Definiendo un esquema de seguridad para redes ATM en base a firewalls

Gómez R, Larraniaga V, Vazquez J
ITESM-CEM
{rogomez, vlarran, jvazquez}@campus.cem.itesm.mx

Resumen

La seguridad computacional ha dejado de ser un simple tema de moda, para convertirse en una necesidad de todo sistema de información. Una de las herramientas más utilizadas para aumentar la seguridad en un sistema computacional son los firewalls. Por otro lado, las redes ATM presentan grandes ventajas para organizaciones que requieren de velocidad en sus transmisiones. En el presente trabajo se propone un esquema de seguridad para redes ATM basado en firewalls.

1. Introducción

La seguridad computacional tiene por objetivo garantizar la *confidencialidad*, la *integridad* y la *disponibilidad* de los recursos de un sistema. En la actualidad, el activo más importante en una organización es la información.

Un sistema posee la propiedad de confidencialidad si la información manipulada por éste no es disponible ni puesta en descubierto para usuarios, entidades o procesos no autorizados. La propiedad de *integridad* se refiere a que los datos manipulados por el sistema no son alterados o destruidos por usuarios, entidades o procesos no autorizados. La *disponibilidad* requiere que la información sea accesible (está disponible) en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.

Una de las herramientas más utilizadas para cumplir con los requisitos anteriores son los firewalls. Un firewall es un conjunto de programas relacionados, localizados en un servidor de red, que protege los recursos de una red privada de usuarios de otras redes. En general, un firewall se coloca entre la red interna confiable y la red externa no confiable. El firewall actúa como un filtro que monitorea y rechaza el tráfico de red a nivel aplicación (aunque es posible hacerlo a otros niveles).

Las redes ATM surgieron a principios de los 80's debido a la necesidad de enviar por la misma red tanto voz como datos. El propósito de las redes ATM es proporcionar una red con multiplexión y conmutación, alta velocidad y bajo retardo para apoyar cualquier tipo de tráfico de usuario, como aplicaciones de voz datos o video. Varios esquemas de seguridad han propuestos sido propuestos para redes ATM. En este trabajo proponemos un nuevo esquema de seguridad para este tipo de redes basado en el uso de firewalls.

El trabajo se encuentra organizado de la siguiente forma. En la siguiente sección se explican las principales características de las redes ATM. La sección tres presenta los principales aspectos de seguridad en redes ATM. La sección cuatro da un panorama general acerca de los firewalls. La sección cinco explica nuestro modelo. Por último se plantean las conclusiones.

2. Las redes ATM

Las redes ATM (Asynchronous Transfer Mode) han tenido un gran impacto en el área de comunicaciones en muchas empresas. Presentan características propias (ver [1], [2], [3] y [4]) que las hacen adecuadas para la transmisión de aplicaciones multimedia.

Estas redes están basadas en una tecnología de comunicación de altas velocidades, el flujo de información esta organizado en paquetes, denominados celdas, de 53 bytes de tamaño fijo. De estos 53 bytes 5 conforman el encabezado y los 48 restantes contienen datos. El encabezado contiene información de donde ha de ser conmutada esta celda (su destino dentro del concentrador o conmutador) y del tipo de datos que contiene. De esta forma una celda puede llevar cualquier tipo de tráfico (voz, datos, o vídeo).

Una red ATM consiste en una serie de conmutadores ATM interconectados por enlaces ATM punto a punto, permitiendo conectar a cualquier par de estaciones. Las redes ATM son orientadas conexión, es decir antes de transmitir las celdas se debe establecer un circuito virtual a través de los conmutadores de la red para conectar las estaciones finales.

Todas las celdas desconocen su destino final, para llegar a éste se van creando tablas a través del circuito virtual que determinan la ruta que han de seguir las celdas para llegar a la estación final. Como la red, o nube de ATM, esta conformada por múltiples conmutadores se puede establecer múltiples circuitos a la vez.

El hecho de que las celdas sean de tamaño fijo permite que, mediante métodos estadísticos, se administre el tráfico de la red y que dicho tráfico se pueda predecir, permitiendo múltiples comunicaciones simultaneas. Otra ventaja de la longitud fija de las celdas, es que permite que la conmutación sea realizada directamente por hardware (esta es la única manera de alcanzar las altas velocidades que ATM permite).

Bajo el punto de vista basado exclusivamente en la transmisión, las redes ATM se pueden dividir en tres capas que se combinan de forma jerárquica de modo que cada capa superior puede tener uno o varios elementos inferiores. Estos elementos son el canal virtual, trayecto virtual y la sección física.

El canal virtual (VC) representa una conexión unidireccional entre usuarios. Es importante resaltar el carácter unidireccional, si dos usuarios desean establecer una conexión full-duplex, es necesario que usen dos canales. Los VC, además de transportar datos entre usuarios, también son usados para transportar la señalización y la gestión de la red.

El trayecto virtual (VP) involucra un conjunto de canales virtuales que atraviesan multiplexadamente la red ATM. Los VP facilitan la conmutación de los canales virtuales, pues conectan tramos enteros de la red ATM. De no existir, por cada conexión entre usuarios se tendrían que reelaborar todas las tablas de ruteo de los nodos atravesados lo cual supondría un incremento del tiempo necesario para establecer una conexión, y un mayor desperdicio de espacio de memoria en los nodos.

La sección física (PS) conecta y proporciona continuidad digital entre los diferentes elementos que componen la red controlando el flujo de bits. Debe mantener en óptimas condiciones las señales eléctricas u ópticas regenerándolas cuando resultan afectadas por atenuación o distorsiones.

2.1 Las redes ATM y las redes locales.

Las características de la tecnología ATM la convierten en una solución muy atractiva para el soporte de redes de área local y grupos de trabajo virtuales. La integración de la tecnología ATM en las redes de área local tiene que contemplar tanto los aspectos de migración como los de coexistencia con las diversas estaciones de trabajo. El problema no es trivial, ATM es una tecnología orientada a la conexión y las tecnologías que existían antes de ella (ethernet, token-ring) eran tecnologías orientadas a no-conexión.

Debido a lo anterior, es necesario definir una capa de software que permita a las redes locales aprovechar las características de ATM. El principal objetivo de la emulación de LAN, es la migración y coexistencia de una LAN existente en con un sistema basado en ATM con el menor cambio en el software de la estación.

Una LAN emulada tiene dos componentes principales: los clientes de LAN Emulation (LECs) y un Servicio de LANEmulation (ELAN)

El software del LEC reside en los convertidores ATM a LAN o en los sistemas finales ATM. Tiene varias funciones, una de las más importantes es la resolución de direcciones, es decir, la correspondencia de direcciones MAC y direcciones ATM.

El software que proporciona el Servicio de LAN Emulation se basa en tres servidores lógicos:

1. LECS: Servidor de Configuración, el cual da a conocer a los clientes información pertinente para que los mismos puedan establecer una conexión,
2. LES: Servidor de LAN Emulation, ofrece a los clientes los servicios de registro y resolución de direcciones físicas a direcciones ATM.
3. BUS: Servidor de difusión y direcciones desconocidas, como en las diferentes arquitecturas de red de área local no están basadas en conexión y ATM es una tecnología orientada a conexión es necesario este elemento para manejar el tráfico broadcast, multicast y unicast desconocido.

La operación de una ELAN requiere de una inicialización, un registro y resolución de direcciones así como de la transmisión de datos. Basándonos en la figura 1 procederemos a explicar estos pasos.

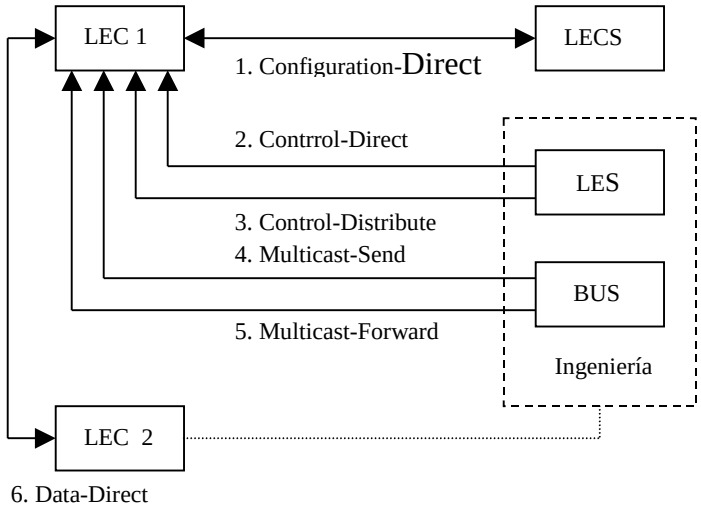


Figura 1. Esquema emulación de LAN en ATM

2.1.1 Inicialización

Una vez que los clientes se conectaron y se agregaron a la nube ATM, obtienen la dirección del LECS, mediante la "Well Known" Address vía el circuito virtual permanente (paso 0 en la figura). Cuando LEC1 tiene la dirección del LECS, se establece una conexión configuration-direct (paso 1 en la figura) y de él se obtiene información diversa, como: tipo de ELAN, MTU y dirección ATM del LES correspondiente.

2.1.2 Registro y resolución de direcciones:

Una vez que LEC1 conoce la dirección del LES, establece una conexión control-direct (paso 2) con el LES, este le asigna un identificador único y LEC1 registra con él su dirección MAC y ATM. En este momento LEC1 ya pertenece a la ELAN *ingeniería*.

El LES establece una conexión control-distribute de regreso a LEC1 (paso 3), mediante las conexiones control-direct y control-distribute. Después de esto, LEC1 puede enviar peticiones LE_ARP y recibir su correspondiente respuesta del LES.

LEC1 envía una petición LE_ARP al LES para obtener la dirección ATM del BUS correspondiente a la dirección Broadcast (FFFFFFFFFFFF). El LEC establece una conexión multicast-send (paso 4) con el BUS y este responde estableciendo una conexión multicast-forward (paso 5) con el cliente.

Terminado lo anterior, podemos asegurar que el cliente está listo para la transmisión de datos.

2.1.3 Transmisión de datos

Suponiendo que LEC2 ya se registró con el LES, y LEC1 quiere establecer una transferencia de datos con él, LEC1 envía una petición LE_ARP al LES. Mientras espera respuesta de el también reenvía el paquete al BUS.

Cuando recibe la respuesta establece una conexión data-direct con LEC2 (paso 6) y así comienza la transferencia de datos entre las dos entidades.

3. Seguridad en redes ATM

Como otros tipos de redes, las redes ATM sufren de todo tipo de ataques ([9], [10], [11], [12], [13], [14]). Algunos ataques típicos son: escucha no permitida, spoofing, negación de servicios, robo de canales virtuales y análisis de tráfico. A notar que el robo de canales ATM y el tráfico de análisis sólo ocurre en redes ATM.

La escucha no permitida se refiere al hecho de que el atacante conecta al medio de transmisión y obtiene un acceso no autorizado de los datos. El hecho de que la mayor parte de las redes ATM están conectadas vía fibra óptica, hace suponer que no es fácil "escuchar" una red ATM. Sin embargo en [15] se reporta que, dependiendo del punto de escucha, un equipo que pueda escuchar una fibra óptica cuesta aproximadamente $2,000 USD,

El spoofing se refiere al hecho de que un atacante se haga pasar por otra persona para tener acceso a los recursos que le pertenecen a la víctima, para tomar ventaja o simplemente para destruir dichos recursos. Este tipo de ataque puede necesitar herramientas especiales para manipular las unidades de datos del protocolo y que el atacante tenga ciertos permisos de acceso. Sin embargo ATM esta siendo usada en dominios públicos, lo que la hace propensa a este tipo de ataques.

ATM es una técnica orientada conexión, la cual es establecida a través de un canal virtual (VC). El canal virtual es manejado a través de un conjunto de señales. El VC es establecido por una señal SETUP y puede desconectarse a través de las señales RELEASE o DROP PARTY. Si un atacante envía una señale RELEASE o DROP PARTY al nodo intermedio de un canal virtual, entonces el canal se desconectará (ver [16]). Enviando este tipo de señales frecuentemente, el atacante puede degradar paulatinamente la comunicación entre dos usuarios.

Si dos switches en una red ATM se ven comprometidos, el atacante puede robar un canal virtual de otro usuario. Digamos que VC1 y VC2 son dos canales virtuales que conectan al nodo A con el nodo B. VC1 es controlado por el usuario U1 y el VC2 es poseído por U2. Si A y B están comprometidos, entonces A puede enviar celdas de VC1 que van de A á B a través de VC2 y B puede enviar de regreso esas celdas a VC1. Ya que los nodos direccionan las celdas basadas en un VCI (identificador de un VC) o VPI (identificador de un VP) en el encabezado de la celda, A y B pueden alterar estos campos en cualquier sentido. Los nodos entre A y B no notarán estos cambios y direccionarán las celdas consideradas de VC2 como si se tratarán de celdas autenticas de VC2. En una red de switcheo pública U1 no ganaría mucho con lo anterior. Sin embargo, en una red ATM, si la calidad de servicio es garantizada, entonces el usuario 1 puede ganar bastante robando un canal de comunicación con mayor calidad, al cual no tiene derecho de acuerdo a la política de control de acceso. El usuario 1 puede ganar aún más si cada usuario tiene que pagar por la comunicación. En ambos casos, el usuario 2 puede ser dañado.

El análisis de tráfico se refiere al hecho de que el usuario puede obtener información colectando y analizando información ([17]) como el volumen, tiempo y las partes de comunicación de un canal virtual. Volumen y tiempo puede revelar una gran cantidad de información al atacante, aún si esta es encriptada, ya que la encripción no afecta el volumen y tiempo de la información.

3.1 Implementado seguridad en redes ATM

Para construir un sistema de seguridad en redes ATM, lo primero que debe hacerse es identificar los requerimiento de seguridad. Este aspecto ha sido discutido ampliamente en forums ATM ([20], [18], [19]) y en la literatura ([17], [13], [11]). En esta sección se discutirán algunos aspectos generales sobre el diseño y construcción de sistemas de seguridad en redes ATM.

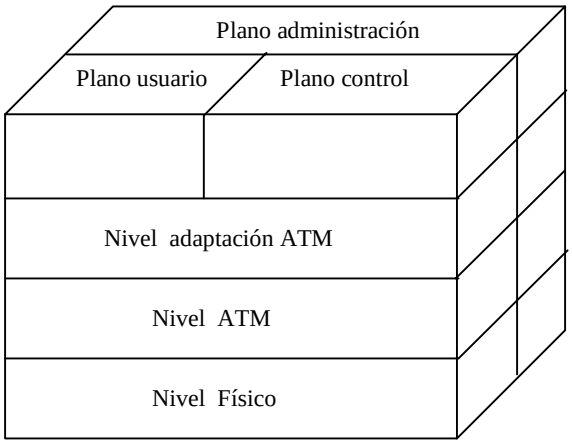


Figura 2. Arquitectura red ATM

Con el objetivo de crear un esquema de seguridad en una red ATM, se debe tomar en cuenta la arquitectura de ATM (figura 2). Esta arquitectura incluye tres planos: el plano del usuario, el plano del control y el plano de administración. Las entidades en el plano usuario son usados para transferir datos de usuario. Las entidades en el plano de control están relacionadas con el establecimiento de la conexión, liberación y otras funciones de conexión. Las entidades del plano de administración llevan a cabo funciones de manejo y coordinación relacionadas tanto con el plano usuario como con el plano de control. Aparte de estas entidades en estos planos, existen las entidades del nivel ATM. El nivel ATM realiza transferencia de datos ATM en interés de las entidades en los otros tres planos. Es obvio que para implementar los requerimientos de seguridad en redes ATM, todos los tres planos y el nivel ATM tienen que ser incluido dentro del esquema de seguridad.

Para resolver el problema de seguridad en ATM, el forum de ATM del grupo de trabajo en seguridad esta trabajando en la infraestructura de seguridad de ATM. Los esfuerzos de este forum dieron como resultado la Fase I de Especificación de Seguridad (ver [18]). Este documento trata los mecanismos de seguridad en el plano usuario y en el plano de control. Incluye mecanismos de autenticación, confidencialidad, integridad de datos y control de acceso para el plano usuario. También incluye mecanismos de autenticación para el plano de control. El plano de administración y el resto del plano de control aún no han sido tocados. La especificación también especifica algunos servicios de soporte de seguridad: negociación de servicios de seguridad y parámetros.

El objetivo de la Fase I de la Especificación de Seguridad es proporcionar una infraestructura lo suficientemente flexible para que sea posible acomodar diferentes algoritmos y longitudes de llaves, proporcionar interoperabilidad entre vendedores, proveer compatibilidad entre los dispositivos sin ninguna extensión de seguridad y proporcionar una separación entre autenticación e integridad de lo que es confidencialidad.

En la seguridad dentro del plano de usuario, el control de acceso es usado para prevenir que entidades no autorizadas establezcan conexiones. Para lograr que la especificación sea independiente de cualquier implementación, la especificación estandariza la información y el mecanismo de intercambio de información requerido por un algoritmo de control de acceso. La autenticación esta diseñada de tal forma que la parte invocadora y la invocada sean genuinas, esta es hecha a partir de técnicas criptográficas con algoritmos de llaves simétricas o asimétricas. El mecanismo de confidencialidad de datos esta basado en las celdas. La parte de datos de la celda se encuentra encriptada de tal forma que no sea accedida por un usuario no autorizado. Hay que notar que el encabezado de la celda no esta encriptado.

La seguridad en el plano de control solo proporciona mecanismos de autenticación de señalamiento el cual buscará una señal de mensaje ATM de su fuente. Esta búsqueda puede ser usada, por parte del receptor o terceras partes, para verificar que el mensaje es de la fuente de la que dice ser. Esto permite proteger redes ATM de ataques de negación de servicio que manipulen las señales.

Ahora bien, lo anterior son propuestas del forum ATM con respecto a seguridad. En el caso de nuestro modelo, debemos tomar en cuenta que estamos emulando ATM sobre redes locales ya existentes, por lo que muchos de los mecanismos propuestos no aplican y, aparte, surgen otros tipos de problemas. A fin de proporcionar una red segura a los usuarios de la red (se habla de unos 9,000 usuarios de la red en la cual se implemento nuestro modelo) se eligió combinar las propuestas anteriores con el uso de un firewall.

4. Los Firewalls

Cuando se habla de seguridad en redes, se requiere que varios requerimientos sean cubiertos. En primer lugar es importante hablar de autenticación, en este caso se debe verificar que los usuarios son quienes dicen ser, confidencialidad, solo los usuarios autorizados puede acceder el contenido de los datos, la integridad, los datos no pueden ser alterados por terceras partes durante la transmisión de estos y por último la no-repudiación, que consiste en que un usuario no puede negar el hecho de que tuvo acceso a un determinado servicio o datos.

Hace algunos años, y aún hoy, los firewalls se han visto como algo infalible en contra de los ataques computacionales a sistemas de información ([5], [6], [7] y [8]). Como su nombre lo indica, esta es una herramienta de seguridad que se utiliza como si tratáramos de erigir una muralla de fuego que rodee nuestros recursos (servidores, información, servicios, etc.) y evitar así penetración de intrusos que los dañen o se aprovechen de ellos.

¿Cómo se erige esta muralla? Lo primero es determinar cuales son los recursos que se quiere proteger, y hasta se va a proteger, pues esta muralla en realidad no es tan infranqueable sino que solamente abre o permite el paso de quienes estén autorizados (ver figura 3)

Esto nos lleva a deducir que se requieren ciertas reglas que determinen que, quien, y como puede uno acceder a los diferentes recursos que se encuentran detrás de la muralla. Una vez definido todo esto, necesitamos dividir nuestra red en dos partes, una en la que se resguardan los recursos y la otra en la que fluye el tráfico de forma normal (DMZ: Zona Desmilitarizada), tal y como se hacía antes de poner la muralla. Esto generalmente se hace con una computadora o un enruteador con dos interfaces y un software en el cual se implantan las reglas que dirigirá el tráfico de entrada hacia la interfaz “segura” así como el tráfico proveniente de la misma.

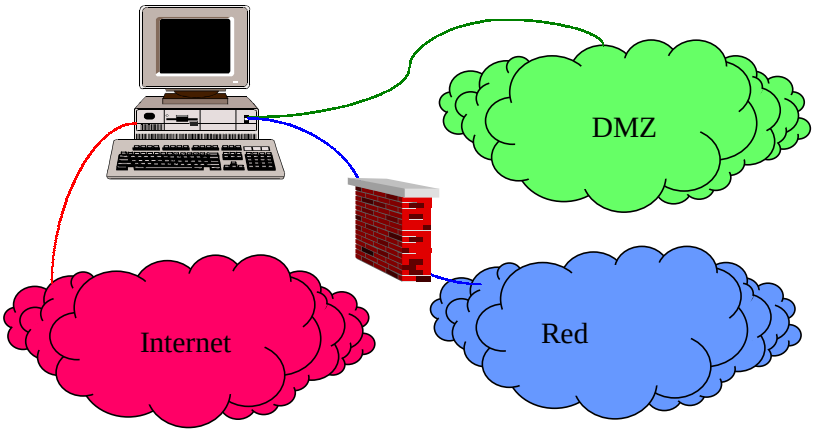


Figura 3 Esquema general red protegida con un firewall

Los firewalls pueden clasificarse de acuerdo al tipo de información que filtran. Puede ser un ruteador comercial con capacidad de filtración de paquetes. En este caso el firewall examina el encabezado de los paquetes que van hacia afuera o vienen entrando a la red privada. Las reglas de este firewall permiten dejar pasar el paquete o descartarlo. Las reglas se fijan en función de las direcciones, protocolos en la capa superior, y puertos, básicamente. Otro tipo de firewall se conoce como proxie a nivel circuito. Este firewall establece una conexión a nivel IP, entre un cliente en una interfaz y un

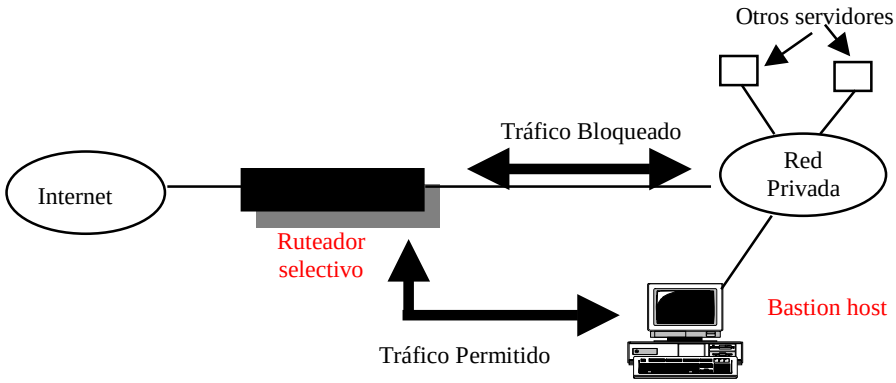
servidor en otra interfaz, no analiza los protocolos de la capa superior; la conexión segura es conocida como circuito. Se le considera proxy, pues es el intermediario entre el cliente y el servidor. El último tipo es el proxie a nivel aplicación Establece una conexión segura a nivel aplicación con un cliente, y por otro lado con un servidor. El diálogo con el cliente y el servidor es independiente. Interpreta el protocolo de aplicación al mismo tiempo que permite el paso o descarta paquetes

Los firewalls de circuito y aplicación, son intermediarios. Ambos reciben un paquete de su origen y lo "adaptan" para entregarlo al destinatario. El firewall de filtro de paquetes no realiza esta función.

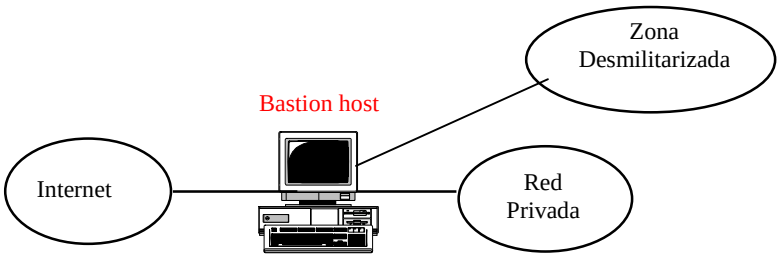
Quizás uno de los pasos más importantes al instalar y configurar un firewall sea trabajar con las interfaces de red. Cada interfaz debe ser configurada manualmente, habilitada y probada por el administrador. Esta tarea cambia de plataforma a plataforma. También es recomendable configurarlas desde la herramienta de administración del firewall.

Existen otras consideraciones a tomar en cuenta cuando se desea implementar un firewall. Entre las más importantes está que el firewall no puede informar nada acerca de las redes que se encuentran dentro de la red protegida. Esto implica que los usuarios de las red interna deben conectarse en el firewall antes de acceder otras redes. De igual forma, para que un usuario externo pueda conectarse a un host de la red interna este debe conectarse primero al firewall. El mismo principio anterior se aplica para el correo electrónico, todo correo que vaya a un host externo o a un host de la red interna debe pasar por el firwall. El firewall no debe montar ningún sistema de archivos vía NFS o RFS, o dejar alguno de sus sistemas de archivos listos para montarse, tampoco no debe correr NIS. Si no son necesarios, compiladores y cargadores deben borrarse. La seguridad de los passwords debe ser reforzada al máximo. El firewall no debe confiar en ningún otro host.

Un firewall se compone de dos tipos de componentes un ruteador selectivo y un bastion-host. Un ruteador selectivo puede ser un ruteador comercial con capacidad de filtración de paquetes. Bloquea el tráfico entre dos redes o servidores específicos. El bastion host contiene la mayor parte del software del firewall. En general se cuenta con dos tipos de configuración, screende host gateway y dual-homed gateway, las cuales se ilustran en la figura 4.



Screened host gateway



Gateway "Dual-Homed"

Figura 4. Tipos de configuración red-firewall

5. El esquema propuesto

El esquema funciona en la red del ITESM-CEM. Después de un análisis se determino que en la comunidad del CEM existen los siguientes perfiles de usuario:

- Alumno
- Profesor
- Administrativo
- Administrador

Entre los diferentes tipos de servicios ofrecidos encontramos:

- El primer servicio que se ofrece es el de conexión a cada una de las máquinas del campus entiéndase por esto, que cada nodo en la red esta conectado físicamente a un switch con un LEC que se integra a una ELAN a través de un LES/BUS y también existe un LEC dentro de esa ELAN que hace las veces de default gateway para todo nodo en la red.
- Sobre este servicio se edifican los demás servicios y estos se encuentran distribuidos en diversos servidores conectados directamente a la nube ATM como LEC de las diferentes ELAN's a continuación un listado de los servicios que se prestan:
- DNS (Domain Name Service) Resolución de nombres
- DHCP (Dynamic Host Configuration Protoco) configuración automática de clientes
- Acceso telefónico
- Radius configuración automática para clientes de acceso telfónico.
- NIS (Network Information Service)
- FTP (File Transfer Protocol) transferencia de archivos
- HTTP (Hyper Text Transfer Protocol) WEB con diversas aplicaciones entre otras comercio electrónico en diversos servidores
- SMTP (Simple Mail Transer Protocol) correo electrónico.
- Servicio de certificados
- Aplicaciones como: LOTUS Learning Space, BANNER , ECOA, MIEVA, SIDI, REDI y consulta de calificaciones

El hablar de Redes Emuladas, o LanEmulation, implica hablar de algunos cambios de cómo se veían anteriormente las redes. Antes una red Ethernet se podía ver como una serie de computadoras conectadas a un medio físico (UTP/ Fibra óptica o Coaxial) y, por las características de los protocolos y medios, cuando se tenían muchos clientes o computadoras conectadas al mismo medio se llegaban a presentar problemas. Un ejemplo de estos problemas son retardos en las transmisiones, lo que provocaba retransmisiones y esto a su vez representaba retardos en otras transmisiones y en otros casos se presentaban problemas conocidos como Broadcast Storm. Con la finalidad de eliminar estos problemas surgen los bridges y enruteadores, estos últimos son equipos con más de una interfaz lo que nos permite separar una subred o dominio de coaliciones en dos; aliviando así la red al separar el tráfico.

Como consecuencia de lo anterior, si se quería conectar una máquina con otro conjunto de máquinas en la misma red, se tenía que tenerlas conectadas físicamente en el mismo medio (a lo mejor ayudándome de un repetidor).

Si hacemos una analogía con nuestro esquema de Firewall anteriormente mencionado y lo tratamos de hacer encajar en una tecnología como ethernet, entonces requeriríamos de una máquina con una tarjeta conectada a un conjunto de computadoras seguras (las que se quiere proteger) y otra tarjeta conectada a lo que se conoce como zona desprotegida.

Es aquí donde surge donde surge la necesidad de cambiar de paradigma, porque al hablar de redes Emuladas realmente estamos hablando de redes virtuales que permiten tener a un grupo de computadoras pertenecientes al mismo dominio de colisiones, en lugares físicos distintos y estar conectados por medios físicamente diferentes de tal suerte que las computadoras que queremos proteger pueden estar en cualquier lugar de mi sitio.

Nuestra propuesta es la siguiente, si se cuenta con una computadora con una tarjeta ATM, la cual puede tener configurados clientes de ELANs distintas, y si esta misma computadora tiene la capacidad de comportarse como Lan Emulation Server, Lan Emulation Configuration Server, entonces podemos definir por un lado a esta máquina como el LanEmulation Configuration Server, LanEmulation Server y Broadcast and Unknown Server de una ELAN segura. Estas mismas entidades atenderán las peticiones de conexión de los diferentes clientes o computadoras que queremos proteger, es decir estos últimos se comportaran como LanEmulation Client de lo que en adelante llamaremos ELAN Sec.

Por otra parte se definirá una LanEmulation Client en la misma tarjeta del servidor o Firewall que nos permita conectarnos con el mundo exterior o sea la red desprotegida. Para agregar un poco de seguridad y que otros clientes no se agreguen a la ELAN segura, tendremos que asegurarnos que el LanEmulation Configuration Server y el LanEmulation Server, solo acepten peticiones de aquellas direcciones ATM que se consideren como clientes seguros

El comportamiento de la red va a depender de las políticas que se implanten en el firewall, se pueden presentar diferentes escenarios (ver figura 5). Cuando una computadora en Internet intente realizar una conexión con un servicio en una computadora detrás del firewall y este estipulado en las políticas que ese servicio no se encuentra accesible desde internet entonces esta petición será denegada. Solo se podrían llevar a cabo aquellas comunicaciones de afuera hacia adentro y de adentro hacia fuera que estuvieran definidas como validas dentro de las políticas del firewall.

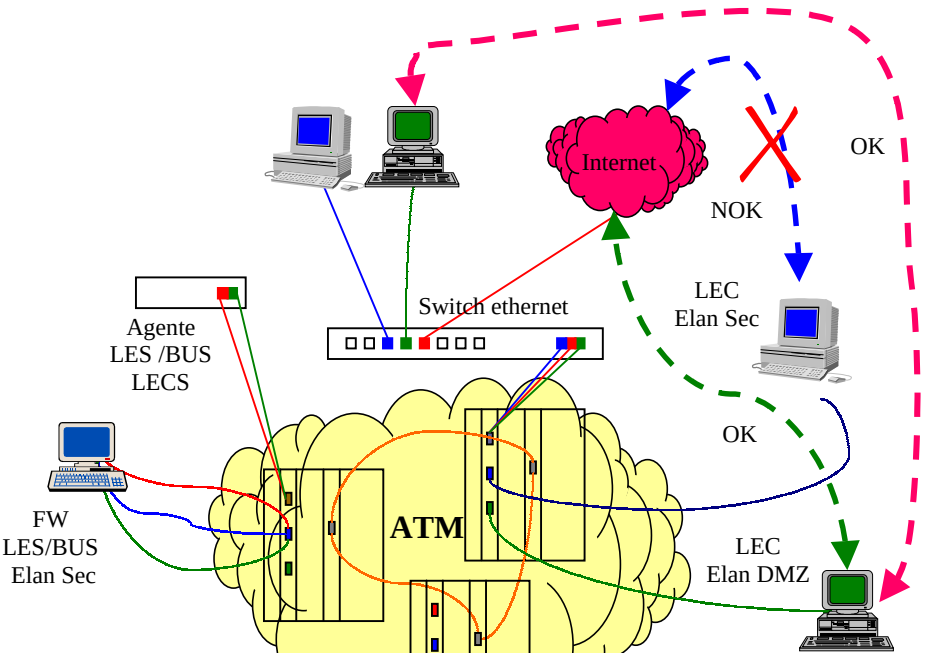


Figura 5. Diagrama general del esquema propuesto

Por otra parte, si tuviéramos que otro servicio no este aún disponible entre las computadoras que se encuentran dentro de la red segura y alguna de ellas intentara realizar una conexión con otra maquina de esta red, esta comunicación tendría que ser protegida desde cada una de las máquina

El esquema propuesta ha sido implementado en una red de aproximadamente 9,000 usuarios y con un conjunto heterogéneo de computadoras que van desde estaciones de trabajo Sun, PC compatibles, servidores SG y una que otra Mac. También es importante remarcar que se cuenta con una variedad importante de protocolos usados: TCP/IP, NetBeui, NetBios, AppleTalk, IPx, Wireless, etc.

El rendimiento de la red no se ha visto afectado por el esquema propuesto, al contrario el acceso a Internet es más rápido y la transferencia de información también. Desde el punto de vista seguridad, no se ha presentado la misma cantidad de problemas que se tenían con el esquema anterior.

6. Conclusiones

Se ha presentado las características principales de las redes ATM y de los firewalls. A partir de estas se presentó un esquema de seguridad basado en firewalls para redes ATM. El esquema ha sido implementado con éxito en la red del ITESM-CEM. En el momento en que se esta escribiendo este documento el esquema se encuentra en operación y sin problema alguno.

Sin embargo los autores están conscientes de que no basta con tener un firewall para garantizar la seguridad de una red. Aún resta trabajo por desarrollar, sobre todo en el área de definición de políticas y su implementación en el esquema propuesto. También hay que tomar el cuenta el gran número de usuarios internos con que se cuenta y el nivel de cada uno de ellos.

Con respecto al trabajo a futuro, se puede decir que en este instante el nivel de encriptamiento se hace sobre IP, se piensa que un futuro este encriptamiento se haga directamente sobre las celdas ATM de la red.

Bibliografía

[1] Pierre Rodin, “Reseaux Haut Debit”, Ed. Hermes, 1999, 2da. edición

[2] W. Stallings, “High-Speed Networks, TCP/ IP ATM design principels”, Ed. Prentice Hall, 1998

[3] J. García, S. Ferrando, M. Piattini, “Redes de alta velocidad”, Ed. Alfaomega ra-ma, 1997

[4] Ulysess Black, “Tecnologías emergentes para redes de computadoras”, Ed. Prentice Hall, 1997

[5] Simson Garfinkel and Gene Spafford, “Practical and Unix Security”, O’Reilly & Associates, Inc, 2da. edición, 1996

[6] Summers Rita, “Secure Computing Threats and Safeguards”, Ed. Mc. Graw Hill, 1997

[7] Hutt A., Bosworth S., Hoyt D., “Computer Security Book”, Ed. John Wiley and Sons Inc., 1995
[8] Chewswick W and Bellovin S, “Firewalls and Internet Security”, Addison-Wesley, 1999
[9] Maryline Laurent, Oliver Paul, Pierre Rolin, “Securing communications over ATM networks”, IFIPSEC’97, Copenhagen, Denmark, mayo 1997
[10] L. Hanson, “The impact of ATM on Security in Data Network”, Proceedings of Compsec International 1995, Conf 12, pp. 318-34
[11] Shew-Cheng Chuang, “Securing {ATM} Networks”, 3rd{ACM} Conference on Computer and Communications Security, New Delhi, India, 1996, pp. 19-30
[12] R. Deng et al, “Securing Data Transfer in Asynchronous Transfer Mode Networks”, Proceedings of GLOBECOM’95, Singapore, Noviembre 13-17, 1995, pp. 1198-1202
[13] J. Kimmins and B. Booth, “Security for ATM networks”, Computer Security Journal, XII(1):21-29, 1996
[14] Richard Taylor, Greg Findlow, “Asynchronous Transfer Mode: Security Issues”, Proc Australian Telecommunication Networks and Applications Conference, pp. 161-166, Diciembre 1995
[15] M. Bacon, “Security: a question of confidence”, Telecommunications (int. ed.) (USA) Vol. 23, No. 11, pp. 51-52, Nov. 1989
[16] Stevenson and N. Hillery and G Byrd, “Secure Communications in {ATM} networls” Communications of the ACM, Vol. 38, No. 2, pp. 45-52, febrero 1995
[17] Richard Taylor, Greg Findlow, “ATM: Security Issues”, Proceedings of Australian Telecommunication Networks and Applications Conference, pp. 161-166, diciembre 1995, pp. 161-166.
[18] Security Working Group, Phase I ATM Security Specification, ATM Forum BTD-SEC-01.03 julio 1997
[19] Security Working Group, Security Framework for ATM Networks. ATM Forum BTD-SEC-FRWK-01.01, julio 1997
[20] M. Peyravian and E.V. Herreweghen, ATM Scope & Requirement, ATM FORUM/95-0579