WPA + EAP-TLS + RADIUS
Aplicado

Toni de la Fuente Díaz
toni@blyx.com
http://blyx.com

Resumen:

Confiuración de una infraestructura WiFi segura usando protocolos que nos aportan fiabilidad en las comunicaciones, auntenticación y control de usuarios. Veremos como configurar un servidor RADIUS en Linux con el software FreeRADIUS soportando EAP-TLS así como configurar 802.1x en un punto de acceso wireless y un ejemplo de configuración en cliente final.

Palabras clave: WPA, RADIUS, EAP-TLS

1. Objetivos:

Vamos a configurar una red wifi segura usando certificados de cliente y servidor para la autenticación. Para montar la red necesitamos:

-Tener ganas (importante).
-Un servidor RADIUS.
-Un AP con soporte WPA y EAP (802.1X)
-Un cliente wifi.

Como servidor RADIUS vamos a utilizar Linux Fedora Core 2 con el sistema de instalación de paquetes apt y como software RADIUS usaremos FreeRADIUS.

El AP (Access Point) será un Dlink 2000AP+ (802.11b/g) con la última versión de firmware instalada para tener soporte WPA en el dispositivo. Hay que tener en cuenta que este hardware se fabricó sin tener en cuenta WPA así que se ha añadido dicha funcionalidad en el firmware por lo que no soportará muchos clientes.

El cliente usado será un portátil con MAC OS X (10.4) cuyo soporte WPA está incluido de forma nativa. No obstante se indican sitios de referencia para configurar otros sistemas operativos.

2. Preparando el sistema, instalación de apt para Fedora:

Instalación de apt para Fedora Core 2
wget http://ftp.freshrpms.net/pub/freshrpms/fedora/linux/2/apt/apt-0.5.15cnc6-1.1.fc2.fr.i386.rpm

rpm -hiv apt-0.5.15cnc6-1.1.fc2.fr.i386.rpm

Ampliamos la lista de repositorios
vi /etc/apt/sources.list.d/dag.list
rpm http://apt.sw.be fedora/2/en/i386 dag

apt-get update

3. Instalación y configuración de FreeRADIUS, el cliente RADIUS y utilidades OpenSSL:

apt-get install freeradius radiusclient openssl-perl

Hacemos que FreeRADIUS se inicie cada vez que arranca el sistema operativo:

chkconfig radiusd on

Todos los archivos de configuración de FreeRADIUS se encuentran en:
/etc/raddb/

Cabe destacar los siguientes archivos de configuración:
radiusd.conf - Archivo general de configuración de FreeRADIUS y del daemon.

eap.conf – Archivo de configuración de las directivas EAP a utilizar. Es un *include* de radiusd.conf

clients.conf – Descripción y credenciales de los diferentes dispositivos que consultan al RADIUS (Aps, NAS, etc).

users – Archivo donde se especifican las credenciales de los usuarios de la red. Se usa este archivo si no existe otro backend para el almacenamiento de los usuarios.

He subido a mi sitio web un tar.gz con todos los archivos de configuración, certificados y scripts para crear los certificados (de CA, de servidor y de clientes), puedes descargar el paquete de la siguiente forma:

wget http://blyx.com/public/wireless/wpa+eap-tls+radius/raddb.tar.gz

Copiamos los archivos descargados a su ubicación original, es decir, /etc/raddb.

Al estar basándonos en la arquitectura PKI, necesitamos generar un conjunto de certificados basados en el modelo cliente/servidor que funcionarán como armazón del proceso de autenticación. Esto significa que debemos crear una Autoridad de Certificación (CA) y generar los certificados tanto para el servidor como para cada cliente.

Vamos a crear los certificados:

Para crear la CA y los certificados se pueden usar los scripts que aparecen en la web http://www.alphacore.net/contrib/nantes-wireless/eap-tls-HOWTO.html.
No obstante, como he dicho antes, están disponibles en el raddb.tar.gz que hemos descargado previamente.

Después de generar los certificados deberemos copiar los archivos root.der y toni.p12 (o el <usuario_que_sea>.p12) al ordenador del cliente e instalarlos, esto lo veremos más adelante.

Para configurar el servidor RADIUS utilizaremos root.pem y radius.blyx.com.pem (o el <nombre_del_servidor>.pem)

Ahora vamos a probar que la configuración del servidor RADIUS la hemos hecho de forma correcta:

radiusd -X
Ready to process requests.

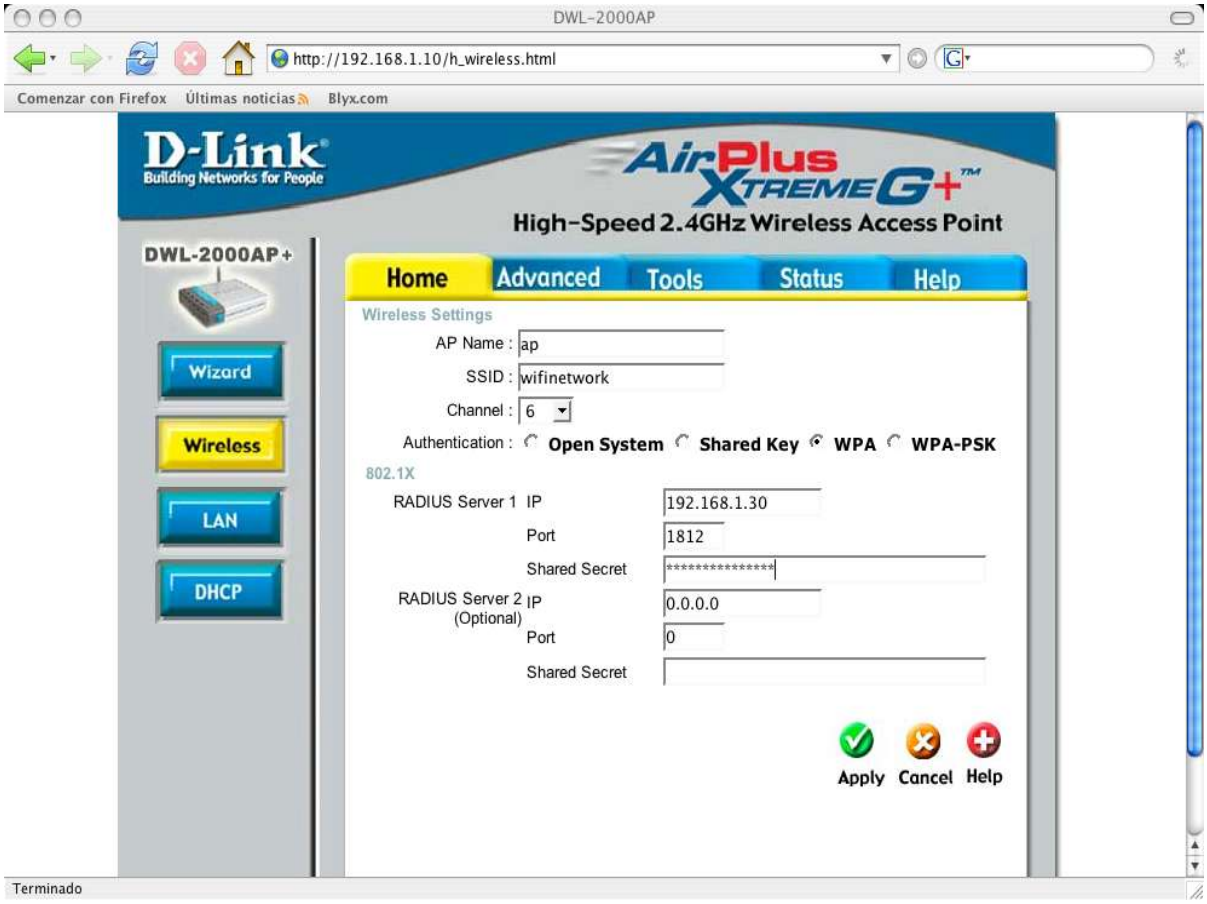
Si todo ha ido bien, pulsamos Ctl+C y arrancamos el servicio:
/etc/init.d/radiusd start

Podemos ver los logs del servidor de la siguiente forma:
tail -f /var/log/radius/radius.log

4. Configuración del AP:

Activamos la configuración en el AP. Seleccionamos WPA, indicamos la IP del servidor RADIUS (recuerda hay que abrir los puertos 1812/UDP y 1813/UDP en el firewall local del servidor RADIUS). **SharedSecret** es el valor que le hemos dado al atributo ***secret*** que se encuentra en el archivo **clients.conf**, en nuestro caso usaremos **laboratorio2005**. Esta clave es usada para cifrar la comunicación entre el cliente RADIUS (AP) y el servidor RADIUS. Como ves, es posible añadir otro servidor RADIUS para

usarlo como *failover*, es decir, en caso de no estar disponible el primero usaría el segundo.



5. El cliente:

No todas las tarjetas wifi soportan WPA (depende del firmware y/o hardware) y 802.1X así que puedes comprobar la tuya en la siguiente dirección:
http://wireless.utah.edu/cgi-bin/dot1x/dot1xCompatibility.pl

En este caso vamos a ver como configurar un cliente Mac OS X 10.4 sobre un PowerBook G4, ya que la tarjeta wifi interna de este portátil soporta WPA de forma nativa así como el SO versión superior o igual a 10.3.8.

La configuración de clientes para acceso a redes 802.1X – EAP-TLS es un poco mas "entretenida" que otras variantes de EAP y es soportada por Linux, Mac OS X, FreeBSD, Solaris y Windows XP SP2, unos de forma nativa y otros con un cliente específico:

Mac OS X:
- -Soporte nativo del sistema.
- -AEGIS Client http://www.mtghouse.com

Linux:
- -Xsupplicant: http://www.open1x.org/
- -AEGIS Client http://www.mtghouse.com
- -wpa_supplicant http://hostap.epitest.fi/wpa_supplicant

FreeBSD:
- -PANA: http://www.opendiameter.org/

Windows:
- -Soporte nativo del sistema Windows XP SP2.

-WIRE1x: http://wire.cs.nthu.edu.tw/wire1x/
-AEGIS Client (98/CE/Me/2K/NT4) http://www.mtghouse.com

Solaris:
-AEGIS Client http://www.mtghouse.com

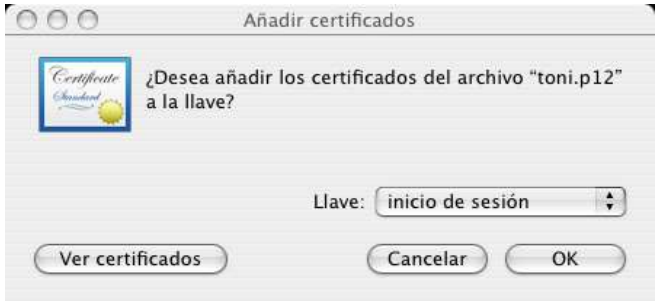
6. Configuración del cliente Mac OS X 10.4:

6.1. Certificados del cliente:

Vamos a configurar el cliente en nuestro flamante Tiger.

Lo primero que debemos hacer es copiar a nuestra máquina cliente los ficheros creados anteriormente en el servidor RADIUS, estos ficheros son: toni.p12 y root.der. La forma más segura es a través de SSH.

Ahora vamos a instalar el certificado de usuario. Hacemos doble click en el archivo toni.p12 y se nos abrirá la siguiente ventana que forma parte de la aplicación "Acceso a llaves":



Aceptamos el certificado "OK" y a continuación introducimos la clave con la que hemos generado el certificado, si analizamos los scripts de creación podemos ver que esta clave es "whatever" (la podemos cambiar, por supuesto). Pinchamos en "OK".

Ahora debemos crear un certificado para unificar la autenticación basada en certificados. Para ello pinchamos en Archivo -> Nueva llave...

Asignamos contraseña a la llave:

Arrastra la Clave privada que está en “Inicio de sesión” -> “Claves” a la llave que hemos creado “Llave de toni”

6.2. Configurar la conexión 802.1X (EAP-TLS)

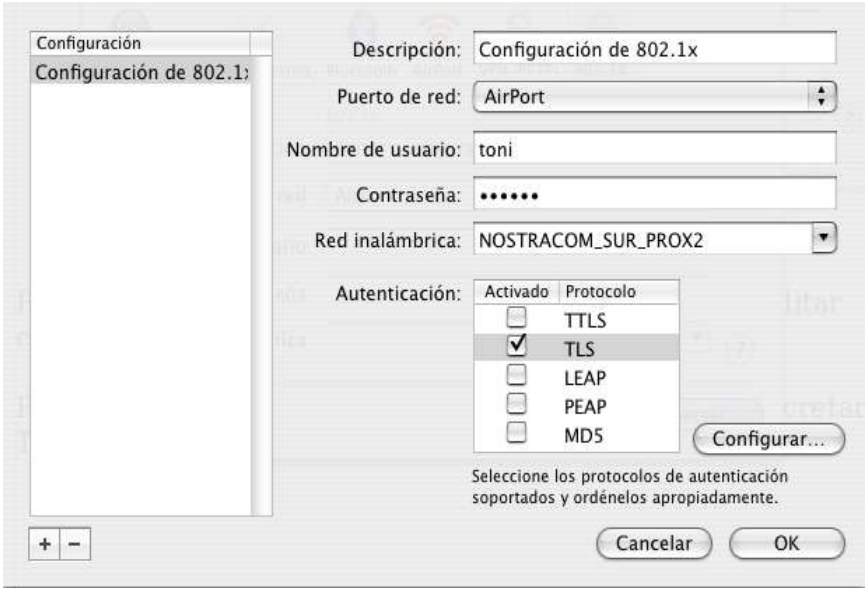
Aplicaciones -> Conexión a Internet

Pincha en Archivo -> Nueva conexión 802.1X...

Ahora podemos ver en la ventada “Conexión a Internet” un nuevo item llamado “802.1X”:

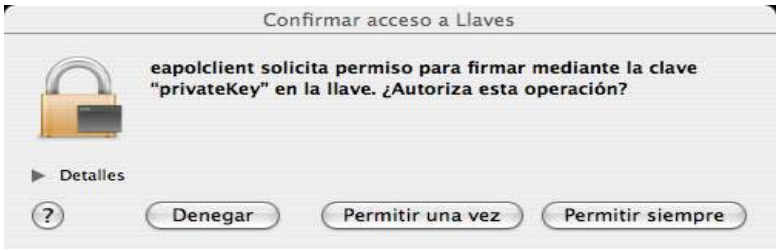
Pinchamos en “Configuración de 802.1x” y luego en “Editar configuraciones...”

Podemos ver que Tiger soporta varios tipos de EAP, concretamente, TTLS, TLS, LEAP, PEAP y MD5. Nosotros usaremos TLS.



Indicamos el nombre de usuario para el cual hemos generado el certificado, la contraseña con la que ciframos el certificado “whatever”, seleccionamos el punto de acceso al que queremos acceder, en mi

caso “NOSTRACOM_SUR_PROX2”, seleccionamos el método de autenticación y activamos TLS. Para seleccionar el certificado que vamos a usar pinchamos en “Configurar...” y seleccionamos nuestro certificado, en mi caso “toni”. Aceptamos pinchando en “OK” y luego “Conectar”.



Pinchamos en “Permitir siempre”

Nos configuramos una IP, si no tenemos DHCP configurado y listo ;-)

Referencias:

Wi-Foo: The secrets of wireless hacking. Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. http://www.wi-foo.com
http://www.freeradius.org/doc/EAPTLS.pdf
http://www.missl.cs.umd.edu/wireless/eaptls/?tag=missl-802-1
http://www.alphacore.net/contrib/nantes-wireless/eap-tls-HOWTO.html
http://www.fi.infn.it/system/WiFi/802.1X/macosx/
http://www.dartmouth.edu/~pkilab/greenpass/gp-web-images/internetconnect2.png
http://www.alphacore.net/spipen/article.php3?id_article=1
http://oriol.joor.net/blog-dev/?itemid=1574