DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL PARA REDES (JULIO 2009)

Nelson Andres Arbelaez Jiménez

Resumen – Proyecto Diseño e Implementación de Seguridad Perimetral para Redes, nace por las necesidades que hoy en día se presentan en las redes de las organizaciones y en los canales WAN. Esta necesidad de proteger las comunicaciones a nivel WAN para evitar el robo de la información, permitiendo la confiabilidad e integridad de los datos por medio del cifrado del canal WAN.

A nivel interno de las organizaciones es necesario controlar el uso inapropiado de Internet y controlar los diferentes usuarios para la navegación Web, brindando protección integral para las compañías, contra contenidos inapropiados, maliciosos, ofensivos y filtración de datos.

I. INTRODUCCIÓN

Hoy en día el desarrollo tecnológico y de las telecomunicaciones da pasos agigantados que en el pasado era imposible pensar lo que hoy en día se tiene en la infraestructura de las redes. Si bien las redes han evolucionado de una manera espectacular, también es cierto que a la par de este desarrollo han crecido en complejidad virus, gusanos, malware, spyware y spam. Dada la importancia y sensibilidad de la información que se debe transmitir se requiere de sistemas que brinden seguridad informática.

La navegación de usuarios en la Web a sitios maliciosos o de dudosa reputación hace que estos problemas sean aun mayores, y difíciles de detectar. Estos problemas mencionados anteriormente causan robo de información como claves, información personal o suplantación de identidad permitiendo acceso a las aplicaciones o información sensible de personas, alterar el funcionamiento de equipos o computadoras o daño total de estos. Pérdida de información o borrado de discos duros o partición de los mismos y cambio de datos.

Los ataques de día cero son imposibles de detectar aun peor las firmas de anti-virus no son capaces de detener este tipo de ataques, por esta razón es conveniente estar conectados a un sistema a base de Reputación esto quiere decir que son sistemas que a nivel mundial que tienen varios censores y equipos que recolectan información del comportamiento, longevidad, y la persistencia de los sitios, esta reputación es por IP, Dominio y URL, y de acuerdo a su clasificación se puede decir que son:

- Sitios Confiables
- Sitios Neutros
- Sitios sin Verificar
- Sitios Sospechosos
- Sitios Maliciosos

II. OBJETIVOS

Diseñar e implementar un sistema para la seguridad de transmisión de datos en redes Wan, que permita controlar la navegación de usuarios a sitios Web y el control de contenido sitios Web por medio de Proxy.

A. Objetivos Específicos

- Implementar Proxy para el control de usuarios y filtro de navegación Web.
- Crear reglas de navegación para los diferentes perfiles de usuarios.
- Escoger los equipos adecuados para el montaje e implementación de cifrado para la transmisión de datos.
- Definir el procedimiento más adecuado para implementar el cifrado.
- Definir tipo de cifrado a implementar.

- Realizar pruebas de verificación del funcionamiento del sistema.

III. CONTENIDO

A. *Marco Teórico*

1) Encripción

La encripción es la transformación de datos en una forma imposible o casi imposible de leer, su propósito es asegurar aislamiento manteniendo la información ocultada de cualquier persona que no tiene los permisos para ver o leer la información, incluso los que tengan acceso a los datos cifrados. El desciframiento es el revés de la encripción; es la transformación de datos cifrados nuevamente dentro de una forma perceptible.

La encripción y el desciframiento requieren generalmente el uso de una cierta información secreta, designado una llave. Para algunos mecanismos de la encripción, la misma llave se utiliza para la encripción y el desciframiento; para otros mecanismos, las llaves usadas para la encripción y el desciframiento son diferentes.

La criptografía de hoy es más que la encripción y el desciframiento. La autentificación es parte de nuestras vidas, Utilizamos la autentificación a través de nuestras vidas cotidianamente cuando firmamos nuestro nombre en un documento por ejemplo, la criptografía proporciona los mecanismos para tales procedimientos, la firma digital es un bloque de caracteres que acompaña a un documento garantizando quién es su autor y que no ha existido ninguna manipulación posterior de los datos esto es integridad. Para firmar un documento digital, su autor utiliza su propia clave secreta, a la que él sólo tiene acceso, lo que impide que pueda después negar su autoría esto es no revocación, de esta forma, el autor queda vinculado al documento de la firma. Por último la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

Hay dos tipos de sistemas criptográficos: Llave secreta y Llave pública

- Llave Pública

En criptografía tradicional, el remitente y el receptor de un mensaje saben y utilizan la misma llave secreta; el remitente utiliza la llave secreta para cifrar el mensaje, y el receptor utiliza la misma llave secreta para descifrar el mensaje. Este método se conoce como llave secreta o criptografía simétrica. Si están en instalaciones físicas separadas, deben confiar en el mensajero, un sistema de teléfono, o un cierto otro medio de la transmisión para prevenir el acceso de la llave secreta. Cualquier persona que oye por casualidad o las intercepciones la llave en tránsito puede leer más adelante, modificar, y forjar todos los mensajes cifrados o autenticados usando esa llave. La generación, la transmisión y el almacenaje de llaves se llama: La gerencia dominante, todos los sistemas criptográficos deben ocuparse de las ediciones de gerencia dominante. Porque todas las llaves en un sistema criptográfico mientras la llave privada debe seguir siendo secreta, la criptografía de llave secreta tiene a menudo una dificultad en el proveer de la gerencia dominante segura, especialmente en sistemas abiertos de gran cantidad de usuarios.

- Llave Secreta

La criptografía llave secreta se refiere a veces como criptografía simétrica. Es la forma más tradicional de criptografía, en la cual una sola llave se puede utilizar para cifrar y para descifrar un mensaje, la criptografía de llave secreta no sólo se ocupa de la encripción, también se ocupa de la autentificación, esta técnica se llama *códigos de la autentificación de mensaje*.

El mayor problema con sistemas criptográficos de llave secreta es que el remitente y el receptor estén de acuerdo con la llave secreta, solo el remitente y el receptor deben conocer la llave o en ambos lugares remotos debe ser configurada la misma llave en el caso de palabra compartida o secreta generalmente la llave secreta es más rápida que criptografía de llave pública.

Al utilizar una función Hash como huella y combinarla con tecnología de llave publica, da como resultado las firmas digitales. La función Hash es una transformación que toma una entrada m o toma un mensaje de longitud variable como entrada y la salida es un mensaje de longitud fija. Este mensaje de longitud fija se llama el valor de Hash. Para que un algoritmo sea considerado criptográficamente seguro debe cumplir las siguientes propiedades:

- Debe ser consistente, es decir, la misma entrada siempre debe crear la misma salida.
- De ser unidireccional, es decir, si se tiene la salida, debe ser considerablemente difícil, más no imposible, comprobar la entrada del mensaje.
- Debe ser aleatoria, o al menos dar la apariencia de aleatoriedad para prevenir que pueda adivinarse el mensaje original.
- Debe ser único, es decir, debe ser imposible encontrar dos mensajes que originen el mismo resumen.

Las funciones Hash unidireccionales son las más utilizadas para proveer una huella digital de un mensaje o archivo, al igual que una huella digital de una persona, una huella Hash es única y provee integridad y autenticidad del mensaje.

Las funciones Hash tienen una variedad de aplicaciones de cómputo generales, pero cuando están empleadas en criptografía, las funciones hash que se eligen generalmente tienen algunas características adicionales.

El problema con las funciones Hash de huella digital es que puede ser forzado y es sujeto a un ataque de **man in the middle**, esto quiere decir ataque de hombre en la mitad, el hombre escucha en un canal que se presume que es seguro y este se hace pasar por el emisor o receptor.

2) Protocolos de Tunneling

Los principales protocolos para hacer tunneling son:

- IPsec

Desarrollado por IETF Internet Enginnering Task Enforcement, IPsec trabaja sobre la capa de red del modelo OSI por lo que puede ser implementado independientemente de las aplicaciones que corran en la red esto garantiza la implementación de una red segura sin importar el tipo de aplicaciones.

- PPTP

Desarrollado por 3COM, Microsoft y Ascend Communications, se propuso como una alternativa a IPsec, trabaja en la capa de enlace capa 2 del modelo OSI este protocolo de tunneling se utiliza para transmisiones seguras de tráfico basado en Windows.

- L2TP

Desarrollado por Cisco, este protocolo se creo con el fin de reemplazar a IPsec, L2TP es una combinación de reenvío de capa 2 de enlace y PPTP y es utilizado para encapsular tramas de tipo punto a punto a través de redes X.25, Frame Relay y ATM.

B. Descripción del Problema

Las comunicaciones en la actualidad es un factor importante de nuestra sociedad, los canales por donde viaja la información no son seguros y es necesario proteger los datos que son enviados a sitios remotos, se debe evitar el robo de la información que es enviada por los canales WAN y la modificación de los datos enviados, a nivel de navegación de usuarios es necesario implementar políticas de navegación para proteger la red interna de ataques destinados a robo de identidad y datos privados como contraseñas o datos guardados en discos duros de los equipos que componen la red de la organización.

C. Estrategia Global de la Solución

Para el desarrollo del proyecto de Diseño e Implementación de Seguridad Perimetral para Redes, se tienen dos fases: La fase uno tiene que ver el cifrado de canal a nivel Wan, esta fase se implementa y diseña de acuerdo al direccionamiento IP y las aplicaciones que van a pasar por el túnel.

Para la implementación del cifrado de Oficina Central y Oficina Remota o Remotas es importante contar con toda la información de la topología de red, direccionamiento Ip de la red tanto de Oficina Central y Remotas para la configuración de los equipos encargados de dar la seguridad a la red y el cifrado de la misma, se debe determinar y diseñar el tipo de Algoritmo de Cifrado que se va a utilizar esto depende de la velocidad del Canal, para esta fase se utilizan los Equipos Marca Secure Computing Snapgear SG 720 para el sitio central, este equipo va ser el concentrador de las VPN IPsec.

El equipo es un Firewall / VPN IPsec UTM esto quiere decir que tiene la característica de administración unificada de amenazas, cuenta con diferentes módulos para la protección de la red y sus componentes tales como PCs, Servidores, equipos con aplicaciones o servicios sensitivos que necesitan un grado alto de seguridad.

La fase II del proyecto de Diseño e Implementación de Seguridad Perimetral para Redes se realiza para el control de contenido y navegación de usuarios, la implementación y desarrollo de la fase II se realiza con un equipo Marca Secure Computing Webwasher es un equipo que nos permite controlar el uso inapropiado de Internet y control de usuarios para la navegación Web, brindando protección contra contenidos inapropiados, maliciosos, ofensivos y filtración de datos, protección bidireccional contra las Amenazas de seguridad en la Web.

Protección basada en reputación, permitiendo garantizar la aplicación de políticas, el cumplimiento de reglamentaciones y un entorno de aplicación productivo.

D. Resultados Obtenidos

Las pruebas realizadas se hacen teniendo en cuenta el estado del túnel. Si este estaba habilitado y no habilitado.

En las pruebas correspondientes se tomaron los tiempos de respuesta de Host a Host y su comportamiento, se observo en las pruebas que el comportamiento de los equipos de cifrado y la respuesta de ping siempre están estables y con tiempos de respuesta óptimos.

Prueba cifrado con transmisión de datos

Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251

La respuesta desde 172.26.17.3 es la transmisión de datos, la respuesta es constante y estable y no presenta ningún inconveniente.

Prueba cifrado sin transmisión de datos

Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249

Pruebas Seguridad Web, pruebas de navegación con los diferentes usuarios identificados en el repositorio de autenticación, y se accede a distintos sitios Web, para la verificación de bloqueo de sitios no deseados y políticas creadas, esto permite constatar que la configuración y el diseño es el adecuado para el desarrollo y la implementación del proyecto.

E. *Conclusiones*

- Antes de cualquier implementación o desarrollo de cualquier proyecto que se realice se debe tener el total conocimiento de la infraestructura de red, así como las rutas o ruteos que tienen configurados los router, las aplicaciones o servicios que deben ser cifrados y si es necesario aplicación de Rip en los encriptores.

- Se debe tener claro cual va se el punto inicial donde inicia el túnel Ipsec y el punto remoto este va ser el terminador del túnel Ipsec, crear las rutas estáticas en los routers para tener conectividad entre los diferentes dispositivos, si no se tiene conectividad a los dispositivos no es posible levantar el túnel.

- El consumo del ancho de banda del canal depende si sobre el canal tienen políticas de (QoS) Calidad de Servicio que restrinjan o limiten el tráfico cursante de la transmisión en este caso por ejemplo puede ser FTP o por el contrario den prioridad al tráfico que se genere por FTP.

- Configuración de reglas de firewall deben ser lo más detalladas y precisas para evitar inconvenientes con la transmisión de datos, cuales son los puertos o protocolos más utilizados para la transmisión.

- Antes de poner en producción los equipos destinados para el cifrado de datos se debe hacer un piloto para realizar las diferentes pruebas de conectividad, configuración del túnel Ipsec, transmisión de datos y respuesta de la solución.

- Para la creación de políticas de navegación es necesario saber cuantos son los grupos que tiene el repositorio de autenticación para crear los diferentes perfiles para los usuarios y sus respectivas políticas, cuales son los servidores que deben actualizarse para hacer la configuración por IP de esta forma no necesitan autenticación en el momento de actualizarse.

- Cuando se hace la exclusión de URL en la política correspondiente, permitir o denegar las paginas Web siempre se debe cargar esta en la memoria dado el procedimiento que es adicionar la url, escoger la categoría a la cual corresponde o se va a realizar la personalización y después cargar en memoria sin no se hace este ultimo paso no se harán las exclusiones de URL que se necesitan.

F. Trabajo Futuro

Para el mejoramiento de la Solución de cifrado de datos a nivel WAN, se puede implementar túneles con VPN SSL. O utilizar un equipo concentrador de VPN SSL para los accesos remotos desde Windows Mobile o cafés Internet aplicando políticas de seguridad como escritorio virtuales para evitar el robo de la información.

REFERENCIAS

Referencias de Internet

[SECU2008]www.securecomputing.com(Navegada el 20 de Junio de 2008).

[TRUS2008]http://www.securecomputing.com/index.cfm?skey=1620&lang=en(Navegada el 28 de Junio de 2008).

[CRSA2008]http://es.wikipedia.org/wiki/Claves_RSA(Navegada el 23 de junio de 2008).

[FIRE2008]http://www.desarrolloweb.com/articulos/513.php(Navegada el 23 de junio de 2008).

[VPNI2008]http://www.freebsd.org/doc/es_ES.ISO8859-1/books/handbook/ipsec.html(Navegada el 30 de junio de 2008).

[SNAP2008]http://www.securecomputing.com/techpubsRC.cfm?pid=69(Navegada el 23 de junio de 2008).

[CRIP2008]http://es.wikipedia.org/wiki/Criptograf%C3%ADa#Historia_de_la_criptograf.C3.Ada(Navegada el 20 de junio de 2008).

[UNIN2009]http://www.uninet.edu/mg/másterges/cinet/Seguridad/Texto/seguridadYPrivacidad/node7.html(Navegada el 15 de Marzo de 2009).

[EISC2009]http://eisc.univalle.edu.co/materias/Administracion_De_Redes_Y_Servidores/material/02_ARS_OSI.pdf(Navegada el 20 de Abril de 2009).

[TCPI2009]http://www.tcpipguide.com/free/t_IPSecOverviewHistoryandStandards(Navegada el 20 de febrero de 2009).