterOS or Zeroshell. This usually involves installing software on the server. With smaller and less important networks, you can reuse old computers for this.
- Use a service, such as AuthenticateMyWiFi, to save time, money, and the knowledge needed in server settings. It also provides client configuration support and ensures easier deployment of enterprise security mechanisms in multiple locations.
- Use free servers like TekRADIUS.
- Use free and open source servers like FreeRADIUS, use plain text files for configuration and administration. Mainly for Linux / Unix computers but can also run on Windows.
- Buy and use RADIUS server software such as Elektron ($ 750) for Windows or Mac OS X and ClearBox ($ 599) for Windows.

Client configuration

In addition to operating the RADIUS server, the Enterprise mode also requires a more complex client configuration on users' computers and wireless devices. Personal mode only requires entering a password when prompted and can be performed by the user. However with Enterprise mode, you need to install the CA on the clients (plus certificates for users if you use EAP-TLS) and then manually configure wireless security settings

and 802.1 authentication. X. This requirement is very useful for IT staff in installing and troubleshooting client configurations or using deployment utilities to help.

If you use Windows Server, you can distribute certificates and configure remote and centralized settings by using Group Policy, at least on Windows computers that are joined to the domain.

For non-domain networks, you can use the free SU1X 802.1X utility or commercial products like XpressConnect and Quick1X. These utilities will allow to specify or capture security and authentication settings and create guest installation programs. Users (even IT staff) can execute the program, automating the computer's configuration. They can also help distribute the CA certificate of the RADIUS server. Some utilities can also perform wireless checks and configuration changes to support deployment, such as removing profiles for existing SSIDs and setting profile preferences.

Complete steps

To help better understand the process of setting up WPA / WPA2-Enterprise and 802.1X, we list all the basic steps in the setup process:

1. Select, install and configure a RADIUS server or use the service.
2. Create a CA to issue and install a digital certificate on the RADIUS server, which can be performed as part of the installation and configuration of the RADIUS server. Alternatively, you can purchase a digital certificate from a public CA such as GoDaddy or Verisign so that you don't have to install a server certificate on all clients. If you use EAP-TLS, you must also create digital certificates for each user.
3. On the server, locate the RADIUS client database with the IP address and shared secret for each AP.
4. On the server, populate user data with the name and password for each user.
5. On each AP, configure WPA / WPA2-Enterprise security and enter the RADIUS server's IP address and shared secret that was created for that particular AP.
6. On each computer and wireless device, configure WPA / WPA2-Enterprise security and configure 802.1X authentication settings.