DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL PARA REDES

NELSON ANDRES ARBELAEZ JIMÉNEZ

FUNDACIÓN UNIVERSITARIA SAN MARTÍN
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE ELECTRÓNICA Y TELECOMUNICACIONES
BOGOTÁ, COLOMBIA
2009, MAYO

DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL PARA REDES

NELSON ANDRES ARBELAEZ JIMENEZ
001024
nelsonarbelaez@hotmail.com

MONOGRAFÍA DE GRADO

ASESOR TÉCNICO
RAFAEL CUBILLOS
FUSM1

FUNDACIÓN UNIVERSITARIA SAN MARTÍN
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE ELECTRÓNICA Y TELECOMUNICACIONES
BOGOTÁ, COLOMBIA
2009, MAYO

Nota de Aceptación:

_____

Ing. Rafael Cubillos
Asesor

_____

Ing. Freud Romero
Jurado

_____

Ing. Diego Díaz
Jurado

Bogotá, Mayo, 2009.

Dedico este trabajo a quienes directa e indirectamente han contribuido al desarrollo del proyecto

AGRADECIMIENTOS

Mis más sinceros agradecimientos a mis padres por el apoyo que me han brindando todos estos años, no he podido tener unos mejores amigos en mi vida, agradezco a las personas que indirectamente y directamente contribuyeron al desarrollo de este proyecto y han creído en mí.

CONTENIDO

Pág.

LISTA DE FIGURAS

1. 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 las 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.

2. **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

3. OBJETIVOS

3.1 OBJETIVO GENERAL

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.

3.2 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.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

4.1.1 Historia de la Criptografía

La palabra criptología proviene de las palabras griegas Kryto y logos y significa estudio de lo oculto, la criptografía es tan antigua como la escritura siempre que ha habido comunicación entre dos personas, o grupos de personas, ha habido un tercero que podía estar interesado en interceptar y leer esa información sin permiso de los otros. Además, siempre que alguien esconde algo, hay personas interesadas en descubrirlo, así que ligado a la ciencia de esconder (la criptografía), se encuentra casi siempre la de descifrar (el criptoanálisis). [CRIP2008]

El primer cifrado que puede considerarse como tal (por tener evidencias no sólo del cifrado, sino también una metodología e instrucciones para llevarlo a cabo) se debe a Julio César: su método consistía en sustituir cada letra de un mensaje por su tercera siguiente en el alfabeto. Parece ser que también los griegos y egipcios utilizaban sistemas similares. Civilizaciones anteriores, como la Mesopotamia, India y China también utilizaban sus propios métodos.

Durante la I Guerra Mundial se utilizaron extensivamente las técnicas criptográficas, lo que impulsó al final de la guerra, el desarrollo de las primeras tecnologías electromecánicas. Un ejemplo de estos desarrollos es la máquina Enigma, utilizada por los alemanes para cifrar y descifrar sus mensajes. [UNIN2009].

Después de la primera Guerra mundial y sus avances en la criptografía se desarrolla la maquina Enigma para el envío de los mensajes entre las tropas alemanas de forma segura.

4.1.2 Maquina Enigma

La máquina Enigma tuvo sus comienzos en 1923 como un producto comercial producido por un alemán llamado Arthur Scherbius destinadas a empresas con necesidad de una comunicación segura. La maquina Enigma atrajo el interés de los militares alemanes y como resultado esta fue retirada del mercado y posteriormente se realizo su producción en masa con sus ajustes de uso militar. Por el estallido de la Segunda Guerra Mundial, el enigma estaba en uso generalizado en la mayoría de las ramas de las fuerzas militares alemanas gracias a su pequeño tamaño, portabilidad y facilidad de uso. La maquina Enigma es una herramienta ideal para su uso como parte confiabilidad integridad y compartir la

información de forma segura, entonces la maquina enigma fue la primera maquina utilizada para el cifrado de los mensajes. [HOME2009].

Entre 1939 y 1945, las formas más avanzadas y más creativas de conocimiento matemático y tecnológico fueron combinadas para dominar comunicaciones alemanas, cabe destacar el desarrollo de la maquina Enigma utilizada para el cifrado de los mensajes en la Segunda Guerra Mundial. [CODE2009].

Después de la Segunda Guerra Mundial, empieza la expansión de las comunicaciones y despierta el interés por el envío de mensajes de forma segura, con el desarrollo de Internet es aun más evidente esta tendencia y la necesidad de brindar seguridad a la información que viaja por ella comienza en desarrollo del uso de las VPNs.

~~4.1.2~~4.1.3 HISTORIA IPSEC

El problema de seguridad se presentó porque hace 25 años, el Internet era de uso exclusivo y su uso era relativamente “privado”. En la actualidad el Internet a crecido como nunca se había pensado y es una necesidad y de uso público. Mientras que el Internet ha crecido, la necesidad de la seguridad ha crecido con ella. Cuando fue desarrollado TCP/IP y los precursores tempranos del Internet fueron desarrollados como redes muy pequeñas usadas por los investigadores del gobierno en el Defense Advanced Research Projects Agency de Estados Unidos (DARPA o ARPA). Todo el hardware fue controlado por la gente que tenia el conocimiento y habría tenido el conocimiento y el discernimiento de la necesidad de seguridad. En ese entonces era más seguro tener todo los componentes de la red bajo llave, y personal de seguridad para asegurar el perímetro en vez de tener encripción de lujo. Después de todo, la manera más fácil de guardar y proteger los datos de alguien que desee espiar o de tratar de robar información sobre la red, era más fácil negarles el acceso a la red.

El problema más conocido con el Internet Protocol original (IPv4) es el colapso debido a su espacio de dirección. Esta situación se presentó debido a la extensión rápida del Internet más allá de expectativas cuando IPv4 fue desarrollado. Esta misma situación es hoy en día un problema de acuerdo a lo que era cuando fue creada y no se pensó la expansión que se tiene actualmente, y cómo ahora está ha llevado a otro problema grave con el IP, la insuficiencia de los medios definitivos de asegurar seguridad en red internas del IP.

Este método funcionó muy bien al principio cuando había solamente algunas máquinas o docena de estas en el Internet e incluso cuando Internet primero comenzó a crecer, fue utilizada por mucho tiempo por los investigadores y profesionales y personal de corporaciones que contaban con los medios para tener un centro de cómputo. Los nuevos sitios fueron agregados a la red lentamente al principio, y por lo menos alguien sabía la identidad de cada nuevo sitio agregado a la red interna pero cada vez con mayor frecuencia. Sin embargo, a medida que el Internet continuó aumentando de tamaño y fue abierto eventual

en el público, la seguridad que mantenía de la red en conjunto llegó a ser imposible. En la actualidad cuando es enviado un paquete o los datos por la red no se puede asegurar que los datos enviados y o los que recibe han sido vulnerados por un atacante. [TCPI2009]

Un número de métodos se han desarrollado durante los años para tratar la necesidad de la seguridad. La mayor parte de éstos se centran en las capas más altas del protocolo OSI, para suplir la carencia del IP y de seguridad. Estas soluciones tienen valores para ciertas situaciones, pero no pueden ser generalizadas fácilmente porque son particulares y destinadas a usos específicos. Por ejemplo, podemos utilizar SSL para ciertos usos como el acceso del World Wide Web (www) o para el uso del protocolo FTP, pero hay docenas de usos con los cuales este tipo de seguridad nunca fue pensado para trabajar.

Cuando la decisión fue tomada para desarrollar una nueva versión de IP (IPv6), ésta era la excelente oportunidad de resolver no apenas los problemas de dirección en el IPv4 más viejo, pero la carencia de la seguridad también. La nueva tecnología de seguridad fue desarrollada con IPv6 en mente, pero puesto que IPv6 ha tardado años para convertirse y desarrollarse para IPv4 e IPv6.[TCPI2009]

Con la necesidad de asegurar la información y los mensajes se crea las firmas digitales asegurando la integridad de los mensajes.

~~4.1.3~~4.1.4 Historia de la Firma Digital

El concepto de firma digital, fue introducido por Diffie y Hellman en 1976 y básicamente es un conjunto de datos asociados a un mensaje que permiten asegurar la identidad del firmante y la integridad del mensaje.

El nacimiento de la firma electrónica se debe sin duda a la necesidad de una respuesta técnica segura para poder realizar la conformidad o el acuerdo de voluntades en una transacción electrónica (comercio electrónico).

En consecuencia, la firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta, a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (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.

La base técnica de la firma digital es el método de cifrado asimétrico o de clave pública. “El cifrado simétrico es la técnica más antigua y más conocida. Una clave secreta, que puede ser un número, una palabra o sólo una cadena de letras aleatorias, se aplica el texto de un mensaje para modificar el contenido de una forma en particular. Esto puede ser tan sencillo como el desplazamiento de cada

letra por un número de posiciones del alfabeto. Siempre que remitente y destinatario sepa la clave secreta, puede cifrar y descifrar todos los mensajes que utilizan esta clave."[SUPP2009].

La criptografía es una rama de las matemáticas que al aplicarse a mensajes digitales proporciona las herramientas idóneas para solucionar los problemas antes mencionados. Se trata del arte o ciencia de cifrar y descifrar información. Al problema de la confidencialidad se le relaciona comúnmente con técnicas denominadas de cifrado y a los problemas de la integridad y la autenticidad con técnicas denominadas de firma digital, aunque ambos en realidad se reducen a procedimientos criptográficos de cifrado y descifrado.

4.2 MARCO TEÓRICO

4.2.1 Sistema de Gestión de Seguridad de la Información (Information Security Management System)

El Sistema de Gestión de Seguridad de la Información se construye sobre la norma ISO 27001, para el caso de Colombia se debe cumplir con la norma ISO 27001 anteriormente conocida como la norma ISO 17779 esta norma contenía trece puntos y la aprobada hoy en día es la ISO 27001. En la actualidad cuando se realiza un sistema de gestión de seguridad de la información las empresas obtienen una calificación de del 30% al 40% de aprobación esto se debe a que la ISO 27001 no es desarrollada para empresas colombianas, la norma fue realizada para el ámbito internacional, la gestión de la seguridad de la información debe realizarse mediante un proceso documentado y conocido por toda la organización. Las empresas Colombianas fallan porque no hay una conciencia sobre la seguridad de la información, muchos de los administradores de red creen que cuentan con los equipos y dispositivos necesario para proteger su red, en algunos casos piensan que nunca les va a ocurrir un ataque o que van a ser infectados y esto propagado a toda su red.

Otras de las falencias es el uso inapropiado de Internet y la ignorancia de los usuarios en temas relativos de seguridad, como no abrir archivos desconocidos, el envío de cadenas por correo electrónico y este correo tener código malicioso embebido, abrir link y estos redireccionar a los usuarios a conexiones no seguras dado el caso pueden generar perdida de información y robo de datos. [ISOO2009]

Otra falla común es el no uso de Firewall para las conexiones a aplicaciones como página Web de la empresa, y conexión interna de aplicativos de la red.

Como Principios de la Seguridad de la Información se tienen:

- Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para la realización del proyecto es importante tener en cuenta varios conceptos tecnológicos y de redes para la claridad del tema propuesto, con el fin de una comunicación segura y la integridad de los datos y la confiabilidad se debe implementar la encripción asegurando la disponibilidad de los mismos de una forma segura y confidencial solamente la persona a la que va destinada la información la puede ver o modificar, para cumplir con la autenticidad del documento es importante tener claro lo que es una firma digital.

4.2.2 Firma Digital

El concepto de firma digital, fue introducido por Diffie y Hellman en 1976 y básicamente es un conjunto de datos asociados a un mensaje que permiten asegurar la identidad del firmante y la integridad del mensaje, una firma digital es básicamente una forma de garantizar que un documento electrónico (correo electrónico, Documento, Archivos Privados, etc) es auténtico. Auténtico significa que usted acreditando quién es su autor y que no ha existido ninguna manipulación posterior de los datos (integridad).

Las firmas digitales se basan en ciertos tipos de cifrado para garantizar la autenticación. El cifrado es el proceso de tomar todos los datos que está enviando un equipo a otro y de codificación en una forma que sólo el otro equipo será capaz de descifrar. Autenticación es el proceso de verificar que la información proviene de una fuente de confianza. Se tiene entonces el proceso de encriptar el mensaje porque solo el autor conoce la clave secreta que ha desarrollado o implementa para que los documentos o datos no sean vulnerados. [COMP2009]

Hay dos tipos de sistemas criptográficos que forman parte de la encripción a continuación se describen estos.

4.2.3 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. [RSAR2009].

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. [RSAR2009]

- 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. [RSAR2009]

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. [ITLN2009]

Las principales funciones de Hash que se utilizan son:

- Secure Hash Algorithm (SHA)

4.2.4 Algoritmo SHA

SHA fue desarrollado por la nacional Institute o Standards and Technology el Uso de SHA-1 [FIPS-180-1] combinado con HMAC [RFC-2104] como mecanismo de autentificación de claves dentro del contexto de ESP y AH. El propósito SHA es asegurar que el paquete es auténtico y que no puede ser modificado en tránsito.

Las dos (2) funciones de Hash más utilizadas son SHA y MD5. MD5 procesa su entrada en bloques de 512 bits y origina un mensaje de 160 bits. SHA consume más recursos para el procesamiento y suele ser más lento que MD5. [ITLN2009]

Para el establecimiento del túnel se implementan Algoritmos de Llave simétrica, entre los algoritmos existentes y que se utilizan para el proyecto son los siguientes:

4.2.5 Algoritmo 3DES

3DES Triple Estandar de Encripción de Datos, triplica la seguridad de DES, mediante el uso del algoritmo DES tres veces con tres diferentes llaves, al aplicar el algoritmo de esta forma y característica nos da como resultado un algoritmo de cifrado fuerte, este algoritmo por lo general lo utilizan las entidades financieras y gobierno. [CSRC2009]

- Ataques contra los Algoritmos Simétricos

Si utilizamos la criptografía para proteger información, hay entidades externas que buscan descifrar la información y robarla para ser útil, un sistema criptográfico debe ser resistente a este tipo de ataques.

Los ataques contra la información cifrada se clasifican en tres categorías:

- Ataques de búsqueda de llaves (Fuerza Bruta)

El ataque de fuerza bruta es casi tan sencillo, pero para utilizar este tipo de ataque se debe armar de paciencia y tener todo el tiempo disponible para romper una llave, el atacante simplemente utiliza conjeturas de usuario y contraseña y utiliza varias combinaciones hasta que encuentra una que funcione. Posiblemente el atacante no tenga éxito pero las probabilidades son buenas si el sitio no esta configurado apropiadamente. [CONT2009]

- Ataques Basados en el sistema

De acuerdo al sistema operativo o sobre que esta corriendo una aplicación conociendo las vulnerabilidades de este, son aprovechadas estas vulnerabilidades por una entidad externa explotando esas vulnerabilidades dependiendo el tipo de aplicación puede llegar al robo de la información.

- Criptoanálisis

Es el arte de crear y analizar las llaves de encripción, con el análisis se llega a romper la llave demostrando su vulnerabilidad.
De hecho, hoy en día se suele invitar a la comunidad científica a que trate de romper las nuevas claves criptográficas, antes de considerar que un sistema es lo suficientemente seguro para su uso.

4.2.6 Algoritmo AES

El algoritmo AES es el estándar avanzado de la encripción, fue publicado pues el FIPS por estándar del NIST, este algoritmo es el sucesor del algoritmo DES. En enero de 1997 la iniciativa de AES fue anunciada y en septiembre de 1997 se instigó al público que planteara cifras de bloque convenientes como candidatos al AES. El algoritmo AES fue seleccionado en octubre de 2001 y el estándar fue publicado en noviembre de 2002.

AES cuenta con tamaños absolutos de 128 bits, 192 bits y 256 bits en contraste con las llaves de 56 bits dadas por el algoritmo DES. [RSAE2009].

AES consiste de dos partes, en describir el proceso de “Cifrado”, y el proceso de “Generación de las subclaves” . El bloque de cifrado tiene una longitud de 128 bits, la longitud de la clave K varia de 128, 192 y 256 bits, en cada caso AES tiene 10,12, y 14 rondas respectivamente.

“El proceso consiste en una serie de cuatro transformaciones matemáticas, las cuales se repiten 10, 12 o 14 veces, dependiendo de la longitud del bloque y de la longitud de la clave. Todos los ciclos, excepto el último son similares y consisten de las siguientes transformaciones:

- Transformación ByteSub (Sustitución de bytes).
- Transformación ShiftRow (Desplazamiento de filas).
- Transformación MixColumns (Multiplicación de columnas).
- Transformación AddRoundKey (Se aplica una or-exclusiva entre los bits del texto y la llave).

En el último ciclo sólo se ejecutan las siguientes transformaciones:

- Transformación ByteSub.
- Transformación ShiftRow.
- Transformación AddRoundKey.

La primer transformación que se ejecuta es la AddRoundKey o suma EXOR entre el texto plano (sin encriptar) y la llave.

El diagrama de flujo representa la secuencia de transformaciones mencionadas." [FIMD2009]

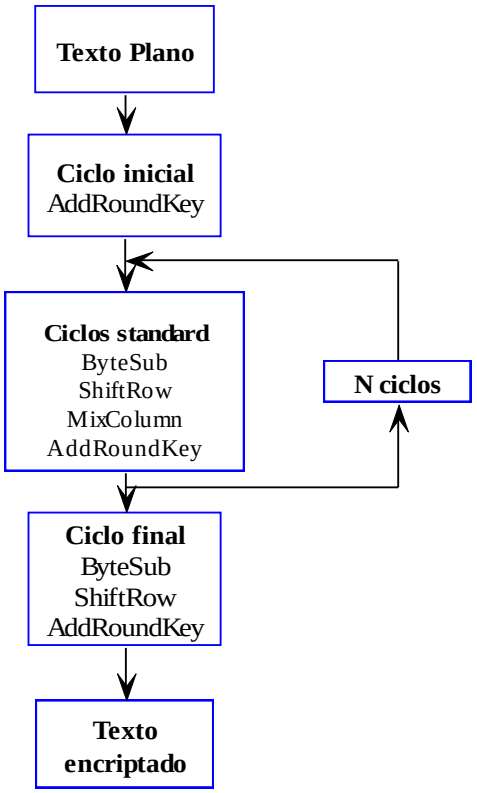

Figura 1. Diagrama de Flujo AES [FIMD2009]

De acuerdo a los anteriores algoritmos y su explicación se procede a la configuración de la VPN.

4.2.7 VPN Virtual Private Network

Una VPN se define como un proceso de comunicación cifrada o encapsulada que transfiere datos desde un punto hacia otro de manera segura, la seguridad de los datos se logra gracias a la utilización de algoritmos fuertes como 3DES o AES, el envío de los datos de manera segura se hace a través de medios inseguros.

Esto quiere decir que consiste en utilizar túneles y criptografía para enviar casi de forma transparente y segura los paquetes a través de una red publica como Internet y los clientes vean la conectividad así obtenida como equivalente a una red de área local privada.

Los mecanismos de seguridad utilizados por una VPN son:

- Autenticación

Es el proceso de asegurar que los datos son enviados y recibidos por quien ser enviados y por quienes deben ser recibidos. La autenticación requiere de un nombre de usuario y contraseña para acceder a un recurso.

- Cifrado

Proceso de cambiar los datos de manera segura, los datos solo pueden ser leídos por el o los receptores autorizados, las VPNs pueden utilizar cifrado asimétrico y simétrico o de llave privada.

- Autorización

Proceso de permitir o denegar acceso a los recursos localizados en la red después que el usuario se ha identificado y autenticado.

- Tunneling

Tunneling es la tecnología de encapsular un paquete de datos en un protocolo de túnel, enviar datos en una red mediante otras conexiones de la red. El tunneling funciona encapsulando el protocolo de red dentro de paquetes transportados por la segunda red, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro por ejemplo el protocolo IPsec o Secure Shell.

4.2.8 Protocolos de Tunneling

Los principales protocolos para hacer tunneling son:

1. 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.

2. 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.

3. 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.

4.3 ESTADO DEL ARTE

En la actualidad hay diferentes fabricantes de equipos para proteger la infraestructura de red para implementar estos se debe estudiar muy bien la necesidad especifica de cada organización.

En algunos casos es necesario proteger el correo electrónico, analizar todos los activos de la red buscando las vulnerabilidades y la más importante proteger la red de las conexiones externas evitando el contando con las aplicaciones y servidores internos.

Muchos de estos fabricantes crean herramientas que no se limitan a detección y prevención de instrucción a base de firmas, la tendencia y futuro de todos los equipos y enlaces depende de la creación de sitios dedicados a prestar un servicio a base de reputación por IP, Dominio y URL.

Equipos Firewall UTM/VPN Ipsec, estos equipos son utilizados para las conexiones frontales y protección de perímetro, gracias a sus bondades estos equipos cuentan con diferentes módulos para la protección y de la red, módulos como IPS/IDS Sistema de Prevención de Intrusos / Sistema de Detección de Intrusos este módulo verifica y realiza un escaneo del trafico que en tiempo real pasa por el equipo y de acuerdo a su comportamiento es bloqueado o permitido. Módulo de Anti-virus.

Equipos NAC Network Access Control por sus siglas en ingles, estos equipos se utilizan para el control de acceso a la red, si un equipo por ejemplo un portátil es conectado a la red local este equipo es escaneado y de acuerdo a políticas de seguridad por ejemplo es que el Anti-virus este actualizado, que tenga los parches de sistema operativo instalados cumpliendo esto se permite la navegación y el acceso a los recursos de la red.

Para la implementación de autenticación fuerte por ejemplo se puede utilizar los Sistemas Single Sign-On

Muchas organizaciones que tienen múltiples aplicaciones y para el acceso a estas es necesario digitar una clave para cada una de las aplicaciones existentes, para mayor seguridad y no tener un archivo Excel con las claves de cada una de las aplicaciones o evitar el olvido de las contraseñas por los administradores de la red y sus diferentes usuarios se implementa actualmente este tipo de solución, se ve un crecimiento del uso de sistemas SSO Single Sign-On estos sistemas se desarrollan con el fin de crear autenticación fuerte y manejo de contraseñas.

El sistema de Single Sign-On se pueden crear políticas de autenticación por ejemplo que se cambie la contraseña cada 15 días utilizando caracteres especiales, pero lo mejor es que el equipo es el que realiza el cambio de contraseñas de las aplicaciones esto quiere decir que el usuario o el administrador solo conoce una única contraseña que es cuando este se autentica ante el dominio, esto da mayor seguridad por esta característica ya que el usuario no sabe las contraseñas de las aplicaciones y deben ser distribuidas por el equipo.

Las ventajas de este tipo de equipos es que permite la autenticación con sistemas biométricos, tarjetas de proximidad, token y para implementaciones nuevas que cuentan con controles de acceso físico como tarjetas magnéticas si el usuario no ha entrado a las instalaciones u oficina no pueden autenticarse en su computadora y si lo hace no le trae el perfil creado para este usuario con los permisos y el número de aplicaciones que maneja. [IMPR2009]

Para un análisis detallado de la red existen Sistemas de Análisis de Vulnerabilidades, estos sistemas son utilizados actualmente para en escaneo de la red, este escaneo se puede realizar a cualquier dispositivo que contenga configuración IP.

Es análisis de vulnerabilidades da como resultado un reporte con el número de vulnerabilidades encontradas y clasificadas por el tipo de prioridad baja, media y Altas y en algunos casos puede mostrar falsos positivos esto quiere decir que en un servidor puede encontrar puertos abiertos en este caso si es un servidor FTP va encontrar el puerto 21 o 2121 abierto porque estos son los puertos que utiliza en protocolo FTP protocolo de transferencia de archivos como es una característica para este tipo de aplicación es un falso positivo.

El análisis de vulnerabilidades permite solucionar vulnerabilidades encontradas en todos los dispositivos de la red y así asegurarnos de posibles ataques o de entidades externas que puedan explotar las vulnerabilidades de los equipos. [NETC2009]

5. METODOLOGÍA

5.1 Etapa 1

Levantamiento de la información necesaria para el desarrollo del proyecto todo en el mes de Enero y Febrero estudio de dispositivos a implementar.

Pruebas con los diferentes equipos de seguridad informática en el mes de Febrero, y pruebas el mes de Marzo con los diferentes tipos de algoritmos de encripción. Pruebas de navegación con Proxy y creación de políticas de navegación.

5.2 Etapa 2

Diseño y estructura de la red para implementar el esquema de seguridad más adecuado en el mes de Abril.

Con las pruebas realizadas en agosto definir el tipo de cifrado a implementar en el proyecto. Implementación de Proxy para el control de navegación Web de los usuarios.

En Mayo se escogen los equipos después de varias pruebas para implementar las aplicaciones del proyecto.

5.3 Etapa 3

En Mayo y Junio proceso de implementación del proyecto después del montaje y corroborar que todo esta funcionando perfectamente presentación e implementación del proyecto.

5.4 DESARROLLO

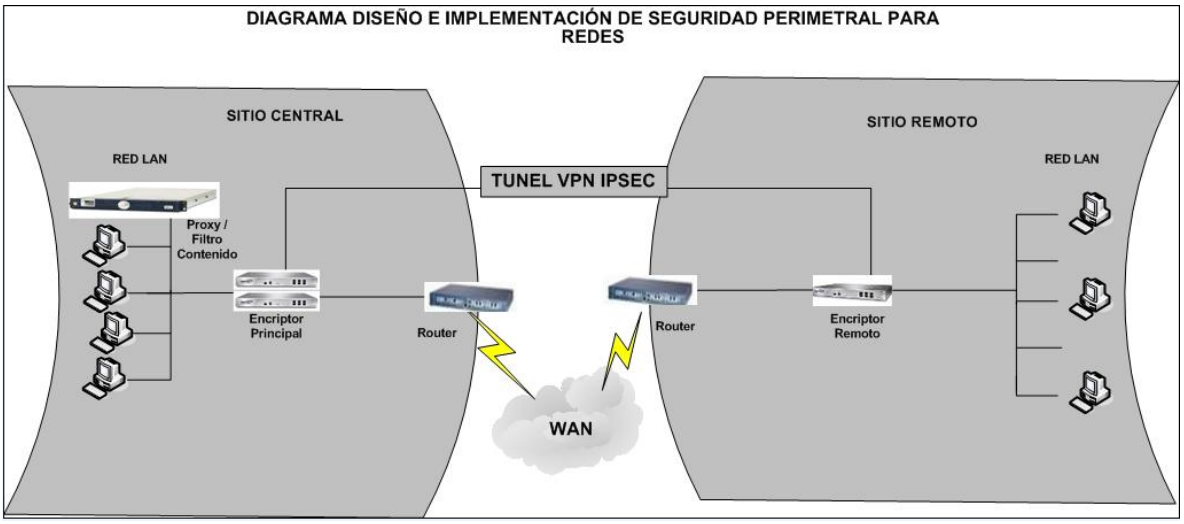

Figura 2. Diagrama Proyecto

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.

Para la implementación a nivel WAN es necesario realizar y diseñar el cifrado de las oficinas o sitio central y sitios remotos, al implementar el cifrado de las diferentes sitios evitamos ataques como el Man In the Middle, que es exactamente una entidad externa que se ubica en la mitad del canal y roba la información que viaja sobre esta o realiza modificación de la información contenida, por esto es necesario cifrar el canal con un método eficaz y robusto para este caso en especial para mayor seguridad y evitar la intrusión de los datos que viajen sobre el

túnel y esto se realiza con Hardware especifico, porque hardware especifico al contener diferentes módulos, estos módulos son los siguientes:

- Firewall
- IPS/IDS
- Anti-Virus
- VPN

El módulo de Firewall nos permite realizar reglas o políticas para los diferentes protocolos como http, https, ftp, Telnet, terminal Server y otras aplicaciones, servicios o trafico que pase por medio del equipo, donde se puede configurar que se bloquee o se permita este tipo de trafico o re-direccionarlo hacia un servidor o puesto de trabajo.

El módulo de IPS/IDS brinda seguridad a todos los recursos de la red, porque este es el módulo que es el sistema de prevención de intrusión y sistema de detección de intrusión, de acuerdo al comportamiento y escaneo del trafico que pasa por el equipo se va a permitir este trafico o se cierra la conexión de este hacia el interior de la organización. Este módulo nos permite parar ataques o virus no conocidos.

El módulo de Anti-Virus es protección a base de firmas esto quiere decir que de acuerdo a las firmas y su base de datos de los virus conocidos estos van a ser bloqueados.

El módulo de VPN este módulo es el alma del desarrollo y la implementación del proyecto, en este módulo se hace la configuración de las VPN IPsec, en el módulo VPN se define el tipo de algoritmo que se va a utilizar si es DES, 3DES o AES. El punto origen y destino del túnel y las fases de negociación para el establecimiento del Túnel. Y muchas características para el desarrollo del proyecto.

Todo el desarrollo y la implementación se realiza con los equipos de Marca Secure Computing Snapgear los equipos para el cifrado de la información y del canal de los sitios remotos son equipos Snapgear SG580, de todos modos los equipos de cifrado de los sitios remotos pueden ser de diferentes modelos dependiendo del número de usuarios y también del número de conexiones que se necesiten, se debe tener en cuenta el crecimiento en la infraestructura de red y aplicaciones.

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.

5.5 FASE I

Resumen de los pasos de la configuración VPN IPsec

- Internet Protocol Security
- Opera en la capa de red
- Permite establecer múltiples túneles
- Provee cifrado y autenticación de paquetes IP
- Hace parte del nuevo estándar de direccionamiento de redes IPv6
- Emplea dos mecanismos:
    - Authentication Header (AH) para autenticación e integridad del encabezado IP
    - Encapsulating Security Payload (ESP) para proveer integridad y cifrado de los datos contenidos en el paquete IP
- Emplea Security Associations (SA) para establecer los parámetros que rigen una comunicación, entre ellos:
- Direcciones origen y destino
- Mecanismo empleado (AH o ESP)
- Algoritmo criptográfico
- Llaves origen y destino
- Cada SA es identificada con un número único en la red de 32 bits llamado el SPI (Security Parameter Index)
- Algoritmos empleados para autenticación e integridad: HMAC-MD5 y HMAC-SHA1, para cifrado son DES, TripleDES y AES
- Para efectuar la negociación y administración de SAs y de llaves de encripción se emplea una combinación de tres protocolos, conocida como IKE (Internet Key Exchange)
    - IKE se compone de:
        - ISAKMP (Internet Security Association and Key Management Protocol) que define las fases para establecer relaciones seguras.
        - SKEME (Secure Key Exchange Mechanism) que describe intercambios seguros de llaves.
        - Oakley que define el modo de operación requerido para establecer una conexión segura.

Los equipos SnapGear Soportan IPSEC, PPTP, L2TP, Conexión Site to Site, host to host, net to net.

SnapGear soporta “VPN Off-Loading” esto quiere decir que se puede tener varios equipos SnapGears adicionales para expandir el número de túneles que soporta cada equipo. El consumo del ancho de banda (BW) depende si sobre el canal tienen políticas de Calidad de Servicio que restrinjan o limiten el tráfico cursante

de la Tx en este caso por ejemplo puede ser FTP o por el contrario den prioridad al tráfico que se genere por FTP.

Una limitante puede ser el ancho de banda del canal, si es un ancho de banda limitado posiblemente no se puede establecer el túnel, si es limitado el canal por ejemplo se tiene un servidor o equipo del cual se extrae la información a través de FTP, si no se tienen políticas de calidad de servicio lo más seguro es que se consuma todo el Ancho del canal.

Para la configuración de los equipos es necesario realizar la configuración de las diferentes interfaces de red, esta configuración se realiza en el menu de Network Setup esta sección contiene todo lo que tiene que ver con la configuración de las interfaces como son las rutas, el direccionamiento IP.

En la opción Connections se muestra y se realiza la configuración de dos interfaces de red, a cada interfaz se le puede configurar un nombre y dirección Ip diferente como lo observamos en detalle en la Figura 3.

En este caso se coloca el nombre a cada una de las interfaces una llamada Router y la otra Firewall.

- Router: Se genera la dirección con la cual se hace consola del encriptor principal.
- Firewall: Se genera las interconexiones a las interfaces del encriptador y enrutador.

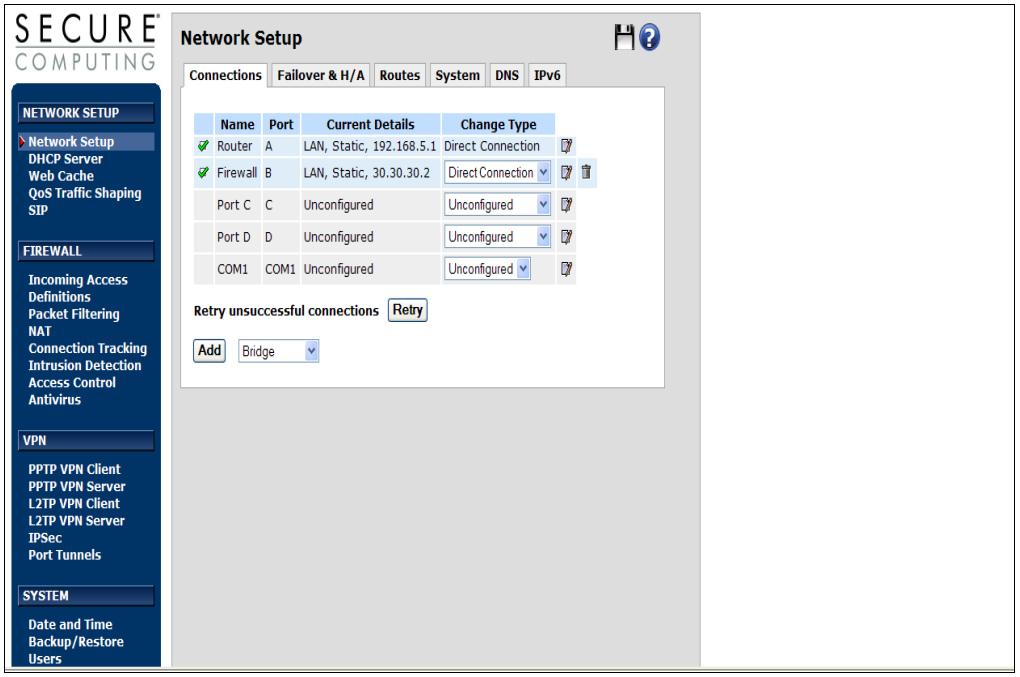

Figura 3. Configuración Red Network Setup

Para la administración del equipo y definir el servicio que se va a habilitar se realiza la configuración en el menú de Firewall en la etiqueta de Incoming Access, en este menú se habilita los pings de verificación de red para validar la interconexión entre los diferentes recursos de la red o los diferentes equipos de cifrado para la implementación del proyecto.

La configuración se puede ver con más detalle en la Figura 4.

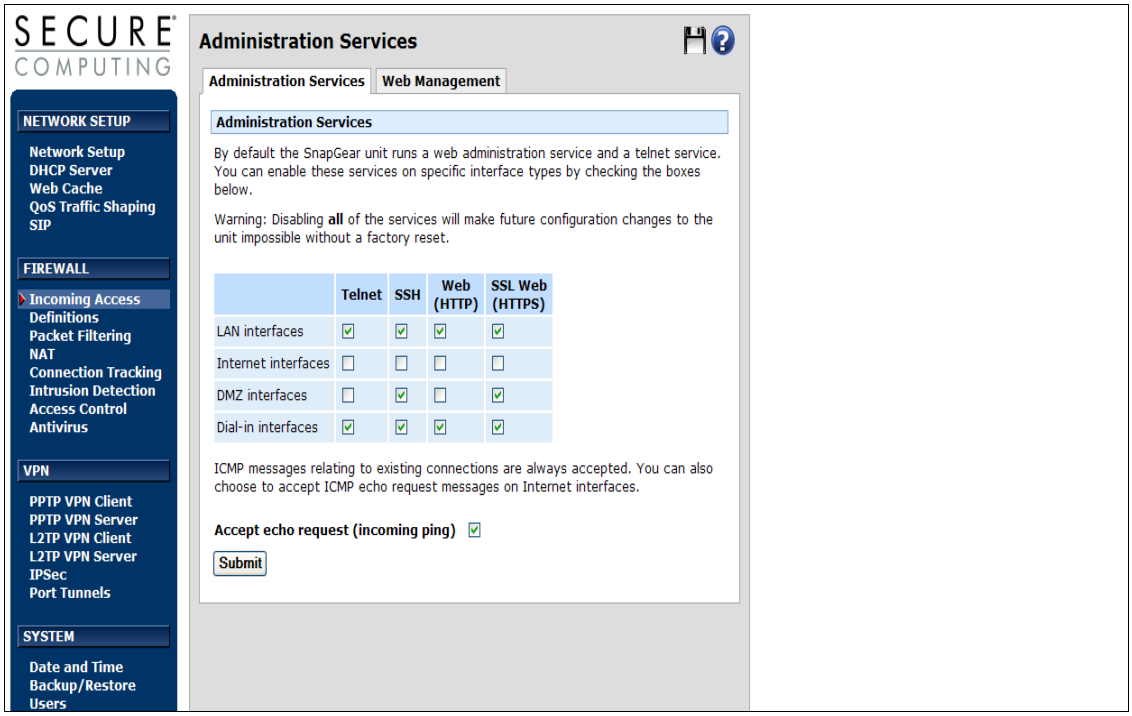

Figura 4. Configuración Aceptar Ping Firewall

El módulo de Firewall en la parte de Definitions se realiza la configuración de los puertos, diferentes protocolos como http, https, ftp, Telnet, terminal Server y otras aplicaciones, servicios o trafico que pase por medio del equipo, en la siguiente figura se ve con más detalle la configuración de los grupos de servicios o puertos específicos necesarios para la implementación.

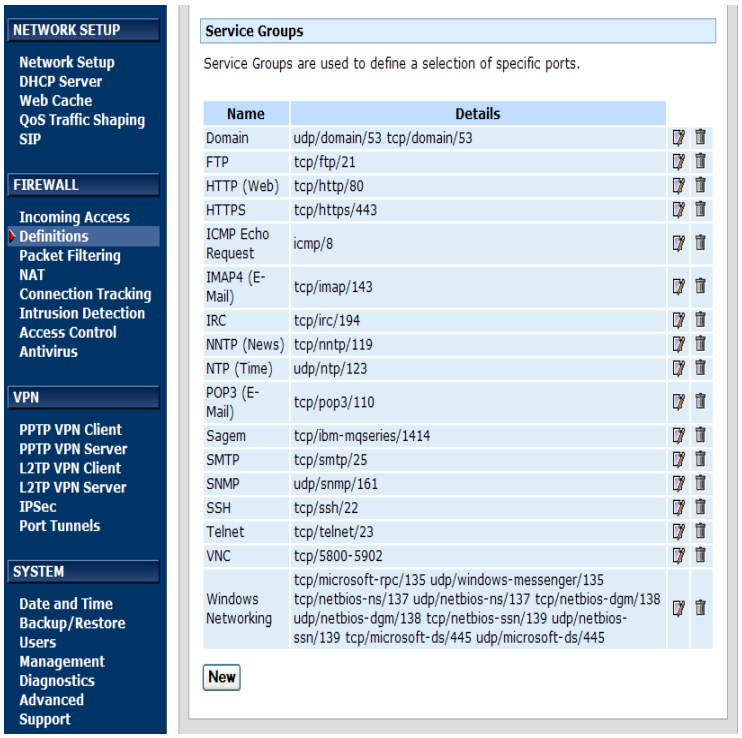

Figura 5. Configuración de puertos Service Groups

En la siguiente imagen se genera cada una las VPN que se necesitan para que haya conexión entre los sitios remotos y el sitio central. Este es un ejemplo claro de las VPNs que se generan para cada red remota, esta imagen muestra si los túneles han sido establecidos y los estados de los mismos.

Si el túnel ha sido establecido y su estados en OK se ve como running y si están caídos se ven con estado Down.

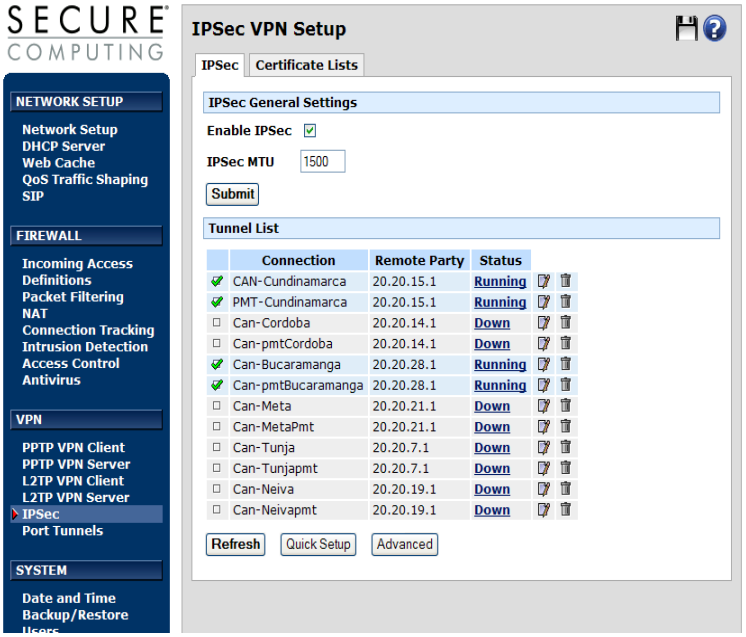

Figura 6. Estados de las VPN Ipsec

5.5.1 ROUTER

Colocar el router conectado directamente al puerto WAN del equipo de cifrado con un cable cruzado de frente sin pasar por ningún switch y que esta pequeña red sea solo de 2 host es decir máscara 252 / 30 para evitar trafico de broadcast innecesario. Hacia la WAN propiamente dicha realizar marcado de paquetes entre los routers para asegurar.

En cuanto a las tablas de enrutamiento si bien el encriptor maneja RIP, existen dispositivos como Core o Routers que son muchos más robustos y dedicados a este tema que puedan realizar protocolos de enrutamientos incluso más sofisticados como IGRP, OSPF, etc. La recomendación es manejar rutas estáticas a nivel del la unida SnapGear.

5.5.2 ENCRIPTOR

Pasos necesarios para la configuración del equipo de Cifrado

Paso 1. Iniciar la configuración de los equipos Snapgear y activación de las interfaces.
Paso 2. Configuración Túnel Ipsec.
Paso 3. Creación de túneles ipsec necesarios para la implementación.
Paso 4. Configuración de punto local.
Paso 5. Configuración de punto remoto.
Paso 6. Configuración parámetro fase 1.
Paso 7. Configuración parámetro fase 2.
Paso 8. Confirmación operaciones VPN.

a). Local Interface: Se debe colocar la interface por donde va a salir todo el trafico hacia le sitio central, es decir este es el puerto que se configuro como WAN dentro del router.

b). Keying: Se recomienda dejar Aggressive Mode (IKE), ya que no solo automáticamente intercambia keys para encriptar y autenticar, sino que utiliza menos mensajes a la hora de establecer el túnel.

c). Authentication: Son tipos de autenticación utilizado por el túnel.

El tipo más común de autenticación es el preshared (PSK) el cual debe ser el mismo en los dos extremos de la VPN. Al crear una VPN Ipsec, el terminador de la VPN no permitirá que el proceso de autenticación continué hasta que la clave dada sea la correcta y la conexión será rechazada. Dependiendo de la versión de software del encriptor SnapGear, se pueden utilizar otros métodos de autenticación como RSA Digital Signaturs el cual emplea llaves publicas o privadas y el x.509 Certicates el cual necesita una entidad certicadora (CA)

d). Preshared Secret

Es la frase común que debe estar habilitada en los dispositivos, esta debe ser la misma para todos los equipos.

Debe guardarse de forma confidencial y además ser cambiada como mínimo cada dos meses para mayor seguridad.

e). IP payload compression (IPcomp)

Proporciona una solución para comprimir los paquetes antes del cifrado ESP, lo que suele aumentar la eficacia de la compresión, pero que puede generar latencia en la red. Normalmente no se habilita pero depende de cliente

f). Dead Peer Detection

Le permite al túnel ser reiniciado si el terminador de VPN deja de responder. Esta característica debe estar disponible y habilitada en los dos extremos del túnel. La forma como trabaja es enviando notificaciones y esperar las respectivas respuestas.

g). Delay (sec)

Es la longitud de tiempo en segundos entre el envió de notificaciones. En caso de una caída del túnel, entre más alto sea este parámetro, será más demorado que el equipo detecte esta situación y por lo tanto el inicio del conteo del parámetro timeout.

h). Timeout (sec)

Es la longitud de tiempo en segundos antes de que el túnel sea reiniciado, luego de detectarse que el DPD no responde. El parámetro típico es de 30 segundos y es el sugerido para la implementación

i). Key Lifetime

Un valor pequeño es mucho más seguro porque las llaves de cifrado van cambiando mucho más rápido, pero esto lleva un overhead en el equipo que puede degradar el rendimiento del mismo. El valor de fábrica es de 3600 sec, es decir cada hora.

j). Rekey Margin

Tiempo que se debe esperar para que la conexión vuelva a negociar el cambio de la clave. Es un concepto parecido al de la duración de la clave y se expresa también en segundos. El valor recomendado es de 600 sec

k). Rekey Fuzz

Indica el porcentaje máximo que debe aplicarse a la clave nueva para que los intervalos sean aleatorios. El porcentaje óptimo es del 100%.

Algoritmos de encripción sugeridos.

3DES – SHA – Diffie Hellman Group 1(768 Bits).

5.5.3 Comparación de Tecnología VPN

En la actualidad existen dos tipos de VPN´s

a). VPN IPSEC esta trabaja en la capa de red, capa tres del modelo OSI, para su funcionamiento se debe tener en el sitio central y sitio remoto equipos Hardware de uso específico esto quiere decir que son equipos desarrollados por diferentes fabricantes entre los cuales se tiene:

McAfee, Juniper, Cisco, Sonicwall, WatchGuard, Netscreen, Fortinet, entre otros, estan son las marcas que se utilizan en la actualidad para la encripcion de canal WAN.

b). VPN SSL Secure Socket Layer esta VPN opera en la capa de aplicación, capa siete del modelo OSI, para su funcionamiento se utiliza un equipo central que soporta un numero especifico de usuarios de acuerdo a la necesidad de acceso remoto permitiendo detectar que se tiene en el equipo remoto que se esta conectando a la VPN SSL, cumpliendo políticas creadas anteriormente en el

equipo central, esta política puede ser por ejemplo que el equipo de escritorio o portátil tenga el anti-virus actualizado, también realiza un escaneo de todo el equipo verificando que este no contenga ningún software malicioso instalado, brindando protección a la red verificando la identidad del usuario o usuarios que se conectan a la VPN, y lo mas importante el acceso a las aplicaciones de la red como aplicaciones tipo servidor, compartir archivos, aplicaciones VoIP entre otros servicios.

5.6 FASE II

Para el desarrollo de la fase II Seguridad Web, la implementación de Proxy para el control de usuarios, filtro de navegación Web y creación de políticas de navegación para los diferentes perfiles, se utiliza un equipo webwasher que es Proxy y permite crear reglas y políticas para los diferentes perfiles de usuario que se tienen para el proyecto, es necesario tener claro como un usuario realiza una petición de navegación a cualquier sitio web para comprender el funcionamiento, esto se explica en detalle con el siguiente diagrama de Flujo de filtro URL.

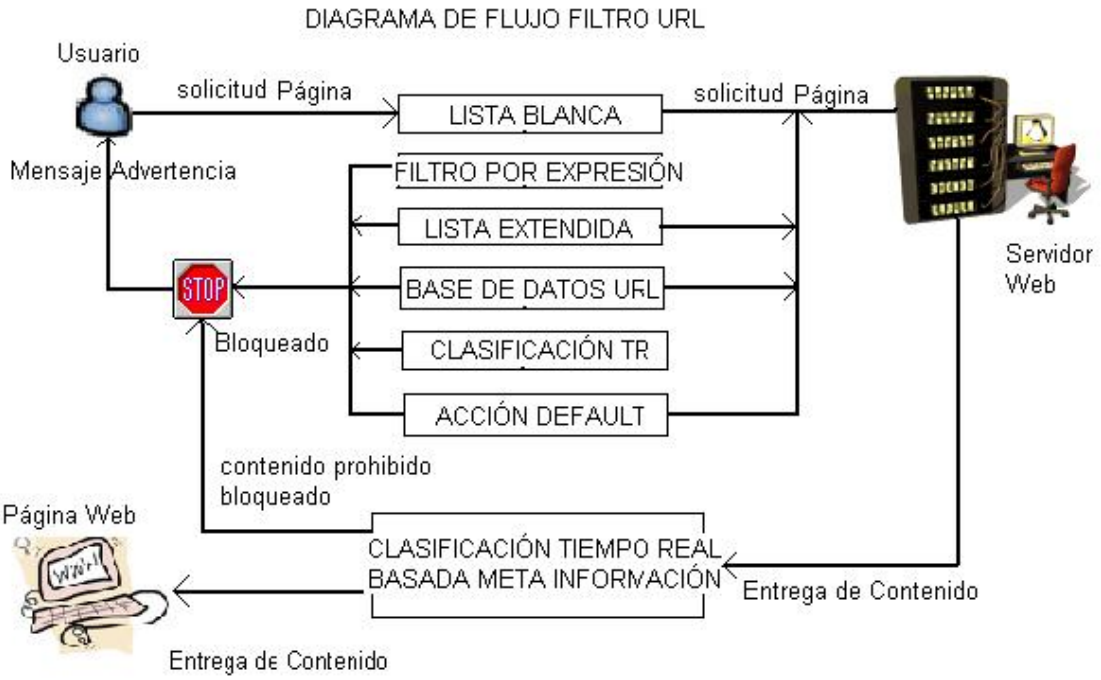

Figura 7. Diagrama de Flujo Filtro URL

En el diagrama de flujo de filtro de contenido se observa cuando un usuario realiza la solicitud de navegación o solicitud de pagina Web, estas solicitudes pasan por diferentes motores para el análisis de la petición de navegación, su orden especifico, la solicitud de navegación pasa primero por las listas blancas, estas

son entradas de diferentes sitios Web que se permite su navegación sin ninguna restricción permitiendo al usuario la entrega del contenido de esta.

Filtro por Expresión, este motor o filtro realiza la verificación si en este existe una entrada o configuración de palabra por ejemplo si contiene la palabra TV si el usuario hace la petición de un sitio que contenga en su dirección de URL o sitio Web la palabra TV automáticamente será bloqueada esta solicitud y el mensaje de advertencia es entregado al usuario que realizo la petición.

Listas Extendidas son listas creadas para una política o políticas de navegación creadas en el equipo para realizar el bloqueo, permitir el acceso a sitio Web, un retardo en la navegación o advertencia al usuario sobre las peticiones que estos realizan.

Base de Datos URL este es el alma del equipo ya que es el motor más importante que tiene el equipo, este motor contiene la lista y actualizaciones de los diferentes Dominios, IPs, y URL como están categorizadas y a que categoría corresponde. Este motor es retroalimentado por medio de Trustedsource.

Clasificación en Tiempo Real esta clasificación se realiza para la reputación de los sitios donde navegan los usuarios o usuario, si el sitio es de mala reputación automáticamente es bloqueada esta solicitud y es enviada la advertencia al usuario.

Acción Default este motor cuenta con la configuración que tiene el equipo que es realizada de fábrica y esta en aplicada a las peticiones que realiza el usuario.

Después de pasar por los diferentes motores y su orden especifico de acuerdo de la política creada para las diferentes categorías que el equipo tiene, se permite o bloquea la navegación.

Para la implementación y configuración del equipo es necesario tener en cuenta la siguiente topología de red para el normal funcionamiento y evitar inconvenientes.

Topología de red

- Provee funcionalidad integrada de Web gateway

Figura 8. Topología de red

Para el proyecto se utiliza el modelo que usa una sola interfase de red, el equipo debe ir instalado en la LAN.

Este tipo de conexión usa solo una interfase de Webwasher la cual recibe las peticiones de navegación de los diferentes usuarios y las respuestas a estas, dependiendo de las políticas de navegación. El equipo cuenta con dos interfaces de red la otra interfaz se utiliza cuando se realiza la configuración del Alta Disponibilidad, para este tipo de configuración es necesario tener un equipo de iguales características para su configuración.

Para la configuración de red de webwasher es necesario tener la siguiente información para la configuración del equipo.

Nombre del Host: _____

Dirección IP: _____

Máscara de Subred: _____

Puerta de Enlace predeterminada: _____

DNS: _____

_____

Rutas Estáticas _____

Esta información es configurado en el equipo para diferenciar este de los otros equipos que componen la red y la configuración de la interfaz de red para la navegación de este, el equipo debe navegar y tener todos los permisos de navegación, esto quiere decir sin ninguna restricción para su normal funcionamiento y actualización de los diferentes módulos que el equipo webwasher contiene.

Para la autenticación de los usuarios Webwasher es capaz de validar credenciales de usuarios para el acceso respecto a las políticas definidas, los siguientes repositorios soportados por webwasher son:

- ☐ Directorio Activo
- ☐ Novell eDirectory
- ☐ openLDAP
- ☐ SunLDAP

Para el proyecto se configura en webwasher la siguiente autenticación para acceso HTTPS, HTTP y FTP:

☐ NTLM NATIVO, protocolo de autenticación integrado.

☐ Agente NTLM, recomendado en todas las configuraciones con el directorio Activo, se instala en un controlador de dominio.

☐ LDAP, protocolo estándar de autenticación.

- ☐ Active Directory
- ☐ Novell eDirectory
- ☐ openLDAP
- ☐ SunLDAP

La configuración de autenticación para el acceso http, https y ftp que se utiliza es el agente NTLM.

Para que esta característica sea configurada de una forma satisfactoria, webwasher necesita comunicarse por los puertos específicos (LDAP y/o NTLM) con el directorio en cualquier caso.

Para una propia autenticación con Ldap es requerido:

Servidores de autenticación IP y FQDN:

Usuario LDAP: este usuario debe tener un perfil suficiente para listar el directorio de autenticación, para ambientes MSAD se recomienda que sea parte del grupo Domain Admin
Usuario:

Contraseña:

Estructura para Autenticación LDAP, ejemplo. CN=name,OU=Unit,DC=domain,DC=com:

Autenticación NTLM Nativo

Windows DCs' IPs y FQDN:

Usuario NTLM: este usuario al igual que el método LDAP, debe tener un perfil suficiente para listar el directorio de autenticación.

Usuario:

Contraseña:

Instalación agente NTLM IP y FQDN: Esta opción es necesaria cuando se instalara el agente en el controlador de domino, para realizar esta configuración se necesita la compañía de los administradores de servidores de autenticación, tener acceso físico y realizar la instalación de los agentes en los servidores que sean necesarios.

Después de tener la información completa y tener claro cual es el método de autenticación podemos observar en el siguiente diagrama de flujo como se realiza la verificación de los usuarios para la navegación.

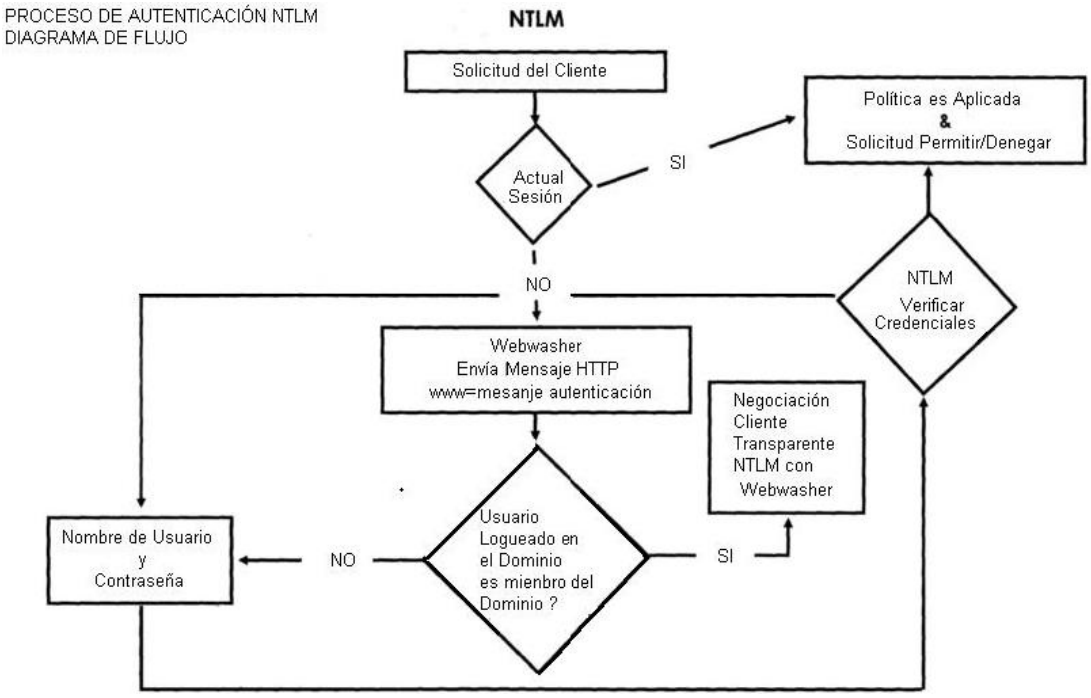

Figura 9. Diagrama de Flujo Proceso de Autenticación

En el diagrama de Autenticación se realiza la solicitud del usuario o cliente, este se valida con el repositorio de autenticación, si el usuario existe y es miembro del dominio es aplicada la política para el perfil del usuario, si es un usuario que no existe en el dominio o no se puede autenticar este debe proveer de nuevo las credenciales el nombre de usuario y la contraseña para validar al usuario y permitir o denegar la navegación.

Cuando se necesita que un equipo no provea credenciales de autenticación las estaciones de trabajo o servidores son excluidos de autenticación por medio de configuración por IP, esto funciona de la siguiente manera, se coloca el en el equipo de filtrado de contenido la IP del servidor o de la estación de trabajo para que estos no realicen verificación de usuario, si se desea se pueden crear usuarios locales en el equipo webwasher si no se cuenta con un repositorio de autenticación esto permite aplicar diferentes políticas de navegación para cada uno de los usuarios creados.

Para la autenticación de los diferentes usuarios se recomienda trabajar con el protocolo NTLM para la integración de Webwasher con el directorio Activo o servidor Ldap. Esta forma nos permite integrarnos fácilmente y tener comunicación con el directorio activo de una forma segura y el intercambio de información se hace de forma cifrada.

Este tipo de configuración se realiza instalando un agente NTLM en un controlador de dominio o en varios controladores de dominio, permitiendo conectividad en todo

momento esto quiere decir que si se cae algún controlador, webwasher se puede comunicar con los siguientes agentes instalados.

5.6.1 CREACIÓN DE POLÍTICAS DE NAVEGACIÓN

Se puede configurar grupos que existan en el repositorio de autenticación y asignar políticas de acceso que permitan o denieguen la navegación según políticas de la organización, en este caso se tiene por ejemplo la creación de dos políticas, estas políticas se aplican al nombre del grupo del directorio activo.
Se tienen tres grupos usuarios restringidos y usuarios no restringidos y usuarios sin navegación.

Las políticas que se crean son usuarios restringidos y usuarios no restringidos y usuarios sin navegación.

La configuración de políticas de navegación permite diferentes roles para usuarios, grupos o departamentos de la organización, además se puede configurar para que direcciones IP o rangos de IPs interactúen con el acceso a Internet.

Definir políticas de navegación para los diferentes usuarios de la organización, esto lo define y se realiza dependiendo el numero de usuarios, grupos o departamento, la definición de las políticas a implementar se debe hacer en acompañamiento de personal autorizado y destinado para la implementación, esto es muy importante para el desarrollo del proyecto porque esta persona cuenta con la información necesaria dado el caso que se necesite por ejemplo cuantos controladores de dominios se tienen y en cuales se va a instalar los agentes NTLM para la autenticación de los usuarios.

Para la creación de políticas de navegación en el módulo de URL Filter de Webwasher cuenta con 91 categorías predefinidas cada una de estas categorías cuenta con sus respectivas sub-categorías como se puede detallar en la siguiente figura:

Figura 10. Configuración Categorías Filtro URL

Por ejemplo lifestyle cuenta con 6 sub-categorías en esta política creada de navegación solo se permite navegar a sitios web de deportes (Sports), Viajes (travel) y Restaurantes (Restaurants) este es un claro ejemplo al momento de crear las políticas de navegación y cuales categorías o sub-categorías se deben bloquear y/o permitir en webwasher. Si se desea se pueden personalizar las categorías existentes o crear nuevas categorías (hasta 500).

La instalación física para Webwasher debe contar con todos los requerimientos técnicos y de seguridad para que su funcionamiento sea optimo, esto quiere decir que el equipo debe ser instalado en un cuarto de equipos e instalado en Rack con regulación de temperatura.

5.6.2 NOTIFICACIONES DE NAVEGACIÓN

Estas notificaciones son importantes para los diferentes usuarios que cuentan con permisos de navegación porque estas notificación le muestran al usuario el porque han sido bloqueados o el tipo de inconveniente que tienen en el momento de navegar y si estos cuentan con permisos de navegación.

Las notificaciones pueden personalizarse con el logo (122x48) y el mensajes que desee la organización acorde con las políticas y estandarizaciones de la organización. Para esto se debe suministrar al menos un logo de la organización y suministrar el texto que deseen adicionar en los mensajes de notificación de navegación de usuarios.

Figura 11. Notificaciones

6. PRUEBAS Y RESULTADOS

6.1 Pruebas y Resultados Fase I

Cifrado de información

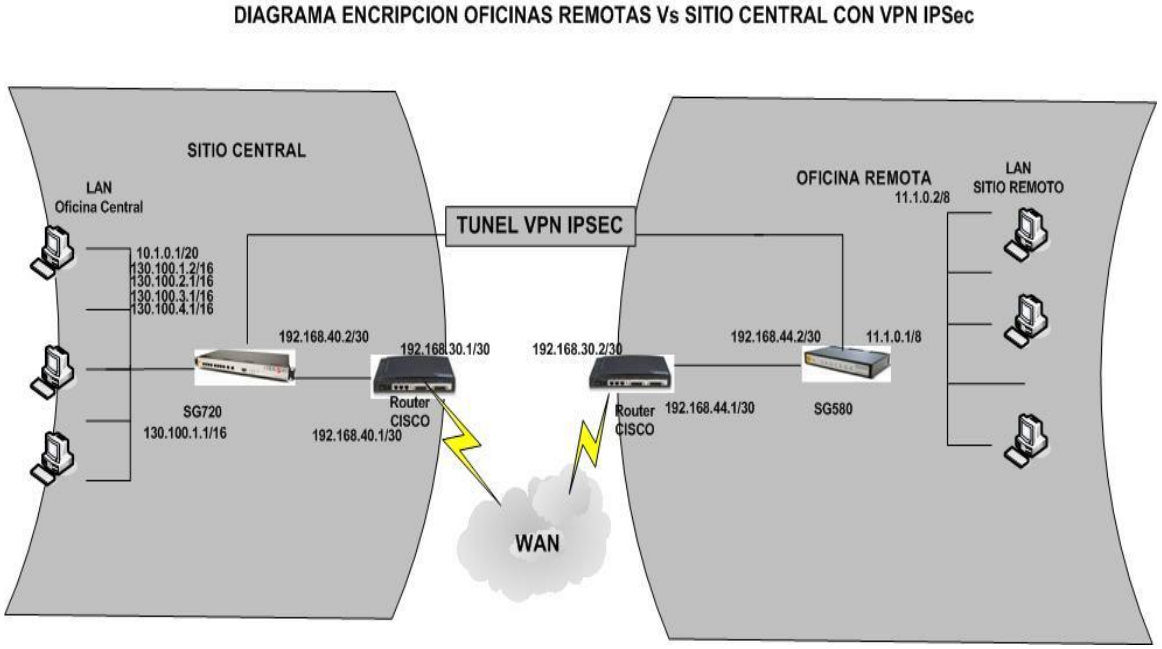

Figura 12. Diagrama implementación VPN IPsec

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.

a). Prueba con Cifrado

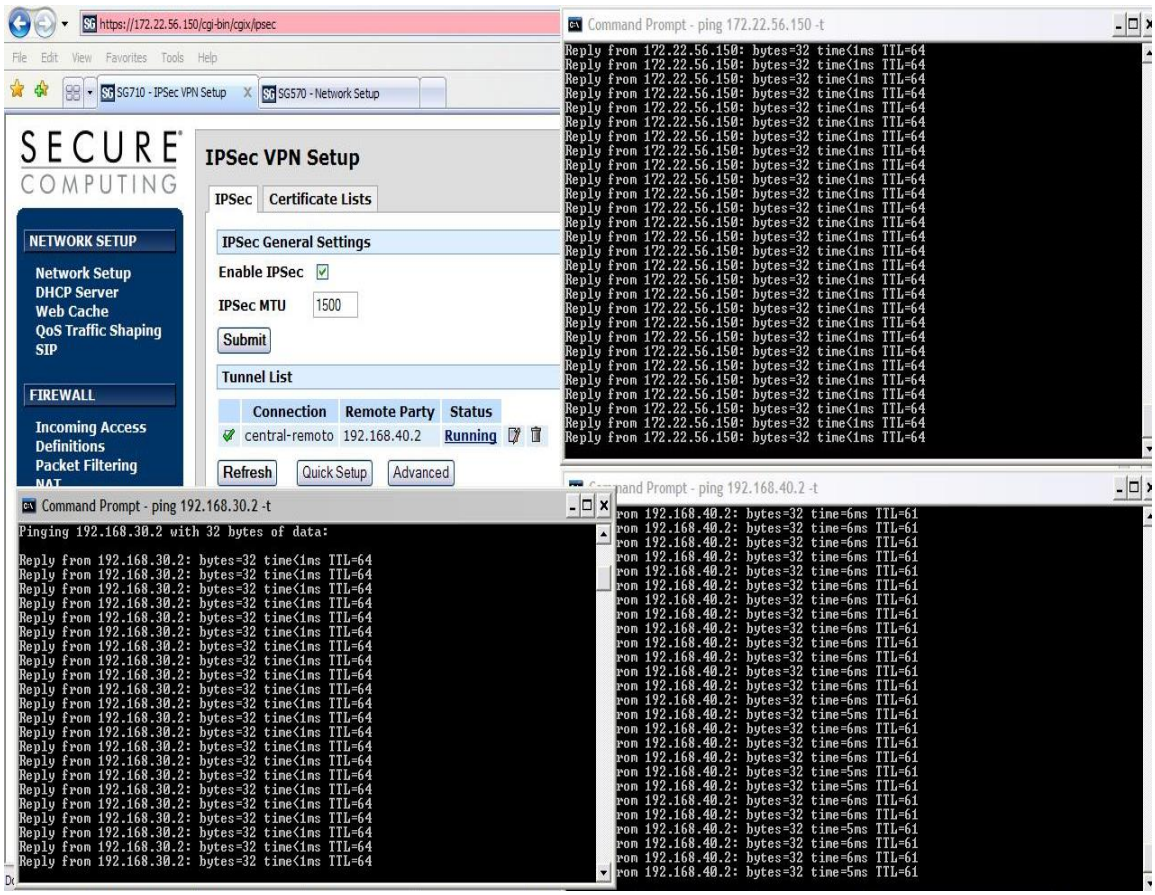

Figura 13. Estado del Túnel Habilitado

Como se observa en la figura (13) el túnel esta habilitado y los tiempos de respuesta son estables, el comportamiento no presenta ningún tipo de inconveniente.

b). Prueba sin Cifrado

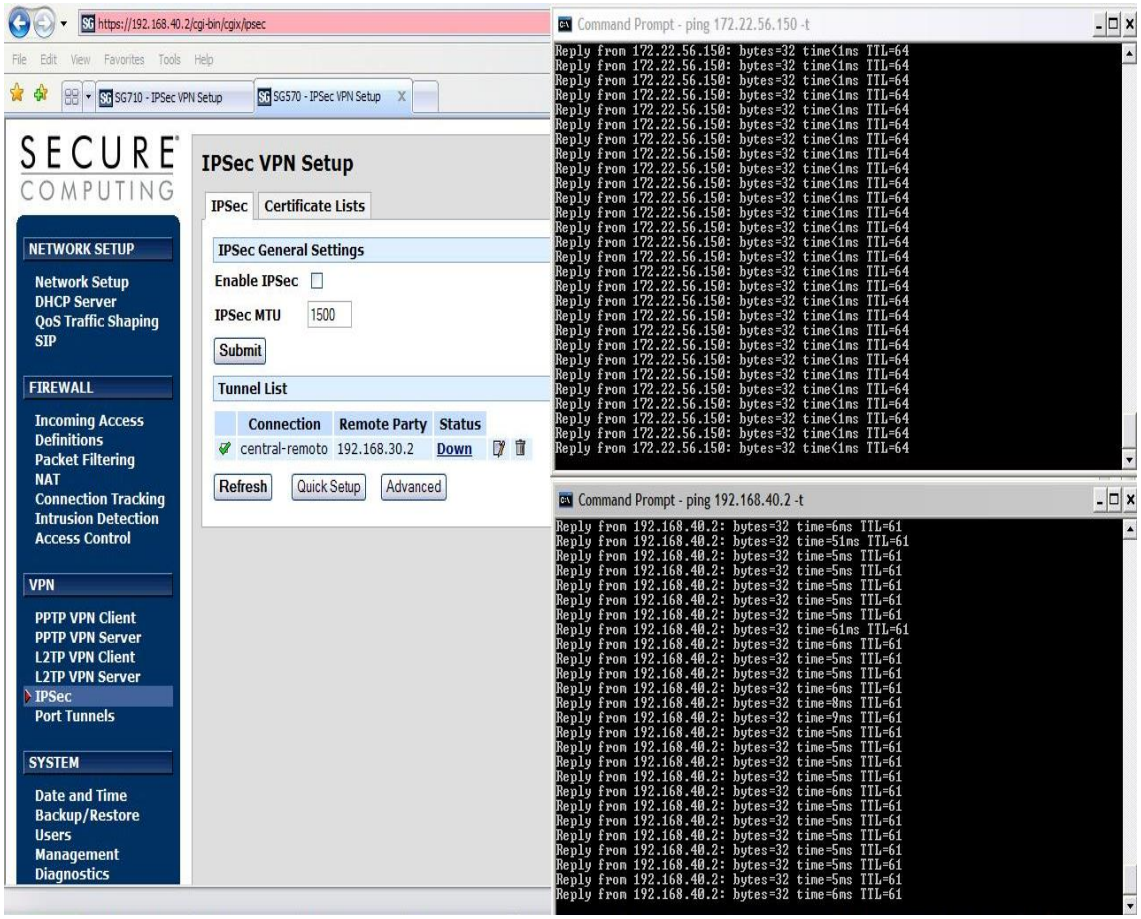

Figura 14. Estado del túnel Sin Habilitar

Como se observa en la Figura 13 no esta habilitado Ipsec y se hace pruebas, los tiempos de respuesta son estables y no se presenta ningún inconveniente.

c). Prueba sin cifrado y sin transmisión de datos

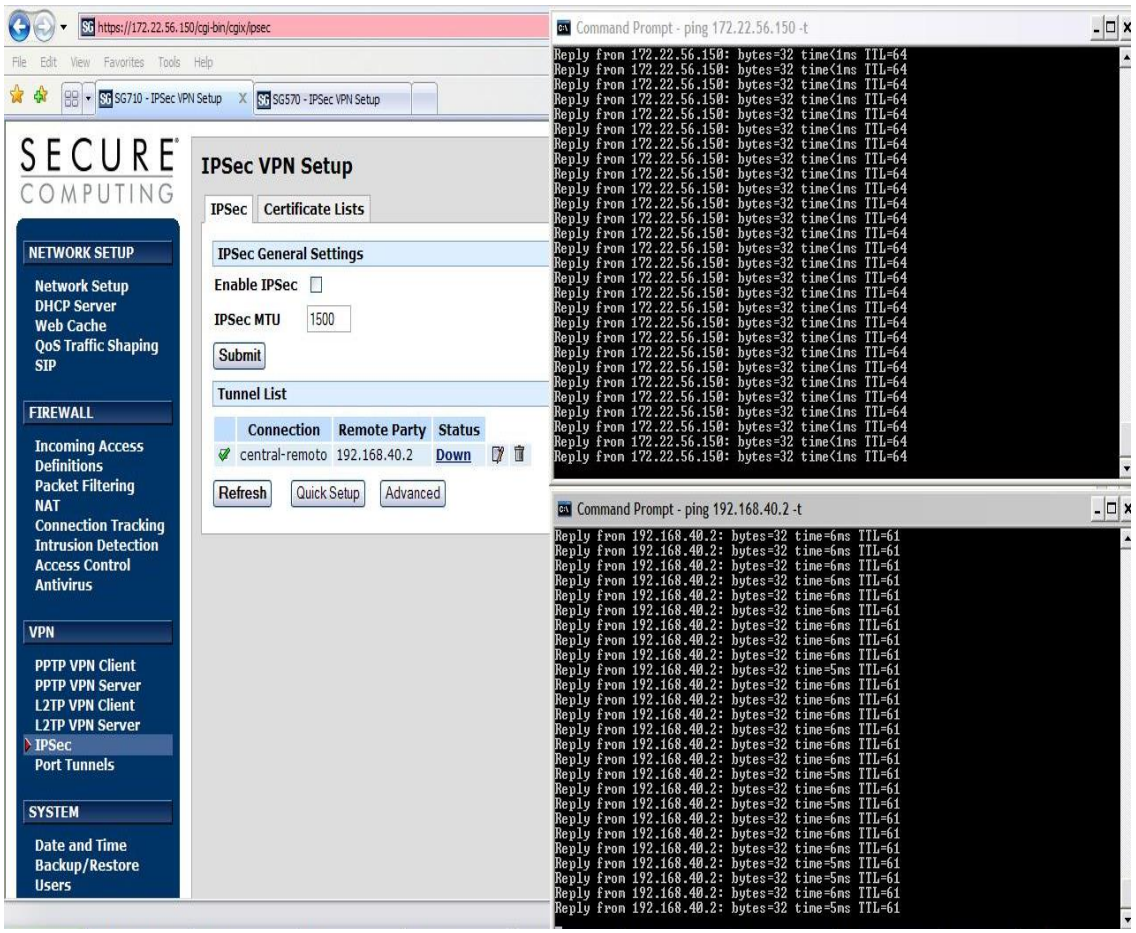

Figura 15. Estado de Túnel Sin Aplicativos y sin habitación VPN IPsec

Como se observa en la Figura 15 no esta habilitada la encripción y no tenemos ningún aplicativo corriendo, en este caso tampoco se tiene ningún tipo de inconveniente.

d). Prueba cifrado con transmisión de datos

Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=12ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms TTL=251
Respuesta desde 172.26.17.3: bytes=32 tiempo=11ms 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.

e). Prueba cifrado sin transmisión de datos

Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=8ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=29ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=48ms TTL=249
Respuesta desde 172.26.17.3: bytes=32 tiempo=7ms TTL=249

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

El consumo del BW depende si sobre el canal tienen políticas de QoS que restrinjan o limiten el tráfico cursante de la Tx en este caso por ejemplo puede ser FTP o por el contrario den prioridad al tráfico que se genere por FTP.

Otra limitante puede ser el BW que tenga el servidor o equipo del cual se extrae la información a través de FTP, si no se tienen políticas de QoS lo más seguro es que se consuma todo el ancho de banda.

Los clientes VPN pueden ser configurados para enrutar el tráfico de Internet a Internet mientras que el tráfico destinado a los lugares remotos puede ir a través de la VPN. Capacidades similares son probablemente disponibles para otros clientes como Safenet. [SECU2008]

6.2 Pruebas y Resultados Fase II

6.2.1 Pruebas Seguridad Web

Se realiza 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.

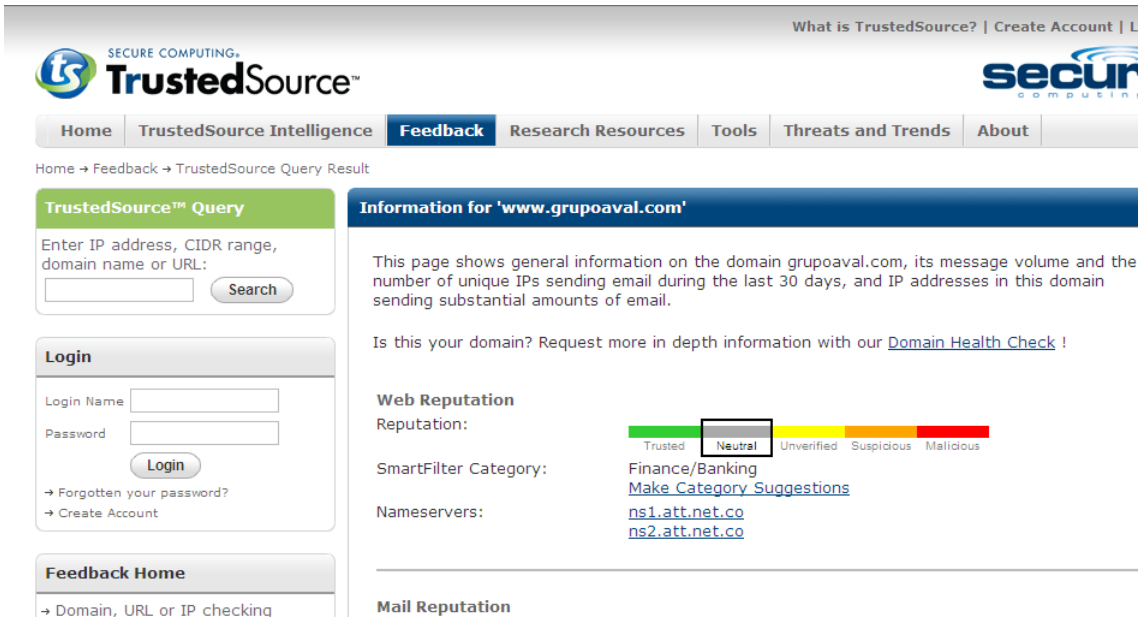

Figura 16. Trustedsource

La pagina www.TrustedSource.org Inteligencia global para proteger su organización, puede buscar la categoría a la cual un URL pertenece.

La tecnología TrustedSource de Secure Computing es un elemento fundamental de nuestras soluciones. TrustedSource, el sistema de reputación host de Internet más preciso y confiable del mundo, define el tráfico de Internet a fin de que sea compresible y procesable. La eficacia inigualable de TrustedSource es el resultado directo de la visión única de Secure Computing en el tráfico de Internet de la empresa. Al acumular datos de más de 7000 sensores ubicados en 51 países, TrustedSource crea un perfil de toda la actividad de los "remitentes" en Internet y luego utiliza este perfil para observar desvíos del comportamiento esperado. A continuación, el sistema genera una "clasificación de reputación" basada en el comportamiento del host de envío. Esta clasificación se incorpora en los productos Secure Computing para permitirles rechazar de manera rápida y precisa el tráfico no deseado.

Además en el sitio Web de TrustedSource podemos consultar sitios que no sabemos como están categorizados para crear nuevas políticas o bloquearlos en el módulo de URL FILTER.

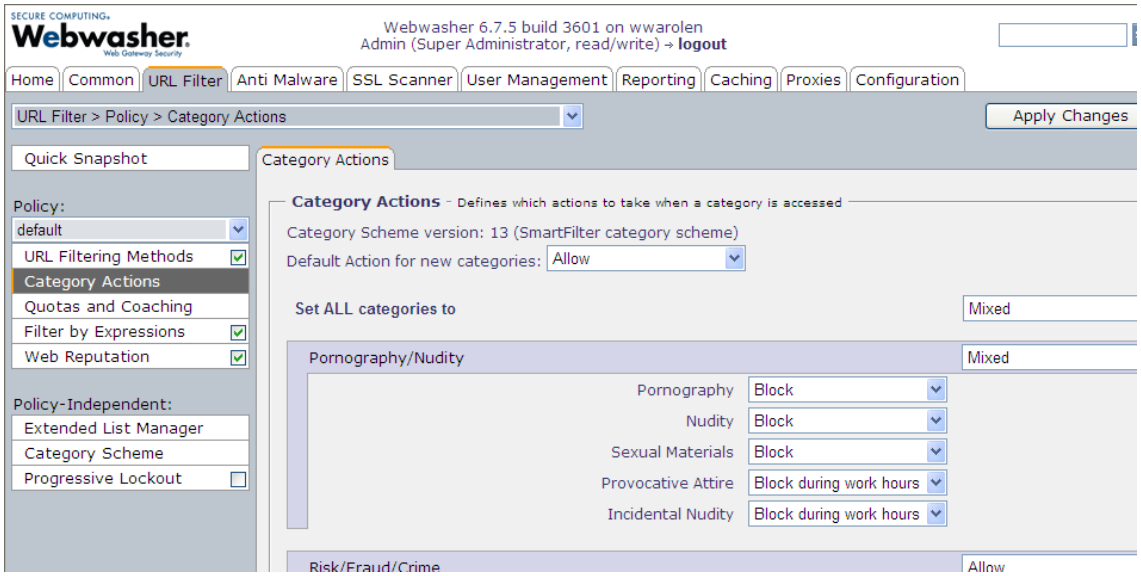

Figura 17. Filtro URL

Permitiendo el bloqueo exacto de los sitios Web que la organización por políticas no desea que sus usuarios puedan consultar.

La implementación se define en dos fases:

1. Instalación básica esto comprende configuración en el webwasher que no impacte la producción y accesos que tiene la organización actualmente.
2. Afinamiento de instalación básica, se realizara ajuste de los diferentes módulos contenidos por Webwasher y sus políticas.

A continuación se detalla algunos mensajes de acceso denegado por webwasher o mensajes de error por políticas creadas:

- La página www.juegos.com esta bloqueada por filtro URL, usted debe verificar si alguna de las categorías que esta en rojo aplica para esta pagina, si aun asi quiere dejarla pasar se debe crear un WhiteList.

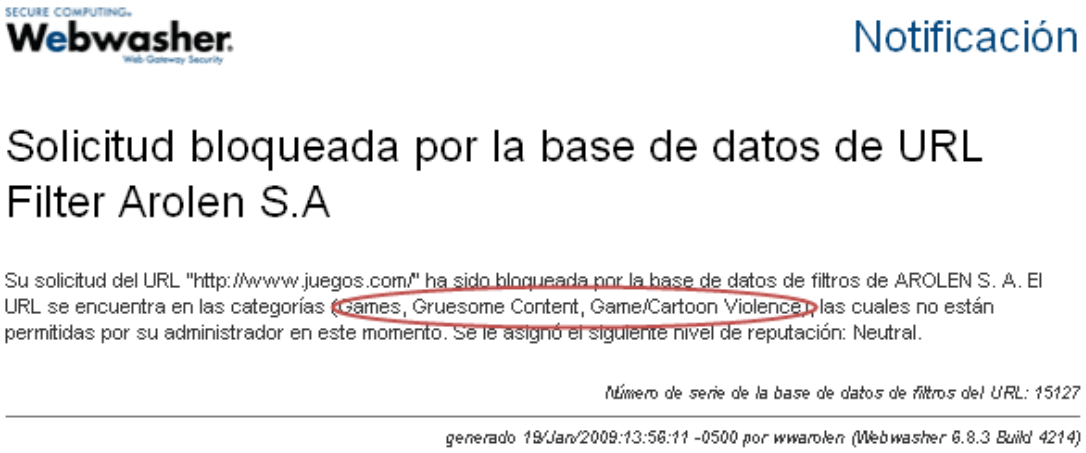

Figura 18. Bloqueo por Base de Datos

- Esta solicitud a sido bloqueada por la opción “Filter by expressions” en url filer, en este caso se boqueo por la palabra “tv”.

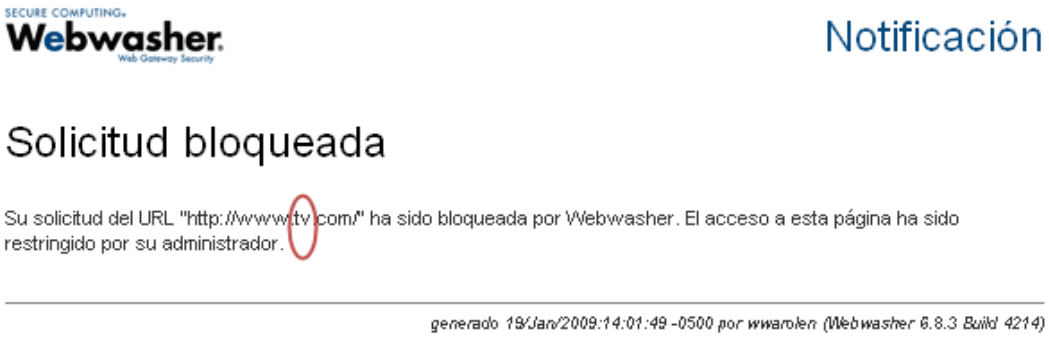

Figura 19. Bloqueo Filtro por Expresión

- El sitio puede tener mala reputación, contiene material o contenido obsceno, si aun así desea dejarla pasar usted puede crear un whitelist y deshabilitar la opción “Web Reputation Filter”

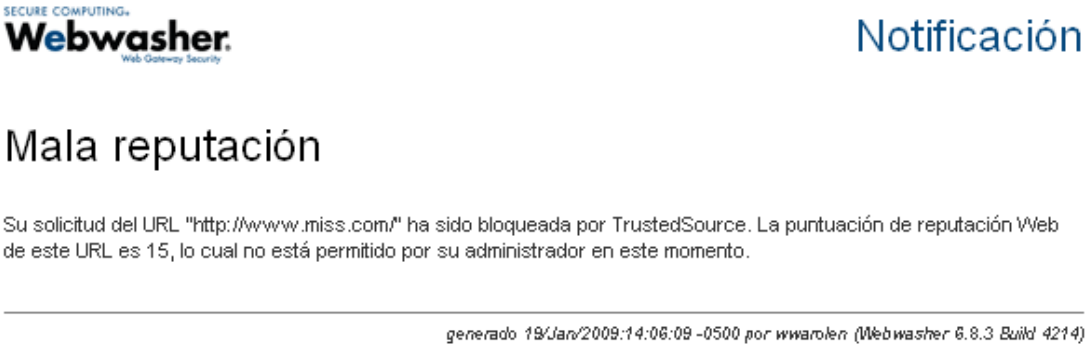

Figura 20. Bloqueo Sitio Mala Reputación

- La descarga del archivo eicar.exe no es permitida, si deseo permitirla se debe crear un Media Type Whitelist en Media Type Filtres.

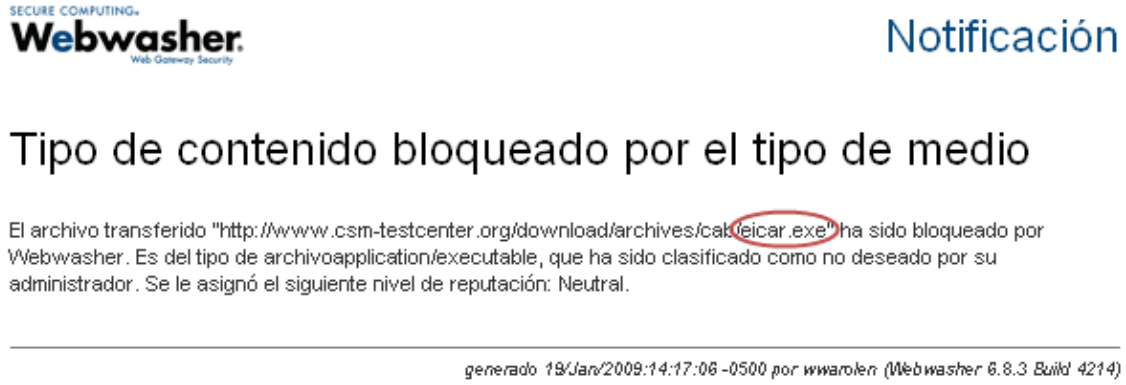

Figura 21. Bloqueo por Tipo de Contenido

- El archivo que estoy tratando de descargar contiene o esta infectado con un virus.

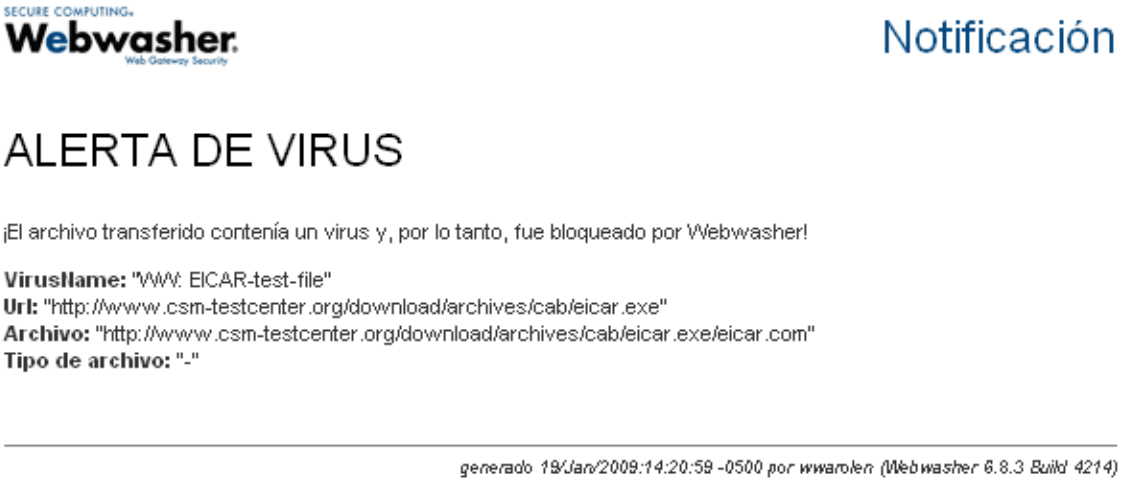

Figura 22. Bloqueo por Virus

- La página no esta disponible, el sitio es erróneo o webwasher no puede alcanzar el sitio.

Figura 23. Notificación no Conexión

6.2.2 Cuadro de Comparación de Equipos

	SECURE COMPUTING	Websense	SurfControl	BlueCoat Systems	McAfee	symantec	TREND MICRO	Aladdin	Barracuda Networks	StBernard
Appliance	✓	partner	✓	✓	✓	✓	✓	partner	✓	✓
Software	✓	✓	✓	-	-	-	✓	✓	-	-
Pass By/Through	✓/✓	✓/✓	✓/✓	-/✓	-/✓	-/✓	-/✓	-/✓	-/✓	-/✓
Anti-Virus	✓	-	✓	✓	✓	✓	✓	✓	✓ (no name)	- (not on iPrism)
Anti-Spam	✓	-	✓	-	✓	✓	✓	✓	- (separate appliance)	- (not on iPrism)
Anti-Spyware	✓	✓	✓	✓	✓	✓	✓	✓	✓	(✓)
ProActive Solution	✓	-	-	-	-	-	-	✓	-	-
E-mail Content	✓	-	✓	-	✓	✓	✓	✓	- (separate appliance)	- (not on iPrism)
Web Content	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SSL Content	✓	-	-	✓	-	-	partner	partner	-	-
Bandwidth Mgmt.	category only	✓	category only	✓	category only	category only	category only	category only	category only	category only

Figura 24. Comparación Equipos de Navegación Web

La Figura 24 muestra las diferentes marcas de equipos para el control de navegación Web de usuarios.

Entre las marcas más reconocidas se encuentra:

Secure Computing como líder del mercado por sus características de seguridad, Websense, BlueCoat, son competidores directos y con características similares.

Los únicos equipos que cuentan con sistema a base de Reputación son Secure Computing y Iron Port.

Otros equipos que ofrecen control de contenido de navegación son SurtControl, McAfee, Sycmantec, trendMICRO, Aladdin, Barracuda, StBernard.

6.2.3 REPORTES

Reportes detallados donde se ve o se puede observar cuales son las categorías más visitadas, cuales son los usuarios con más peticiones, las políticas más

utilizadas, día, hora, y verificar el sitio Web donde los usuarios hacen sus consultas.

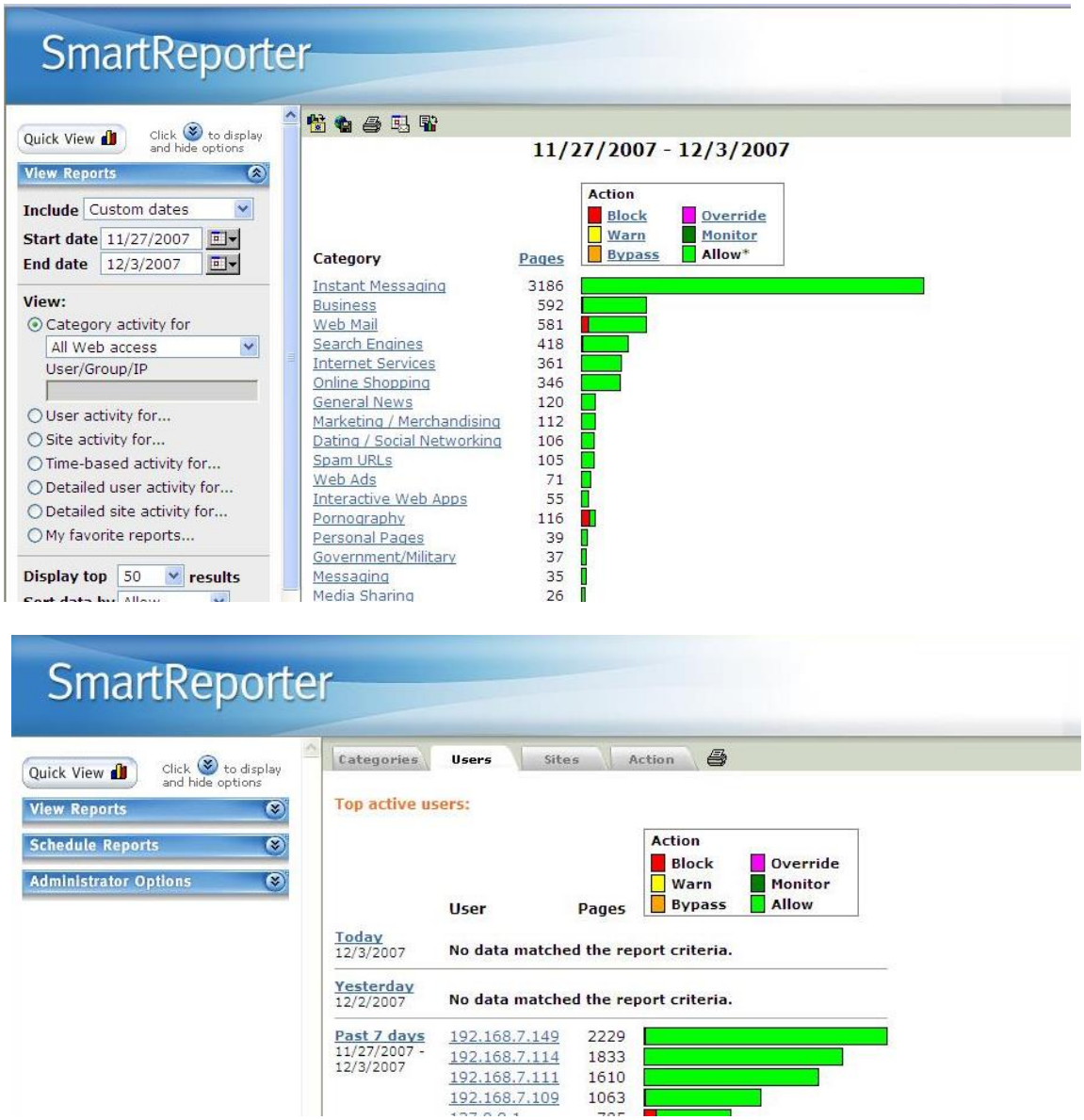

Figura 25. Reportes

7. 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.

- Siempre que a un usuario le salga una notificación de navegación se debe revisar esta para saber porque ha sido denegado el acceso, falla en la verificación de certificado digital o esta haciendo una petición a un sitio de mala reputación.

- Para personalizar las notificaciones de navegación el logo y el texto se debe parar los servicios de opt webwasher-csm para que los cambios realizados sean tomados.

- Para los cambios en las políticas creadas de navegación a un determinado usuario este cambio debe hacerse en la política que el usuario pertence.

- La instalación del equipo de filtrado web debe ir en la lan.

- Si existen varios controladores de dominio y estos están en diferentes redes se debe habilitar el puerto 9531 para el intercambio de usuario y password, este intercambio se hace de forma segura utilizando protocolo SSL.

8. RECOMENDACIONES

Los equipos encargados de manejar el cifrado, manejan otros módulos entre ellos firewall y filtrado Web básico, si se desea robustecer la solución se pueden configurar estos para crear reglas para permitir o denegar servicios o protocolos.

Pero no siempre los equipos y dependiendo del fabricante soportan la activación de los módulos adicionales de seguridad por ende se va a tener degradación en el performance de los equipos.

Si se desea se puede implementar a los usuarios tarjetas de proximidad o Token para la autenticación de los usuarios de una forma segura a sus puestos de trabajo o Computadores personales.

Instalar equipos dedicados para el cifrado de correo.

Antes de cada instalación o desarrollo del proyecto documentarse y conocer la topología de red, servicios, aplicativos y dado el caso los puertos que ulitizan las aplicaciones o servicios de la organización.

Verificar el normal funcionamiento de todos los dispositivos de red, así como los tiempos de respuesta de los canales que disponga cada organización.

9. TRABAJO FUTURO

Implementar equipos para el análisis de vulnerabilidades de red.

Correlacionadores de Log, hay de diferentes características y funcionalidades unos dedicados únicamente a firewall y otros a recolectar los log de los diferentes dispositivos de la red para sacar un reporte detallado de los eventos que se tienen en un determinado tiempo o en tiempo real, además estos reportes dependiendo el fin o programación de reporte nos sirven para solucionar posibles fallas en la red o en la infraestructura de red.

Single Sign One hay equipos dedicados al manejo de contraseñas para los administradores de red o los encargados de red es indispensable la implementación de este tipo de dispositivos ayudan con el manejo de múltiples contraseñas y aplicaciones este tipo de solución nos permite tener la granularidad de utilizar autenticación fuerte por ejemplo utilizar token.

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.

10. GLOSARIO

Trusted Source

Sistema a base de reputación por URL, IP y Dominio y es el resultado al acumular datos de más de 7000 sensores ubicados en 51 países, TrustedSource crea un perfil de toda la actividad de los "remitentes" en Internet y luego utiliza este perfil para observar desvíos del comportamiento esperado. A continuación, el sistema genera una "clasificación de reputación" basada en el comportamiento del host de envío. [TRUS2008]

RSA[CRSA2008]

El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado.

Firewall[FIRE2008]

Un firewal es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewal examina el tipo de servicio al que corresponde, como pueden ser el web. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

VPN IPsec[VPNI2008]

IPsec es un protocolo que está sobre la capa del protocolo de Internet (IP). Le permite a dos o más equipos comunicarse de forma segura, puede utilizarse para cifrar directamente el tráfico entre dos equipos (conocido como modo de transporte) o para construir “túneles virtuales” entre dos subredes, que pueden usarse para comunicación segura entre dos redes corporativas (conocido como modo de túnel). Este último es muy conocido como una red privada virtual (Virtual Private Network, o VPN)

11. BIBLIOGRAFÍA

11.1 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)

[CODE2009]www.codesandciphers.org.uk(Navegada el 25 de abril de 2009)

[UAZU2009]http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/modelo_osi3.htm(Navegada el 27 de Abril de 2009)

[ITLN2009]http://www.itl.nist.gov/fipspubs/fip46-2.htm(Navegada el 25 de Abril de 2009)

[CSRC2009]http://csrc.nist.gov/(Navegada el 23 de Abril de 2009)

[RSAE2009]http://www.rsa.com/rsalabs/node.asp?id(Navegada el 25 de Abril de 2009)

[HOME2009]http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html#machine(Navegada el 2 de Mayo de 2009)

[SUPP2009]http://support.microsoft.com/kb/246071/es(Navegada el 2 de Mayo de 2009)

[ISOO2009]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103(Navegada el 23 de abril de 2009)

[RSAR2009]http://www.rsa.com/rsalabs/node.asp?id=2157(Navegada el 24 de febrero de 2009)

[ITLN2009]http://www.itl.nist.gov/fipspubs/fip180-1.htm(Navegada el 24 de febrero del 2009)

[ELRI2009]http://www.elrinconcito.com/articulos/Des_Aes/Des_Aes.htm(Navegada el 19 de mayo de 2009)

[CONT2009]http://www.continuitycentral.com/feature0429.htm(Navegada el 23 de abril de 2009)

[FIMD2009]www3.fi.mdp.edu.ar/electronica/articulos/Criptografia.doc(Navegada el 19 de mayo de 2009)

[IMPR2009]http://www.imprivata.com/onesign_sso(Navegada el 10 de enero de 2009)

[NETC2009]http://www.netclarity.com/enterprise-nacwall.html(Navegada el 23 de abril de 2009)

[COMP2009]http://computer.howstuffworks.com/digital-signature.htm(Navegada el 10 de Junio de 2009)