Universidad Técnica Federico Santa María

Departamento de Electrónica

Informe de Proyecto: Autenticación de redes a través de 802.1x

ELO-322

Integrantes:

Gian Carlo Espinaza

Carlos Rosas

Samuel Sabaini

Profesor:

Agustín González

INTRODUCCION

El presente informe tiene como objetivo explicar lo que se entiende por autenticación de redes a través de el protocolo 802.1x y a su vez proporcionar un pequeño manual acerca de la configuración de un servidor Radius en el sistema operativo freeBSD para la autenticación de una red wifi doméstica.

El sistema operativo freeBSD será virtualizado a través del software VMware para trabajar sobre plataforma UNIX y Windows a la vez.

El objetivo es analizar los diferentes componentes necesarios para desarrollar un sistema de control de acceso a redes inalámbricas basado en autenticación y autorización.

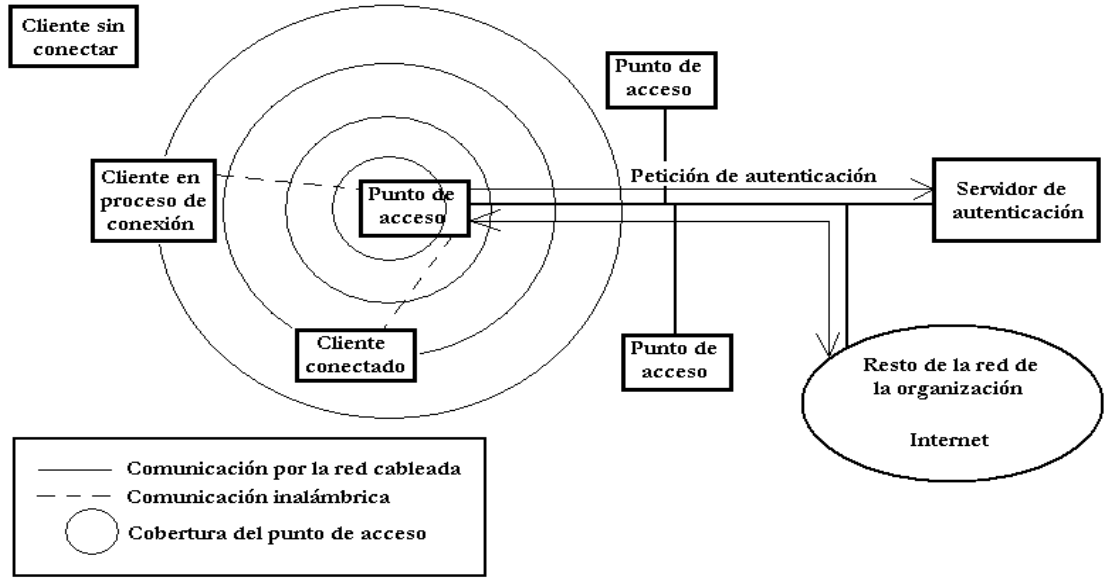
¿QUE ES LA AUTENTICACION DE REDES A TRAVES DE 802.1X?

A grandes rasgos, el estándar 802.1x trata de una arquitectura de control de acceso para redes inalámbricas. Este sistema hace uso de certificados digitales para proporcionar a los usuarios tanto servicios de autenticación como de autorización, gestionando confiabilidad en la comunicación.

802.1X plantea un escenario con tres entidades básicas como son el cliente, el elemento que proporciona la conectividad a la red (punto de acceso) y el servidor de autenticación encargado de averiguar si un determinado cliente ha sido autorizado a hacer uso de dicha red.

Para que un usuario pueda realizar la autenticación, a éste se le debe conceder un certificado digital, los cuales permiten que un usuario desconocido para el sistema pueda hacer uso de la red con solo proporcionarle el certificado adecuado. Además en este certificado pueden incluirse ciertos atributos acerca del usuario, como el tiempo máximo que puede utilizar la red, los servicios a los que puede acceder o los recursos que puede utilizar.

A continuación se muestra un esquema del proceso que se lleva a cabo para la autenticación del usuario:



Este proceso consta básicamente de tres fases: autenticación, autorización y distribución de la clave de cifrado.

Fase de autenticación

La primera fase funciona siguiendo el estándar IEEE 802.1X, es decir, cuando el cliente entra en el área de cobertura del punto de acceso, este le pide su identidad, y el cliente se la proporciona. Tras esta fase inicial se realiza el proceso de establecimiento de conexión entre los extremos, donde según el estándar tanto el cliente como el servidor de autenticación se autentican mutuamente mediante certificados.

Fase de autorización
En esta fase, el cliente indica al servidor de autenticación cual es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados que demuestran que dicho usuario está autorizado a realizar el uso de la red que pide. Entonces el servidor evalúa los certificados y comprueba si todo es correcto y si el nivel de privilegios del cliente es el necesario, continuando con el protocolo si todo va bien y desautorizando al cliente a acceder a la red si hay algún problema.

Fase de distribución de clave
En esta fase del protocolo, únicamente participan el punto de acceso y el servidor de autenticación, y consiste en que éste último le pase al primero un descriptor de la clave que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca.

RADIUS:

Es el tipo de servidor que se utiliza para la autenticación de redes.

El servidor RADIUS puede autenticar ya sea a los usuarios (ejemplos son contraseña de usuario y certificado de usuario) o el sistema (normalmente, dirección MAC o certificado de equipo)..

RADIUS constituye un conjunto de estándares que controla la autenticación, la autorización y la contabilidad (AAA). RADIUS incluye un proceso proxy para validar clientes en los entornos con varios servidores.

Manual para configuración servidor Radius

Lo primero a realizar es la virtualización del sistema operativo freeBSD a través del software VMware, y una vez hecho éste procedimiento se sigue de la siguiente manera una vez instalado freeBSD en nuestra máquina virtual.

Configuración de los servidores

Descarga e instalación mediante ports de FreeRadius.

La instalación de freeRadius es de la siguiente manera.

 # cd /user/ports/net/freeradius/ ; make install clean

Se configura la instalación agregando el modulo de compatibilidad con mysql.
Para comprobar la correcta instalación ejecutamos freeRadius con el siguiente comando:
 # radiusd -x

Descarga e instalación mediante ports de Mysql.

Msql con la instalación de freeRadius se logra instalar pero no de la mejor forma por eso se reinstala mediante ports.

 # cd /user/ports/databases/msql50-server/ ; make reinstall

Crear la base de datos.

Para la creación de la base de datos de radius se utiliza el motor de base de datos mysql, ejecutando el siguiente comando.

 # mysql

Una vez adentro del motor mysql se genera la base de dato de radius y se le asigna los privilegios al usuario root:

mysql> connect radius;
mysql> \. /usr/ports/net/freeRadius-mysql/work/freeradius-1.1.7/doc/examples/mysql.sql

Configuración de mysql:

mysql> insert into radgroupcheck values (“”, “autenticacion”, ”Auth-Type”,“:=”,“EAP”);
mysql> insert into radgroupcheck values (“”, “autenticacion”, “Framed-Protocol”, “:=”, “PPP”);
mysql> insert into radgroupcheck values (“”, “autenticacion”, “Service-Type”, “:=”, “Framed-User”);
mysql> insert into radgroupcheck values (“”, “autenticacion”, “Framed-Compression”, “:=”, “Van-Jacobsen-TCP-IP”);
mysql> insert into radgroupcheck values (“”, “autenticacion”, “Tunnel-Medium-Type”, “:=”, “6”);
mysql> insert into radgroupcheck values (“”, “autenticacion”, “Tunnel -Type”, “:=”, “13”);
mysql> insert into radgroupcheck values (“”, “autenticacion”, “Tunnel-Private-Group”, “:=”, “4”);
mysql> insert into usergroup values (“Carlos”, “autenticacion”,””);
mysql> insert into radcheck values (“”,“Carlos”, “Password”, “==”, “elo322”);
mysql> insert into radreply values (“”, “Carlos”, “Framed-IP-Address”, “:=”, “192.168.1.102”);

Configuración de freeRadius:

Para que freeRadius interactúe con mysql hay que configurar los archivos de freeRadius que se encuentran en /usr/local/etc/rabddb.

Primero se configura el archivo de cliente (clients.conf), el cual va a recibir la petición de los accesspoint o router en este caso.
Al final del archivo se agregan las siguientes líneas:

client 192.168.3.1{
secret = radiusELO322 % secret es la clave entre el servidor radius y el router.
shortname = router
}

Una vez configurado los clientes se procede a la configuración de la base de datos que se encuentra en la carpeta sql.conf. Se modifican las líneas de comando para que se pueda comunicar con la base de datos.
 # Connect info
server = "localhost"
login = "radius"
password = ""

 # Database table configuration
radius_db = "radius"
Se configura el archivo de radius.conf para que utilice la base de datos que creamos. Para esto se descomentan las líneas que se muestran a continuación en el archivo:

```
  authorize {
  preprocess
  chap
  mschap
  suffix
  eap
  sql
}
authenticate {
  Auth-Type PAP {
          pap
  }
  Auth-Type CHAP {
          chap
  }
  Auth-Type MS-CHAP {
          mschap
  }
eap
}
preacct {
  preprocess
  acct_unique
  suffix
}
accounting {
  detail
  radutmp
  sql
}
session {
  radutmp
  sql
}
post-auth {

sql
}
pre-proxy {
}
post-proxy {
  eap
}
```

Creación de certificados para EAP/PEAP.

Para la creación del certificado se utiliza el programa openssl-stable y los script que vienen en freeRadius. Solo hay que modificar y ejecutar.
Antes de crear los certificados hay que instalar openssl, mediante ports.
Se instala openssl-stable mediante el siguiente código:

 # cd /user/ports/security/openssl-stable ; make install

Luego de esto se modifican los archivos del script de freeradius, para que encuentren el programa openssl.
Se modifica lo siguiente en el archivo **CA.all.** (Ubicado en: /usr/ports/net/freeradius-mysql/work/freeraidus-1.1.7/scripts/):
SSL=/usr/local/openssl
echo "newreq.pem" | /usr/local/openssl/misc/CA.pl –newca

Se modifica lo siguiente en el archivo **certs.sh** (ubicado en: /usr/ports/net/freeradius-mysql/work/freeraidus-1.1.7/scripts/):

["$SSL"= ""] && SSL=/usr/local/openssl
/usr/local/bin/openssl gendh > dh

En el archivo **CA.certs** se modifican las siguientes líneas de comandos y se agregan los datos personales para generar el certificado.
["$SSL"= ""] && SSL=/usr/local/openssl

Se ejecuta el script para generar el certificado digital de la siguiente forma:
./ certs.sh
O bien si se está en otro directorio se procede de la siguiente manera:
#sh /user/ports/net/freeradius/work/freeradius-1.1.7/scripts/certs.sh

Por medio de un script para subir archivos a internet se puede enviar el certificado digital a nuestra página ELO y posteriormente descargar éste archivo

Habilitación de certificados

Una vez creados el certificado hay que habilitar a freeradius para que lo pueda leer. Para esto se configuran dos archivos: eap.conf y radiusd.conf.
El archivo eap.conf se deja de la siguiente forma:

```
eap {
default_eap_type = eap
timer_expire     = 60
tls {
private_key_password = lala
private_key_file = ${raddbdir}/certs/cert-srv.pem
certificate_file = ${raddbdir}/certs/cert-srv.pem
CA_file = ${raddbdir}/certs/demoCA/cacert.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
```

}

peap {
default_eap_type = mschapv2
}
mschapv2 {
}
}
En el archivo radiusd.conf solo modificamos la siguiente línea:
modules {
$INCLUDE ${confdir}/eap.conf
mschap {
}
}
Para comprobar el funcionamiento correcto del servidor freeradius ejecutamos radius.
 # radiusd –x

Habilitar el estándar 802.1x a los PC.
Se copia el certificado en el pc y se guarda en "Entidades emisoras raíz de confianza".

Configurar red inalámbrica.
Se va a la administración de redes inalámbricas de Windows y se selecciona la red y se va a opciones avanzadas.
Se agrega nueva red con las siguientes especificaciones:
Autentificación de red WPA
Cifrado TKIP
Tipo de EAP EAP protegido por (PEAP)
Luego vamos a configuraciones de Tipo de EAP y se selecciona certificado de la red.

Conclusión

La seguridad es un requisito en estos tiempos y como se apreció en este trabajo con un poco de conocimiento y aprendizaje se puede configurar un sistema seguro.

Este sistema de autentificación esta implementado en todos los dispositivos en que este estándar utiliza. Por esto la seguridad está al alcance de cualquiera que desee utilizarlo.

Este estándar autentifica al usuario para mejorar la seguridad y otorgando acceso solo al usuario permitido.

Referencias:

http://www.freebsd.org/
http://www.forat.info/2006/08/11/instalacion-de-mysql-server/
http://www.ecualug.org/files/07%20-%20NcN_2005_WPA_EAP-TLS_RADIUS_Aplicado.pdf
http://wiki.freeradius.org/SQL_HOWTO
http://itdump.wordpress.com/2007/11/23/how-to-setup-port-based-authentication-on-cisco-switch-with-samba-in-debian/
http://personales.alumno.upv.es/~hecmargi/manuales/linux/freeradius/