Control de acceso y administración de recursos de red mediante un servidor AAA en el GAD Municipal de Urcuquí usando software libre

Carlos A. Vásquez, William E. Vaca

***Resumen*— El presente documento presenta el diseño e implementación de un esquema de red que proporciona el servicio de Autenticación, Autorización y Auditoria (AAA) en el GAD Municipal San Miguel de Urcuquí, para el control de acceso y administración de recursos de red, empleando soluciones basadas en software libre.**

La autenticación de usuarios se realiza empleando el método EAP-TTLS que basa su seguridad en certificados digitales, un directorio centralizado almacena las credenciales de acceso y permite la asignación dinámica de recursos de red mediante VLAN, finalmente, en una base de datos MySQL se almacenan todos los eventos generados por los usuarios del sistema AAA.

***Palabras clave*— AAA, EAP-TTLS, IEEE 802.1X, RADIUS, LDAP, MySQL, VLAN**

I. INTRODUCCIÓN

Las redes de datos son esenciales para el crecimiento y desarrollo de las empresas, tienen la capacidad de soportar nuevas tecnologías evolucionando fácilmente a la par de los cambios y aplicaciones que día a día se desarrollan.

Actualmente, existen muchos riesgos de seguridad relacionados con las redes de comunicación, técnicas de ingeniería social, ataques de negación de servicio, uso indebido de aplicaciones, hasta la sustracción de datos, amenazas que pueden originarse desde fuera de la empresa o de propios empleados que intencionalmente o por falta de conocimientos pudieran llegar a comprometer la operatividad de toda la infraestructura de red.

Con la implementación del sistema AAA en la red de datos del GADMU se garantiza un proceso seguro de acceso a la red a través de métodos de autenticación basados en certificaos digitales, se administran los recursos de red en base a políticas de seguridad y mediante la integración de una base de datos MySQL, se registran todos los eventos generados por los dispositivos que exitosamente accedieron al sistema.

Documento recibido el 5 de diciembre de 2014. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte.

C.A. Vásquez, trabaja en la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador (e-mail: cavasquez@utn.edu.ec).

W.E. Vaca, egresado de la Carrera de Ingeniería Electrónica y Redes de Comunicación (e-mail: william_889@hotmail.com).

II. CONCEPTOS BÁSICOS

A. Sistemas AAA

El estándar AAA se utiliza en el diseño de sistemas de control de acceso a redes de datos, proporcionando los servicios de autenticación, autorización y contabilidad de forma centralizada.

- **Autenticación.-** Es el proceso de mayor relevancia en los sistemas AAA, sirve de base a todo el sistema completo, debido a su directa relación con los procesos de autorización y contabilidad. La autenticación permite comprobar la identidad de un usuario a través de los siguientes elementos: Algo que se conoce, como un número de identificación personal (PIN) o contraseña; algo que se tiene, como una tarjeta ATM o una tarjeta inteligente; algo que identifique físicamente al usuario de forma única, como una huella dactilar, el reconocimiento de voz, escaneo de la retina ocular, etc. Utilizar más de un factor para identificar al usuario añade credibilidad al proceso de autenticación [1].

- **Autorización.-** Es el proceso mediante el cual a un usuario se le asigna una determinada cantidad de recursos o servicios de red, en base a las actividades que realice y las políticas de acceso establecidas por el administrador. Está obligatoriamente relacionado con el proceso de autenticación, si un usuario no se autentica correctamente los siguientes procesos se descartan. Para cumplir con el proceso de autorización, los sistemas AAA utilizan soluciones como bases de datos o directorios que permiten almacenar las políticas de acceso de cada usuario.

- **Contabilidad.-** Una vez realizado el proceso de autenticación y autorización se produce la fase de contabilidad o "Acconunting". Ésta inicia cuando el equipo autenticador o NAS autoriza al suplicante acceder a los servicios de red.
  La contabilidad es el proceso estadístico y de recolección de datos sobre la conexión, el buen tratamiento de la información recolectada durante el proceso de autenticación y autorización permite al administrador de la red gestionar la futura demanda de sus sistemas para planificar su crecimiento.

B. *Radius*

RADIUS son las siglas de **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice, que significa: autenticación remota para usuarios de servicio telefónico. Es un protocolo cuya infraestructura de red se basa en un modelo cliente-servidor, donde los servicios de autenticación, autorización y contabilidad son administrados por un equipo proveedor de recursos, en este caso el servidor radius y los clientes son aquellos que acceden a los servicios ofertados por la infraestructura de red [1].

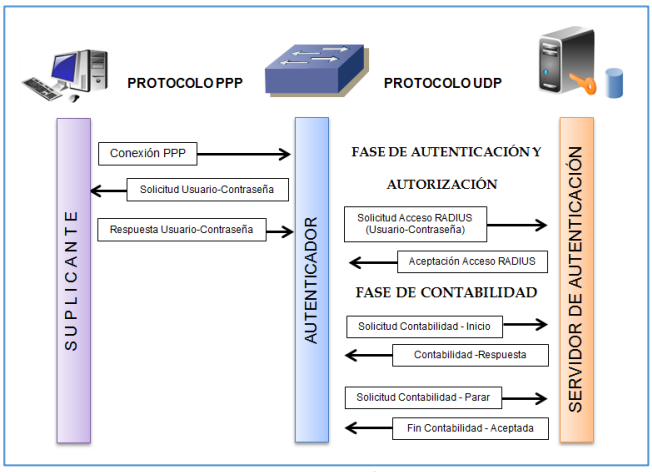

Figura 1. Comunicación RADIUS

RADIUS utiliza el puerto UDP 1812 para el proceso de autenticación y 1813 para el registro de la información (contabilidad).

C. *IEEE 802.1x*

Es un estándar de autenticación que permite controlar el acceso a los servicios de red a través de sus puertos, opera en la capa dos del modelo OSI, asegura el intercambio de las credenciales de usuario o dispositivo evitando cualquier acceso no autorizado a la red [3].

Una infraestructura de red 802.1x requiere de tres elementos para operar: suplicante, equipos autenticadores y servidor de autenticación.

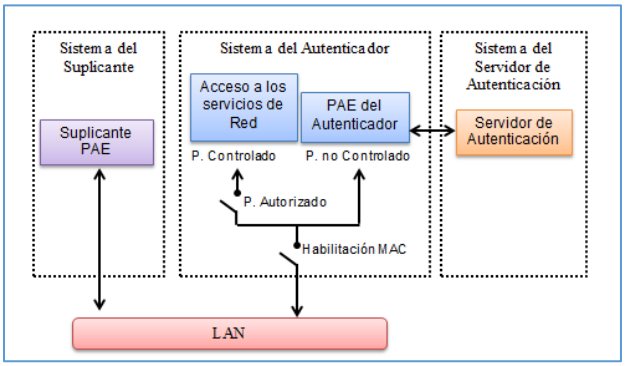

Figura 2. Principio de Operación de puertos 802.1x

- **Suplicante.-** Es un software que se instala en los clientes del equipo autenticador, utilizado en ambientes cableados e inalámbricos. El suplicante se carga en el dispositivo del usuario y se utiliza para solicitar acceso a la red.
- **Autenticador.-** Es el componente a través del cual los usuarios acceden a los servicios de red, se encuentra entre el dispositivo que necesita ser autenticado y el servidor utilizado para realizar la autenticación. Ejemplos de Autenticador son conmutadores de red y puntos de acceso inalámbricos.
- **Servidor de Autenticación.-** Es un equipo que recibe mensajes mediante una comunicación RADIUS y utiliza esa información para comprobar la autenticidad del usuario o del dispositivo que intenta acceder a la red, por lo general se emplean bases de datos para realizar este proceso tales como SQL, Microsoft Active Directory, LDAP, etc.

D. *Eap-ttls*

El Protocolo de Autenticación Extensible (EAP) se encuentra definido en el RFC 3748 y permite múltiples métodos de autenticación, uno de ellos EAP-TTLS. Transport Layer Security (TLS), es el sucesor del protocolo SSL, permite establecer una conexión segura mediante la creación de un canal cifrado entre el cliente y el servidor para el envío de las credenciales de acceso durante el proceso de autenticación [4].

Se requiere únicamente la instalación de un certificado digital en el servidor RADIUS, reduciendo considerablemente la complejidad del sistema de autenticación debido a que no existe necesidad de instalar y gestionar los certificados de todos los dispositivos de la red.

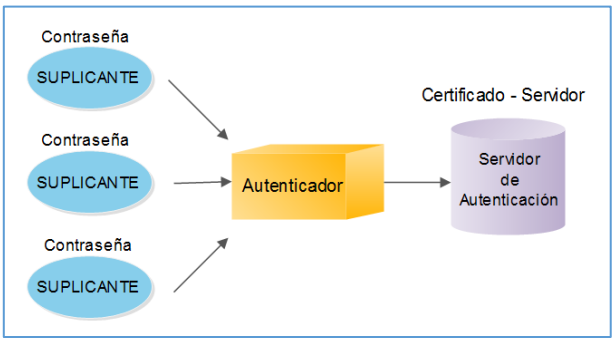

Figura 3. Ubicación de certificados digitales EAP-TTLS.

La comunicación TTLS se establece en dos fases, el primer túnel TLS se crea para el intercambio de credenciales donde el cliente se autentica con el servidor o viceversa, esto permite crear un canal seguro usando mecanismos criptográficos para el intercambio de información que procederá en la siguiente fase.

En la fase posterior, el cliente se autentica con el servidor utilizando cualquier mecanismo menos seguro como PAP, CHAP, MS-CHAP. De esta manera EAP-TTLS soporta conexiones con bases de datos de autenticación manteniendo en todo momento un medio seguro para el intercambio de datos.

E. Secuencia de una comunicación AAA [5]

A continuación se describe, paso a paso, el proceso de entramado y la secuencia de operación del sistema AAA empleando 802.1X /EAP-TTLS.

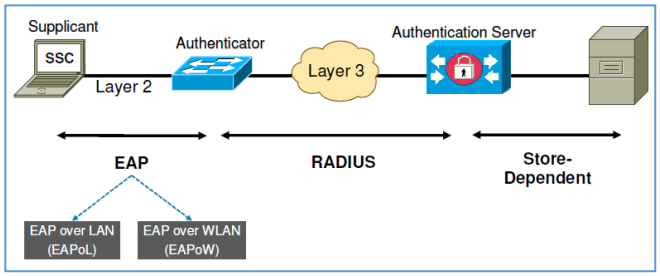

Figura 4. Protocolos usados en una comunicación AAA

1) El inicio de la comunicación se produce cuando el suplicante envía el paquete EAPOL – Start, solicitando acceso al cliente radius; esto significa que el campo "Tipo" tiene asignado el valor 01 hexadecimal.
2) En esta etapa del proceso el autenticador tiene bloqueado el puerto de acceso, solo recibe tramas 802.1X, el resto son descartadas. Cuando el switch recibe una trama EAPOL-Start solicita al suplicante un identificador válido para el acceso.
3) Con el método de autenticación EAP-TTLS es posible usar una identidad anónima para establecer el túnel seguro, de esta manera el nombre de usuario enviado por el suplicante se protege.
4) El autenticador extrae el mensaje recibido y lo encapsula en un paquete RADIUS. Los datos se envían al servidor a través de atributos (AVP) que contienen información del suplicante y del equipo autenticador a través del cual el usuario intenta acceder a la red.
5) En esta fase, el servidor inicia el proceso de autenticación. Para que el suplicante identifique el método de autenticación, el servidor envía el paquete usando el código 21 (EAP-TTLS) y las banderas configuradas en (0010 0000) que indican el inicio del mensaje y la versión TTLSv0.
6) Una vez iniciado el proceso EAP, el autenticador deja de tomar decisiones, simplemente se encarga de comunicar al suplicante con el servidor mediante los protocolos EAPOL Y RADIUS.
7) Cuando el suplicante recibe el mensaje de inicio EAP-TTLSv0, arranca el proceso de intercambio de paquetes empleando el protocolo Handshake, que consiste en la transmisión de una secuencia de mensajes para negociar los parámetros de seguridad de la sesión TLS, utilizada para la transferencia de datos entre el suplicante y servidor.
8) El servidor debe responder el mensaje de saludo del cliente con una serie de paquetes que incluyen: el mensaje Server Hello, el certificado digital del servidor RADIUS y el mensaje Server Hello Done.
9) El suplicante envía un mensaje de intercambio de claves secretas generadas a partir de los datos recibidos. Las claves se calculan empleando los valores aleatorios generados en los mensajes Client y Server Hello.
10) Antes de transmitir la clave secreta al servidor, se cifra mediante la clave pública del certificado del servidor. Tanto el suplicante como el servidor realizan el mismo proceso de forma local y obtienen la clave privada para la sesión segura.
11) Si el servidor es capaz de descifrar estos datos y completar el protocolo, el cliente tiene la seguridad de que el servidor tiene la clave privada correcta. Este paso es crucial para demostrar la autenticidad del servidor. Sólo el servidor con la clave privada que coincide con la clave pública del certificado puede descifrar los datos y continuar la negociación del protocolo TLS/SSL.
12) Una vez establecido el túnel, el suplicante usa el canal TLS/SSL para enviar las credenciales de acceso (usuario + contraseña) de forma segura.
13) El servidor RADIUS verifica internamente en el directorio LDAP si las credenciales de usuario enviadas por el suplicante son válidas, y si procede, responde con un mensaje EAP Access-Accept.
14) Finalmente, el autenticador configura el estado del puerto como Autorizado y envía un paquete EAPOL EAP-Success al suplicante, informando que la autenticación ha sido exitosa.

F. LDAP

Es un protocolo ligero de acceso al directorio, permite almacenar información relacionada a una organización en particular, por ejemplo nombres de usuario, contraseñas, certificados digitales, cuentas de correo, etc. Las especificaciones técnicas se definen en los RFC 4510 - 4519.

LDAP no es una base de datos relacional, es un protocolo que regula el acceso a los datos almacenados, optimizado especialmente para proporcionar una repuesta rápida a operaciones de búsqueda y lectura de la información [6].

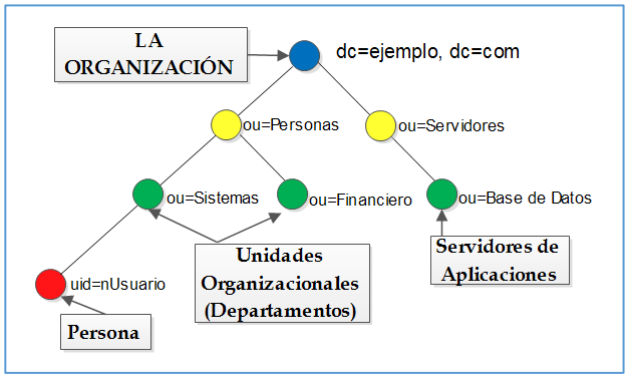

Figura 5. Estructura general de un directorio LDAP

La unidad básica de información en un directorio es la entrada, que describe a un objeto del mundo real que puede ser: personas, departamentos, servidores, impresoras, etc. Un ejemplo de modelo típico de un directorio se puede apreciar en la Figura 5, que muestra algunos objetos reales en una organización.

III. DISEÑO DE LA INFRAESTRUCTURA DE RED TCP/IP CON SERVICIO AAA

El servicio AAA de la red de datos del GAD Municipal San Miguel de Urcuqui se diseña en base al estándar IEEE 802.1x para el control de acceso a la red usando como método de autenticación EAP-TTLS.

A. Consideraciones técnicas 802.1x / Eap-ttls

Los componentes básicos de un sistema 802.1x son: suplicante, autenticador y el servidor de autenticación, sin embargo, la solución planteada en la red de datos del GADMU requiere cuatro componentes adicionales, una autoridad certificadora, un firewall, un directorio LDAP y una base de datos SQL.

- La CA (Autoridad Certificadora) se emplea para generar el certificado digital que el servidor RADIUS utiliza en el proceso de autenticación EAP-TTLS.
- El firewall en la arquitectura 802.1x realiza la función de router, es decir, permite la comunicación entre las diferentes zonas de red.
- El directorio LDAP permite almacenar las credenciales de usuario de todos los usuarios del GADMU y las políticas de acceso configuradas mediante la asignación de VLANs.
- La base de datos SQL registra los equipos autenticadores de la red y la información generada en el proceso de contabilidad.

B. Requerimientos de Suplicante

El software que se instala en los dispositivos de usuario final utilizado para acceder a la red (cableada o inalámbrica) debe soportar el método de autenticación EAP-TTLS.

TABLA 1.
REQUERIMIENTOS TÉCNICOS SUPLICANTE

SISTEMA OPERATIVO	EAP-TTLS
Windows XP	SecureW2
Windows 7	SecureW2
Windows 8	Cliente Nativo
Ubuntu 12.04 LTS	Cliente Nativo
Android OS	Cliente Nativo

C. Requerimientos de Autenticador

Los equipos que ofrecen el servicio de acceso a la red y se ubican entre los dispositivos de usuario que requieren ser autenticados y la plataforma de servidores AAA, deben cumplir con los requerimientos técnicos detallados en la Tabla 2.

TABLA 2.
REQUERIMIENTOS TÉCNICOS AUTENTICADOR

REQUERIMIENTO	DESCRIPCIÓN
RENDIMIENTO	
Capacidad	▪ 48 puertos 10/100 ▪ 2 puertos 10/100/1000
FUNCIONES	
RADIUS	✓ Seguridad RADIUS
Autenticación	✓ IEEE 802.1X (función de Autenticador)
VLAN	▪ 256 VLAN simultáneas ▪ VLAN de administración ▪ VLAN de usuarios temporales sin autenticación ▪ Asignación dinámica de VLAN mediante servidor Radius con autenticación 802.1x
Contabilidad	✓ Soporte de IEEE 802.1X Acconunting

D. Requerimientos de servicios AAA

Cada uno de los servicios del sistema AAA (autenticación, autorización y contabilidad) deben cumplir parámetros mínimos de funcionalidad que permitan el control de acceso y la administración de recursos de red en el GADMU. En la Tabla 3 se detallan los requerimientos.

TABLA 3.
REQUERIMIENTOS TÉCNICOS SERVICIOS AAA

SERVICIO	DESCRIPCIÓN
AUTENTICACIÓN	
Servidor	FreeRADIUS
Control de acceso	IEEE 802.1x
Método de autenticación	EAP-TTLS
Conexión	Equipo Autenticador (SW CISCO)
AUTORIZACIÓN	
Servidor	OpenLDAP
Almacenamiento de contraseña	Algoritmo MD5 o SHA
Asignación de recursos	Soporte de VLAN dinámica
Conexión	Servidor FreeRADIUS
CONTABILIDAD	
Servidor	MySQL
Conexión	Servidor FreeRADIUS
FIREWALL	
Zona wan	Salida a internet
Zona dmz	Servidores AAA
Zona local	Interfaces virtuales por cada VLAN
Comunicación inter-VLAN	Soporte 802.1Q (Troncal)
Proxy	Modo Transparente

IV. IMPLEMENTACIÓN DEL SERVIDOR AAA

En base al esquema actual de la red del GAD Municipal San Miguel de Urcuqui, se implementa el servicio AAA en un escenario (ver Figura 6) con equipos de similares características e iguales funcionalidades con la finalidad de garantizar que la solución es factible implementarla en la red de datos de la institución.

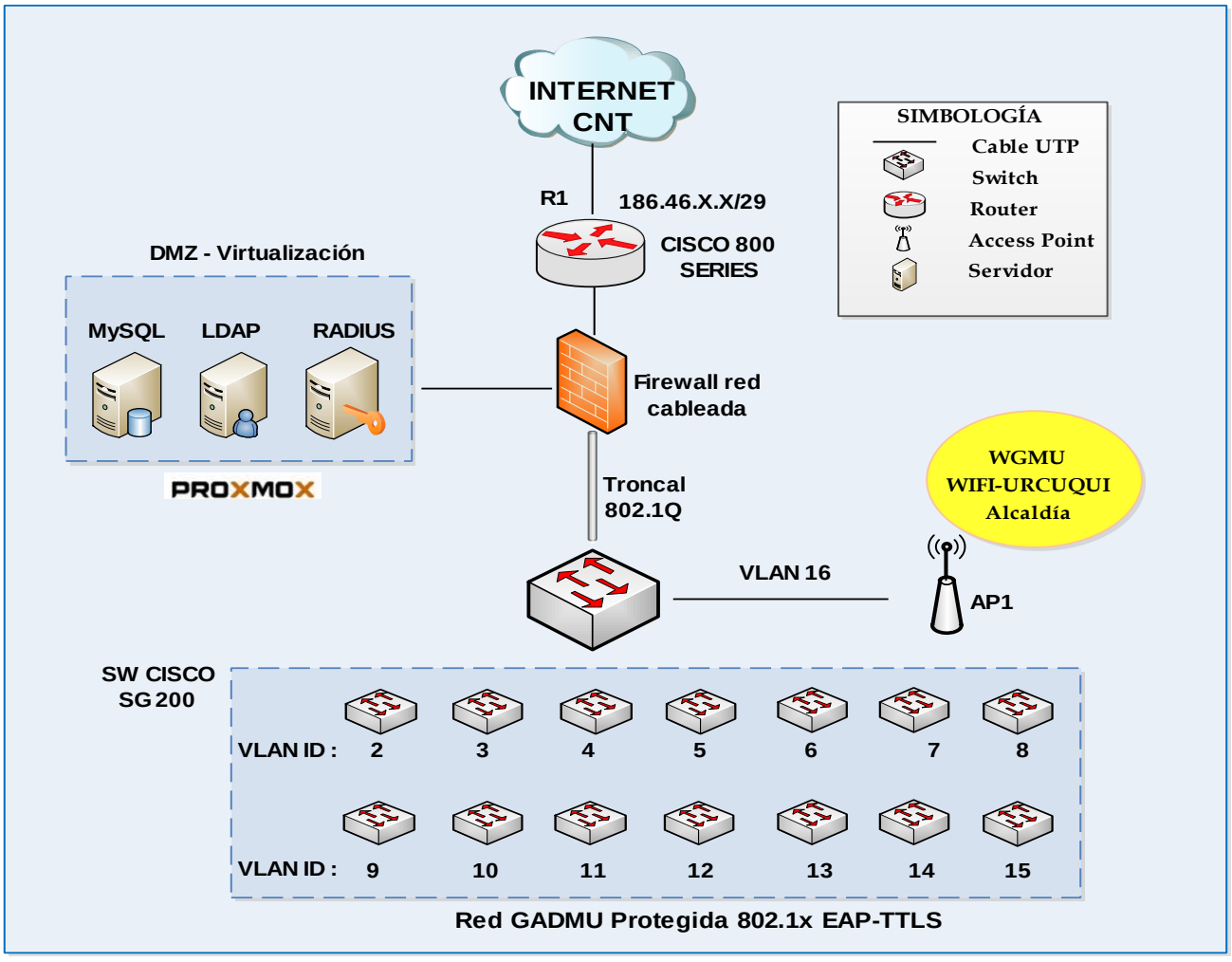

Figura 6. Integración del servicio AAA en la red del GADMU.

A. Servidor AAA

El servicio AAA requiere la instalación de tres servidores: FreeRADIUS para el servicio de autenticación EAP-TTLS, OpenLDAP como directorio de almacenamiento de credenciales de usuario y la base de datos MySQL para el registro de clientes NAS de RADIUS, así como el servicio de Acconunting.

- **Proxmox VE**

Para optimizar el uso de hardware se utiliza la tecnología de virtualización Proxmox VE 3.0, específicamente a través de OpenVZ, una de las soluciones de mejor rendimiento para servidores Linux. La tecnología de contenedores virtuales usa imágenes precargadas para instalar sistemas operativos Linux de forma eficiente, la asignación de recursos de hardware para los contenedores OpenVZ de los servidores AAA se muestra en la Tabla 4.

TABLA 4.
RECURSOS VIRTUALES SERVIDOR AAA

PARÁMETROS	FREERADIUS	OPENLDAP	MYSQL
procesadores	1	1	1
disco duro	6 GB	6 GB	6 GB
memoria	512 MB	512 MB	512 MB
Nodo	proxmox-aaa	proxmox-aaa	proxmox-aaa
plantilla	Ubuntu 12.04	Ubuntu 12.04	Ubuntu 12.04
swap	512 MB	512 MB	512 MB
vmid	200	210	220

- **Certificados digitales con tinyca2**

Usando TinyCA2 se crea la autoridad certificadora raíz para el GAD Municipal San Miguel de Urcuqui, con la finalidad de emitir y gestionar todo el sistema de certificados que se requieran en los servidores de la institución.

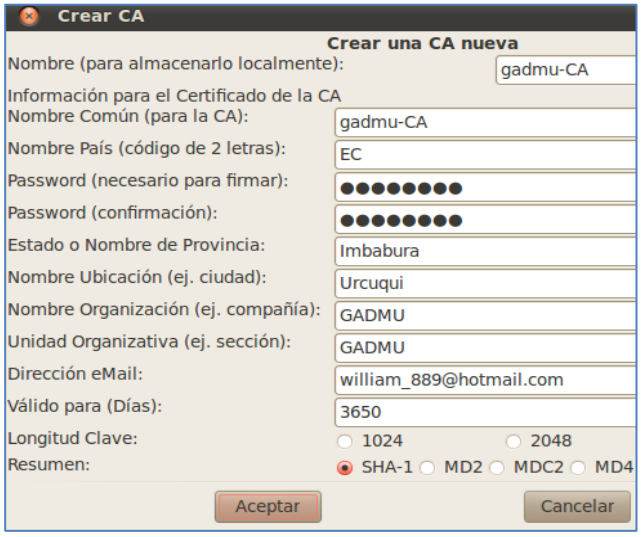

Figura 7. Creación de la Autoridad Certificadora Raíz

El certificado raíz gadmu-CA se instala en el repositorio de certificados de confianza de todos los clientes EAP-TTLS, esto permite al suplicante verificar que el servidor al que se está autenticando es el verdadero, evitando de esta manera que las claves de acceso se expongan fácilmente ante cualquier persona.

- **Servidor FreeRADIUS**

FreeRADIUS es un paquete estándar soportado por múltiples sistemas operativos, permite realizar instalaciones a gran escala empleando múltiples servidores AAA. Soporta conexiones con varios tipos de bases de datos, tanto para la autorización como para la contabilidad, es compatible con una gran cantidad de métodos de autenticación que en conjunto forman un sistema AAA muy robusto y confiable.

El servidor y sus dependencias se pueden descargar directamente desde los repositorios mediante el comando mostrado en la Figura 8. Una de las grandes ventajas que representa utilizar Ubuntu Server 12.04 como sistema operativo base es el manejo de un repositorio actualizado, esto agiliza el proceso de instalación de cualquier software y sus dependencias.

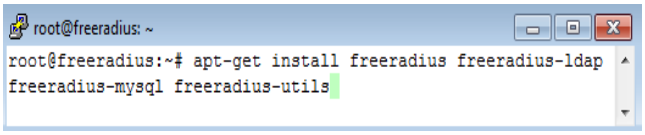

Figura 8. Instalación de freeradius Ubuntu Server 12.04 LTS

- **Servidor OpenLDAP**

El GAD Municipal San Miguel de Urcuqui no cuenta con un directorio de usuarios para almacenar las credenciales de acceso requeridas en el proceso de autenticación a la red de datos, por lo que se crea un directorio utilizando OpenLDAP [7].

El esquema del directorio (ver Figura 9) se diseña usando como referencia las unidades departamentales de la institución, se crea un grupo de usuarios por cada VLAN, las contraseñas se establecerán y almacenarán siguiendo las recomendaciones de la política de seguridad.

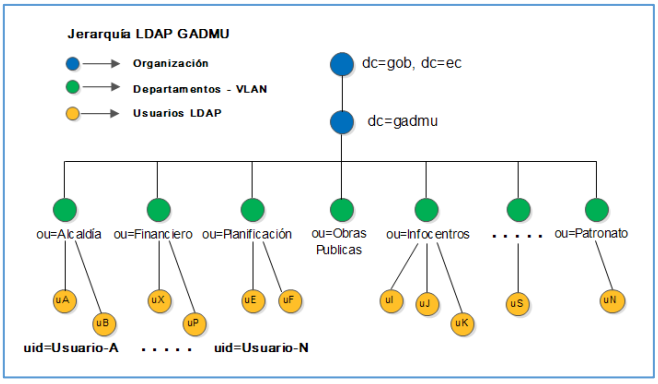

Figura 9. Jerarquía LDAP GADMU

- **Servidor MySQL**

MySQL es un sistema de gestión de código abierto para bases de datos relacionales. Los datos se almacenan en tablas separadas con el fin de acceder a la información de manera rápida y flexible.

FreeRADIUS tiene la capacidad de usar MySQL como base de datos para el proceso de autenticación y contabilidad en el servicio AAA, la instalación de FreeRADIUS incluye scripts de configuración que permiten crear automáticamente las tablas para el ingreso de la información.

Para la instalación de la base de datos MySQL se descarga el paquete lamp-server, una combinación de software basada en código abierto que incluye: el servidor HTTP apache, la base de datos MySQL y algunos componentes extras que se requieren para construir la base de datos que se usará en el proceso de contabilidad del servicio AAA.

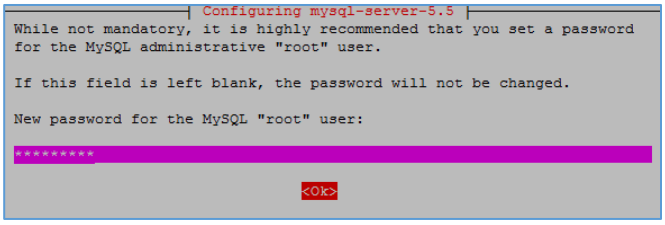

Figura 10. Solicitud de contraseña para el usuario root de MySQL

Una vez preparado el servidor MySQL se debe crear una base de datos RADIUS con algunas tablas y campos relacionados. Para evitar el trabajo de crear campo por campo toda la estructura de la base de datos de forma manual, FreeRADIUS incorpora scripts SQL para automatizar este proceso.

B. Autenticador cableado

La implementación del servicio 802.1x para el control de acceso a redes cableadas se lo hace en el switch Cisco Small Business SF300, conmutador de red que opera como dispositivo de capa 2 o 3 según se lo configure.

- **VLAN**

Para lograr la comunicación entre equipos de diferentes VLANs es necesario usar un dispositivo de capa tres que realice el proceso de enrutamiento de paquetes de distintas redes. El puerto del router debe soportar el protocolo IEEE 802.1Q, mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas [8].

Figura 11. Resumen de VLANs creadas switch cisco FS-300

La implementación del estándar IEEE 802.1Q se realiza en el puerto eth0 del Firewall GNU/Linux, para activar el servicio se debe configurar los requerimientos básicos que habilitan las interfaces virtuales en la tarjeta de red Ethernet.

- **802.1X**

Para activar el servicio RADIUS se accede al menú: Seguridad > RADIUS > Añadir. En la página desplegada se debe configurar los parámetros del servidor FreeRADIUS que se usará como servidor de autenticación para la red de datos del GADMU. Luego de haber añadido el servidor RADIUS se debe configurar los parámetros del estándar IEEE 802.1X en el switch SF-300, tanto en forma global como individual en cada puerto.

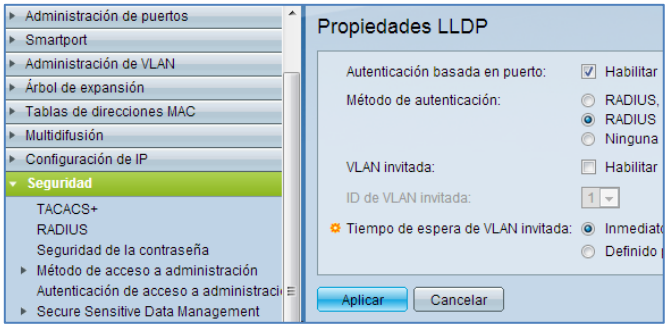

Figura 12. Autenticación basada en puerto global switch cisco SF-300

En la página Seguridad > 802.1X > Autenticación del Puerto, se deben definir varios parámetros del estándar 802.1X para cada puerto.

1) Puerto: Seleccionar la interfaz del switch para habilitar la autenticación.
2) Control del puerto administrativo: El modo automático hace que la interfaz cambie entre el estado autorizado y no autorizado según el intercambio de paquetes de autenticación entre el switch y el suplicante.
3) Asignación RADIUS VLAN: La asignación dinámica de VLAN funciona exclusivamente cuando el modo 802.1X está configurado en sesión múltiple. Esta opción hace que un puerto autenticado correctamente se una a la VLAN asignada por el servidor RADIUS de forma automática.

Los atributos que el servidor debe enviar al switch son: Tunnel-Type = VLAN, Tunnel-Medium-Type = 802 y Tunnel-Private-Group-Id = ID de VLAN.

C. Autenticador inalámbrico

Como autenticador inalámbrico se emplea el router AP Linksys WRT-54GL el cual utiliza un hardware compatible con Linux, por lo que permite cargar un firmware distinto al original. El sistema operativo usado en el router inalámbrico para realizar las pruebas de funcionalidad es DD-WRT, un firmware basado en Linux y liberado bajo la licencia GPL, para instalarlo es necesario descargar los archivos DD-WRT de su página oficial y cargarlo en el AP accediendo al menú: Administración > Firmware Upgrade > Seleccionar Archivo > Upgrade.

En el menú: Wireless > Wireless Security, se establece WPA2-Enterprise como el modo de seguridad por defecto para los usuarios de la red inalámbrica, empleando los algoritmos TKIP y AES en conjunto para lograr mayor compatibilidad con los suplicantes. En la Figura 13, se pueden ver todos los parámetros configurados en el AP WRT-54GL.

Figura 13. Configuración del servidor RADIUS AP WRT-54GL

D. Suplicante

Para acceder a la red de datos protegida por el sistema AAA, los usuarios requieren de un software adicional (suplicante) que soporte el método de autenticación EAP-TTLS implementado, cualquier dispositivo que incumpla con este requerimiento no podrá conectarse a la infraestructura de red de ninguna forma.

SecureW2 es un cliente TTLS para las plataformas Windows, en el caso de sistemas operativos como GNU/Linux o Android no es necesaria su instalación debido a que tienen soporte nativo para este tipo de autenticación, incluso Windows en su última versión (Windows 8) lo trae por defecto.

Figura 14. Suplicante SecureW2

E. Firewall-Shorewall

Shorewall es una herramienta de código abierto que permite crear firewalls robustos sobre plataformas GNU/Linux, se basa en el sistema Netfilter/iptables integrados por defecto en el kernel de Linux, mediante el cual se definen las reglas y políticas para el manejo de los paquetes que transitan a través de él.

La configuración y administración de Shorewall se lo hace con la herramienta de administración Webmin, el procedimiento general seguido para la puesta en marcha del firewall se detalla a continuación:

- Editar los parámetros básicos para activar el servicio Shorewall en Ubuntu Server.
- Definir las zonas de red: WAN, LAN, DMZ, FW, VLANs.
- Agregar las interfaces de red del sistema que usará Shorewall para la gestión de las reglas y políticas del firewall.
- Configurar las acciones por defecto para el tráfico entre zonas del firewall.
- Definir las reglas para permitir o denegar el acceso a servicios o puertos desde y hacia las zonas del firewall.

V. CONCLUSIONES

Con la implementación del servidor AAA utilizando software libre se logró controlar el acceso a todos los usuarios de forma centralizada y la asignación dinámica de recursos de red se realizó exitosamente de acuerdo al rol que desempeña cada trabajador dentro de la institución, obteniendo una relación costo beneficio positiva que garantiza la viabilidad del proyecto.

Se determinó el método de autenticación EAP-TTLS como el más adecuado y seguro para implementar el sistema AAA en el GAD Municipal de San Miguel de Urcuquí, que a través de un canal seguro establecido mediante certificados digitales garantizan la confidencialidad de los datos en el proceso de autenticación.

Integrando el servidor RADIUS con el directorio LDAP se logró una administración centralizada del sistema AAA, sincronizando las cuentas de usuario de autenticación con los privilegios de acceso para el proceso autorización.

Se denegó el acceso a todos los usuarios que no cumplieron con los requerimientos de autenticación y se asignó de manera dinámica los recursos de red utilizando redes virtuales (VLAN) dinámicas.

Los tres servidores usados para proveer el servicio de autenticación, autorización y auditoria en la red del GADMU se instalaron sobre el entorno de virtualización PROXMOX, lo cual garantiza una reducción de costos significativa al momento de su implementación.

Cuando se utiliza un directorio LDAP para almacenar las credenciales de usuario, el sistema automáticamente almacena las contraseñas de usuario usando algoritmos hash, debido a que estos hash son irreversibles es necesario elegir PAP como método de autenticación interno dentro del túnel TLS.

La información de contabilidad es posible registrar en una base de datos relacional SQL únicamente cuando el equipo autenticador (router inalámbrico o switch) es capaz de enviar los datos relacionados con la contabilidad 802.1x, caso contrario el administrador de red tiene la posibilidad de administrar el servicio usando los registros log por defecto generados por el servidor FreeRADIUS.

Los equipos autenticadores usados en la implementación del sistema, soportan el servicio de contabilidad 802.1x, lo que permitió registrar en la base de datos MYSQL toda la información referente a los usuarios que accedieron al sistema correctamente y los intentos fallidos de conexión, detallando el día y la hora de dicho acceso o rechazo.

En las pruebas de acceso se utilizó el sistema operativo Windows 7 debido a que no tiene soporte nativo para el método de autenticación EAP-TTLS y se debe instalar un suplicante para añadir la funcionalidad, el software empleado fue SecureW2.

La asignación dinámica de VLAN se lo hizo a través del directorio LDAP, para que un puerto del switch pueda moverse dinámicamente entre una y otra red virtual se debe configurar en modo general, si el puerto está en modo acceso es miembro sin etiquetar de una sola VLAN por lo que no se puede unir a redes diferentes.

VI. REFERENCIAS

[1] Fernández, Y., Ramos, A., & García, J. (2008). *RADIUS / AAA / 802.1X : Sistemas basados en la autenticación en Windows y GNU/Linux.* Madrid: RA-MA Editorial.

[2] Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS).* Obtenido de http://tools.ietf.org/pdf/rfc2865.pdf

[3] *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control.* (2 de Febrero de 2010). Obtenido de IEEE Std 802.1X-2010: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

[4] Funk, P., & Blake, S. (Agosto de 2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0).* Obtenido de http://tools.ietf.org/pdf/rfc5281.pdf

[5] Nakhjiri, M., & Nakhjiri , M. (2005). *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility.* USA: John Wiley & Sons Ltd. doi: 10.1002/0470017465.

[6] Howes, T., Smith, M., & Good, G. (2003). *Understanding and Deploying LDAP Directory Services* (2nd ed.). Boston: Pearson Education, Inc.

[7] Butcher, M. (2007). *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services.* Reino Unido: Birmingham: Packt Publishing Ltd.

[8] CISCO. (2008). *CCNA 3 Exploration 4.0: Conmutación y conexión inalámbrica de LAN.* Obtenido de http://es.scribd.com/doc/17481738/Cisco-CCNA-3-Exploration-Conmutacion-y-Conexion-Inalambrica-de-Lan-Version-40-Espanol

VII. BIOGRAFÍA

Director – Ing. Carlos A. Vásquez A.
Nació en Quito provincia de Pichincha el 19 de Septiembre de 1981. Ingeniero en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional (EPN) en Quito-Ecuador en 2008. Master en Redes de Comunicación, Pontificia Universidad Católica del Ecuador, Quito-Ecuador. Actualmente es Docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador.

William E. Vaca A.
Nació en Ibarra-Ecuador el 7 de Mayo de 1988. En el año 2005 obtuvo su título de Bachiller en Ciencias con especialización Físico Matemático en el "Colegio Nacional Teodoro Gómez de la Torre". Actualmente, es egresado de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.