AuthenticateMyWiFi wifi authentication

When compared to a traditional product based on a RADIUS server, the nature of hosting in AuthenticateMyWiFi is to bring immediate benefits.

Network Administration **- When you need to secure a commercial Wi-Fi network, use the popular Pre-Shared Key (PSK) technique of WPA or WPA2 (also known as WPA / WPA2 Personal), though it is good. However, it is not really good enough if you want to keep the Wi-Fi network as high as possible** .

Therefore, you need to have WPA / WPA2 Enterprise to perform RADIUS server authentication, but adding a RADIUS server to the network often results in a price and complexity that many companies - especially companies. Small company - cannot or cannot accept.

AuthenticateMyWiFi provides the same authentication service as a RADIUS server, but promises simple installation, easy administration as well as a comfortable price, and although the list of features is just basic, the interface Administration is a bit simple, but AuthenticateMyWiFi is still really promising.

When compared to a traditional product based on a RADIUS server, the nature of hosting in AuthenticateMyWiFi is to bring immediate benefits. With a standalone platform, it doesn't need to care about compatibility with Windows, Mac, or Linux. Also, because Web-based, AuthenticateMyWiFi can be managed, both locally and remotely, from any Internet-connected browser. Finally, the service can support access points in many areas, eliminating the need to have multiple RADIUS servers in multiple offices or have to configure a server via NAT and firewalls to communicate with the remote office.

Price: From $ 13 to $ 36 a month ($ 130 to $ 360 a year), depending on the number of users and the number of access points required.

Advantages : Simple in installation and maintenance; independent platform; multi-region support; Cheap

Disadvantages : user interface is somewhat somewhat; lack of advanced features found in many conventional RADIUS products.

Server, AP and user account settings

The first step to making AuthenticateMyWiFi work involves setting up access points and user accounts through the Web administration console. Depending on the level of service you choose, AuthenticateMyWiFi will serve up to 100 access points and some with user accounts, but you must manually create AP and user accounts. There is currently no function to import users from a back-end database or import a list of users / APs from a text file or CSV. (Vendors reported that both functions were planned together with the schedule for the first launch). Luckily for users here, AuthenticateMyWiFi's administration console is extremely simple and doesn't require too much information - such as MAC address and shared security for users' passwords, names and passwords. User account - so the installation process is quick and easy. You only have to handle a handful of access points or users.

The next step, also as fast and simple as the first step, is to configure access points to use WPA / WPA2 Enterprise, which involves pointing them to the IP address of AuthenticateMyWiFi, specifying ports UDP for RADIUS authentication, logging (services using the default UDP 1812 and UDP 1813) and entering the above shared security.

A caveat: While trying to configure a Netgear WNDR3700 to use RADIUS, we found that routers will not accept any invalid RADIUS server IP addresses outside the local subnet, wearing Despite the fact that the documentation clearly stipulates the RADIUS servers can be located on the LAN or on the WAN. We don't know how common this problem is with other Wi-Fi hardware models and manufacturers, and although it's not what you encounter when dealing with commercial-grade devices, the Small businesses using SoHo or consumer-level devices will want to check first to make sure they don't prevent you from using an external RADIUS server.

Client configuration

The final step is to configure all clients (they can be wireless or wired) to connect to Wi-Fi through 802.1x authentication. This is the hardest and most time-consuming task (especially if you have a lot of clients), but fortunately, AuthenticateMyWiFi's 14 manual PDF pages provide detailed instructions - complete with photos. screen illustration - on how to change configuration properties for Windows (XP / Vista / 7) and Mac OS X systems (The provider says it also works on a utility that automates the process configure client for Windows systems.)

Very casually, AuthenticateMyWiFi only supports half a dozen or EAP forms that are officially endorsed by the Wi-Fi Alliance, but it is said to be one of the most popular forms, v2 PEAPv0 / EAP-MSCHAP, providing authentication. via username and password.

Restrict access and login

If you want to have AuthenticateMyWiFi restrict access to your network under certain conditions, there are a number of different options to choose from. You can limit user access to specific access points or from specific computers, limit network access on schedule and weekdays, set user accounts to expire. on time and date given. (However, there is still a lack of options that we would like to see as the ability to lock users after a certain number of incorrect password entries.)

Naturally, AuthenticateMyWiFi's user interface from helping turns into an obstacle when trying to configure the above access restrictions. In one case: when creating a limited device or access point for a user, you must type in the appropriate MAC address instead of selecting from the list. Similarly, when setting the login time limit there is also no list or drop-down menu to enter the parameters. Instead, you must specify the access time in a single school via alphanumeric abbreviations, for example: ***Wk0800-2000, Sa 0900-1200*** ie only allow access from 8:00 to 20:00 hours. weekdays and from 9:00 am to 12:00 pm on Saturdays, and be careful to enter the correct information otherwise there will be a warning to enter invalid parameters or typographical errors (in fact, This field will accept repeat errors without protest. In addition, it is not possible to specify a time zone, so all time must be represented by the Eastern time.

AuthenticateMyWiFi's activity records the basic login information such as the client's MAC client, the MAC and SSID of the connected access point, as well as the time a user logs in and out of the network. Logs can only be viewed directly from the control panel, but are not exported as files for offline monitoring. It also does not support warning events such as unsuccessful logins, etc.

Price

AuthenticateMyWiFi offers a four-layer price chart that is easy to compare with a price of $ 600- $ 800 for a regular RADIUS product. The base service level can serve up to 10 users and 5 access points at a cost of $ 13 / month or a $ 130 discount if prepaid for a year. Highest level is $ 36 / month or $ 360 / year with service scale supporting up to 61-100 users and 31-100 access points plus automatic user assignment for VLAN networks, a feature but the lowest classes are missing. All plans include technical support via e-mail. (There is also a free version of the service, but its practical usefulness is quite limited because it is limited to a single access point and a single user).

Conclude

AuthenticateMyWiFi does not provide the same power and flexibility as many of the RADIUS or free server products or products that are as effective as open source, based on Linux, FreeRADIUS or IAS / NPS (Internet Authentication Service / Network Policy Server) in Windows Server 2003 and 2008, respectively. However, it does not provide many pages of complex configuration options or a too high price, so if you are looking for a reliable, non-style RADIUS with a reasonable cost, AuthenticateMyWiFi is a Product worth considering.