Componentes básicos para una red segura bajo VPN*

Basic elements for a secure network under the VPN

Edgar Arturo Bustos Caldas
Magíster en Telemática de la Universidad Martha Abreu Central de las Villas (Cuba). Ingeniero de sistemas Universidad Distrital. Especialista en las áreas de ingeniería de software, Multimedia para la docencia, redes de computadoras. Docente del programa de Tecnología en Redes de Computadores y Seguridad Informática de Uniminuto.
ebustos@uniminuto.edu

Resumen

Siempre que se piense en seguridad para una red de área Local (Lan) o global (Wan) se debe tener en cuenta las alternativas mas óptimas tecnológicas que ofrecen el mercado , como ejemplo "Vpn, Ipsec, Claves públicas, Firewall" elementos que acompañados de un buen diseño de red y estrictas políticas de seguridad se pueden garantizar en un alto porcentaje la seguridad en su red; sin dar una garantía en su totalidad . Siempre los muros infranqueables son violados y en su mayoría son atacados internamente y para este tipo de ataques es casi imposible mantener segura la red sin descuidar a los ataques externos (hackers).

Palabras clave. Redes seguras, seguridad en redes, componentes básicos de una red segura, redes y seguridad, componentes de una red segura, estándares de seguridad.

Abstract

When considering local (LAN) or global (WAN) network security, the best technological alternatives in the market should be taken into account. For instance, the Vpn, Ipsec, Public Keys, and Firewall with a good network design and strict security policies can ensure a high level of security in your network, but however, it does not guarantee total security. The most secure barriers are somehow vulnerable and most of them are attacked internally. For these types of internal attack, it is almost impossible to maintain a secure network without overlooking external attacks (hackers.)

Keywords. Secure network, security of networks, basic elements of secure networks, network and security, security standards.

*(Virtual Private Network)Redes Privadas Virtuales

Introducción

La seguridad es uno de los aspectos más importantes del diseño lógico de las redes. A veces, se pasa por alto durante el diseño de una red, pues se considera una cuestión operativa en vez de una cuestión de diseño. No obstante, si se tuviera en cuenta en el momento del diseño se podrán evitar problemas de rendimiento y escalabilidad de la red.

Por otra parte, este planteamiento surge de un interés particular del investigador por las telecomunicaciones y de la convicción de que son los diseñadores de redes, más que quienes operan los sistemas, quienes deben tener las capacidades y competencias para proponer alternativas de solución tecnológica que mejoren, agilicen y hagan efectivos los procesos.

Estándares y tecnologías de seguridad

Cuando se inicia un proceso de diseño del sistema de seguridad de una red de datos, en primer lugar el diseñador, se debe regir según los estándares de seguridad actuales, ejemplo ISO/IEC 17799:2000. Lo anterior implica un conocimiento de las tecnologías vigentes, dando lugar a un segundo momento que corresponde a la aplicación del diseño del sistema de seguridad y porcentaje del manejo operativo que se le ha venido dando a este proceso al interior de las organizaciones.

Con relación a las tecnologías vigentes, es importante detenerse en el análisis del uso de las Redes Privadas Virtuales – VPN. Actualmente, las VPN aportan grandes beneficios para obtener una red segura y como una estrategia tecnológica de seguridad la VPN debe estar basada en función de las necesidades que tienen las organizaciones, la cual se resume en las demandas actuales de los servicios IP VPN.

Tecnológicamente se podría conceptuar que las VPN son arquitecturas de red más escalables y flexibles que las WAN tradicionales, debido a que permiten a las organizaciones agregar o eliminar sus sistemas localizados remotamente, producción, clientes, soporte, normas y consumidores de forma fácil y poco costosa.

Además, la seguridad bajo el esquema de VPN requiere que la conexión a través de Internet sea cifrada. El servidor de acceso remoto exige el uso de protocolos de autenticación y cifrado. Los datos confidenciales quedan ocultos a los usuarios de Internet, pero los usuarios autorizados pueden tener acceso a ellos a través de la VPN.

Entre las principales características de las VPN se pueden mencionar:

A. Diseño de red simplificado.
Esto debido a que con la tecnología VPN se simplifica en términos de diseño de arquitectura, flexibilidad y mantenimiento, debido a que se reducen los costos asociados a la gestión de red.

B. Administración centralizada.
En cuanto a la compatibilidad, como las VPN aceptan la mayor parte de los protocolos de red más comunes (incluidos TCP/IP, IPX y NetBEUI), este tipo de redes puede ejecutar de forma remota cualquier aplicación que dependa de estos protocolos de red específicos. Algunos proveedores soportan la característica de administración centralizada de sus productos VPN, esto representa una fuerte característica de seguridad y un buen mecanismo para la resolución de problemas.

C. Prioridad de tráfico.
Esto agrega gran flexibilidad a las organizaciones que contratan el servicio, en cuanto a la utilización de los enlaces de Internet, debido a que se puede decidir en qué orden se preserva el ancho de banda según el tipo de tráfico permitido y de acuerdo a su importancia. Protegiendo la red: VPN y Firewall. La mayoría de las organizaciones hoy día protegen sus instalaciones mediante firewalls. Estos dispositivos deben configurarse

para que permitan pasar el tráfico VPN. Tal como se muestra en la Figura 1, donde el servidor VPN está colocado detrás del firewall, en la zona desmilitarizada (DMZ) o en la propia red interna.

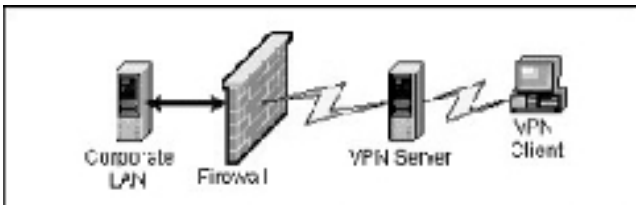

Figura 1. Ubicación del servidor VPN y el Firewall

Ventajas y desventajas de las VPN

Como se mencionó anteriormente, una red privada virtual es un esquema económico y flexible de comunicación que proporciona las características y los beneficios propios de una red privada, sin la necesidad de invertir en la infraestructura que esta requiere, pero también posee ventajas y desventajas que a continuación se enumeran:

D. Ventajas de las VPN

- Ahorro en costes
- No se compromete la seguridad de la red empresarial
- El cliente remoto adquiere la condición de miembro de la LAN (permisos, directivas de seguridad)
- El cliente tiene acceso a todos los recursos ofrecidos en la LAN (impresoras, correo electrónico, base de datos.)
- Acceso desde cualquier punto del mundo (siempre y cuando se tenga acceso a Internet).

E. Desventajas de las VPN

- No se garantiza disponibilidad (NO Internet o NO VPN)
- No se garantiza el caudal (red pública)
- Gestión de claves de acceso y autenticación delicada y laboriosa
- La fiabilidad es menor que en una línea dedicada
- Mayor carga en el cliente VPN (encapsulación y cifrado)
- Mayor complejidad en la configuración del cliente (proxy, servidor de correo)
- Una VPN se considera segura, pero no hay que olvidar que la información sigue viajando por Internet (no seguro y expuestos a ataques).

Seguridad IP

Con la explosión del uso masivo de Internet, tanto los ordenadores personales como las redes de ordenadores, pueden ser vulnerables a diversos tipos de ataques. Internet ha pasado a ser, sin ningún tipo de dudas, la mayor red pública de datos a través de la cual se facilitan comunicaciones personales y empresariales y en este caso educativas, en todo el mundo. El volumen de tráfico de datos que se mueve en Internet crece exponencialmente de forma diaria.

Entre las principales consecuencias de estos ataques se encuentra la pérdida de datos de vital importancia, violación de la privacidad y caída de la red durante largos periodos, por lo tanto la implementación de sistemas de seguridad que protejan la red es de vital importancia. Por tanto a continuación se destacan los siguientes aspectos de IPSec.

IPSec se ha convertido en el estándar criptográfico para los servicios de nivel IP, ofreciendo confidencialidad, integridad y autenticación de los extremos. IPSec se ha convertido en el estándar criptográfico para los servicios de nivel IP, ofreciendo confidencialidad, integridad y autenticación de los extremos. El estándar es obligatorio para soluciones IPv6, para el cual fue definido, y ha sido adaptado para soluciones IPv4, en las que es optativo.

El principal concepto que define IPSec es el de Asociación de Seguridad (SA). Una SA representa una conexión lógica unidireccional entre dos entidades IPSec, y ofrece servicios de seguridad al tráfico mantenido por ella. Estos servicios de

seguridad son proporcionados por dos cabeceras que son añadidas al nivel IP: AH (Authentication Header) y ESP [9] (Encapsulating Security Payload). La primera ofrece integridad en las conexiones, autenticación de origen y opcionalmente servicio anti-reenvío. La segunda es más completa y además de los servicios ofrecidos por AH ofrece confidencialidad. Tanto AH como ESP se basan en la existencia de una suite criptográfica previamente negociada para el autenticado y cifrado de los paquetes, tal y como se verán.

La implementación IPSec utilizada ha sido KLIPS (KerneL IP Security) incluida en el software FreeS/WAN. Esta solución permite establecer túneles seguros sobre redes no confiables, siendo los paquetes IP enrutados entre los SGs separados por cualquier topología de red. El resultado es una conexión IP virtual que nos permite definir nuestra VPN.

F. Intercambio de claves: IKE

Los mecanismos de seguridad de IPSec se basan en que las entidades deben establecer una negociación, en la cual ambas partes se ponen de acuerdo en los algoritmos criptográficos utilizados, en qué claves utilizar, y otros parámetros. Esta negociación no se puede establecer a nivel de red, por lo que es necesario un protocolo de nivel superior. El estándar actual es IKE (Internet Key Exchange), también conocido como Internet Security Association and Key Management Protocol (ISAKMP/Oakley)[10]. Este protocolo se basa en una negociación en dos fases. En la primera se establece una SA ISAKMP con la cual las entidades realizan la negociación y autenticación. En la segunda se establece una SA que será usada para la comunicación entre los extremos.

G. Infraestructura de Clave Pública

La solución que ofrece los mecanismos y elementos necesarios de gestión de información criptográfica para el establecimiento de comunicaciones seguras, es lo que se llama PKI (Public Key Infrastructure) o Infraestructura de Clave Pública.

Un entorno de VPN implica, normalmente, a grandes grupos de usuarios y nodos, intercambiando información sobre canales inseguros. Desde este punto de vista, una PKI certificando los valores de clave pública usados es necesaria para proveer de dinamismo al establecimiento de canales seguros. Existen dos puntos de unión entre una PKI y una VPN. El primero es cuándo se deben emitir certificados para los usuarios, de modo que deba verificarse la identidad de cada entidad que lo solicite, siendo en este caso los administradores de red los responsables para la certificación de los sistemas. La información privada es almacenada en una tarjeta inteligente, mientras que la información pública es publicada en un directorio accesible para todos los usuarios de la organización.

La políticas de seguridad en la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incansablemente tecnologías que las protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y de las comunicaciones.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa, ya que muchos son los criminales informáticos (agrupaciones, profesionales, aficionados y accidentales) que asedian día a día las redes. De forma cotidiana estos hackers aportan novedosas técnicas de intrusión, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

Así, el manejo de adecuadas políticas de seguridad es fundamental para la integración de las organizaciones en el entorno de Internet, bajo modelos de Extranet, ya que esta se halla expuesta a una serie de vulnerabilidades externas y de las cuales debe quedar completamente protegida.

Por otra parte, una adecuada configuración del Firewall es esencial, pero también debe tener en cuenta otros aspectos, como protegerse de ataques y virus a través de los servidores de correo, evitar que sus servidores web sean manipulados malintencionadamente o que sufran un ataque de "Denegación de Servicio" (DNS).

Igualmente, los dispositivos de detección de intrusión deben estar atentos a proteger el tráfico de la red, buscando patrones de ataque. En caso de detectar un ataque, estos dispositivos generarán alarmas e informarán al Firewall para que ponga fin a la conexión de los atacantes a la red.

Para aumentar al máximo la seguridad de la red se puede dotar a los usuarios móviles de token cards o de certificados digitales evitando así el uso de passwords de acceso por terceras personas no autorizadas.

La seguridad es, a menudo, el primer objetivo perseguido por las organizaciones dado que Internet es considerada una red "demasiado pública" para realizar comunicaciones privadas.

Sin embargo, y aplicando las correspondientes medidas de protección y seguridad, Internet puede convertirse en una red altamente privada y segura. Para poder alcanzar este punto, toda red debe cumplir principalmente tres objetivos de seguridad:

Proporcionar la seguridad adecuada. Un sistema mínimo de seguridad debe, al menos, validar a los usuarios mediante passwords con el fin de proteger los recursos de accesos no autorizados. Además, la inclusión de métodos de encriptación permitirá la protección del tráfico a lo largo de su tránsito.

Además, proporcionar facilidad de administración. La elección de seguridad para la VPN debe ser sencilla de administrar, así como las funciones de administración deben ser seguras frente a posibles accesos ilegales. Así mismo, el sistema de seguridad en el acceso a la red deben ser totalmente transparente a los usuarios.

En cuanto a los pro y contra de los sistemas de seguridad para las redes son los siguientes:

Aunque el desarrollo de estos sistemas logra un alto porcentaje de seguridad este no logra un 100% debido a las intrusiones de hackers y ma-

TECNOLOGIA	PUNTOS FUERTES	PUNTOS DEBILES	EN DESARROLLO
IPSEC	• Opera independientemente de las aplicaciones de niveles superiores • Subconjunto de IPv6 • Ocultación de direcciones de red sin emplear NAT • Acoplamiento de las técnicas criptográficas existentes y futuras	• No proporciona la gestión de usuarios • Interoperabilidad entre los fabricantes • No estandarizado	• Estandarización de todas las facetas de PKI, incluyendo los protocolos de intercambio de certificados y el formato de éstos • El IETF está en su desarrollo
Cortafuegos	• Gestión centralizada de los parámetros de seguridad autenticación y acceso • Disponibilidad de herramientas común para las modificaciones de las reglas del túnel • Disponibilidad de ACLs para usuarios remotos	• Reducción del modo de operación debida a la encriptación software • Precisa un alto control con los cambios al añadir nuevas reglas VPN	• Mismos objetivos que IPSec • Soluciones capaces de realizar la encriptación por medio del hardware
PPTP	• Soporte tunneling extremo a extremo y entre servidores • Posibilidad de valor añadido para el acceso remoto • Proporciona capacidad multiprotocolo • Empleo de encriptación RSA RC4	• No proporciona encriptación de datos para los servidores en acceso remoto • Precisa un servidor NT como terminador del túnel • Sólo usa encriptación RSA RC 4	• Integración con IPSec
L2F	• Habilita el tunneling multiprotocolo • Soportado por la gran mayoría de fabricantes	• No posee encriptación • Autenticación débil • No dispone de control de flujo sobre el túnel	• Implementaciones que emplean el nombre de usuario y dominio en el establecimiento de túnel
L2TP	• Combina L2F y PPTP, necesidad de únicamente una red de paquetes para operar bajo X.25 y FRAME RELAY	• Aún no implementado	• Estandarización y operación en proceso • Será adoptado por los fabricantes para el acceso remoto una vez complete
VTCP/Secure	• Mecanismos de encriptación y autenticación fuerte • Proporciona seguridad extremo a extremo • Tunneling basado en nombre de dominio	• Protocolo propietario • Las configuraciones LAN-LAN no están permitidas • No es multiprotocolo	• Compatibilidad con IPSec

Tabla. Análisis comparativo de las tecnologías de seguridad.

nipulaciones internas y externas que pueden hacer los usuarios e intrusos en la red. Igualmente a continuación en el presente cuadro se realiza un análisis de tecnologías de seguridad y sus ventajas y desventajas.

Otros elementos importantes para mantener una red segura

Lo más importante para su aplicabilidad de una red segura es establecer correctamente las políticas de seguridad y de acceso. Una característica fundamental de este tipo de sistema de seguridad en la red privada virtual es que debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

El objetivo fundamental del diseño de arquitectura del sistema de seguridad que se ha tenido en cuenta, es conseguir un sistema que en su conjunto sea de alta disponibilidad (tolerante a fallos) y escalable (que pueda crecer en el futuro), de tal forma que la atención, servicio y transmisión de la información a los usuarios de la red privada virtual se vea garantizada y pueda incrementarse según la demanda.

Las funciones a tener encuenta que cubiertas por el sistema, se pueden sintetizar en las siguientes:

- Se recomienda situar el sistema de gestión de ancho de banda y tráfico (calidad de servicio) entre el router de conexión a Internet el mas recomendable sería mediante routers optimizados para VPN. Estos routers proporcionan, a partir del software IOS, la capacidad de enrutamiento completa a nivel 3, incluyendo protocolos de routing externo (BGP), encriptación mediante IPsec y 3DES, fuerte perímetro de seguridad gracias al Firewall y al IDS incluido en el software y definición de calidad de servicio necesarios (QoS) además de la gestión del ancho de banda. Todo esto va a permitir la creación de una red privada virtual escalable, segura y eficiente.y la primera línea de cortafuegos (segmento WAN).

- Cortafuegos. La arquitectura propuesta está compuesta por dos líneas de cortafuegos soportadas en productos de distintos fabricantes. De esta manera se consigue un mayor nivel de seguridad ya que el intruso tendría que atacar y superar las defensas de dos productos distintos y al mismo tiempo separar y segmentar los servicios de acuerdo al público objetivo al que están destinados. El sistema de cortafuegos formará una arquitectura de dos niveles proporcionando mayor estabilidad, seguridad y rendimiento al servicio.

- Nivel 1. Cortafuegos perimetrales, encargados de filtrar todas las conexiones provenientes tanto de Internet como de otros organismos. Esta solución de cortafuegos permitiría a la red en el caso que decidiera adquirir otra conexión adicional a Internet, aunque sea de otro proveedor, realizar una gestión de las líneas Internet, proporcionando mecanismos de alta disponibilidad con balanceo de carga entre líneas, sin necesidad de incorporar hardware adicional.

- Nivel 2. Cortafuegos internos, encargados de filtrar todas las conexiones provenientes de los cortafuegos perimetrales y de los usuarios de la red VPN o Intranet. Este tipo de cortafuegos deben contar con las siguientes características técnicas: dispositivos de hardware dedicado que permitan poner en marcha las políticas de seguridad de la organización y que restrinja los accesos a los recursos de la red según los permisos y el sentido del tráfico, no generar impacto en el funcionamiento de la red, algoritmo de seguridad adaptativo, NAT/PAT, realizar funciones de filtrado de paquetes y de proxy simultáneamente, configuración redundante, filtrado de URL's, IPSec para VPN, bloqueo y filtrado de ActiveX y Applets de JAVA, protección del correo mediante

chequeo de comandos SMTP, prevención de ataques de fragmentación y prevención de ataques masivos.

• Antivirus. El sistema de antivirus se conectará directamente al cluster de cortafuegos perimetrales. De este modo, todo el tráfico que pase por dichos cortafuegos, sensible de ser analizado, se reenviará al antivirus, el cual lo analizará en busca de patrones de virus conocidos. En el caso de que detecte algún virus, actuará sobre unas políticas definidas. Es recomendable que los sistemas de antivirus y diferentes consolas de administración y tratamiento de históricos estén situados en su propio segmento de red (segmento gestión), exclusivo para ellos. Siguiendo las premisas del presente diseño, estos productos se deberían instalar en configuración de alta disponibilidad.

Al mismo tiempo, se implanta un sistema antivirus residente en los puestos de trabajo, los servidores departamentales, los servidores web y los servidores de correo, los cuales se gestionan mediante una única consola, ubicada en el segmento de gestión, desde la que se realizan las actualizaciones y descargas de firmas en los referidos equipos. Este sistema antivirus tendrá una tecnología distinta del otro antivirus perimetral, para así obtener una protección mayor frente a posibles ataques.

Una solución segura ha de ser diseñada para empresas u organizaciones con redes multiplataforma, y para aquellas que necesiten administrar en forma centralizada la seguridad de su red. Puesto que es una solución que impide a los virus y a cualquier otro tipo de contenido malicioso entrar en las redes corporativas, de entidades de cualquier tamaño.

• Sondas de detección de intrusión. El sistema de detección de intrusión será el encargado de analizar el tráfico, de determinados segmentos de la red, en busca de intentos de ataque a los sistemas que conforman la plataforma Internet / Intranet. En el caso de que detecte un intento de ataque, actuará mediante unas políticas definidas. En todos y cada uno de los segmentos de red que se definan en el sistema, actuará al menos un sensor de red para detectar posibles intrusiones en el sistema. Este sistema analiza el tráfico de red en tiempo real. Además se incluyen las sondas necesarias para todos los servidores críticos del sistema. Se dispondrá de tres sondas ubicadas en los segmentos de DMZ, Intranet y BBDD.

VPN. Para el acceso de usuarios móviles (conectados a través de Internet), se establecerá un sistema de seguridad basado en VPN (en modo túnel + cifrado del canal), asegurando la privacidad de las comunicaciones extremo a extremo. Cada usuario móvil tendrá un cliente VPN y el servidor VPN será el cluster de cortafuegos internos. La autenticación de usuarios se realizará contra un servidor AAA

Gestión de Históricos. Para tener un control unificado de lo que acontece en cada uno de los clusters de cortafuegos (cortafuegos perimetrales y cortafuegos internos), se dotará a la plataforma de un servicio centralizado de históricos.

• Segmento DMZ. Se utiliza para proporcionar los servicios a los clientes y como interfase entre la red interna e Internet. En este segmento se albergarán los siguientes equipos:

- Servidor Web. Encargado del servicio web corporativo para las dependencias de una organización
- Servidores Web Otras sucursales regionales..
- Servidor DNS Secundario. Encargado de resolver los nombres de las máquinas que conforman la plataforma Internet / Intranet. Es una réplica (acceso en modo sólo lectura) del servidor DNS Primario, ubicado en el Segmento Intranet.
- Servidor Relay Correo. Encargado de rea-

lizar las siguientes funciones: Relay de correo entrante y saliente de los usuarios de la red, Relay de correo entrante y saliente de los usuarios de Otros Organismos, Servidor SMTP de los usuarios de la red y Servidor SMTP de los usuarios de Otros nodos.

• Segmento buzones. Tiene como finalidad proporcionar los servicios de correo electrónico externo. En este segmento se albergarán los siguientes equipos: Servidor POP3. Encargado de servir los mensajes de correo de los usuarios de otras dependencias y estudiantes.

• Segmento gestión. Su utilidad consiste en independizar y asegurar la gestión y administración del equipamiento de seguridad. En este segmento se albergarán los siguientes equipos: servidor AAA. Encargado de realizar la autenticación de los usuarios que se conectan a través de la VPN, Consolas de Gestión; encargadas de la administración de los dos clusters de cortafuegos, perimetrales y cortafuegos internos), de la gestión centralizada de Históricos y del gestor de ancho de banda y de los dos antivirus, el servidor y la consola del Sistema de detección de intrusiones y en este segmento se incorporará también la consola gráfica y el servidor de gestión de red y sistemas.

• Segmento LAN. Sirve para agrupar a los usuarios internos de una organización. En este segmento se albergarán los siguientes equipos: equipos usuarios red interna. PC de los usuarios que conforman la red interna.

• Segmento Intranet. Dedicado a dar servicios de Intranet a los funcionarios de la organización. En este segmento se albergarán los siguientes equipos: Servidor Web Intranet. Encargado del servicio Web Intranet de la red, Servidor IMAP. Encargado de recibir los mensajes de correo de los usuarios de la red, Servidor DNS Primario. Encargado de resolver los nombres de las máquinas que conforman la plataforma Internet / Intranet de la red. Es el Master (acceso en modo lectura / escritura). Tiene una réplica en el Segmento DMZ (DNS secundario).

• Segmento BBDD. Utilizado para asegurar y aislar el repositorio general de datos. En este segmento se albergarán los siguientes equipos: Servidor BBDD, encargado de almacenar los datos de las distintas aplicaciones que posee la red.

• Otras consideraciones. El proceso de apertura y servicio a los clientes mediante procedimientos informáticos conlleva que en el futuro se tengan que utilizar transacciones SSL para garantizar la seguridad de determinados procesos. Puesto que este sistema criptográfico de clave pública es lento, ya que requiere mayores recursos de procesado, se hace necesario incorporar tarjetas aceleradoras a los servidores que proporcionen estos servicios. Se realizarán, de acuerdo a un calendario prefijado, análisis para verificar las posibles vulnerabilidades del sistema y así tenerlo actualizado.

Todos los equipamientos enunciados se gestionan y administran mediante consolas y servidores ubicados en el segmento de gestión. Con respecto a las consolas de gestión y supervisión es necesario realizar las siguientes consideraciones: No es recomendable la integración de las consolas de los productos de cortafuegos en una única, debido principalmente a razones de seguridad, por lo que recomendamos que se use la propia consola de cada producto.

No obstante, será necesario integrar en la fase de implantación un sistema centralizado de gestión de red y sistemas con el sistema de gestión de los equipos y productos de seguridad. De esta manera se controla y verifica la disponibilidad de los servicios 24X7.

Hay que tener muy presente que toda esta tecnología no tendrá validez si no se realiza al mismo

tiempo un programa de concienciación e información de usuarios y administradores. En los usuarios externos, conviene utilizar un sistema de autenticación fuerte basado en tokens de usuario con introducción de una contraseña diferente cada vez que se conecte.

- Descripción de la arquitectura (ver figura 2). Este diseño propuesto está destinada a dar soporte a los servicios de una red preste en Internet a sus clientes. Esta arquitectura esta soportada por grandes bloques la plataforma de seguridad y los distintos segmentos que conforman la red. A continuación, se describen los segmentos usados.
- Segmentos. Para dotar a la plataforma de un mayor rendimiento y seguridad se ha dividido la red en segmentos, según el tipo de servicios y el tráfico generado. En los siguientes apartados se da una breve descripción de los segmentos que albergan.
- Segmento WAN. Dedicado a la conexión Lan con la red externa. En este segmento se albergarán los siguientes equipos: ver figura 2.

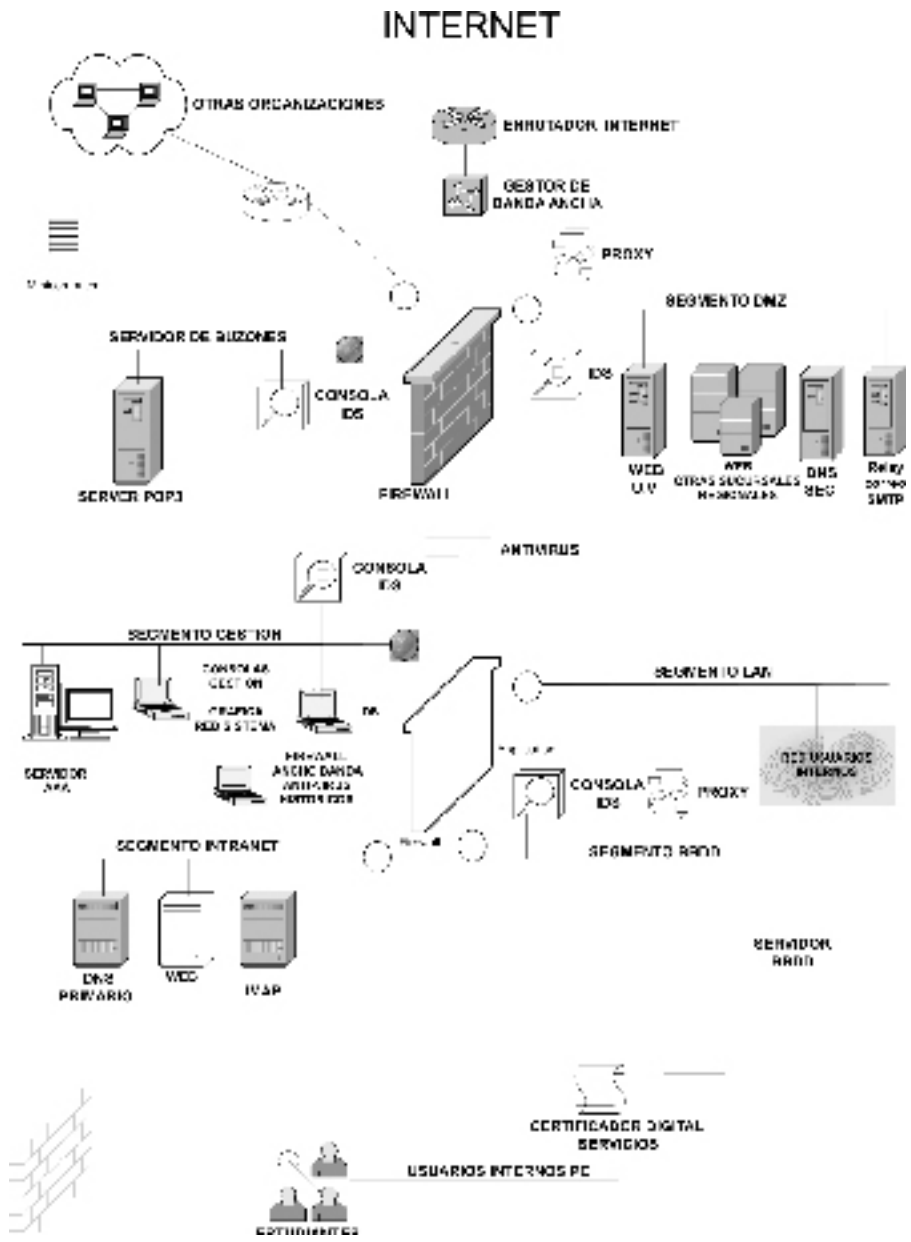

Figura 2. Diseño conceptual de la red segura. Fuente. Autor.

Es importante destacar que este proyecto de infraestructura sirve como marco para asegurar la confidencialidad, integridad y disponibilidad de las operaciones y además para que todas las personas y organismos vinculados a la red puedan utilizarlos a la hora de proporcionar a estos los servicios que ellos requieren.

Se trata de elaborar una referencia válida, homogénea para todos y, al mismo tiempo, adaptable a las distintas exigencias de seguridad que se presenten de acuerdo con las demandas externas.

Conclusión

Con el desarrollo del artículo se realizó un análisis orientado a determinar los aspectos más relevantes relacionados con la implementación de un diseño de sistema de seguridad para la red el cual sirva

como herramienta de apoyo en la obtención de una comunicación segura.

Así mismo, con la propuesta de los elementos tecnológicos a tener en cuenta se espera brindar soluciones de manejo de la información en red; por otra parte es importante destacar que un buen diseño de un sistema de seguridad representa una gran solución para un red en cuanto a protección de datos, confidencialidad e integridad de estos.

Referencias bibliográficas

Atkinson R., 2002. RFC 2401, Security Architecture for the Internet Protocol,.

Bustos, Edgar A. Tesis Maestría , propuesta de un modelo de seguridad para la plataforma de la universidad virtual basado en la Utilización de VPN.

Fernández Gómez, Eva I. 2002. Learning: implantación de proyectos de información On-Line. Ra-Ma, Librería y Editorial Microinformática

García, Carlos. 2000. E-learning tele formación: diseño, desarrollo y evaluación de la formación a través de Internet Ediciones Gestión , S.A.

http://www.cisco.com/warp/public/44/solutions/network/vpn.shttp://www.sceu.frba.utn.edu.ar/e-learning/bibliotec@/definiciones.htm

Kent S., Atkinson R., RFC 2402, IP Authentication Header, 2003.

Muñoz, Manel Ramon. 2002. Introducción al e-learning UOC Universitat Oberta de Catalunya.

Navarro Buitrago, Félix; Zayas Manero, Ramón; Meléndez Gil, Francisco. 2004. E-learning : visión y tendencias Génesis XXI.