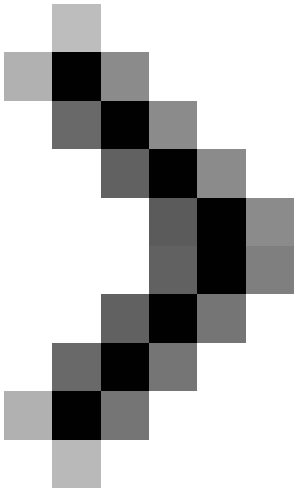
Instructions for using FreeRADIUS for Wi-Fi authentication - Part 2

In this article, I will show you how to open the CentOS firewall and configure access points (APs).



Instructions for using FreeRADIUS for Wi-Fi authentication - Part 1
In Part 1 of this series, I have shown you how to install FreeRADIUS to perform 802.1 X / PEAP authentication, with the aim to run WPA or WPA2 Enterprise encryption on a Wi-Fi network . We have loaded a PC with CentOS 5.3 and installed FreeRADIUS version 2.1.6. In addition, we have created a number of user accounts and have entered some details of the AP.

In this article, I will show you how to open the CentOS firewall and configure access points (APs). The next is to distribute the CA file to all computers and configure them with authentication and encryption settings. Finally, set up SQL so you can store AP information and user information in a database instead of text files.

Open the firewall

CentOS has an attached firewall enabled by default. In order for RADIUS traffic to reach FreeRADIUS, you must open the ports it uses. Click **System** > **Administration** > **Security Level** and **Firewall** . Then click the arrow to expand the **Other Ports** section. Add UDP ports 1812 and 1813 and then click **Apply** .

Restart the server to load new settings

If you make configuration changes while FreeRADIUS is running, then you must restart the server for your changes to take effect. To *stop* the server, go to the terminal window and press **Ctrl + C.** Then type ' **/ usr / sbin / radiusd -X** ' again (or press the up arrow key) to start the restart process. If you are opening a new terminal window, you must type **'su'** first to run in root mode.

Now the server will run and prepare to accept authentication requests from Wi-Fi users.

When your encrypted network works, you can skip ' **–X** ' to start FreeRADIUS without debugging. The server will work in the background and you can refer to the log files and data interpretation.

Configure the AP

This is also when you can configure APs. After setting them up to use WPA (TKIP) or WPA2 (AES) Enterprise encryption, you must enter the RADIUS settings. These settings include the IP address of the FreeRADIUS machine, the port (1812), and the secrets you defined for some AP. Most APs support explanations to store session information. If you need an explanation, you must enter the same details of the server with port 1813.

Install CA file on all computers

Although the PEAP authentication protocol does not require client certificates, you must still install a certificate for the Certificate Authority (CA) on each computer. This is because we will use the self-signed certificate for the server instead of buying a signed certificate from a CA that Windows can recognize, such as VeriSign or GoDaddy.

You need to copy the ***etc / raddb / certs / ca.der file*** to all computers. You can copy it to a USB drive and paste it into each computer. To copy, open a new terminal and type " **su** " to enter root mode, or use an existing mode, and run a copy command, such as "c **p / etc / raddb / certs /ca.der / *newlocation* / certs** ".

Tip: To find the path to the device, such as USB, click **Places** > **Computer** , open the device and right-click any file on the device, then select **Properties** and copy the **Location** value.

Now, on each Windows computer, right-click the certificate file and select **Install Certificate** . Then place it in the **Trusted Root Certification Authorities** repository. On the confirmation dialog, select **Yes** to install.

Configure computers with authentication and encryption settings

On WEP and WPA / WPA2-personal networks, you only select the network and will be prompted for the key. Although connecting to enterprise encrypted networks is more complicated in configuration, once configured, you can simply connect to the network by entering a username and password, even if you have You can save this

information so you don't have to enter it multiple times.

If no profile exists in the network, you need to create a new profile. Then configure the settings. Remember, you are using WPA (TKIP) or WPA2 (AES) Enterprise encryption with PEAP authentication. In the PEAP properties dialog, you need to choose to validate the server certificate and select the certificate you imported. In addition, you can enter the server's IP address to use when validating. Then ensure that you use the Password method (EAP-MSCHAP v2). Click the Configure button to ensure (*Automatically use my Windows logon name and password*) settings on the dialog box not checked.

It should be noted that, the first time you connect to the network, the Validate Server Certificate dialog box will appear, sometimes it can hide behind other windows. Then click Ok to accept the certificate and continue connecting.

Set up SQL for users and look up APs

If you have a large number of users and APs, or you change their details or APs on a regular basis, then you can use a database to store information. instead of text files. You can install and configure your server or use a hosted server, for example from a website provider. Either way, you must install the FreeRADIUS MySQL package (freeradius2-mysql).

Now you need to load the default database structure into the database server. If you are running your server in CentOS, run the " **mysql -uroot -prootpass radius " from a Terminal.** If you use a remote server or host hosted from a provider, then run " **gedit** " with a root Terminal and use the Text Editor to open ***etc / raddb / sql / mysql / schema.sql*** . Then *copy* and *paste* the SQL commands into the server to run them.

If you want to use SQL for details of the AP, load the ***etc / raddb / sql / mysql / nas.sql file*** into your database.

You need to edit the FreeRADIUS configuration files to tell the server to use SQL. From the root Text Editor ,, open ***etc / raddb / radiusd.conf*** and do not comment the line **"$ INCLUDE sql.conf** ". Open ***etc / raddb / sites-enabled / inner-tunnel*** and do not comment " **sql** " from **Authorize** . Now FreeRADIUS will use files and SQL.

You need to give FreeRADIUS a database connection and login details. From the original editor, open ***etc / raddb / sql.conf*** . Then make sure **database = 'mysql'** . If you are using a remote database or a preconfigured database, enter the server address. Make sure you enter the Username and Password for your server. With the **radius_db value** , enter the database name. If you are using SQL for AP details, do not comment " **readclients = yes** ".

Finally, insert rows into the table to define user accounts. The format is similar to the format for user files:

username attribute op value
egeier Cleartext-Password: = pass123

Here is an example of what you can insert into the table for information about the AP if enabled:

shortname nasname type secret
192.168.0.1 private-network-1 other testing123

Troubleshoot

Note that during server setup or after making changes, use debug mode to see server actions. If you encounter logon or connection problems, check carefully and debug the section and analyze recent changes.

You finished reading the article "**Instructions for using FreeRADIUS for Wi-Fi authentication - Part 2**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
