UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE COMUNICACIÓN

"SERVIDOR AAA PARA VALIDACIÓN Y CONTROL DE ACCESO DE USUARIOS HACIA LA INFRAESTRUCTURA DE NETWORKING DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

INFORME TÉCNICO

AUTOR: Luis Carlos Plasencia Bedón

DIRECTOR: Ing. Carlos Vásquez

Ibarra, Julio 2012

ÍNDICE DE CONTENIDOS

Servidor AAA para validación y control de acceso de usuarios hacia la infraestructura de Networking de un ente del ministerio de defensa nacional (Julio de 2012)

Carlos Plasencia – Autor, Ing. Carlos Vásquez - Director

***Resúmen*—En los tiempos actuales la seguridad de la información es un tema de suma importancia para cualquier organización o institución, debido a las facilidades de las comunicaciones que se brinda a los usuarios a través de servicios internos y públicos (Internet) para el desarrollo de sus actividades laborales, por tal motivo no se debe descuidar la protección de los datos que circulan por la red. El presente proyecto mediante la implementación de un servidor AAA valida el acceso de los usuarios que ingresan a la infraestructura de networking del ente del Ministerio de Defensa Nacional con la finalidad de asegurar la conexión a la red sólo a usuarios autorizados y complementariamente a la solución se utiliza infraestructura UTM desarrollada sobre software libre que controla el acceso de usuarios a los recursos de red de la institución.**

***Index Terms*— Estándar 802.1x, GNU Linux, LDAP, Servidor AAA, UTM.**

I. ESTUDIO DE SITUACIÓN ACTUAL Y REQUERIMIENTOS DE ACCESO DE USUARIOS DEL ENTE DEL MINISTERIO DE DEFENSA NACIONAL

A. Análisis del estado actual de la entidad

El ente del Ministerio de Defensa Nacional es el encargado de administrar y gestionar el backbone principal de las comunicaciones a nivel nacional, y en la actualidad no consta de métodos y esquemas que garanticen la confidencialidad, integridad y disponibilidad de la información que se maneja internamente en la red LAN (Local Area Network, Red de Área Local).

No existe control de los usuarios que acceden a los recursos de la red, pudiendo de esta manera existir intrusiones de sujetos con fines desconocidos que pueden perjudicar o comprometer la información que circula por la red.

La institución cuenta con dos infraestructuras, una de telefonía y otra de networking, las mismas que son administradas en los cuartos de telecomunicaciones ubicados en cada bloque del edificio. Tanto la infraestructura de telefonía como la de networking cuentan con su propio personal de administración, sin embargo, no poseen normas de control de acceso de los individuos que ingresan a dichos cuartos, creando una amenaza de seguridad. En este sentido las personas que acceden a los cuartos de telecomunicaciones, fácilmente pueden desconectar el cable de conexión de un usuario que se encuentre ausente y usurpar la información que se transmite por la red.

En la actual infraestructura no se cuenta con mecanismos de autenticación de usuarios para el acceso hacia los recursos de red tanto en la red cableada como en la red inalámbrica.

Actualmente no se cuenta con infraestructura para control de navegación de internet por lo que cada usuario puede utilizar este recurso sin medida, causando problemas de lentitud a otros que lo necesitan para desarrollar sus actividades laborales. De igual forma no existe control de los usuarios que acceden desde las redes LAN y de datos hacia aplicaciones internas como correo institucional, portales web, sistemas integrados, entre otros.

Una de las mayores debilidades en cualquier organización, es que los directivos se preocupan sólo de poseer el servicio de internet sin tomar en cuenta la optimización del recurso para el desempeño laboral, y tampoco piensan en lo peligroso que puede ser al no contar con esquemas de control de acceso del tráfico de internet, por lo que se vuelven vulnerables a ciertos ataques que puedan producirse desde el exterior de la red.

B. Recomendaciones y políticas del SGSI afines al control de acceso de usuarios

El ente del ministerio de defensa Nacional posee un Sistema de Gestión de Seguridad de Información (SGSI) basado en la norma ISO-27001. El SGSI es un documento que ayuda a las instituciones u organizaciones a establecer políticas, procedimientos y controles en relación a los objetivos de la razón de ser de la institución, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización.

En este documento se encuentran definidas las políticas sobre el correcto uso de los recursos informáticos además especifica las recomendaciones para la gestión de contraseñas tanto de usuarios como de administradores con las respectivas responsabilidades sobre ellas como por ejemplo:

Garantizar que las contraseñas cumplan con las características siguientes:

- Utilizar al menos 8 caracteres.
- Utilizar letras mayúsculas, minúsculas, símbolos y números.
- Los usuarios deben cambiar las contraseñas cada 120 días.
- Los administradores deben cambiar las contraseñas cada 90 días.
- No deben re-utilizarse contraseñas.

II. INTEGRACIÓN DEL ESTANDAR IEEE 802.1X

A. Importancia del control de acceso en la seguridad de la información

El control de acceso, en sistemas de información, es la capacidad de controlar la interacción de un elemento activo (usuario, dispositivo, servicio) con un recurso informático (red de datos, sistema, servicio). Adicionalmente, el control de acceso implica procedimientos de identificación, autenticación y autorización para permitir o denegar el uso de los recursos así como para llevar un registro de este.

La seguridad es un tema importante en las redes tanto cableadas como inalámbricas, porque alrededor de la red local se encuentran personas que buscan obtener información confidencial para utilizarla con fines desconocidos que pueden perjudicar la seguridad de la información y la imagen de la institución.

En la gran mayoría de instituciones y empresas se reciben ataques desde su propia red, generalmente efectuados por empleados que tienen desconocimiento en el uso de los sistemas informáticos o insatisfechos con intereses ocultos. Evitar que dichos ataques se lleven a cabo mejora la calidad de los procesos de seguridad de la institución.

B. Conceptos de seguridad de información

El objetivo de la seguridad de información es proteger los datos de la institución, se debe considerar tres aspectos muy importantes en la preservación de la misma, los cuales son la confidencialidad, integridad y disponibilidad.

- La confidencialidad consiste en permitir que la información esté autorizada y sea únicamente vista por las personas a quienes está destinada, es decir, se refiere a la privacidad de la información. Para este fin se utilizan mecanismos de encripción de los datos.
- La integridad hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad, por ejemplo: la huella digital, firma digital, entre otros.
- La disponibilidad hace referencia a que la red, hardware y software sean confiables, es decir se puedan recuperar rápido y completamente ante eventos de una interrupción. Para poder lograr este objetivo se emplean generalmente mecanismos de redundancia de enlaces, hardware y software, con el fin de que en caso de que un evento interrumpa el funcionamiento de uno de estos elementos del sistema, el respaldo redundante solucione el problema lo más rápido posible.

C. Ataques y vulnerabilidades

Es importante conocer el por qué implementar esquemas o métodos de seguridad de información, y además, entender contra qué hay que tomar medidas de prevención.

- Un ataque es una técnica empleada para aprovechar alguna debilidad o falla de un sistema (vulnerabilidad), por ejemplo una amenaza podría ser el

ataque de negación de servicio, siendo la vulnerabilidad el empleo de un esquema de seguridad diseñado sin considerar esta amenaza.

- Una amenaza es toda posible interrupción de operación, integridad, disponibilidad de la red o sistema, pudiendo ser la misma de origen natural, por negligencia, por intrusos, mala manipulación o por intenciones indebidas como los hackers.
- Una vulnerabilidad es una debilidad propia de los sistemas que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones, causados por un error en el diseño, configuración o implementación de las redes o servicios.

D. Estándar IEEE 802.1X.

Los estándares son un conjunto de especificaciones tecnológicas establecidas por un organismo controlador que en este caso es el Instituto de Ingenieros en Electrónica y Electricidad, conocidos con sus siglas en inglés como IEEE, para que los productores y desarrolladores de tecnología tengan una normativa que les permita lograr que los dispositivos puedan operar entre sí.

IEEE 802.1X permite implementar un acceso seguro, empleando medios de comunicación como Ethernet, Token Ring y LANs inalámbricas 802.11. El empleo del protocolo RADIUS (Remote Autentication Dial-Up Server, Servidor de Autenticación Remota Dial-In) es opcional dentro de IEEE 802.1X, la IEEE espera que varios autenticadores IEEE 802.1X funcionen como un cliente y servidor de autenticación a la vez.

El estándar IEEE 802.1X define el control de acceso a redes basadas en puertos, es decir, permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o evitando el acceso por ese puerto si la autenticación falla. Gracias a él se exige autenticación antes de dar acceso a las redes ethernet. En el control de acceso a redes basadas en puertos se utilizan los elementos físicos que componen una infraestructura de conmutación de la red LAN para autenticar los dispositivos agregados al puerto de conmutación. No se pueden enviar ni recibir tramas en un puerto de conmutación ethernet si el proceso de autenticación ha fallado.

A pesar de que se diseñó para redes ethernet fijas, este estándar se ha adaptado para su uso en redes LAN inalámbricas con IEEE 802.11. Windows XP soporta la autentificación IEEE 802.1X para todos los adaptadores de red basados en redes LAN, incluyendo las ethernet y las inalámbricas.

IEEE 802.1X se apoya en el protocolo de autenticación EAP (Extensible Autentication Protocol, Protocolo de Autenticación Expandible), aunque en realidad es EAPoL (Extensible Autentication Protocolo over LAN, Protocolo de Autenticación Expandible sobre LAN) de forma que se puede usar en redes ethernet, 802.11, Token-Ring y FDDI (Fiber Distributed Data Interface) Interfaz de Datos Distribuida por Fibra).

Cuando un nodo requiere tener acceso a otro recurso de una red LAN, el Access Point o switch de acceso pregunta la identidad de dicho nodo, el tráfico permitido entre el nodo y el punto de acceso o switch es EAP hasta que el nodo sea autenticado.

El proceso de autenticación 802.1X/EAP, consiste de tres elementos importantes, un suplicante (usuario), un autenticador (Access Point o switch) y un servidor de autenticación (FREERADIUS). El suplicante es el dispositivo que solicita acceso a la red generalmente el usuario. El autenticador es un dispositivo intermediario que pasa las tramas desde el usuario al servidor de autenticación, generalmente el punto de acceso inalámbrico o un switch de acceso. El servidor de autenticación es el dispositivo que actualmente autentica el usuario, generalmente el servidor FREERADIUS.

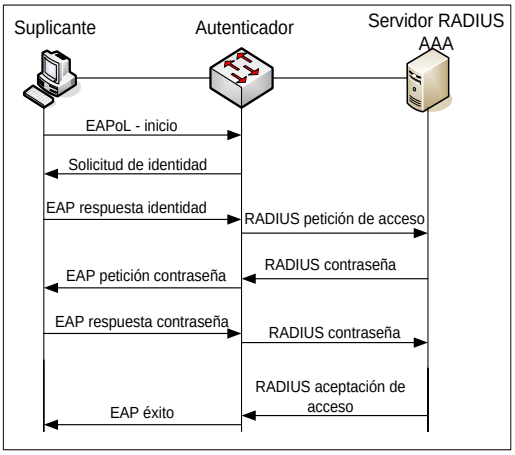

Fig. 1. Autenticación 802.1X. Se muestra las tramas intercambiadas entre el suplicante y el autenticador y los mensajes entre el Autenticador y servidor de autenticación.

1) Tramas 802.1X

En la autenticación se utiliza el protocolo EAP (especificado en el RFC-3748) para intercambiar información de autenticación entre el Suplicante y Servidor de Autenticación. EAP puede utilizar diversos mecanismos de autenticación tales como MD5, Kerberos, Encriptación con Clave Pública (PKE), Contraseñas de un solo uso (OTPs), entre otras. EAP consiste en un simple encapsulado que puede correr sobre diferentes niveles de enlace. Las tramas de autenticación deben ser transportadas entre el Suplicante y el Servidor de Autenticación. Para ello se ha elegido un protocolo que transporta EAP directamente sobre un servicio de Red de Area Local (EAPOL).

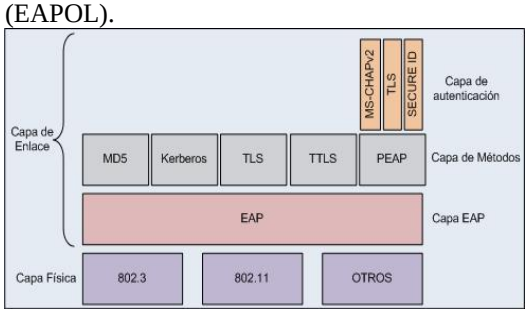

Fig. 2. Arquitectura 802.1X. Presenta el modelo de 802.1X por capas con los respectivos métodos de cifrado.

Los campos presentes en una trama 802.1X son los siguientes:

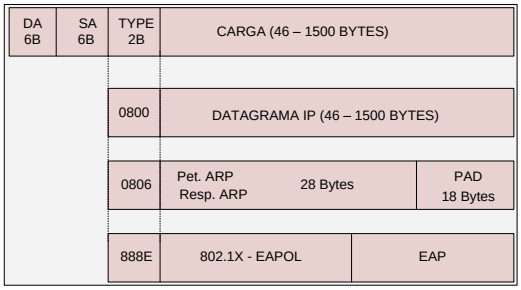

Fig. 3. Trama Ethernet. Campos presentes en una trama Ethernet con soporte de 802.1X.

Para el proyecto se utiliza las tramas de tipo 888E las cuales sirven para determinar el tipo de comunicación que se va a establecer antes de acceder a la red, en este caso una autenticación 802.1X.

2) Definición de servicios AAA

Las siglas AAA significan Autenticación, Autorización y Contabilidad (en inglés Authentication, Authorization, Accounting).

Los niveles de confidencialidad, integridad y disponibilidad de la información se complementan con niveles adecuados de autenticación, mecanismos de control de acceso, definición de niveles de acceso a servicios o perfiles y control del tiempo que los usuarios permanecen conectados durante el desempeño de sus labores.

La autenticación Garantiza que la identidad del individuo que se valida corresponda a su propietario. Cada usuario que intente acceder a la red de datos o servicios de la misma, posee un distintivo único que es su identidad, por lo que, para poder acceder a los servicios de red deberá autenticarse con sus respectivas credenciales. En este caso las credenciales serán el nombre de usuario y contraseña, pues a través de éstas se define si el usuario cuya identidad se quiere verificar es quien dice ser.

La autorización es la asignación de recursos adicionales, que permite tener un control de acceso por usuario después de la autenticación. Permite realizar un control de acceso de un usuario a determinados servicios de la red, en función de un perfil prestablecido, el cual será aplicado en base a la identidad del usuario que fue autenticado.

La contabilidad se refiere a llevar el registro de toda la actividad realizada por un usuario desde el momento que accedió a la red hasta que finalizó su sesión, es decir, permite llevar un control de uso del sistema en base a la identidad de quién accedió, a que accedió y por cuánto tiempo permaneció dentro del sistema.

3) Protocolo RADIUS

RADIUS (Remote Authentication Dial-In User Server) es un protocolo que permite gestionar la "autenticación, autorización y contabilidad" de usuarios sobre un determinado recurso.

El protocolo RADIUS proporciona un servicio de acceso centralizado. Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan acceso a Internet o grandes redes corporativas, en un entorno con diversas tecnologías de red incluyendo módems, xDSL, VPN (Virtual Private Network, Red Privada Virtual) y redes inalámbricas.

Los mensajes RADIUS se envían como mensajes de datagramas de usuario UDP. El puerto UDP 1812 se utiliza para los mensajes de autenticación RADIUS y el 1813 para los mensajes de administración de cuentas RADIUS. La carga UDP de un paquete RADIUS sólo incluye un mensaje RADIUS.

El formato de un mensaje RADIUS se presenta en la siguiente figura:

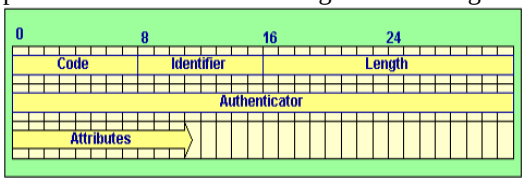

Fig. 4. Formato del Mensaje RADIUS. Campos del mensaje que se intercambian entre el autenticador y el servidor AAA.

Los campos en un paquete RADIUS son:
Code (Código). Un octeto que contiene el tipo de paquete.

Tabla 1. Tipo de paquete RADIUS

Valor	Descripción
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

- *Identifier (Identificador).* Un octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud adecuada.
- *Length.* Longitud del paquete (2 octetos).
- *Authenticator (Verificador).* Valor usado para autenticar la respuesta del servidor RADIUS. Es usado en el algoritmo de encubrimiento de contraseña.
- *Attributes (Atributos).* Aquí son almacenados un número arbitrario de atributos. Los únicos atributos obligatorios son el User-Name (usuario) y el User-Password (contraseña).

4) Protocolos EAP

Algunos de los mecanismos de autenticación EAP, se presenta con una breve descripción de cada uno:

- EAP-MD5, MD5-Challenge requiere nombre de usuario y contraseña, es equivalente a CHAP, poco empleado en autenticación en ambientes inalámbricos.
- Lightweight EAP (LEAP), envía un nombre de usuario y contraseña al servidor de autenticación, es protocolo propietario desarrollado por CISCO y es considerado no seguro por lo que se está dejando fuera LEAP para emplear PEAP.
- EAP-TLS, crea una sesión TLS (Transport Layer Security) dentro de EAP, entre el suplicante y el servidor de autenticación, siendo necesario en el servidor y el cliente un certificado digital y una infraestructura PKI (Public Key Infraestructure, Infraestructura de Clave Pública), esta autenticación es bidireccional.
- EAP-TTLS, se establece un túnel encriptado TLS para transporte de datos de autenticación, dentro de este túnel TLS otros métodos de autenticación se pueden emplear.
- PEAP (Protected EAP, EAP Protegido), emplea como EAP-TLS un túnel encriptado TLS, los certificados de suplicante para EAP-TTLS y EAP-PEAP son opcionales, pero los certificados del servidor de autenticación son necesarios.
- EAP-MSCHAPv2, requiere un nombre de usuario y contraseña, y en resumen es encapsulamiento EAP de MS-CHAP-v2.

5) Selección del sistema operativo para la implementación del servicio AAA

En el mercado actual existe un sinnúmero de sistemas operativos para todos los gustos, para todas las aplicaciones, para todo el mundo, y en el momento de elegir tal o cual sistema operativo el usuario elige el que se preste más a las necesidades.

Para la implementación del servicio AAA se optó por el sistema operativo Debian GNU/Linux por las siguientes razones:

- Mantener el estándar de aplicaciones sobre el mismo sistema operativo.
- Aprovechamiento de funcionalidades de virtualización sin costos.
- Decreto 1014 que apoya el uso de software libre.
- Compatibilidad con aplicaciones existentes.
- Características propias del sistema operativo.

6) Importancia de la alta disponibilidad

La alta disponibilidad (High Availability) es una arquitectura de diseño del sistema y la implementación está asociada a asegurar la continuidad operacional de los servicios. La disponibilidad se refiere a: continuidad de acceso a sistemas y poder realizar nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un

usuario no puede acceder al sistema, se dice que está no disponible, el servicio se encuentra interrumpido. El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible y es un parámetro que sirve para definir los tiempos de recuperación del servicio.

III. DISEÑO DEL SERVIDOR AAA

A. Diseño de la solución

Debido a la inexistencia de esquemas de control de acceso de los usuarios que acceden a la red, la solución implementada ha tomado en cuenta algunos aspectos importantes como:

- Los equipos de parte activa son de la marca 3Com y soportan el estándar 802.1X.
- El uso del sistema operativo Microsoft Windows XP en los usuarios de la institución es estándar. Esta característica facilita la integración de la solución ya que IEEE 802.1X es nativo para este sistema operativo.
- La institución cuenta con una base de datos centralizada de usuarios LDAP.
- La institución dispone de hardware para la implementación de servicios.

El control de acceso de los usuarios hacia la infraestructura de networking se realiza mediante la utilización del estándar 802.1X. En el siguiente esquema se presenta la integración de la solución AAA y la arquitectura de red implementada en la institución:

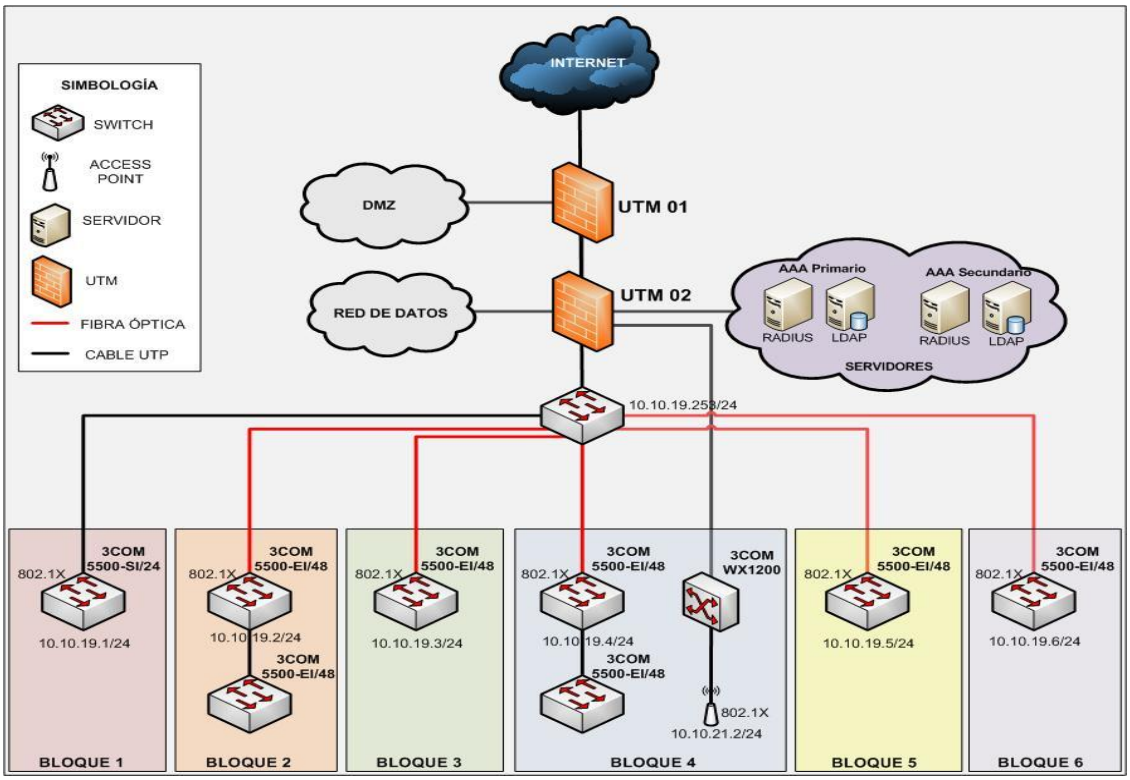

Fig. 5. Arquitectura de red implementada. Muestra la integración de la solución AAA y UTM para control de tráfico entrante y saliente entre zonas.

El diseño implementado consta de un servidor AAA primario y de un servidor AAA secundario, cada servidor cuenta con su propia base de datos de autenticación de usuarios LDAP. El servidor AAA primario autentica contra la base de datos LDAP-Master y el servidor AAA secundario autentica contra la base de datos LDAP-Slave. Estas bases de datos se encuentran sincronizadas y todos los cambios que se realice en el LDAP-Master se replican automáticamente hacia el LDAP-Slave. Se debe tomar en cuenta que los datos se pueden modificar sólo en el LDAP-Master porque solamente éste tiene privilegios de escritura sobre la base, mientras el LDAP-Slave tiene privilegios sólo de lectura.

Al tener el esquema Master-Slave de la base de datos se evita que exista inconsistencia en los datos.

El esquema de implementación es redundante ya que es uno de los servicios más críticos de la institución. Si por algún motivo el servidor AAA primario no estuviese disponible, ningún usuario de la red interna LAN podría acceder a los servicios de red, y por lo tanto causaría la interrupción en la operación de sus actividades.

El estándar 802.1X se configura en el equipo cliente para que los usuarios se autentiquen con el nombre de usuario y contraseña luego de iniciar la sesión.

En los switch 3Com 5500 que conforman la capa de acceso a la red se configura el estándar 802.1X para interactuar entre los usuarios y el servidor AAA de autenticación. En todos los equipos de acceso se configura tanto la dirección IP del servidor AAA primario como la dirección IP del servidor AAA secundario para obtener alta disponibilidad del servicio.

B. Funcionamiento de la implementación

El esquema de funcionamiento se muestra en la siguiente figura:

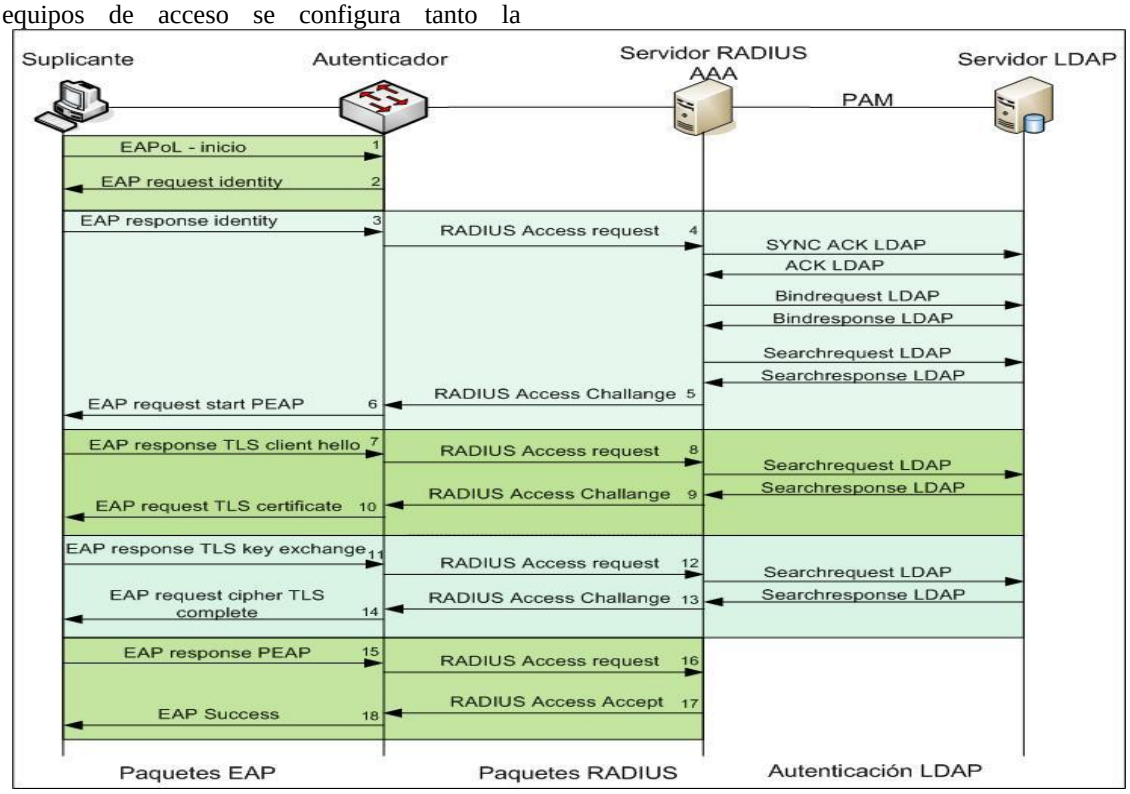

Fig. 6. Funcionamiento del sistema AAA. Intercambio de tramas entre el equipo del usuario y el autenticador, mensajes enviados entre el autenticador y el servidor AAA y consultas al servidor LDAP

1. El suplicante inicia solicitando conexión de red. Para darle acceso al usuario se iniciará el proceso de autenticación enviando un mensaje EAPoL de inicio hacia el equipo de acceso (Switch o AP).
2. El autenticador envía un mensaje de solicitud de identidad al usuario.
3. El usuario envía un EAP de identidad al autenticador.
4. La trama EAP response identity se encapsula en un mensaje RADIUS y el autenticador envía un mensaje de petición de acceso al servidor RADIUS.
5. El servidor RADIUS inicia la negociación del método EAP que se utilizará para el establecimiento del canal seguro enviando una trama RADIUS Access-challenge.
6. El autenticador envía al usuario un EAP con petición de establecimiento de canal con EAP de tipo PEAP.
7. El usuario negocia el método de la conexión y envía al autenticador un EAP de respuesta con el saludo para establecimiento del canal TLS (client hello).
8. EL autenticador encapsula el mensaje EAP-Response en un mensaje RADIUS-request y lo envía al servidor.
9. EL servidor verifica el mensaje enviado por el usuario y le responde con su certificado en un mensaje RADIUS-Challenge. El mensaje contiene un server hello[1] + server certificate[2] + server hello done.
10. El autenticador recibe el mensaje RADIUS y envía el certificado del servidor al usuario en un EAP-request TLS de credencial del usuario.
11. El usuario responde un mensaje EAP intercambiando la contraseña en el

[1] Server hello.- Saludo del servidor en respuesta de un client hello.
[2] Server certificate.- Certificado del servidor.

canal cifrado. El mensaje EAP-response TLS contiene el client key Exchange, change cipher spec y encrypted handshake message.

12. La trama EAP-Response TLS se encapsula en un mensaje RADIUS-Request y se envía al servidor RADIUS, el mensaje llega encriptado con la contraseña del usuario y es verificada en la base de datos LDAP.
13. El servidor responde:
    a. Si la contraseña del usuario es correcta el servidor responde con un mensaje RADIUS-Challange para finalizar el establecimiento del canal TLS.
    b. Si las credenciales no son correctas rechaza la conexión (RADIUS-Reject) y el puerto del switch al que se conecta el usuario se pone en estado down.
14. El autenticador recibe un RADIUS-Challange para finalizar de establecer el canal TLS y le envía al usuario un EAP-Request de canal cifrado completo.
15. El usuario envía un mensaje EAP-PEAP de respuesta y solicita acceso a la red.
16. La solicitud de acceso a la red es enviara al servidor mediante un mensaje RADIUS-request.
17. El servidor responde con un mensaje de RADIUS-ACCEPT hacia el autenticador.
18. El autenticador envía un mensaje EAP-Succsess y el usuario ya se encuentra habilitado para usar los recursos de la red.

C. Requisitos del sistema para la implementación 802.1X

Los elementos que conforman la arquitectura de funcionamiento de la integración del servidor AAA con la infraestructura de la institución son:

- Cliente: Windows XP con Service Pack 2 o 3, el uso de éste sistema operativo se encuentra estandarizado en todo el edificio.
- Servicio de autenticación: servidor RADIUS desarrollado en software libre.
- Método de autenticación: EAP-PEAP
- Cifrado usado con PEAP: MSCHAPv2
- Base de datos de autenticación de usuarios: LDAP.
- Clientes para autenticación: Switch 3Com 5500-EI.
- Clientes para autenticación inalámbrica: AP con soporte del estándar 802.1X.

D. Diseño de la infraestructura del servidor de autenticación

Para la implementación del servidor de autenticación AAA primario y secundario se dispone de una cuchilla Intel HS-22 y HS-21 de la infraestructura BLADE, las mismas que tienen las siguientes características:

- Procesador: Intel XEON 3.2 GHz
- Memoria: 32 GB
- Disco Duro: 2 x 140 GB configurados en RAID 1
- Interfaces de red: 2 (10/100/1000)

El esquema de virtualización implementado es el siguiente:

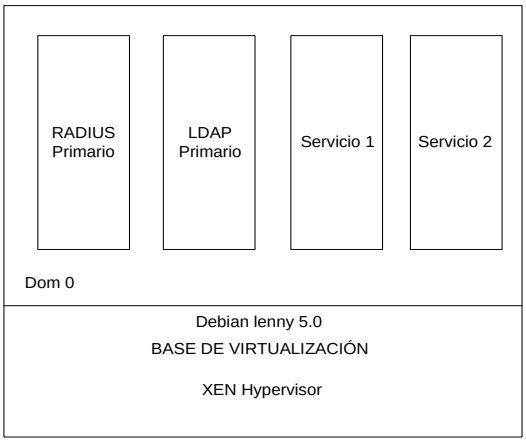

Fig. 7. Esquema de virtualización. Muestra las máquinas virtuales instaladas sobre el servidor físico.

La máquina virtual que ejecuta el servicio RADIUS primario tiene asignado los siguientes recursos:

- Memoria: los requerimientos básicos para ejecutar una máquina virtual con sistema operativo Debian Lenny es de 256 MB. Los usuarios que se controlan en la institución crecen constantemente, por tal razón está asignada 1 GB de memoria RAM.
- Espacio en Disco: este servidor almacena los registros de los usuarios que acceden a la red, por lo tanto tiene asignado 20 GB de disco.

E. Control de acceso a aplicaciones

Una vez que los usuarios son autenticados y autorizados ya pueden hacer uso de los recursos de la red. Hasta este momento ya se conoce que los usuarios que ingresan a la red son sólo aquellos que están autorizados en la institución, pero se debe tomar en cuenta que no se está teniendo control del acceso hacia las aplicaciones y servicios institucionales.

Con la implementación de un servidor UTM interno que controle el tráfico desde los entes externos hacia los servicios internos de la institución se reduce la posibilidad de obtención de información de manera no autorizada, además se controla el acceso de los usuarios hacia las aplicaciones necesarias para el desarrollo de sus actividades, de igual manera a los usuarios de la red LAN hacia servicios públicos.

IV. IMPLEMENTACIÓN DEL SERVIDOR AAA EN LA RED INTERNA DEL ENTE DEL MINISTERIO DE DEFENSA NACIONAL

A. Configuración del servidor AAA

La instalación del servidor AAA está realizada sobre la plataforma LINUX con el sistema operativo Debian Lenny 5.0 con el software FREERADIUS 2.0.4, el mismo que utiliza la base de datos LDAP Master existente.

La versión de freeradius que incluye los repositorios del sistema operativo no soporta el protocolo EAP-PEAP, por lo cual la versión instalada de freeradius es compilada, ya que a ésta se habilita el soporte de los protocolos de encripción EAP-PEAP, EAP-TLS y EAP-TTLS, además incluye, el módulo OPENSSL, los cuales son necesarios para aplicar un método de encriptación seguro para el intercambio de información entre el servidor AAA y el usuario.

Cada vez que se realiza una actualización del sistema operativo se instalan las nuevas versiones de los paquetes y en ciertos casos traen nuevos cambios que pueden afectar el funcionamiento normal del servicio. Para evitar que esto suceda se utiliza la protección de la versión instalada.

El método de autenticación de freeradius utilizado es PEAP el cual se basa en los certificados digitales del servidor, por lo tanto es necesario generarlos utilizando OPENSSL y luego cargarlos al servidor AAA.

1) Configuración de FREERADIUS

Los ficheros que se deben modificar para el funcionamiento de FREERADIUS son los siguientes:

- *eap.conf*.- Define el método de encriptación para el envío de datos.
- *radiusd.conf*.- El fichero principal de freeradius.
- *defaulf*.- Definir la utilización del módulo LDAP.
- *inner-tunnel*.- Sincronización del túnel para comunicación del servidor freeradius.
- *clients.conf*.- Define las entidades que tendrán la función de autenticador.
- *ldap.conf*.- Conexión con la base de datos de los usuarios LDAP.
- *ldap.attrmaps*.- Definir atributos para asignación dinámica de VLAN.
- *samba.schema*.- Esquema samba para control de dominios.

B. Configuración del autenticador

Los equipos que van a cumplir está función son los 7 switches de la marca 3Com de la serie 5500G-EI y el switch 3Com 5500-SI, en los mismos que se realizan las configuraciones para que soporten el método de encriptación EAP.

C. Configuración del equipo del usuario

Para que el usuario pueda acceder a la red y a sus recursos, la tarjeta de red se configura para que soporte la autenticación 802.1X, caso contrario el puerto en el que se encuentra conectado el equipo, por ningún motivo puede acceder a la red.

D. Implementación de UTM interno y externo

Una vez que el usuario es autenticado y autorizado para hacer uso de los recursos de red, mediante la implementación del UTM se le limita el acceso únicamente a los servicios necesarios.

Los servidores encargados del control del tráfico hacia la red interna de la institución tienen instalado el siguiente software:

- Sistema Operativo: Debian Lenny 5.0
- Firewall: Shorewall
- IDS: Snort
- IPS: PSAD

- Monitoreo de tráfico: NTOP
- Monitoreo Ancho de banda MRTG

V. CONCLUSIONES Y RECOMENDACIONES

A. CONCLUSIONES

El servidor AAA valida a los usuarios que intentan acceder a la infraestructura de networking de la institución, consultando la base de datos de usuarios LDAP, si el usuario no es encontrado o la contraseña es incorrecta, el servidor rechaza la petición de acceso del usuario, y no le permite hacer uso de los recursos ofrecidos en la institución.

El método de autenticación PEAP es uno de los más utilizados dentro de implementaciones AAA debido a la facilidad de integración y por su elevado nivel de seguridad. Cuando el usuario se autentica contra el servidor usando su nombre y contraseña el canal se cifra usando TLS basado en la confianza del certificado digital del servidor.

Poseer esquemas de seguridad es imprescindible para proteger la información que circula por la red. Como se apreció en el presente trabajo con la implementación del estándar 802.1X se controla a los usuarios que acceden a la red interna de la institución otorgando acceso únicamente al usuario permitido.

El sistema de autentificación esta implementado en todos los dispositivos que soportan el estándar 802.1X. En la actualidad la mayoría de equipos de acceso de distintas marcas están diseñados con soporte del estándar facilitando la integración de seguridad en redes que no poseen control de acceso de sus usuarios.

Usar bases de datos para realizar la autenticación de usuarios centraliza y facilita la administración de usuarios, ya que si se desea cambiar de contraseña, sólo se cambia una sola vez.

La implementación de infraestructura de seguridad trabaja adecuadamente cuando se encuentra apoyada por normas y políticas sobre el uso de recursos informáticos como son: usuarios, contraseñas, internet, portales web, etc.

El sistema operativo Linux seleccionado para la instalación del servidor AAA fue Debian para mantener un estándar a nivel de las aplicaciones y servicios en la institución, además por las ventajas que posee en cuanto a la virtualización, ya que la limitación que se presenta es por la capacidad de hardware más no por la cantidad de máquinas virtuales que pueden crearse sin costo alguno.

Llegar a tener seguridad total en una red es inalcanzable pero con la mejora continua y la adopción de métodos y estándares de seguridad de la información se mantiene un nivel de seguridad aceptable que reduce los riesgos de la red.

A pesar de las existencias de nuevas técnicas y dispositivos innovadores con respecto a la administración de seguridad, se puedan usar viejas técnicas o soluciones para adaptarse a cada situación. Por ejemplo el uso de shorewall para control de tráfico entre zonas no es una herramienta nueva, sino es una aplicación con bastante trayectoria pero que posee gran versatilidad en el bloqueo de tráfico no permitido.

El uso de soluciones Open Source en las instituciones públicas del país se ha convertido en un punto fundamental en la implementación de soluciones tecnológicas. El trabajo y tiempo dedicado a estas tecnologías brinda cierto nivel de confianza y reduce en gran medida el costo de desarrollo.

B. RECOMENDACIONES

Se debe implementar bitácoras en las que se registre cambios en los sistemas implementados y se debe actualizar cada vez que se modifique una configuración o se implementen nuevos esquemas.

Cada vez que un usuario deje de utilizar el sistema de autenticación y servicios asociados debe ser eliminado de la base de datos LDAP, para facilitar la administración de la misma y mantenerla organizada.

Se debe realizar evaluaciones periódicas del funcionamiento tanto de la infraestructura de control de usuarios como las normas y políticas que se están aplicando en la institución con el fin de verificar si se están mitigando los riesgos de seguridad de la información, y en el caso de que no se estén cumpliendo les permita tomar medidas.

Para el buen funcionamiento de las herramientas de seguridad es necesario educar a los usuarios para el manejo adecuado de las mismas, ya que de nada sirve implementar las mejores

herramientas si los usuarios no respetan las políticas y normas descritas en el SGSI y documentos de seguridad de la institución.

Al emplear mecanismos de autenticación basados en nombre de usuario y contraseña, es necesario difundir a los usuarios las normas y políticas y la importancia del cumplimiento de las mismas.

Se debe establecer políticas de respaldo de información de los servicios críticos de la institución, en este caso es importante realizar backups de la base de datos de usuarios LDAP, configuraciones del servidor AAA y switches de acceso.

Se recomienda la implementación de servicios AAA en las redes que se quiera tener control de los usuarios que acceden a los recursos de la red evitando el acceso no autorizado de personas ajenas a la institución.

Es recomendable implementar la arquitectura de paravirtualizacion en entornos que se posea infraestructuras de servidores robustas para aprovechar al máximo sus recursos.

VI. BIBLIOGRAFÍA

3Com Switch 5500 Family. *Configuration Guide.*http://support.3com.com/infodeli/tools/switches/5500/DUA1715-0BAA01.pdf

TUTORIAL NTOP: http://www.armgasa.com/index.php?option=com_content&view=article&id=70:ntop&catid=53:ntop&Itemid=71

Red Hat- RPM y su importancia para Linux http://www.clubso.com.ar/forum/topic_1538last

http://www.cypsela.es/especiales/pdf206/confidencialidad.pdf

Buyya, Rajkumar. HIGH PERFORMANCE CLUSTER COMPUTING: ARCHITECTURES AND SYSTEMS Vol. 1, Prentice All, Australia, 1999.

Freeradius con Soporte EAP-TLS e Integrado LDAP.http://wiki.canaima.softwarelibre.gob.ve/mediawiki/index.php?title=Especial:PdfPrint&page=Freeradius

DISEÑO E IMPLEMENTACIÓN DE UN CLIENTE RADIUS EN LINUX. http://dspace.epn.edu.ec/bitstream/15000/8963/5/T10761CAP1.pdf

Consideraciones para la implementación de 802.1x en WLAN's. http://www.sans.org/reading_room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlan-039-s_1607

Cisco Systems, FUNDAMENTOS DE SEGURIDAD DE REDES, Pearson Educación, Madrid, 2005.

SEGURIDAD POR NIVELES. http://www.jampudia.com/wp-content/uploads/2011/09/Seguridad_por_Niveles_v001.pdf

Debby Russell & G.T. Gangemi (1991). *COMPUTER SECURITY BASICS*, Estados Unidos, O'reilly.

Dhanjani Nitersh, *CLAVES HACKERS EN LINUX Y UNIX*, Mc Graw-hill, Madrid, 2004.

Shorewall. http://shorewall.net/

La importancia de la seguridad de la información. http://blog.zerial.org/seguridad/la-importancia-de-la-seguridad-en-la-informacion/

GUÍA DE INSTALACIÓN DE DEBIAN GNU/LINUX. http://www.debian.org/releases/stable/i386/

http://www.slideshare.net/lamugre/ataques-y-vulnerabilidades

Snort. http://www.snort.org/

FERNÁNDEZ, Yago; RAMOS, Antonio & GARCÍA MORAN, Jean (2009), *AAA RADIUS 802.1x - Sistemas Basados en la autenticación En Windows Y Linux/GNU Seguridad Máxima* (1ra Edición), España-Alfaomega.

GARFINKEL Simson, *SEGURIDAD PRÁCTICA EN UNIX E INTERNET*, Mc Graw-hill, México, 1999.

GÓMEZ VIEITES Alvaro, *ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA*, Alfaomega, México, 2007.

Jassell Jonathan (2002), *RADIUS*, Estados Unidos, O'reilly.

Conoce a Debian *GNU/Linux* [Más que una distribución GNU/Linux, su movimiento, filosofía y comunidad] http://teotihua.org/articles/articulo_debian.pdf

PEAP http://technet.microsoft.com/es-es/library/cc757996%28v=ws.10%29.aspx

[16] *Instalación Y Configuración De Un Servidor Radius.* http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

¿Qué es un SGSI? http://www.iso27000.es/sgsi.html#section2a

Intrusion Detection and Log Analysis with iptables. http://cipherdyne.org/psad/

RED HAT ENTERPRISE VIRTUALIZATION. http://ar.redhat.com/rhecm/rest-rhecm/jcr/repository/collaboration/jcr:system/jcr:versionStorage/bb4efb500a05260150d9554f7c1dd58a/3/jcr:frozenNode/rh:resourceFile

Setting Up 802.1X Authentication with Debian Linux y Freeradius Part 1. http://www.fatofthelan.com/technical/setting-up-802-1x-authentication-with-debian-linux-and-freeradius-part-1

SGSI, Sistema de Gestión de Seguridad de la Información interno del Ente del Ministerio de Defensa Nacional.

Virtualization With Xen On Debian Lenny (AMD64). http://www.howtoforge.com/virtualization-with-xen-on-debian-lenny-amd64

¿QUÉ ES LA VIRTUALIZACIÓN?. http://www.tecnologiapyme.com/software/que-es-la-virtualizacion

Sistemas de Cableado Estructurado. http://www.slideshare.net/lpajaro/ansi-tiaeia-568-b

TABLE OF CONTENTS

AAA server for validation and control user access to the Networking infrastructure of an entity of National Defense Ministry (July 2012)

Carlos Plasencia – Author, Ing. Carlos Vásquez - Director

***Abstract*—Today's information security is an issue of paramount importance to any organization or institution, due to communications facilities provided to users through internal services and public (Internet) for the development of work activities, for that reason we must not neglect the protection of data flowing through the network. This project by implementing an AAA server validates the user access to enter the networking infrastructure of the entity of the Ministry of National Defense in order to secure the connection to the network only to authorized users and in addition to the solution UTM infrastructure developed using free software that controls user access to network resources of the institution.**

***Index Terms*—802.1x, GNU Linux, LDAP, AAA Server, UTM.**

I. STUDY OF STATE AND REQUIREMENTS OF THE BOARD OF USER ACCESS MINISTRY OF NATIONAL DEFENSE

A. Examining the current status of the entity

The entity of the Ministry of Defense is responsible for administering and managing the main backbone of the national communications, and currently has no methods and schemes to ensure the confidentiality, integrity and availability of information handled internally LAN (Local Area network).

There is no control of the users who access network resources and can thus be no intrusion of subjects with unknown purposes that may harm or compromise the information flowing through the network.

The institution has two infrastructures, a telephone and a networking; they are administered in telecommunications rooms located in each building block. Both telephony infrastructure such as networking has its own administrative staff, however, have no access control rules for individuals who enter these rooms, creating a security threat. In this sense the people accessing telecommunications rooms, can easily disconnect the cable connection from a user who is absent and usurp the information transmitted over the network.

In the current infrastructure is not available user authentication mechanisms for access to network resources in both wired and wireless network.

Currently there is no infrastructure for internet navigation control so each user can use this resource without measure, slowly causing problems to others who need to develop their work activities. Similarly there is no control of users accessing from the LAN and data to internal applications as institutional mail, web portals, integrated systems, and others.

One of the major weaknesses in any organization, is that managers are concerned only have internet service without taking into account the optimization of the resource for job performance, and not think about how dangerous it can be to not have schemes access control internet traffic, so that they become vulnerable to certain attacks that can occur from outside the network.

B. Recommendations and policies of user access control related ISMS

The entity of the National Defense Ministry has a System Information Security Management (ISMS) based on ISO-27001. The ISMS is a document that helps institutions and organizations to establish policies, procedures and controls in relation to the objectives of the reason for the institution, to always keep the risk below the level assumed by the organization itself.

In this document are defined policies on the proper use of computing resources also specifies recommendations for password management for

both users and administrators with the respective responsibilities on them such as:

Ensure that passwords meet the following:

- Use at least 8 characters.
- Use uppercase and lowercase letters, symbols and numbers.
- Users must change passwords every 120 days.
- Administrators must change passwords every 90 days.
- Do not re-used passwords.

II. INTEGRATION OF STANDARD IEEE 802.1X

A. Importance of access control in information security

Access control in information systems is the ability to control the interaction of an active element (user, device, service) with a computer resource (data network, system, service). Additionally, access control involves identification procedures, authentication and authorization to allow or deny the use of resources and to keep track of this.

Safety is an important issue in both wired and wireless networks, because around the local network are people who seek to use confidential information for purposes unknown that may prejudice the security of information and the image of the institution.

In the great majority of institutions and companies are under attack from its own network, usually made by employees who have ignorance in the use of computer systems or dissatisfied with vested interests. Prevent such attacks take place improves the quality of security processes of the institution.

B. Information security concepts

The objective of information security is protecting the data of the institution; consider three very important in preserving it, which are confidentiality, integrity and availability.

- Confidentiality is to allow the information is authorized and is only seen by those to whom it is intended, that is, concerns the privacy of information. To this end encryption mechanisms are used in the data.
- Integrity means that the contents remain unchanged unless modified by authorized personnel, and this modification is recorded, ensuring accuracy and reliability. The integrity of a message attaching gets another set of data integrity checking, for example, the fingerprint, digital signature, among others.
- Availability refers to the network, hardware and software are reliable, ie you can recover quickly and completely to interruption events. To achieve this goal are generally employed link redundancy mechanisms, hardware and software, so that in case of an event disrupts the functioning of one of these system elements, the redundant backup solve the problem as quickly as possible.

C. Attackers and Vulnerabilities

It is important to know the why to implement schemes or methods of information security, and also understand from what you have to take preventive measures.

- An attack is a technique used to exploit a weakness or failure of a system (vulnerability), such a threat could be the denial of service attack, with the vulnerability using a security scheme designed without considering this threat.
- A threat is any possible interruption of operation, integrity, availability of the network or system, it may be natural, through negligence or intrusion, mishandling or improper intentions as hackers.
- Vulnerability is a weakness typical of systems that allows an attacker to violate the confidentiality, integrity, availability, access control and consistency of the system or its data and applications, caused by an error in the design, configuration or implementation of networks or services.

.

D. IEEE 802.1X standard.

Standards are a set of technological specifications set by a competition watchdog in this case is the Institute of Electrical and Electronic Engineers, known by its acronym in English as IEEE, for producers and technology developers have legislation that allows them to ensure that the devices can operate with one another.

IEEE 802.1X can implement secure access, using media such as Ethernet, Token Ring and

802.11 wireless LANs. The use of protocol RADIUS (Remote Dial-Up Server Authentication, Server Remote Authentication Dial-In) is optional within IEEE 802.1X, IEEE expects several IEEE 802.1X authenticators operate as a client and authentication server at a time.

IEEE 802.1X standard defines the access control port-based network, ie, enables authentication of devices connected to a LAN port, establishing a point to point connection or preventing access to that port if authentication fails. Because it requires authentication before providing access to Ethernet networks. In the control network access ports are used based on the physical elements that make up an infrastructure of the LAN switching to authenticate devices attached to switch port. Cannot send or receive frames in Ethernet switch port if the authentication process failed

Although Ethernet was designed for fixed networks, this standard has been adapted for use in wireless LANs IEEE 802.11. Windows XP supports IEEE 802.1X authentication for all network adapters based LANs, including Ethernet and wireless.

IEEE 802.1X is based on the EAP protocol (Extensible Authentication Protocol, Expandable Authentication Protocol), although in reality is EAPoL (Extensible Authentication Protocol over LAN) so that it can be used in Ethernet networks, 802.11, Token-Ring and FDDI (Fiber Distributed Data Interface).

When a node requires access to another resource in a LAN, the Access Point or access switch question the identity of the node, the traffic allowed between the node and the access point or switch is EAP until the node is authenticated.

The authentication process 802.1X/EAP consists of three major elements, a supplicant (user), an authenticator (access point or switch) and an authentication server (Free RADIUS). The supplicant is the device requesting network access generally the user. The authenticator is an intermediary device that turns the frame from the user to the authentication server, typically the wireless access point or switch access. The authentication server is the device now authenticates the user, usually the Free RADIUS server.

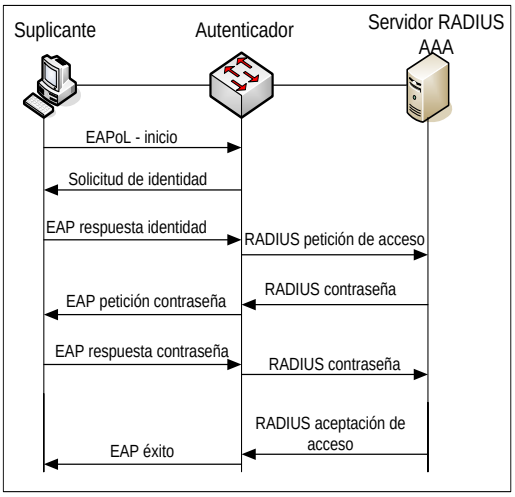

Fig. 1. 802.1X authentication. Shown frames exchanged between the supplicant and the authenticator and the messages between the authenticator and authentication server.

1) 802.1X frames

For authentication using the EAP protocol (specified in RFC-3748) to exchange authentication information between the Supplicant and Authentication Server. EAP can use different authentication mechanisms such as MD5, Kerberos, Public Key Encryption with (PKE), one-time passwords (OTPs), among others. EAP is a simple package that can run on different levels of link. Authentication frames to be transported between the Supplicant and the Authentication Server. For this we have chosen a protocol that carries EAP service directly on a Local Area Network (EAPOL).

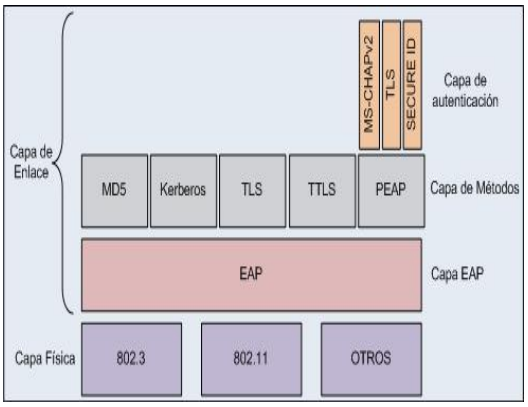

Fig. 2. 802.1X architecture. Displays the 802.1X model in layers with respective encryption methods.

The fields present in an 802.1X frame are as follows:

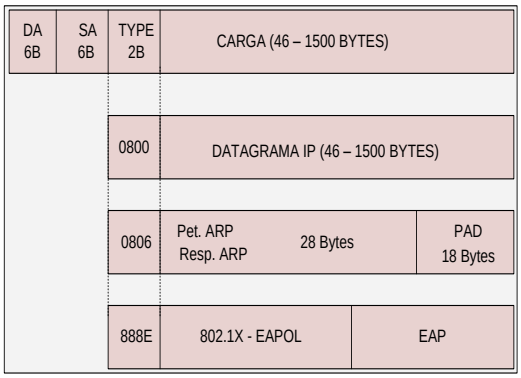

Fig. 8. Ethernet frame. Fields present in an Ethernet frame support 802.1X.

For the project using the 888E type frames which serve to determine the type of communication to be set before accessing the network, in this case an 802.1X authentication.

2) Definition of AAA services

AAA means Authentication, Authorization and Accounting.

The levels of confidentiality, integrity and availability of information are supplemented by appropriate levels of authentication, access control mechanisms, defining levels of access to services or profiles and time control which users are connected for the performance of their duties.

Authentication ensures that the individual's identity is validated appropriate to its owner. Each user tries to access the data network or services of the same, has a distinctive identity that is unique, so that in order to access network services must authenticate with their credentials. In this case the credentials are the user name and password, because through these defined if the user whose identity is being verified who claims to be.

Authorization is the allocation of additional resources, which enables access control by user after authentication. Allows control user access to specific network services, according to a preset profile, which will be applied based on user identity that was authenticated.

Accounting refers to keeping track of all activity performed by a user from the moment he agreed to the network until the end of your session, ie it allows to keep track of system usage based on the identity of who accessed agreed to and for how long he remained in the system.

3) RADIUS Protocol

RADIUS (Remote Authentication Dial-In User Server) is a protocol for managing the "authentication, authorization and accounting" of users on a particular resource.

The RADIUS protocol provides centralized access service. For this reason, one of the main uses of RADIUS is in companies that provide Internet access to large corporate networks, in an environment with multiple network technologies including modems, xDSL, VPN (Virtual Private Network) and network wireless.

RADIUS messages are sent as User Datagram messages UDP. UDP port 1812 is used for RADIUS authentication messages and messages in 1813 for RADIUS accounting. The UDP payload of a RADIUS packet includes only one RADIUS message.

The RADIUS message format is shown in the figure below:

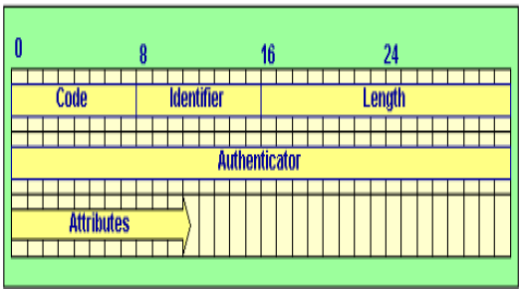

Fig. 4. Format of the RADIUS message. Fields of the message exchange between the authenticator and the AAA server.

The fields in a RADIUS packet are:

- *Code (Code).* A byte that contains the packet type.

Table 2. RADIUS Packet Type

Valor	Description
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

- *Identifier (ID).* A byte that allows the RADIUS customer to link a RADIUS response to the request properly.
- *Length.* Packet length (2 bytes).
- *Authenticator (Controller).* Value used to authenticate the RADIUS server response. It is used in the password hiding algorithm.
- *Attributes.* Here are stored an arbitrary number of attributes. The only required

attributes are the User-Name (user) and User-Password (password).

4) EAP Protocols

Some of the EAP authentication mechanisms are presented with a brief description of each:

- EAP-MD5, MD5-Challenge requires username and password, is equivalent to CHAP, little used in authentication in wireless environments.
- Lightweight EAP (LEAP), sends a username and password to the authentication server is proprietary protocol developed by Cisco and is considered unsafe at being left out to use LEAP PEAP.
- EAP-TLS, create a session TLS (Transport Layer Security) within EAP, between the supplicant and the authentication server, being necessary to the server and client digital certificates and PKI (Public Key Infrastructure, Key Infrastructure Public), this authentication is bidirectional.
- EAP-TTLS, establishing a TLS encrypted tunnel for transporting authentication data within the TLS tunnel authentication methods can be used.
- PEAP (Protected EAP, Protected EAP), EAP-TLS used as a TLS encrypted tunnel, certificates of supplicant for EAP-TTLS and EAP-PEAP are optional, but the authentication server certificates are required.
- EAP-MSCHAPv2, requires a user name and password, and in short is encapsulating EAP-MS-CHAP v2.

5) Select the operating system to implement the AAA service

In today's market there are a number of operating systems for everyone, for all applications, for everyone, and when to choose one or another operating system the user chooses to pay more to the needs.

To implement the AAA service was chosen by the operating system Debian GNU / Linux for the following reasons:

- Maintain standard application on the same operating system.
- Use of no-cost virtualization capabilities.
- Decree 1014 which supports the use of free software.
- Compatibility with existing applications.
- Features of the operating system.

6) Importance of High Availability

High availability (High Availability) is a system architecture design and implementation is associated with ensuring the operational continuity of services. Availability refers to: continuity of access to systems and to perform new work, update or alter existing work or collect the results of previous work. If a user cannot access the system, is said to be unavailable, the service is interrupted. The term downtime (downtime) is used to define when the system is not available and is a parameter used to define service recovery times.

III. AAA SERVER DESIGN

A. Solution design

Due to the lack of access control schemes of users accessing the network, the implemented solution has taken into account some important aspects such as:

- The teams are active part of the 3Com brand and support the 802.1X standard.
- Using Microsoft Windows XP operating system on the users of the institution is standard. This feature facilitates the integration of the solution as IEEE 802.1X is native to the operating system.
- The institution has a centralized database of LDAP users.
- The institution has hardware for implementing services.

Controlling user access to the networking infrastructure is done by using the 802.1X standard. The following diagram shows the AAA solution integration and network architecture implemented in the institution:

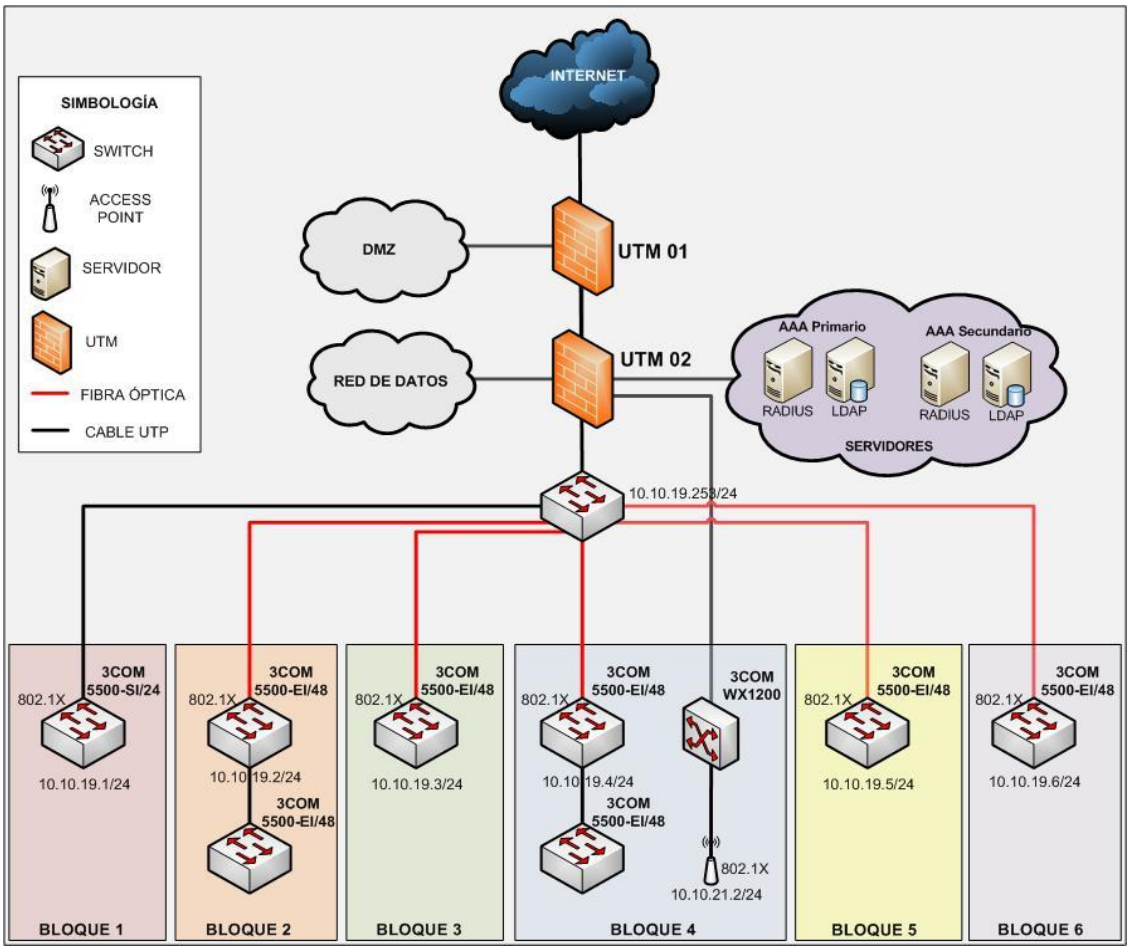

Fig. 59. Network architecture implemented. Shows the integration of the AAA and UTM solution to control inbound and outbound traffic between zones.

The design implemented AAA server consists of a primary and secondary AAA server, each server has its own database, LDAP user authentication. The AAA server authenticates against the primary database-Master LDAP and AAA server authenticates against secondary LDAP database-Slave. These databases are synchronized and all changes to be made in the LDAP-Master automatically replicated to the LDAP-Slave. It should be noted that the data can only be modified in the LDAP-Master because it only has write privileges on the base, while the Slave LDAP is read-only privileges.

By having the Master-Slave diagram of the database prevents inconsistency exists in the data.

The implementation scheme is redundant because it is one of the most critical services of the institution. If for some reason the primary AAA server is unavailable, any user on the LAN internal network could access the network services, and therefore cause disruption in the operation of their activities.

The 802.1X standard is set on the client computer to allow users to authenticate with username and password after login.

3Com in 5500 that make the access layer to the network is configured 802.1X standard to interact between users and the AAA server for authentication. In all access equipment is configured as the IP address of the primary AAA server IP address as the secondary AAA server for high availability of service.

B. Operation of the implementation

The scheme of operation is shown in the figure below:

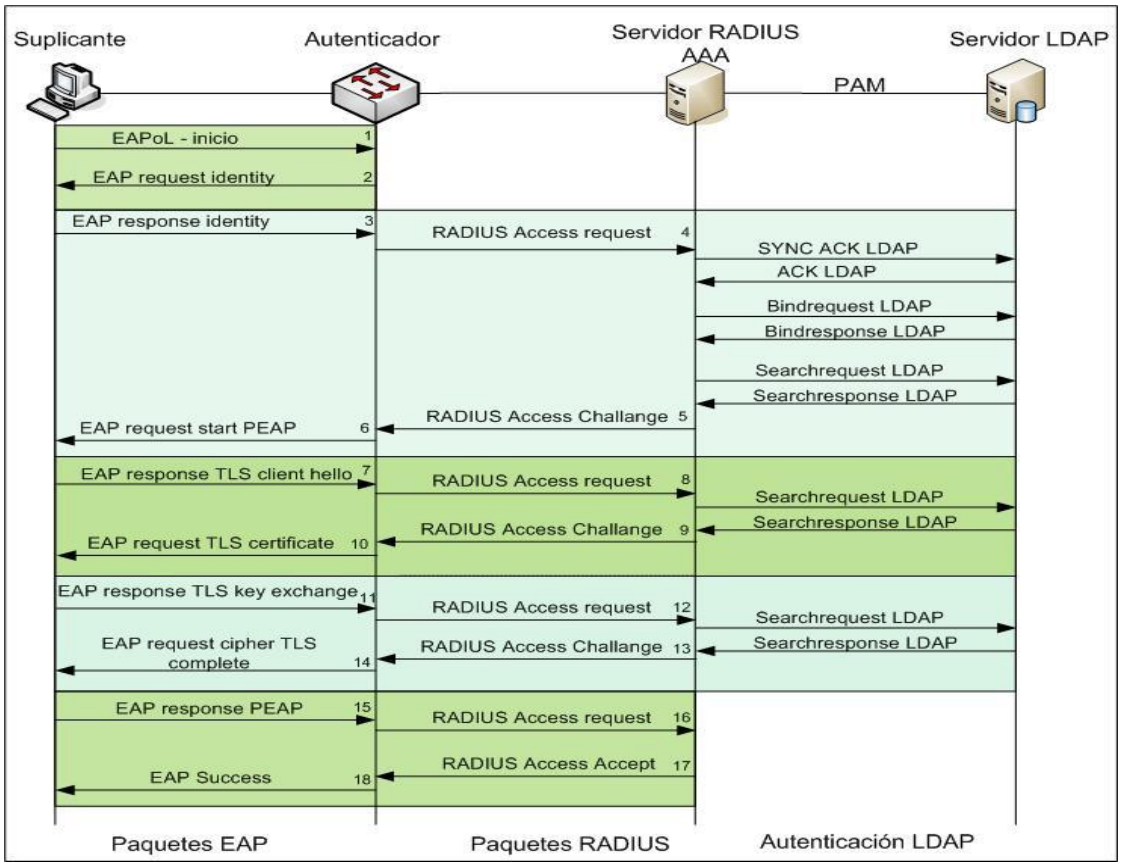

Fig. 6. AAA system operation. Exchange of frames between the user's computer and the authenticator, messages sent between the authenticator and the AAA server and queries the LDAP server

1. The supplicant requesting network connection starts. To give access to the user starts the authentication process by sending a message starting EAPoL to access equipment (Switch or AP).
2. The authenticator sends a request message to the user identity.
3. The user sends an EAP identity to the authenticator.
4. EAP frame identity response is encapsulated in a RADIUS message and the authenticator sends an access request to the RADIUS server.
5. The RADIUS server initiates the EAP method negotiation that will be used to establish the secure channel by sending a RADIUS Access-Challenge frame.
6. The authenticator sends an EAP user with channel establishment request with EAP type PEAP.
7. The user negotiates the connection method and the authenticator sends an EAP response to the greeting for establishing the TLS channel (client hello).
8. The Authenticator encapsulates the EAP-Response message in a RADIUS-request message and sends it to server.
9. The server verifies the message sent by the user and responds with its certificate in a RADIUS-Challenge message. The hello message contains a server hello[3] + server certificate[4].
10. The authenticator receives the RADIUS message and sends the server certificate to the user in an EAP-TLS credential request of the user.
11. The user responds with an EAP message exchange password on the encrypted channel. The message EAP-TLS response containing the client key exchange, change cipher spec and encrypted handshake message.
12. The plot TLS EAP-Response message is encapsulated in a RADIUS-Request and sent to the RADIUS server, the message gets encrypted with the user's password and is verified in the LDAP database.
13. Server responds:
    a. If the user's password is correct, the server responds with a RADIUS-Challange to finalize the establishment of the TLS channel.
    b. If credentials are not correct rejects the connection (RADIUS-Reject)

[3] Server hello.-. Greetings from the server in response to a client hello.
[4] Server certificate.- Certificate Server.

and the switch port it connects to the user puts down state.

14. The authenticator receives a RADIUS-Challange to finish establishing the TLS channel and the user sends an EAP-Request full encrypted channel.
15. The user sends an EAP-PEAP response and requests access to the network.
16. The request for access to the network is sent to the server using a RADIUS-request message.
17. The server responds with a RADIUS-ACCEPT message to the authenticator.
18. The authenticator sends an EAP-Succsess and the user is already authorized to use the network resources.

C. System requirements for the 802.1X

The elements of the architecture of operating the AAA server integration with the infrastructure of the institution are:

- Client: Windows XP with Service Pack 2 or 3, using this operating system is standardized throughout the building.
- Authentication Service: RADIUS server developed in free software.
- Authentication Method: EAP-PEAP
- Encryption used with PEAP: MSCHAPv2
- Database user authentication: LDAP.
- Customers for authentication: 3Com Switch 5500-EI.
- Clients for wireless authentication: AP support 802.1X standard.

D. Infrastructure design of the authentication server

To implement the AAA authentication server primary and secondary has an Intel blade HS-22 and HS-21 BLADE infrastructure, they have the following characteristics:

- Processor: 3.2 GHz Intel XEON
- Memory: 32 GB
- Hard Drive: 2 x 140 GB configured in RAID 1
- Network interfaces: 2 (10/100/1000)

The virtualization scheme implemented is as follows:

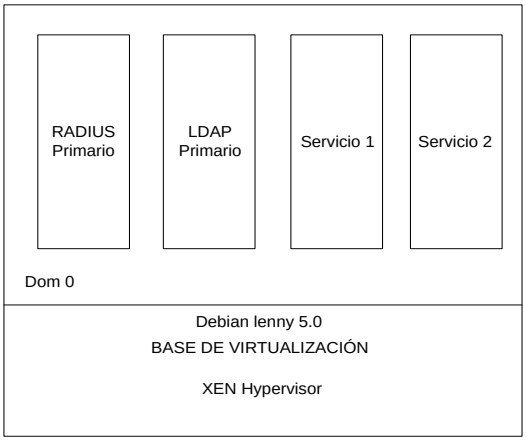

Fig. 7. Virtualization scheme. Lists the virtual machines installed on the physical server.

The virtual machine running the primary RADIUS service is assigned the following resources:

- Memory: the basic requirements for running a virtual machine operating system Debian Lenny is 256 MB. Users who control the institution constantly growing, therefore it is assigned 1 GB of RAM.
- Disk Space: This server stores the records of users accessing the network, therefore it has allocated 20 GB of disk.

E. Application Access Control

Once users are authenticated and authorized, and can make use of network resources. So far it is known that users entering the network are only those authorized in the institution, but it should be noted that not being in control of access to applications and corporate services.

With the implementation of an internal UTM server that controls the traffic from external entities to the internal services of the institution reduces the possibility of obtaining information in an unauthorized manner, also controls the user access to the necessary applications for the development of their activities, just as users of the LAN to public services.

IV. AAA SERVER IMPLEMENTATION IN THE INTERNAL NETWORK ENTITY OF THE MINISTRY OF NATIONAL DEFENSE

A. AAA Server Configuration

The AAA server installation is performed on the Linux platform with the operating system Debian Lenny 5.0 with FreeRADIUS 2.0.4 software, which uses the same database existing LDAP Master.

Freeradius version repositories including operating system does not support EAP-PEAP,

for which the installed version of freeradius is compiled, since it enables support for encryption protocols EAP-PEAP, EAP-TLS EAP-TTLS and also includes the OpenSSL module, which are necessary to implement a secure encryption method for exchanging information between the AAA server and the user.

Every time you upgrade the operating system is installed the new versions of packages and in some cases bring further changes that may affect the normal operation of the service. To avoid this protection is used on the installed version.

The authentication method is PEAP freeradius used which is based on digital certificates on the server, so it is necessary to generate them using OpenSSL and then load them to the AAA server.

1) Setting up FreeRADIUS

Files to be modified to operate FreeRADIUS are:

- eap.conf. - Sets the encryption method for sending data.
- radiusd.conf. - The main file of freeradius.
- defaulf. - Define the use of the LDAP module.
- inner-tunnel. - Synchronization of the tunnel for freeradius server communication.
- clients.conf. - Defines the entities that have the role of authenticator.
- ldap.conf. - Connection to database LDAP users.
- ldap.attrmaps. - Define attributes for dynamic VLAN assignment.
- samba.schema. - Outline samba control domains.

B. Configuring the Authenticator

The teams that will fulfill this function are the 7 switches Brand 3Com 5500G-EI series and 3Com 5500-SI, in the same settings are made to withstand the EAP encryption method.

C. Configuring the user's computer

For the user can access the network and its resources, the network card is configured to support 802.1X authentication, otherwise the port is connected to the computer, for any reason you can access the network.

D. UTM implementation of internal and external

Once the user is authenticated and authorized to make use of network resources through the implementation of UTM will only limit access to needed services.

The servers in charge of traffic control to the internal network of the institution have the following software installed:

- Operating System: Debian Lenny 5.0
- Firewall: Shorewall
- IDS: Snort
- IPS: PSAD
- Monitoring of traffic: NTOP
- Monitoring MRTG band width

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The AAA server validates users attempting to access the networking infrastructure of the institution, the database querying LDAP user if the user is not found or password is incorrect, the server rejects the request for user access, and not allowed to use the resources offered in the institution.

The authentication method is PEAP one of the most used in AAA implementations due to the ease of integration and its high level of security. When the user is authenticated against the server using your username and password is encrypted using the TLS channel based on trust server's digital certificate.

Possess security schemes is essential to protect the information flowing through the network. As was observed in this study with the implementation of the 802.1X standard is controlled by users accessing the internal network of the institution granting the user access only allowed.

The authentication system is implemented on all devices that support the 802.1X standard. Currently most access equipment brands are designed to support standard facilitating the integration of network security that do not have access control of its users.

Using databases to authenticate users and facilitates centralized user administration, because if you want to change your password, only changed once.

The implementation of security infrastructure works properly when it is supported by standards and policies on the use of computing resources such as: users, passwords, internet, web portals, etc..

The Linux operating system selected for installation of Debian AAA server was to maintain a standard level of applications and services in the institution, and the advantages it has in terms of virtualization, as presented is limited by the hardware capacity but not by the number of virtual machines that can be created at no cost.

Getting to have total security in a network is unreachable but with the continuous improvement and adoption of methods and standards of information security is maintained acceptable level of security that reduces the risk of the network.

Although stocks of new techniques and innovative devices with regard to security management, can use old techniques or solutions to fit every situation. For example using shorewall to control traffic between zones is not a new tool, but rather is an application path but has a great versatility in blocking traffic is not allowed.

The use of open source solutions in public institutions of the country has become a key point in implementing technology solutions. The work and time spent on these technologies provides some level of trust and greatly reduces the cost of development.

B. RECOMMENDATIONS

Journals should be implemented in which record changes in the systems implemented and must be updated every time you change a setting or implementation of new schemes.

Each time a user stop using the authentication system and associated services should be removed from the LDAP database to facilitate the administration of it and keep it organized.

Should conduct periodic assessments of the functioning of both the user control infrastructure and the rules and policies being implemented in the institution to see if they are mitigating the risks of information security, and if not being met them to take action.

For the proper functioning of the security tools necessary to educate users to the proper management of them, and it is pointless to implement the best tools if users do not respect the policies and standards described in the ISMS and safety documents the institution.

When using authentication mechanisms based on user name and password, you need users to disseminate the rules and policies and the importance of compliance with them.

Policies should be established data backup of critical services of the institution, in this case is important to make backups of the database users LDAP AAA server configurations and access switches.

It recommends the implementation of AAA services on the networks you want to have control of users accessing network resources by preventing unauthorized access by outsiders to the institution.

It is advisable to implement paravirtualization architecture environments that possess robust server infrastructure to maximize its resources.

VI. REFERENCES

3Com Switch 5500 Family. Configuration Guide. http://support.3com.com/infodeli/tools/switches/5500/DUA1715-0BAA01.pdf

TUTORIAL NTOP: http://www.armgasa.com/index.php?option=com_content&view=article&id=70:ntop&catid=53:ntop&Itemid=71

Red Hat, RPM and its importance for Linux http://www.clubso.com.ar/forum/topic_1538last

http://www.cypsela.es/especiales/pdf206/confidencialidad.pdf

Buyya, Rajkumar. HIGH PERFORMANCE COMPUTING CLUSTER: ARCHITECTURES AND SYSTEMS Vol 1, Prentice All, Australia, 1999.

Freeradius EAP-TLS Support and Integrated

DESIGN AND IMPLEMENTATION OF A CUSTOMER IN LINUX RADIUS. http://dspace.epn.edu.ec/bitstream/15000/8963/5/T10761CAP1.pdf

Considerations for deploying 802.1x on WLAN's.

Cisco Systems, FUNDAMENTALS OF NETWORK SECURITY, Pearson Education, Madrid, 2005.

SECURITY LEVELS.
http://www.jampudia.com/wp-content/uploads / 2011/09/Seguridad_por_Niveles_v001.pdf

Debby Russell & G.T. Gangemi (1991). COMPUTER SECURITY BASICS, USA, O'reilly.

Dhanjani Nitersh, KEY IN LINUX AND UNIX HACKERS, Mc Graw-Hill, Madrid, 2004.

Shorewall. http://shorewall.net/

The importance of the information security. http://blog.zerial.org/seguridad/la-importancia-de-la-seguridad-en-la-informacion/

INSTALLATION GUIDE DEBIAN GNU / LINUX.
http://www.debian.org/releases/stable/i386/

http://www.slideshare.net/lamugre/ataques-y-vulnerabilidades

Snort. http://www.snort.org/

FERNANDEZ, Iago; Ramos, Antonio & GARCIA MORAN, Jean (2009), 802.1x RADIUS AAA - Authentication Based Systems For Windows And Linux / GNU Maximum Security (1st Edition), Spain-Alfaomega.

Simson Garfinkel, PRACTICE SAFETY AND INTERNET UNIX, Mc Graw-Hill, Mexico, 1999.

Alvaro Gomez Vieites, ENCYCLOPEDIA OF COMPUTER SECURITY, Alfaomega, Mexico, 2007.

Jassell Jonathan (2002), RADIUS, USA, O'reilly.

Meet Debian GNU / Linux [More than a GNU / Linux, movement, philosophy and the community]
http://teotihua.org/articles/articulo_debian.pdf

PEAP
http://technet.microsoft.com/es-es/library/cc757996% 28v = WS.10% 29.aspx

Installing and configuring a RADIUS server.
http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

What is an ISMS?
http://www.iso27000.es/sgsi.html # section2a

Intrusion Detection and Log Analysis with iptables. http://cipherdyne.org/psad/

Red Hat Enterprise Virtualization. http://ar.redhat.com/rhecm/rest-rhecm/jcr/repository/collaboration/ jcr: system / jcr: versionStorage/bb4efb500a05260150d9554f7c1dd58a/3/jcr: frozenNode / rh: ResourceFile

Setting Up 802.1x Authentication with Debian Linux and Freeradius Part 1.

ISMS Management System Information Security Internal Entity Ministry of National Defense.

Virtualization With Xen On Debian Lenny (AMD64).
http://www.howtoforge.com/virtualization-with-xen-on-debian-lenny-amd64

What is virtualization?.
http://www.tecnologiapyme.com/software/que-es-la-virtualizacion

Structured Cabling Systems.
http://www.slideshare.net/lpajaro/ansi-tiaeia-568-b

Autor - Luis Carlos Plasencia Bedón nacido el 23 de marzo de 1985 en la ciudad de Ibarra. Segundo hijo de Juan Plasencia y Pilar Bedón.
La educación primaria la realizó en la escuela Modelo Pdte. Velasco Ibarra. Cursó la secundaria en el Colegio Nacional Teodoro Gómez de la Torre obteniendo el título de bachiller en Ciencias Físico-Matemáticas en el año 2002. La educación superior la realizó en la Universidad Técnica del Norte estudiando la Carrera de Ingeniería Electrónica y Redes de Comunicación.
Actualmente ocupa el cargo de Especialista en TI en la empresa Redsoluciones ofreciendo soluciones Tecnológicas desarrolladas sobre software libre.

Director – Ing. Carlos A. Vásquez A. Nació en Quito provincia de Pichincha el 19 de Septiembre de 1981. Ingeniero en Electrónica y Telecomunicaciones (CUM LAUDE), Escuela Politécnica Nacional (EPN) en Quito-Ecuador en 2008. Actualmente es Docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador, dictando las materias de Networking II y III, Proyectos de Redes, Administración de Redes. Cumple la función de vocal principal del Consejo Académico de la Carrera de Ingeniería en Electrónica y Redes de Comunicación. Aprobó los cursos CCNA 1, 2 ,3 ,4 de estudiante en el período junio 2006 – marzo 2007 en la Escuela Politécnica Nacional y el CCNA 1 de Instructor en la ESPOL, y cursa la Maestría en Redes de Comunicación (2do Semestre), Pontificia Universidad Católica del Ecuador, Quito-Ecuador.