Seguridad aplicada a un carrier transaccional

Larry Medina Aguirre[1], José Escalante[2]

[1]Ingeniero Eléctrico en Electrónica 2006

[2]Director de Tópico. Ingeniero Eléctrico en Electrónica, Escuela Superior Politécnica del Litoral, 1996, Diplomado en Telecomunicaciones, Ecuador, Escuela Superior Politécnica del Litoral, 1997. Profesor de ESPOL desde 1998

RESUMEN

El presente trabajo se refiere a la Implementación de Seguridad Informática en una Red Wan, para recibir transacciones desde un carrier en forma segura.

La implementación estará dada con herramientas proporcionadas mediante un software de Firewall, Reglas y Políticas que darán seguridad a una Red de comunicaciones(Wan y Lan), para el efecto se utilizará un PC con Windows 2000 professional.

El objetivo primordial de esta implementación es dar soluciones de la seguridad Informática en la Red de Comunicaciones de un Cliente, para lo cual realizaremos una aplicación mediante una simulación teórico-práctico, que detallaremos en el presente proyecto.

ABSTRACT

The present work refers to the the Implementation of Computer Security in a network Wan, to receive transactions from a carrier in sure form.

The implementation will be given with proportionate tools by means of a software of Firewall, Rules and Political that will give security to a net (Wan and Lan), for the effect a PC will be used with Windows 2000 professional.

The primordial objective of this implementation is to give solutions of the Computer security in the Net of Communications of a Client, for that which we will carry out an application by means of a theoretical-practical simulation that we will detail project presently.

INTRODUCCION

La seguridad Informática mediante la aplicación de un software de firewall hoy en día es de extrema importancia, dado que muchos sistemas de comunicaciones a nivel de empresas privadas e instituciones en general, manejan información que dada la confidencialidad que los datos requieren, muchas empresas no la poseen y es necesario e importante su aplicación para darle mayor seguridad.

Los gobiernos del mundo están muy interesados en conocer la forma en la que las empresas protegen su información e infraestructura. En Estados Unidos, este interés se ha traducido en las recientes legislaciones Sarbanes-Oxley, HIPAA y GLBA (Gramm-Leach-billey Act). En el caso de la ley Sarbanes-Oxley, los gerentes generales y gerentes financieros deben firmar un documento anual donde justifiquen que los registros e información utilizados para informar sobre el desempeño comercial son precisos a su leal saber y entender. Antes de que los gerentes generales o gerentes financieros den fe de la integridad de la información corporativa, deben ellos mismos y la empresa entender cuáles son los controles de seguridad y procedimientos; de lo contrario, podrían comprobar la gravedad de las multas impuestas o ser encarcelados por cometer este tipo de delito.

A nivel internacional, el Acuerdo Base II exige que los bancos y proveedores del servicio de inversión a nivel mundial implementen procedimientos para medir y mitigar el crédito y el riesgo operativo. Esto implica un análisis de riesgos que le exija a las empresas afectadas analizar minuciosamente su tecnología, la continuidad de la empresa, la seguridad del ciberespacio, las operaciones, el procesamiento y el riesgo de las transacciones.

CONTENIDO

CAPITULO 1: TECNOLOGIAS, CONCEPTOS Y PROTOCOLOS

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadores), así como a la puesta en órbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

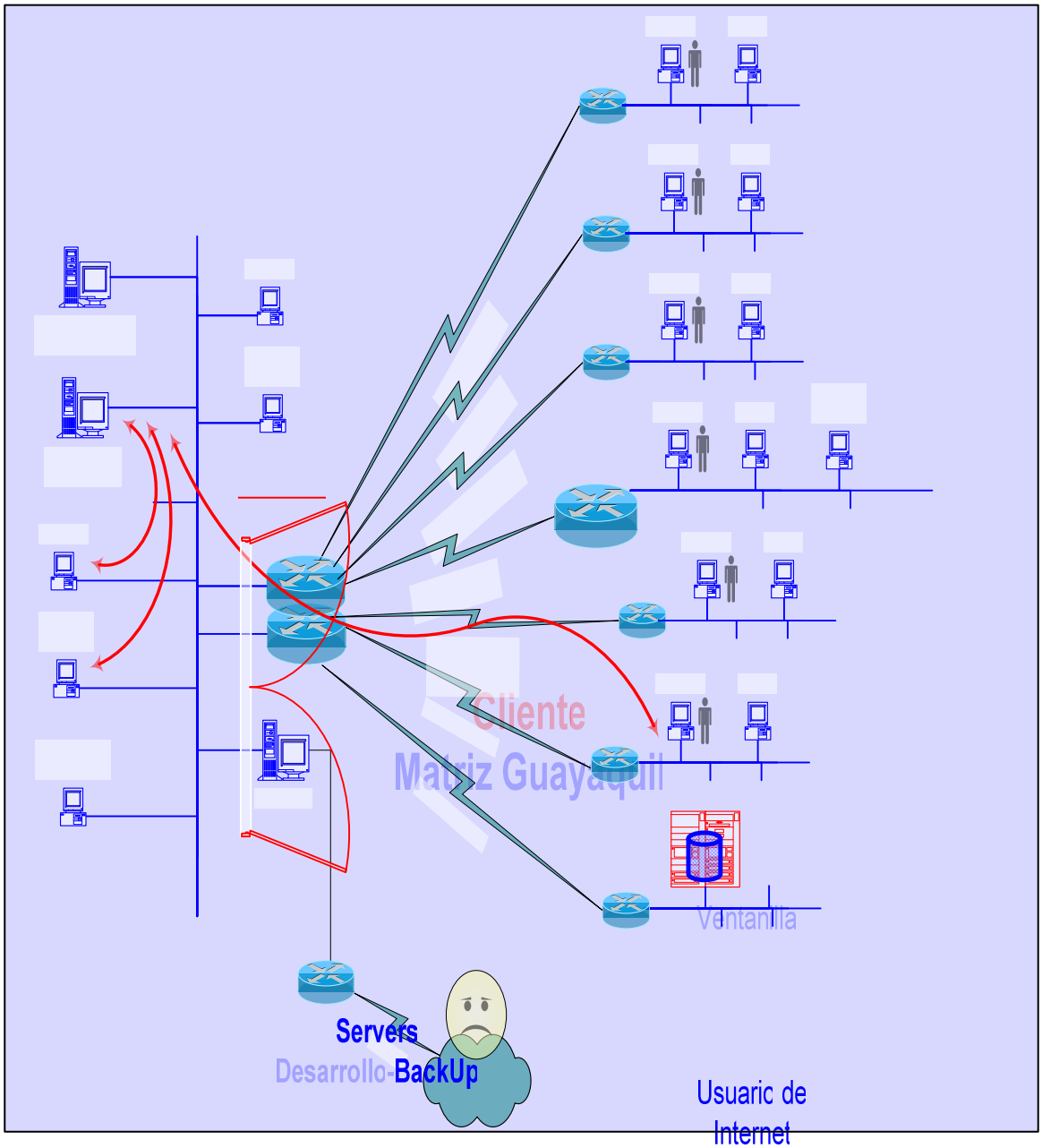
La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

Este capítulo básicamente se refiere a los conceptos de redes sus topologías, conceptos de Firewall, y protocolos de seguridad.

CAPITULO 2: SITUACION ACTUAL DEL CLIENTE Y DEL CARRIER

El capítulo II describe los problemas y falencias de la red del cliente y del carrier realizando una evaluación de dichas redes, analizando su backbone lan y wan, los equipos que tiene el cliente, tipos y velocidad de enlaces de comunicaciones para verificar la vulnerabilidad de la situación actual y dar una solución a estas falencias de seguridad informática.

Rack de comunicaciones del cliente



Vulnerabilidad de la red del cliente

Servers
PRODUCCION

Open Door

Ventanilla

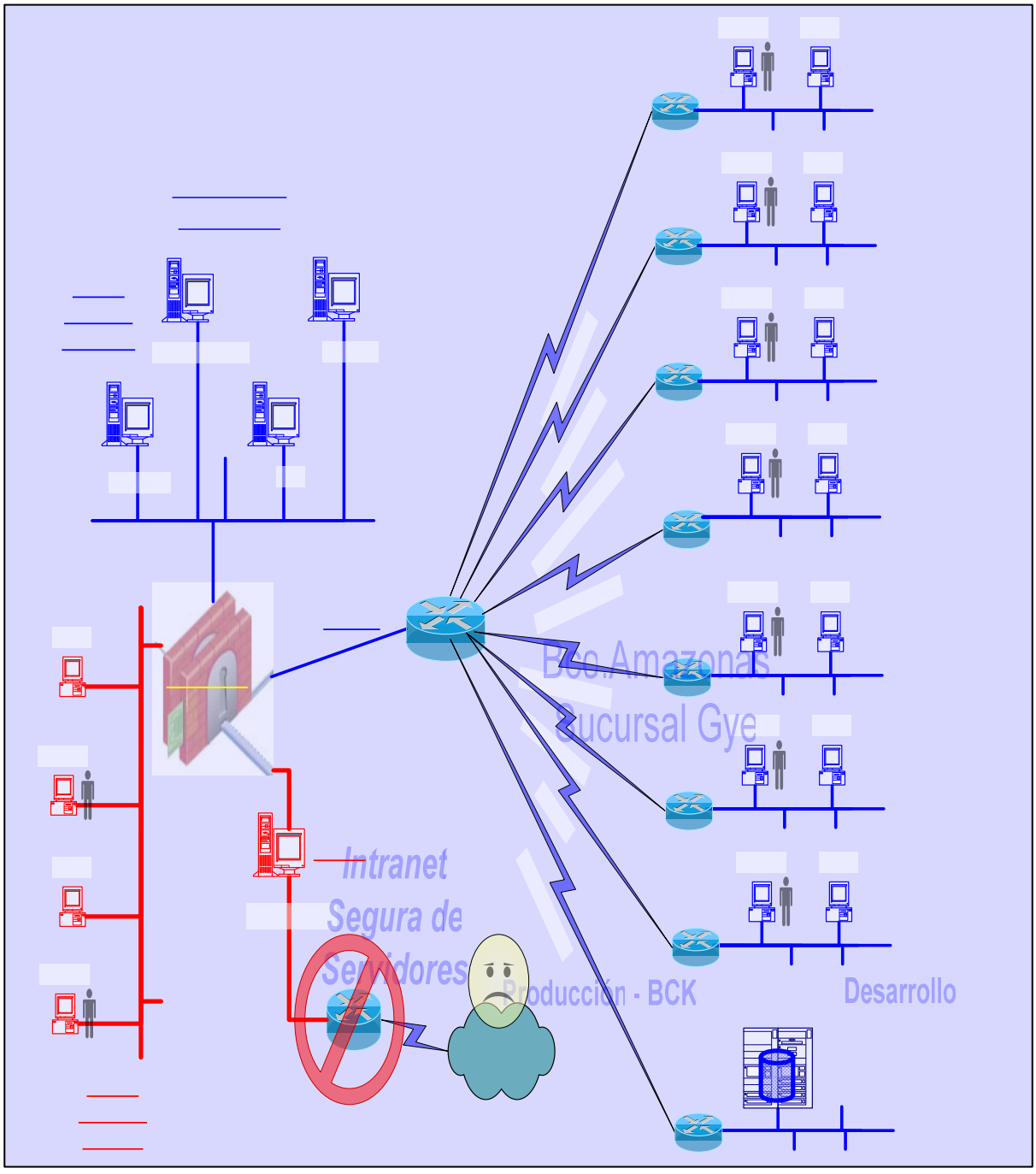
Usuario de

64 Kbps IMPSAT

32 Kbps IMPSAT

11 Mbps IMPROL

256 Kbps PORTA



Red protegida del cliente

Producción

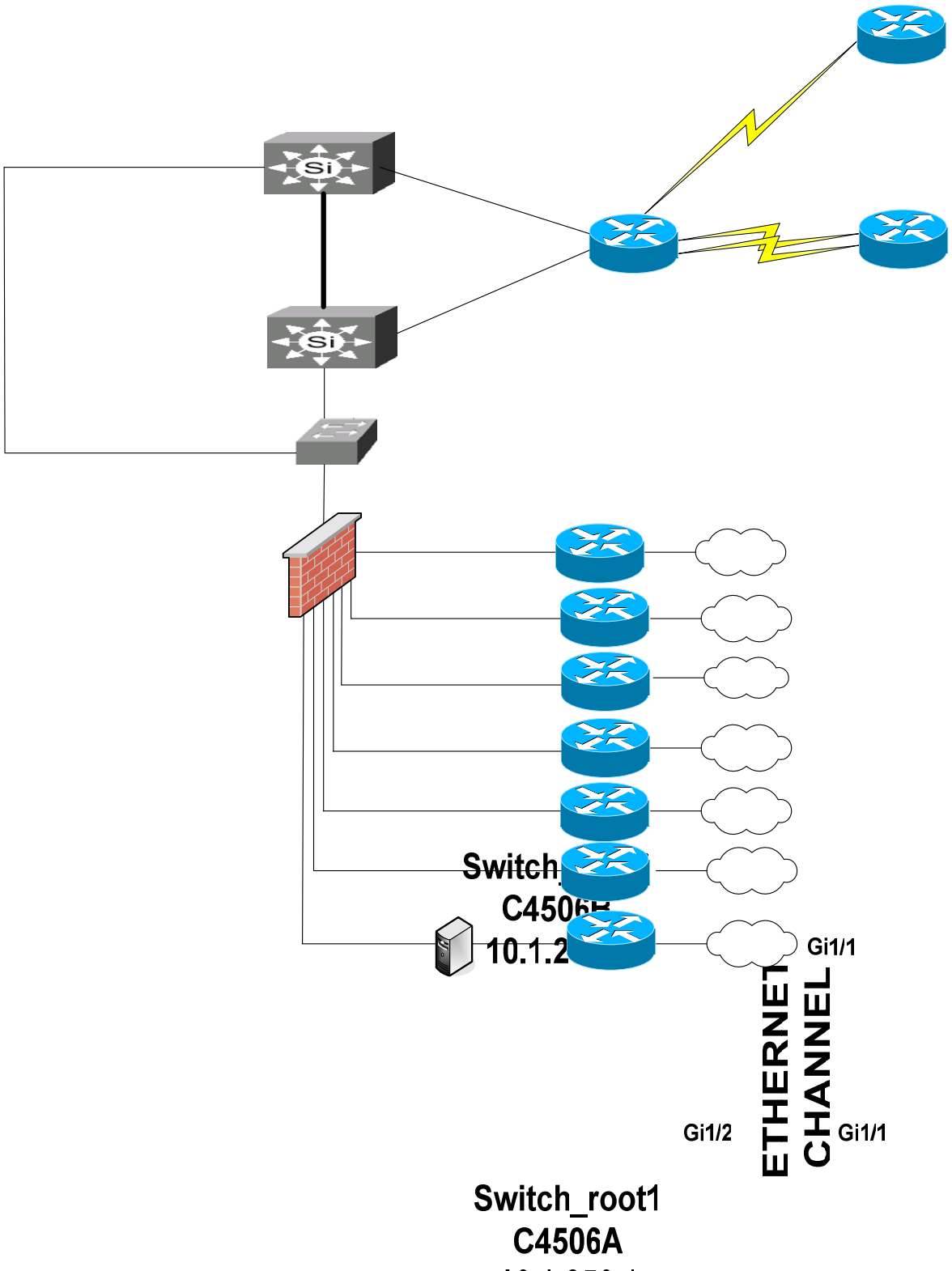
Bono

Extranet

Usuario

CAPITULO 3: IMPLEMENTACION DE SEGURIDAD APLICADA A UN CARRIER TRANSACCIONAL

Hablaremos sobre el hardware y software de seguridad a utilizar, el esquema de implementación los pasos para la instalación del Firewall en el cliente, la instalación del software de administración, creación de reglas y políticas de seguridad.



CAPITULO 4: ANALISIS ECONOMICO

El Firewall esta orientado o destinado para ofrecer seguridad a una Institución o Empresa que posean infraestructura de redes WAN y LAN, por tanto se pueden instalar en instituciones que requieran este servicio.

La instalación o implementación requiere corto tiempo una vez que se tiene los equipos necesarios.

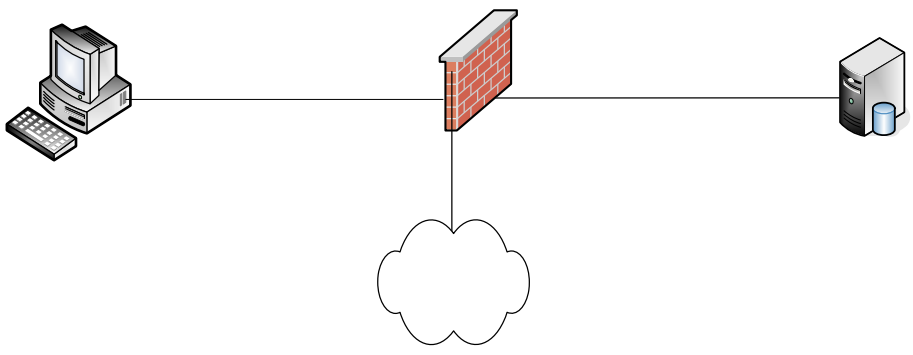
Debemos anotar que siendo el Firewall una tecnología que tiene vigencia en el Mundo desde 1997 sin embargo en nuestro País recién se comienza a implementar por los años 2000 y son pocas las empresas que la disponen, por tanto, estamos seguro que una vez que se difunda mas esta tecnología serán muchas las empresas que la implementarán.

Básicamente en este capítulo se describirá el análisis económico del software y hardware a utilizar, costos de instalación, licenciamiento y actualizaciones de licencias.

CAPITULO 5: DEMO

En este capítulo se realiza una demostración de la seguridad utilizando el software Check Point en una pequeña red simulando el proyecto.

Para simular la seguridad a implementarse en este proyecto se utilizarán tres Pc´s, como muestra la figura, los cuales van a representar el Firewall, el cliente y el carrier, se realizarán pruebas las cuales ilustrarán el funcionamiento del software de seguridad Check Point.



EQUIPAMIENTO A UTILIZAR

- 1 Pc Intel Pentium IV 2.4 Ghz,, 512 MB de memoria RAM
- 1 Pc Intel Pentium III 900 MhZ, 256 MB de memoria RAM
- 1 Pc Intel Pentium II 500 MHz
- 1 Switch de 8 puertos 10 BaseT
- 2 Patch cord punto a punto
- 1 Patch cord cruzado
- 2 tarjetas de red 10/100 Base T
- Software Check Point
- Software FTP Cliente servidor

CONCLUSIONES

Con seguridad que a lo largo de este trabajo ha quedado demostrado que nuestros problemas no están solucionados simplemente con la implementación de un esquema de firewall; de hecho si en realidad no forma parte de una política de seguridad integral de la organización de nada servirá tener la configuración más segura en lo que a firewall respecta.

Una vez superado este punto, es decir existe la voluntad política dentro de la organización de implementar una política de seguridad seria, todo el personal de la misma esta concientizado de ello y fundamentalmente la más alta dirección esta impulsando este desafío, es conveniente pensar en la implementación de un esquema de firewall.

A partir del hecho ya consumado que constituye la interconectividad a través de Internet, es fundamental la utilización de filtros debido a que seguramente nuestra organización estará también accediendo a los servicios que Internet nos ofrece. Qué arquitectura es la más apropiada tendrá que ver seguramente con la criticidad de nuestros servicios, lo valioso de nuestra información, los servicios que ofreceremos y obtendremos de Internet, y de los recursos con los cuales contemos para llevar adelante este desafío.

Y por último, debemos tener en cuenta que este tema no consiste solo en implementar un firewall y problema resuelto. La importancia operativa es tal que debemos estar constantemente revisando las políticas, los logs, etc. para poder determinar si estamos siendo vulnerables en algún aspecto. Por otro lado un firewall, en mi opinión personal debe asemejarse a un antivirus, el cual si no se actualiza constantemente deja de ser seguro. Tengamos en cuenta que el firewall constituye la puerta de acceso a nuestra información vital, por ende a nuestro negocio y por último a nuestro dinero.

REFERENCIAS

1. Larry Medina, " Seguridad aplicada a un carrier transaccional " (Tópico de graduación, Facultad de Ingeniería Eléctrica y Computación, Escuela Superior Politécnica del Litoral, 2006)
2. Internet Routing Architectures. Bassam Halabi. http://www.cis.ohio-state.edu/hypertext/information/rfc.html
3. Firewalls y seguridad en internet http://www.monografias.com
4. CheckPoint_NGX_Firewall_SmartDefense_User_Guide http://www.checkpoint.com/support/technical/documents/docs_r60.html
5. José Manuel Huidobro, Redes y Servicios de Telecomunicaciones Paraninfo 2000, pp 272-284
6. William Stalling, Comunicaciones y redes de computadoras Prentice Hall, 2002, pp 397-419
7. Check Point Software Technologies, Secure Virtual network getting started guide Check Point Software Technologies, 2002, pp 102-122
8. Karanjit Siyan y Chris Hare, Internet y Seguridad en Redes, Prentice Hall, 2000 pp 110-125.