INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría

ELECTRICAL AND ELECTRONICS ENGINEERING

Implementation of network access control by using authentication, authorization and accounting protocols

José R. Arana[*], Leandro A. Villa[**], Oscar Polanco[§]**

** Levicom Argentina SRL, Carvajal Tecnología y Servicios.***
Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle.
jose.arana@outlook.com, leandro.villa@correounivalle.edu.co,
§ oscar.polanco@correounivalle.edu.co

(Recibido: Mayo 28 de 2012 - Aceptado: Mayo 16 de 2013)

RESUMEN

Este artículo presenta el diseño e implementación de un sistema de control de acceso a la red que proporciona el servicio de Autenticación, Autorización y Auditoría (AAA) usando software libre, empleando los protocolos estándar IEEE 802.1x y RADIUS, con base en una infraestructura de clave pública, un servicio de directorio centralizado que almacena las políticas de seguridad para cada usuario y una base de datos MySQL en donde se registranlos eventos del servicio AAA; todo esto se probó en un ambiente corporativo con 300 estaciones de trabajo. En el sistema se logró: tres métodos de autenticación mediante el uso de EAP-TLS, PEAP y EAP TTLS; la administración segura de la información, concerniente a los usuarios que pueden acceder la red y los permisos que cada uno de ellos posee; el uso de certificados digitales para demostrar la identidad de un usuario o de un equipo que ejecute cualquiera de los sistemas operativos más populares. También se ha configurado un servidor RADIUS para que use dos puntos de información de políticas; un servidor de directorio OpenLDAP y el Directorio Activo de Microsoft. Lo anterior posibilita un control de acceso a red escalable, sin demandar un alto presupuesto.

***Palabras clave**: Control de acceso, Autenticación, Autorización, Auditoría.*

ABSTRACT

This paper presents the design and implementation of a network access control system which provides the Authentication, Authorization and Accounting (AAA) service using GNU Licensed Software, employing the standard protocols IEEE 802.1x and RADIUS, based on a Public Key Infrastructure (PKI), a centralized directory service, which stores the security policies assigned to each user, and a MySQL database, where the authentication events of the AAA service are registered, all of this was tested in a production corporate environment with 300 workstations. On the system, it was achieved: three authentication methods by using EAP-TLS, PEAP and EAP TTLS; secure management of information, in a central database, about users that can access the network and the privileges that each of them own; use of digital certificates to prove the identity of a user or network device running any of the popular operating systems. Also has been configured a RADIUS Server to use two points of policy information, one of them is the OpenLDAP directory server, the other is the Active Directory from Microsoft. This enables a scalable network access control, without demanding a high budget.

***Keywords**: Access Control, Authentication, Authorization, Accounting.*

1. Introducción

Las compañías están cada vez más basando sus modelos de negocios en proveer acceso a recursos. Estos recursos pueden ser páginas Web, acceso a Internet, cuentas de correo electrónico, o cualquier activo de información que necesite estar protegido o controlado.

¿Cómo puede un usuario indicarle a un sistema (especialmente a uno que por defecto no confía en nadie) que él está autorizado a usar determinados servicios computacionales? ¿Cómo puede el propietario de un sistema marginar a los usuarios no autorizados, mientras provee acceso cómodo a los usuarios autorizados? El trasfondo a estos dos interrogantes es: con las fallas de seguridad en los diferentes protocolos y aplicaciones, y con un entorno de Internet público hostil, debería existir algún mecanismo mediante el cual un usuario autorizado pueda usar los recursos a los que tiene derecho, dejando a los usuarios no autorizados sin acceso. Éste es el propósito de la autenticación, autorización y auditoría de redes, es decir, diferenciar, asegurar y auditar a los usuarios. Actualmente se cuenta con herramientas basadas tanto en software comercial Bhaiji (2008) y Qazi (2007) como libre Arana (2010) para realizar estas tareas. El presente artículo se apoya principalmente en el uso de software libre para plantear el diseño e implementación de una infraestructura de red TCP/IP básica y escalable, cuyas funciones son: proporcionar el servicio de autenticación, autorización y auditoría (AAA) Yago (2009), Nakhjiri (2005); usar el protocolo 802.1x Geier (2008) entre una estación cliente y el punto de ejecución de políticas (PEP); usar el protocolo RADIUS Rigney et al. (2000) y Rigney (2000) entre el PEP y el punto de decisión de políticas (PDP). Lo anterior, aplicado en un ambiente corporativo real con múltiples sitios geográficamente distantes, interconectados bajo una red de área amplia.

La figura 1 presenta la red TCP/IP prototipo diseñada e implementada con el objetivo de proporcionar el servicio AAA de manera escalable y que permite: tener varios métodos

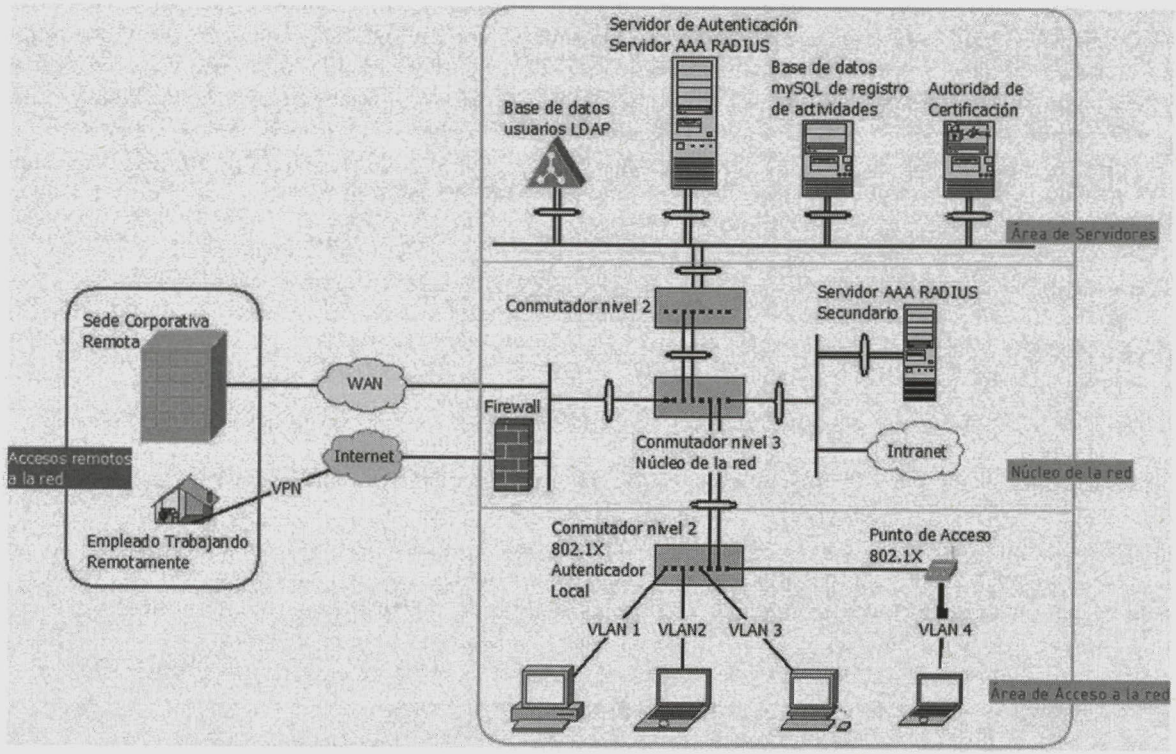

Figura 1. *Red prototipo que permite proporcionar el servicio AAA.*

de autenticación acordes con las políticas que el administrador de la red desee instituir, mediante el uso de EAP-TLS Simon et al. (2008), PEAP y EAP TTLS; la consulta de información, en una base de datos central, acerca de los usuarios que pueden acceder la red y los permisos que cada uno de ellos posee; el uso de certificados digitales para demostrar la identidad de un usuario o de un equipo. El diseño considera un aislamiento fuerte entre los equipos a ser autenticados para ingresar a la red y los servidores que proveen el servicio AAA, esto con el fin de evitar al máximo posibles ataques contra estos equipos de misión crítica. También, para que la red sea robusta y tolerante a fallas de conectividad, los equipos de misión crítica que proporcionan el servicio AAA deben tener redundancia en sus enlaces, principalmente los equipos que tienen el Directorio de usuarios y el Servidor RADIUS, ya que, sin estos, ningún usuario podría ingresar a la red. Además, es deseable que cada departamento o grupo dentro de una empresa esté separado por medio de VLAN, lo cual permite proteger la información confidencial que cada uno posee. Una buena práctica que siempre se debería llevar a cabo es la de asignar una VLAN separada para los visitantes, configurar dicha VLAN con restricciones muy estrictas para acceder a Internet e impedir su acceso a la Intranet.

2. Metodología

El Servidor FreeRADIUS y todas las demás herramientas que permiten implementar una red con el servicio de autenticación, autorización y auditoría se configuraron en un computador de escritorio de una agencia de publicidad, la cual tiene sus unidades de negocio en tres ciudades (Cali, Bogotá y Medellín), en un entorno de 300 estaciones de trabajo (50 en Cali, 100 en Medellín, 150 en Bogotá). El equipo se conectó a la infraestructura de red en la sede de Cali, la cual está interconectada con las sedes de Bogotá y Medellín por una red WAN. En la ciudad de Bogotá también se configuró un Servidor RADIUS en una máquina virtual con sistema operativo Ubuntu versión 10.4.

A continuación se describen los pasos que se siguieron para habilitar dicho servicio.

2.1 Autenticación

Para el sistema de autenticación, autorización y auditoría de redes se instaló FreeRADIUS versión 2.1.7, el cual se configuró para permitir tres tipos de autenticación: Certificados digitales (EAP-TLS) Roser (2002), EAP protegido (PEAP) y EAP TTLS. El usuario que desee ingresar a la red podrá usar alguno de estos tres métodos de autenticación, escogiendo el que mejor se ajuste a las características de su equipo o el que el administrador de red haya definido por defecto para el acceso a la red. A continuación se ilustran los tipos de autenticación configurados.

2.1.1 Configuración para usar certificados digitales de identificación personal (EAP-TLS)

Se implementó una Autoridad de Certificación mediante la herramienta libre OpenSSL, la cual es la encargada de emitir todos los certificados digitales de los dispositivos de red o usuarios que requieran comprobar sus identidades ante otros equipos. Para que la estación de un usuario pueda establecer confianza con la Autoridad de Certificación de la red y, como consecuencia, aceptar y confiar en los dispositivos de red que la autoridad ha certificado, es necesario que dicha estación tenga instalado el certificado raíz de confianza de la Autoridad de Certificación, pudiendo así comprobar la validez de un certificado digital de identificación de un tercero, que en este caso será el del servidor de autenticación RADIUS, es decir, el punto de decisión de políticas.

Al tener una Autoridad de Certificación y usar certificados digitales dentro de la red, se puede implementar autenticación mutua, eliminando la posibilidad de que un atacante obtenga los datos de un usuario, por ejemplo, cuando el atacante simule ser el servidor RADIUS. La figura 2 muestra el certificado del servidor Radius instalado en una estación MAC OSX (en general, los tres tipos de autenticación fueron probados para los sistemas operativos MAC OSX, Linux y Microsoft Windows).

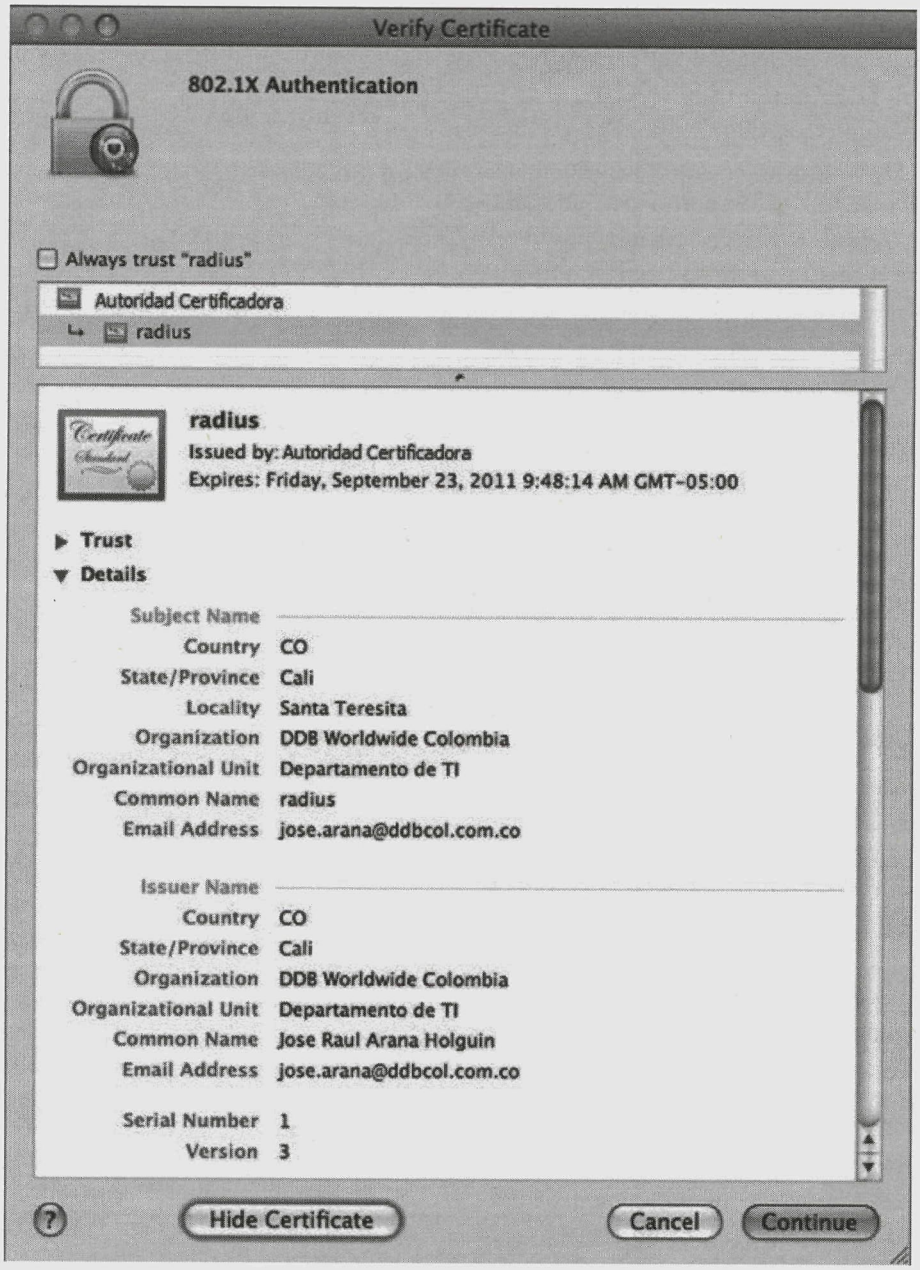

Figura 2. *Certificado digital del Servidor RADIUS instalado en una estación MAC OSX.*

2.1.2 Configuración para usar nombre de usuario y contraseña con EAP Protegido (PEAP)

Se configuraron los parámetros de red en las estaciones clientes a las que se les permite el acceso, esto con el propósito de que establezcan conexión solamente con el punto de ejecución de políticas que presente la identidad del servidor RADIUS (mediante un certificado digital expedido por la Autoridad de Certificación). El servidor RADIUS verificará las credenciales de la estación cliente. También se configuró el servidor RADIUS para que tenga dos tipos de servidores de directorio centralizado como puntos de información de políticas: OpenLDAP (licencia GNU) y Directorio Activo (AD) de Microsoft. El uso de OpenLDAP permite otorgar los permisos

que tiene cada usuario en la red, puesto que este servidor de directorio tiene los pares atributo-valor necesarios para informar al servidor RADIUS a qué VLAN será direccionado el usuario.

2.1.3 Configuración para usar nombre de usuario y contraseña empleando EAP dentro de un Túnel Seguro en la Capa de Transporte (EAP-TTLS)

Al igual que con EAP-PEAP, se configuraron las estaciones de los usuarios que acceden a la red para que se realice una autenticación mutua antes de hacer el intercambio de credenciales del usuario, de tal forma que no se realice la entrega de credenciales si el punto de ejecución de políticas no presenta un certificado válido del servidor RADIUS.

Los sistemas operativos de Microsoft Windows no tienen compatibilidad por defecto con este tipo de EAP, por lo que fue necesario instalar un software adicional con licencia GNU (con nombre "wpa_supplicant") que administra la conexión inalámbrica. Esto no fue necesario para los demás sistemas operativos probados (MAC OSX y Linux), puesto que tenían compatibilidad por defecto con este tipo de EAP.

2.2 Configuración del punto de ejecución de políticas

2.2.1 Punto de ejecución de políticas de tipo inalámbrico

En el caso de que el punto de ejecución de políticas sea un punto de acceso inalámbrico (AP), para habilitar su operación con el servidor RADIUS, es necesario configurar en el AP la dirección IP y el puerto del servidor Radius.

2.2.2 Punto de ejecución de políticas de tipo cableado

Además de crear las VLAN en el conmutador capa 2 (2950-24 marca Cisco), se habilitó el servicio AAA mediante las siguientes líneas de configuración.
Para usar AAA en la autenticación:

aaa new-model
aaa authentication dot1x default group radius
dot1x system-auth-control

Para habilitar AAA en el puerto de acceso Ethernet (en donde se conecta la estación del usuario):
interface FastEthernet0/2
switchport mode access
dot1x port-control auto

Para configurar la dirección IP y la clave (compartida) del servidor RADIUS:
radius-server host 10.60.60.60 auth-port 1812 acct-port 1813 key secretomuysecreto
Para configurar la dirección IP del conmutador Cisco Catalyst 2950
interface Vlan1
ip address 10.30.30.30 255.255.255.0

En el servidor RADIUS fue necesario autorizar los puntos de ejecución de políticas con permiso para hacer consultas AAA que permitan validar a los usuarios que deseen ingresar a la red. En el archivo "clients.conf" del servidor se ingresaron los PEP autorizados para usar el servidor RADIUS como punto de decisión de políticas; se especificó la dirección IP y el secreto compartido de los PEP (conmutador Ethernet capa 2 y punto de acceso inalámbrico) mediante las siguientes líneas.
client cali {
ipaddr = 10.10.10.10
secret = secretomuysecreto }

2.3 Autorización

La red tiene como punto de información de políticas (PIP) al servidor de directorio OpenLDAP OPENLDAP (2012), en el cual se almacenó la información de los usuarios que desean ingresar a la red. En esta información se encuentran los pares atributo-valor que permiten que el PEP establezca los permisos para cada usuario que se verán reflejados en su asociación a una VLAN determinada, ubicando a cada usuario en una VLAN diferente dependiendo del departamento al que pertenezca; dicha VLAN puede estar configurada con las restricciones que crea conveniente el administrador. También

se usó un atributo-valor que permite restringir el horario en que puede ingresar cada usuario a la red. Si intenta acceder a la red en un horario diferente al establecido en su perfil, la petición será negada. Los pares atributo-valor nombrados son los siguientes:

radiusLoginTime: especifica el horario en el que se tendrá permiso para acceder a la red.

radiusTunnelMediumType: se especifica el estándar que manejará el conmutador de capa 2 que hará la implantación de las políticas para la estación del usuario que ingresa a la red.

radiusTunnelPrivateGroupId: este valor establece la VLAN que se activará para el acceso a la red de determinado usuario.

radiusTunnelType: En este valor se especifica en qué tipo de segmentación lógica de red se harán las restricciones sobre los usuarios.

La figura 3 presenta una vista de las políticas implementadas en el perfil de un usuario. También fue necesario configurar el conmutador capa 2 con el comando "*aaa authorization network default group radius*" para habilitar la función de autorización, lo que a su vez activa la asignación automática de la VLAN indicada por el servidor RADIUS con base en el perfil residente en el PIP.

2.4 Auditoría

Se usó una base de datos mySQL para el registro de la información del acceso de los usuarios en varias tablas creadas con las plantillas que contiene el servidor FreeRADIUS. Mediante las funcionalidades de OpenSSL, se creó un certificado digital para el Servidor Web Apache, con el cual se pudo establecer una conexión segura para consultar la base de datos mySQL usando la interfaz Web de phpMyAdmin desde

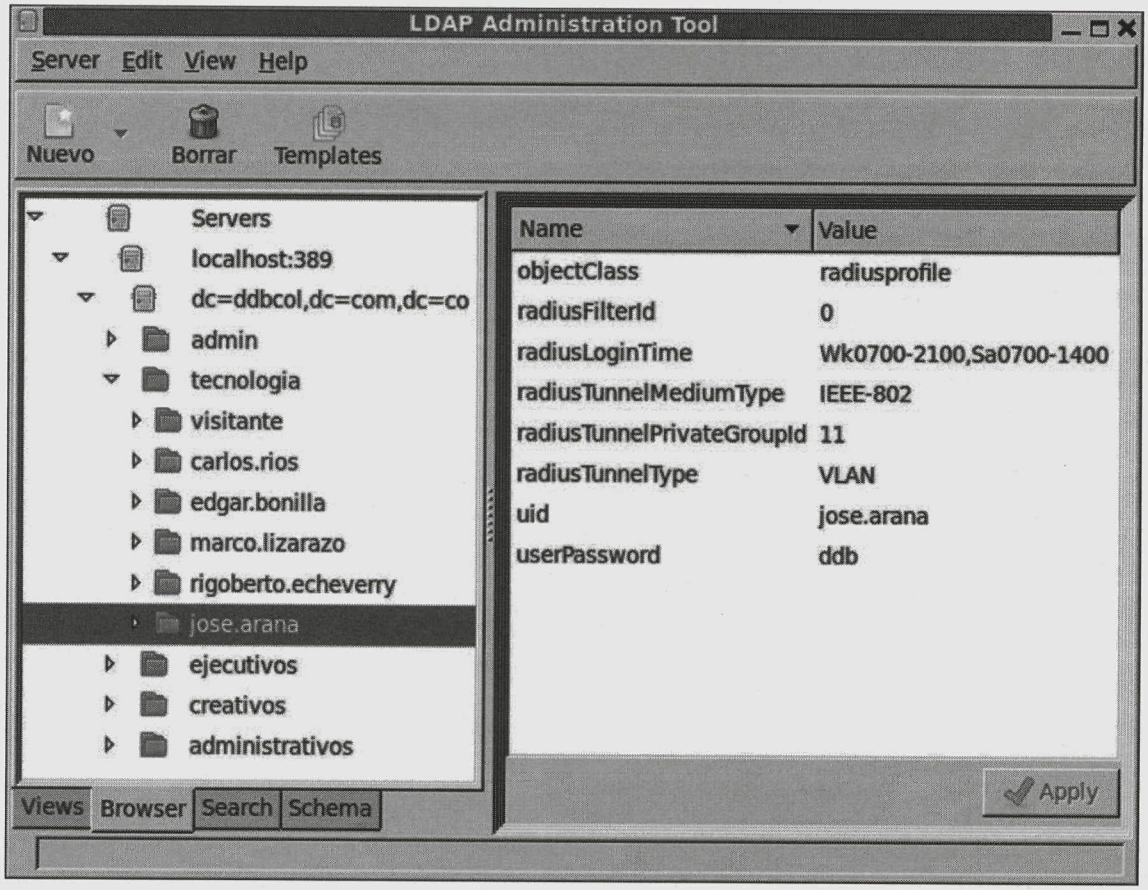

Figura 3. *Información de un usuario en el punto de información de políticas.*

un equipo remoto. Para que el servidor RADIUS registre en la base de datos la información de los usuarios que han logrado autenticarse, es necesario configurar la característica de auditoría en los puntos de ejecución de políticas; para el conmutador capa 2, esto se realizó mediante el comando "*aaa accounting dot1x default start-stop group radius*".

El conmutador Ethernet capa 2 que hace la función de PEP para los usuarios que ingresan a la red mediante el sistema de autenticación, autorización y auditoría, tiene la capacidad de enviar los datos de auditoría de dichos usuarios. Entre los datos que puede enviar, se tienen: Nombre del usuario, Puerto al cual está conectado en el conmutador capa 2, Hora de ingreso y salida de la red, Cantidad de datos enviados y recibidos por el usuario, Dirección MAC del equipo que está ingresando a la red y del punto de ejecución de políticas que atendió al usuario.

3. Resultados y discusión

3.1 Entorno de pruebas realizadas

En la tabla 1 se detalla el número de estaciones fijas y móviles que se instalaron en cada ciudad con sus respectivos tipos de autenticación. El Servidor RADIUS de Cali se integró a la red como punto de decisión de políticas para que los puntos de acceso inalámbricos de Cali, Bogotá y Medellín se apoyen en éste al ejecutar el proceso AAA, cuando estos últimos requieran hacer el papel de puntos de ejecución de las políticas. También fue posible emplear, como punto de información de políticas, tanto al directorio OpenLDAP que se encuentra en Cali y contiene solamente la información de los usuarios de Cali, como al Directorio Activo de Bogotá, que contiene los usuarios de toda la empresa. Todos los elementos necesarios para proveer la red con un sistema de autenticación, autorización y auditoría de redes se instalaron en una misma máquina (al no requerirse más complejidad dadas las características de la red en la que se implementó) teniendo presente la eventualidad de su expansión futura, dando la posibilidad de que sea escalable y replicable. Las políticas de seguridad que se definieron son:

a) Asignación de VLAN de acuerdo al perfil del usuario

b) El acceso a la red queda restringido para los visitantes al horario laboral; lunes a viernes de 7:00 a.m. hasta 8:00 p.m.

c) Se lleva un registro en la base de datos mySQL de los ingresos exitosos y fallidos a la red.

d) Registrar en la base de datos mySQL la información relevante de los usuarios autenticados exitosamente: Nombre de usuario, Hora de ingreso y salida de la red, Cantidad de datos enviados y recibidos por el usuario, Dirección MAC del equipo que está ingresando a la red y Dirección IP del punto ejecución de políticas que atendió al usuario.

3.2 Autenticación

Los tres tipos de autenticación disponibles en el sistema (EAP-TLS, EAP-PEAP, EAP-TTLS) funcionaron bien, el servidor RADIUS negaba el acceso cuando se proveían credenciales

Tabla 1. *Descripción de perfiles de software y hardware probados.*

Ubicación	Estaciones Fijas Windows EAP-TLS	Estaciones Móviles Windows EAP - PEAP	Estaciones Fijas Windows EAP - TTLS	Estaciones Fijas MAC-OS EAP - TTLS	Estaciones Móviles MAC-OS EAP - PEAP	Estaciones Fijas MAC-OS EAP-TLS
Cali	10	10	5	15	5	5
Bogotá	20	60	0	30	35	5
Medellín	10	40	0	15	30	5

erradas o se presentaba un certificado digital de identificación personal inválido o revocado. Se realizaron peticiones de acceso a la red con credenciales de usuario inválidas de forma sucesiva sin lograr éxito y sin que se presentara una negación del servicio a los demás usuarios válidos por parte del Servidor RADIUS.

Fue posible configurar las estaciones de trabajo de los usuarios corporativos, para que ejecutaran el proceso de autenticación con el punto de ejecución de políticas (autenticación mutua), únicamente cuando este último les presentara un certificado digital de identificación válido del Servidor RADIUS, expedido por la Autoridad de Certificación en la que dichas estaciones confían; si no se cumplía este requisito, el proceso de autenticación era detenido. La figura 4 muestra éxito en la verificación de los certificados (EAP-TLS) y la figura 5 presenta el acceso exitoso bajo EAP-TTLS de una estación Microsoft Windows administrada por "wpa_supplicant". El acceso de los usuarios a la red con sistema AAA se realizó con los sistemas operativos más populares disponibles, entre ellos Windows en las versiones XP, Vista y 7, MAC OSX versiones 10.5 a la 10.6 y Ubuntu en la versión 10.4. Con todos los sistemas operativos anteriores fue posible hacer la configuración descrita para acceder a la red, logrando una conexión exitosa y sin inconvenientes, utilizando todos los tipos de autenticación disponibles, distribuidos de manera uniforme en cada ciudad.

3.3 Autorización

Se verificó que en las horas de mayor congestión para el sistema AAA, cuando inician labores los empleados de la empresa (del orden de 300 empleados), el servidor tuvo buen desempeño,

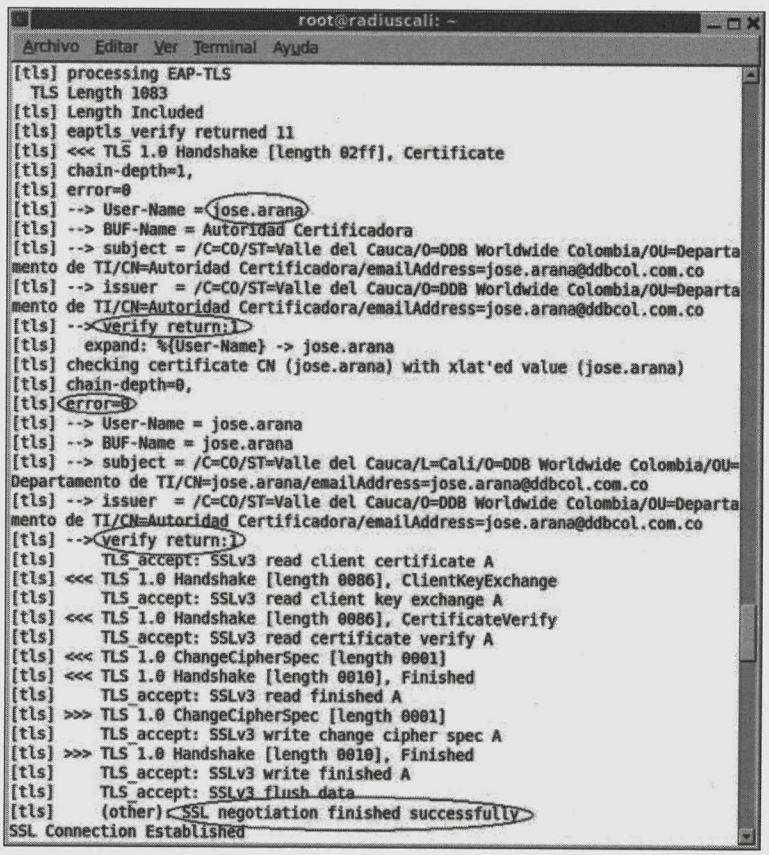

Figura 4. *Verificación exitosa de los certificados.*

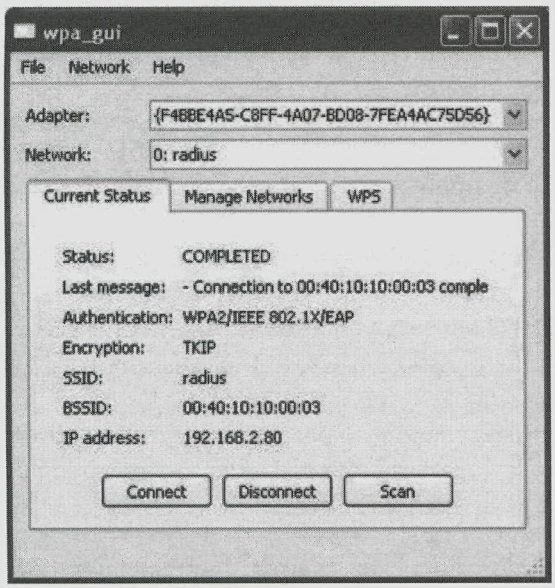

Figura 5. *Conexión exitosa usando EAP-TTLS administrado por "wpa_supplicant" en Windows.*

y permitió el acceso rápido a las personas que presentaron credenciales válidas, la conexión a la red se establece en menos de 5 segundos. La figura 6 presenta la información cuando el servidor RADIUS acepta una conexión y le asigna la VLAN 3 a la respectiva estación cliente. Es recomendable tener redundancia en el sistema AAA para lograr una mayor tolerancia a fallas, esto se puede conseguir, configurando en los puntos de ejecución de políticas un Servidor RADIUS alterno para el caso en que falle el principal. En nuestro caso, el servidor principal se instaló en la ciudad de Cali y el servidor secundario en la ciudad de Bogotá.

3.4 Auditoría

El sistema de auditoría funcionó correctamente y dejó registros en la base de datos mySQL, tanto para los usuarios que tuvieron éxito en el proceso de ingreso a la red, como para los usuarios que fueron rechazados. El sistema registra el día y la hora del acceso o rechazo. Se configuró la herramienta "dialup-admin", que permite buscar y mostrar en una interfaz Web, desde cualquier computador de la red, la información de auditoría que está registrada en las bases de datos mySQL. También se pudo observar que el consumo de recursos del sistema AAA no es elevado (del orden del 2%), cuando se usa en un servidor de doble núcleo con 1 Gigabyte de RAM (en una red de 300 empleados). Esto abre la posibilidad de implementar el Servidor RADIUS o el sistema AAA completo en un hardware de propósito único, lo que hace de esta implementación una opción viable para desarrollar un producto unificado que provea todas las características necesarias para implementar una red con sistema de AAA a un bajo costo. Equipos como el CM-X300 de la empresa Compulab permitirían realizar esta tarea,

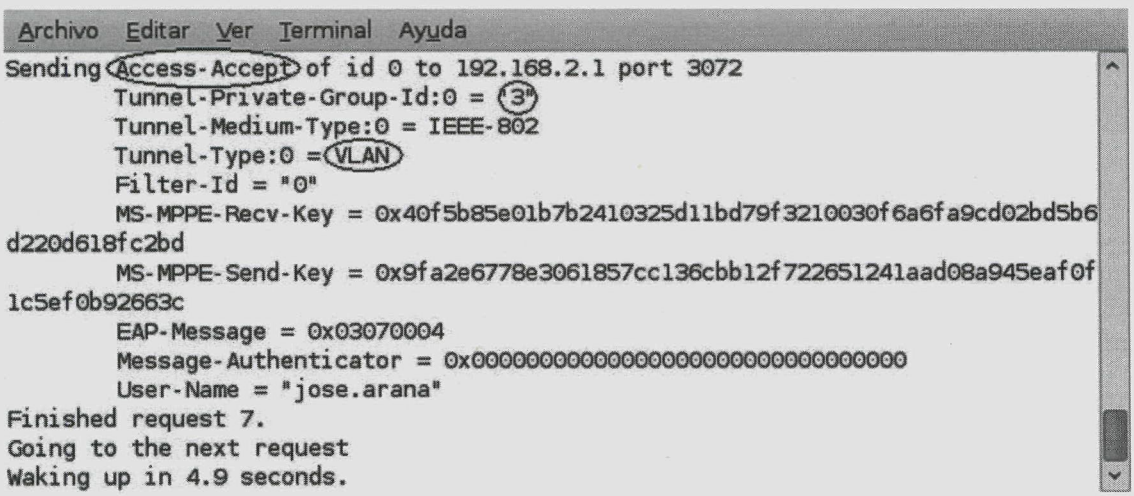

Figura 6. *Información del acceso aceptado.*

adecuando el sistema que se tiene actualmente en un computador a dicho hardware.

4. Conclusiones

Fue posible configurar tres tipos de autenticación en el servidor de autenticación, usando en uno de estos, la infraestructura de clave pública completa (EAP-TLS) y, en los otros dos, un esquema de credenciales basado en el nombre de usuario y la contraseña (EAP-PEAP, EAP-TTLS), con certificados de identificación personal en los servidores de autenticación, lo que permite realizar autenticación mutua, haciendo muy seguro el acceso a la red.

Al tener una infraestructura de clave pública implementada, fue posible revocar los certificados de identificación personal de usuarios que no se desea que ingresen a la red, ya sea porque han dejado de formar parte de la empresa o porque sus certificados han sido robados o comprometidos.

Se demostró que si un usuario presenta un certificado de identificación personal revocado, el acceso a la red le será denegado. El acceso de los usuarios a la red con sistema AAA se probó con los sistemas operativos más populares disponibles; estos fueron: Windows en las versiones XP, Vista y 7, MAC OSX versiones 10.5 a 10.6 y Ubuntu en la versión 10.4.

Con todos los sistemas operativos se demostró que fue posible usar los tres esquemas de autenticación disponibles, realizando autenticación mutua entre las partes del proceso de AAA, consiguiendo una conexión exitosa, segura y sin inconvenientes.

Se implementaron, en el sistema AAA, las políticas que mejoraron considerablemente la seguridad de acceso a la red, estas políticas son: asociación automática de los usuarios autenticados exitosamente a una VLAN definida para cada perfil, restricciones en el horario de acceso a la red, registro en una base de datos de los accesos exitosos o fallidos, registro de los datos concernientes al equipo del usuario que ha sido autenticado exitosamente y ha ingresado a la red, como también las actividades de dicho usuario dentro de la red para efectos de control y seguimiento.

Se logró configurar el Servidor RADIUS para que use dos puntos de información de políticas; uno de ellos es un servidor de directorio OpenLDAP, el cual tiene soporte completo para todas las funcionalidades necesarias de las políticas que se establecen para cada usuario, el otro es el servicio de directorio de Microsoft, el Directorio Activo, que sólo posee las credenciales de los usuarios de varias ciudades (nombre de usuario y contraseña) de la red corporativa donde se implementó el servicio AAA.

Se configuraron varias herramientas Web que permiten administrar las funcionalidades implementadas en el Servidor de Autenticación. La herramienta que permite ver el contenido de las bases de datos mySQL a través de una interfaz Web se llama "phpMyAdmin", con la cual es posible detallar toda la información registrada de los usuarios que han accedido a la red.

Otra herramienta configurada para realizar búsquedas en la información de auditoría de la base de datos mySQL y mostrarla de forma amigable fue "Dialupadmin", la cual es una herramienta que está incluida con el servidor RADIUS FreeRADIUS. Esta herramienta permite filtrar la búsqueda de los datos de auditoría de la base de datos mySQL usando cualquier atributo que esté dentro de la base de datos. Es muy útil para generar reportes de ingreso de los usuarios que han accedido a la red. Mediante la Autoridad de Certificación de la red, se creó un certificado digital para el Servidor Web (que permite que todas las herramientas anteriores funcionen), el cual se configuró para que sólo establezca conexión usando cifrado SSL y el protocolo HTTPS. Lo anterior le proporciona seguridad al tráfico de dicho Servidor.

Al comparar la solución AAA propuesta con soluciones de control de acceso a red comerciales (por ejemplo, aquellas basadas en dispositivos de los fabricantes Bradford, Fortinet o Cisco),

podemos afirmar que los dispositivos comerciales tienen funciones de seguridad adicionales muy particulares, a veces exclusivas, cuyo funcionamiento se complementa (no compite) con la solución planteada. También, hay que resaltar que la solución propuesta se puede escalar fácilmente mediante la utilización de computadores más robustos y se puede tener alta disponibilidad mediante el uso de varios servidores AAA en un ambiente corporativo en general. Finalmente, esta solución se puede mejorar mediante el remplazo de RADIUS por las implementaciones del protocolo DIAMETER Fajardo et al. (2012), el cual se encuentra en estado de estándar propuesto (de la IETF) y opera sobre TCP, tiene mayor número de parejas atributo-valor, mejor soporte de movilidad y de notificación de error.

5. Referencias bibliográficas

Arana, J. (2010). *Diseño e implementación de una red con sistema de autenticación escalable como aplicación directa de los protocolos de autenticación, autorización y auditoría de redes.* Trabajo de Grado, Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Cali, Colombia.

Bhaiji, Y. (2008). *Network Security Technologies and Solutions (CCIE Professional. Development).* Indianapolis: Cisco Press, Inc.

Fajardo, V., Arkko, J., Loughney, J., & Zorn, G. (2012). *Diameter Base Protocol.* In IETF (The Internet Engineering Task Force) Request for Comments 6733. http://tools.ietf.org/html/rfc6733

Geier, J. (2008). *Implementing 802.1X security solutions for wired and wireless networks.* Indianapolis, IN: Wiley Pub.

Nakhjiri, M. (2005). *AAA and network security for mobile access : radius, diameter, EAP, PKI and IP mobility.* Chichester, England Hoboken, NJ: John Wiley & Sons.

OPENLDAP (2012). *OpenLDAP Software 2.4 Administrator's Guide.* http://www.openldap.org/doc/admin24/

Qazi, H. U. (2007). *Comparative Study of Network Access Control Technologies.* Magister thesis, Department of Computer and Information Science, Linköpings universitet, Linköping, Suecia. http://liu.diva-portal.org/smash/record.jsf?pid=diva2:23688

Rigney, C. (2000). *RADIUS Accounting.* In IETF (The Internet Engineering Task Force) Request for Comments 2866. http://www.ietf.org/rfc/rfc2866

Rigney, C,. Willens, S., Rubens, A., & Simpson, W. (2000). *Remote Authentication Dial In User Service (RADIUS).* In IETF (The Internet Engineering Task Force) Request for Comments 2865. http://www.ietf.org/rfc/rfc2865

Roser, K. (2002). *EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant.* http://freeradius.org/doc/EAPTLS.pdf

Simon, D., Aboba, B., & Hurst, R. (2008). *The EAP-TLS Authentication Protocol.* In IETF (The Internet Engineering Task Force) Request for Comments 5216. http://tools.ietf.org/html/rfc5216

Yago, F. (2009). *AAA / RADIUS / 802.1x, Sistemas Basados en la Autenticación en Windows y Linux/GNU.* Madrid: Rama.