Universidad Central de Venezuela
Facultad de Ingeniería
Escuela de Ingeniería Eléctrica

EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD EN LOS SISTEMAS DE NOTIFICACIÓN Y REGISTRO DE EVENTOS PARA LA GESTION DE REDES

Ing. Mary July Hernández

TRABAJO DE GRADO PRESENTADO ANTE LA ILUSTRE UNIVERSIDAD CENTRAL DE VENEZUELA PARA OPTAR AL TITULO DE ESPECIALISTA EN COMUNICACIONES Y REDES DE COMUNICACIONES DE DATOS

Tutor:

Prof. Vincenzo Mendillo

Caracas, Octubre de 2004

DEDICATORIA

A Dios que siempre esta conmigo,

A mis padres que los amo.

A mi sobrino, lo más importante de mi vida.

AGRADECIMIENTO

A la ilustre Universidad Central de Venezuela.

Agradezco a Dios por darme salud y fe para culminar este proyecto.

A mis padres Maritza y Julio Hernández, por todo el apoyo y por el sacrificio que han tenido para la culminación de mi especialización.

A Gipsy Azuaje de la Secretaria de Postgrado, por toda su paciencia y por su bella amistad.

Especial agradecimiento a mi amigo Henry Vega por todo su apoyo, cariño, dedicación y paciencia durante el periodo de la especialización.

Especial agradecimiento a mi Tutor Académico Profesor Vincenzo Mendillo por todo su apoyo, compresión, paciencia, dedicación y amistad que me ha brindado siempre durante todo el periodo de la especialización, permitiendo culminar esta meta en mi vida.

A Jenny Morales, Juan Ruz, Ney López y Reinaldo Chirinos por todo su apoyo cariño y compresión para seguir adelante en este reto.

Al comité de Estudios de Postgrado, en especial al Prof. Jean Pierre Chassande quien ya no se encuentra con nosotros, pero me dio la oportunidad de realizar la especialización.

A la profesora Maria Álvarez de Marco Regulador de las Telecomunicaciones, por la oportunidad que me brindó en un momento de crisis.

Y a todas aquellas personas que de alguna forma colaboraron en la terminación de la misma.

A todos muchísimas gracias!!

RESUMEN

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
POSTGRADO EN ESPECIALIZACIÓN EN COMUNICACIONES
Y REDES DE COMUNICACIÓN DE DATOS

EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD EN LOS SISTEMAS DE NOTIFICACIÓN Y REGISTRO DE EVENTOS PARA LA GESTION DE REDES

Autor: Ing. Mary July Hernández
Tutor: Prof. Vincenzo Mendillo
Año: 2004

RESUMEN

Los sistemas de gestión de redes proveen facilidades para alertar condiciones críticas como congestión, fallas o ataques de intrusos. Para este fin se suelen utilizar los protocolos Syslog y SNMP, los cuales sin embargo adolecen de ciertas fallas en lo que a seguridad se refiere.

En este trabajo se estudian y evalúan los sistemas de notificación y registro de eventos basados en Syslog y SNMP con el fin de buscar posibles mejoras de seguridad que sean relativamente fáciles de implantar.

Se describen las pruebas llevadas a cabo con varios protocolos y tecnologías (PPTP, L2TP/IPSec, Kiwi Secure Tunnel y OpenVPN), los cuales establecen un canal seguro ("túnel") entre la fuente y el destino de los mensajes de notificación, creando así lo que se conoce como VPN (*Virtual Private Network*).

Además se explica la utilización de *máquinas virtuales* y *redes virtuales* para realizar dichas pruebas. Una máquina virtual es esencialmente una forma de tener otra computadora corriendo dentro de la máquina física real, en forma simultánea e

independiente. Con las redes virtuales creadas con máquinas virtuales se pueden probar los protocolos y tecnologías para túneles, sin requerir recursos de hardware adicionales.

Entre las diferentes tecnologías de túneles estudiadas y probadas, la que representa la mejor alternativa para la mejora de la seguridad en los mensajes de notificación y registros de eventos es el Protocolo de Túnel de Punto a Punto (PPTP), debido a su facilidad de uso y transparencia a los protocolos transportados.

Para trabajos futuros se recomienda probar y evaluar la nueva versión 3 de SNMP, la cual incorpora fuertes mecanismos de seguridad, aunque todavía no están fácilmente disponibles agentes SNMPv3.

También se recomienda probar y evaluar las distintas propuestas de Syslog seguro, tales como SDSC Secure Syslog, syslog-ng y msyslog, entre otros, las cuales ofrecen la posibilidad de utilizar el protocolo TCP para la transmisión de los mensajes, funciones avanzadas de filtrado y el registro de los mensajes directamente en una base de datos tipo SQL.

TABLA DE CONTENIDO

INDICE DE FIGURAS Y TABLAS

CAPITULO I - TEMA DE INVESTIGACION

I.1 Planteamiento del Problema

La proliferación de Internet así como el crecimiento de redes corporativas han creado una creciente necesidad de notificar y registrar los eventos rutinarios o extraordinarios que ocurre día a día, a fin de que el personal técnico y los propios usuarios tengan acceso a información relativa a las condiciones de la conectividad, errores, fallas, alarmas, intentos de acceso, violación de la seguridad y cualquier otra información relevante sobre la red y los equipos.

Los sistemas operativos, las aplicaciones y los procesos que corren en los sistemas informáticos pueden enviar notificaciones sobre su propio estado y para indicar que han ocurrido ciertos acontecimientos. Estos mensajes de notificación son de diferentes categorías y prioridades a fin poder distinguir más rápidamente los problemas severos de las advertencias que no requieren atención urgente. Los mensajes se envían usualmente a un sistema centralizado donde aparecen en la consola del operador y también se guardan en un registro (log) durante un cierto periodo de tiempo.

Casi todas las actividades realizadas en un equipo (como un router o firewall) o en sistema operativo (como Windows o Unix) son susceptibles de ser, en mayor o menor medida, monitoreadas y registradas: desde las horas de acceso de cada usuario al sistema hasta las páginas Web más frecuentemente visitadas, pasando por los intentos fallidos de conexión, los programas ejecutados o incluso el tiempo de CPU que cada usuario consume. Obviamente esta facilidad para recoger información tiene muchas ventajas. Por ejemplo es posible detectar un intento de ataque nada más al producirse el mismo, así como también detectar usos indebidos de los recursos o actividades sospechosas.

Sin embargo, también existen desventajas, ya que la gran cantidad de información que se genera puede crear confusión y hacer más difícil detectar problemas. Además puede causar mucho tráfico y crear archivos de registro (logs) muy voluminosos, todo lo cual puede ser aprovechado para ataques de negación de servicio.

Entre los números sistemas de notificación y de registro de eventos que existen, Syslog es uno de los más utilizados. Está descrito en la RFC3164 y originalmente fue diseñado por la Universidad de California para su sistema BSD Unix, pero la versatilidad del mismo lo han convertido en un componente ubicuo en la mayoría de versiones

modernas de Unix y en toda clase de equipos y sistemas donde las comunicaciones están basadas en TCP/IP. A pesar de los años que han transcurrido desde la aparición de Syslog, éste ha evolucionado relativamente poco debido a que ha sido siempre un servicio extremadamente flexible.

En términos muy simples, el protocolo Syslog proporciona un medio de transporte para permitir que una máquina envíe mensajes de notificación de sucesos a través de redes IP. Estos mensajes son enviados a servidores Syslog. La máquina que envía la notificación puede ser una estación de trabajo, un servidor Web o un dispositivo de red tal como switch, router o firewall. Lo importante es que dicha máquina o equipo tenga la capacidad de enviar mensajes en el formato Syslog.

Los mensajes en sí pueden contener cualquier clase de información que la máquina esté configurada para generar y enviar. Por ejemplo, es común que un router envíe un mensaje Syslog cuando una o más de sus interfaces cambien de estado (de up a down o viceversa). Un router se podría también configurar para generar mensajes Syslog cuando se viole la lista de control de acceso (ACL). Es importante observar que el dispositivo que envía el mensaje Syslog debe poder establecer conectividad de la red con el servidor Syslog y que éste debe entender el formato de los mensajes Syslog. La entrega del mensaje Syslog entre el dispositivo que envía y el servidor Syslog no está garantizada, ya que Syslog es un protocolo tipo “mejor esfuerzo”.

La arquitectura de un sistema Syslog consiste de máquinas que generan los mensajes (llamadas “dispositivos” o “remitentes”) y máquinas que reciben los mensajes (llamadas “colectores” o más comúnmente “servidores Syslog”). Un sistema Syslog también puede incluir máquinas (llamadas “relays”) que reciben mensajes de un dispositivo y les transmiten otras máquinas. Algunos dispositivos pueden enviar mensajes Syslog a múltiples colectores y los relays pueden también filtrar mensajes (por ejemplo, remitiendo sólo los mensajes urgentes).

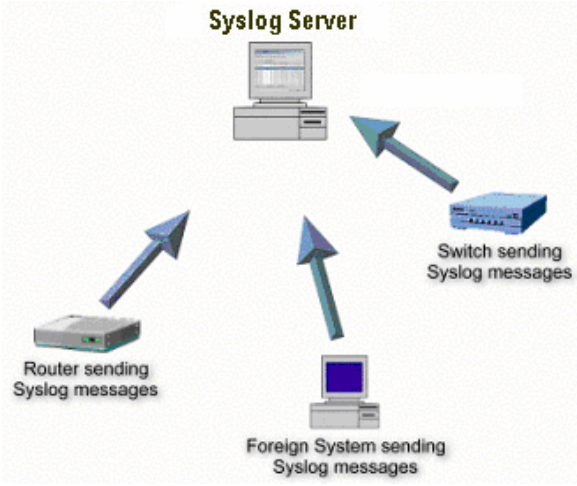


Figura I-1 – Arquitectura de un sistema Syslog

Los mensajes Syslog son transportados generalmente por UDP (User Datagram Protocol), aunque algunos dispositivos y colectores pueden utilizar TCP para mayor confiabilidad, debido a que UDP es solamente un servicio de “mejor esfuerzo”. El puerto de destino asignado a Syslog es 514. Cuando se usa TCP, el puerto de destino es usualmente 1468.

Además de Syslog, hay otro mecanismo que se utiliza comúnmente para notificar eventos y es mediante los traps de SNMP (*Simple Network Management Protocol*). Este es un protocolo del conjunto TCP/IP diseñado para facilitar la gestión de dispositivos de red, tales como servidores, estaciones de trabajo, routers y switches. La arquitectura de SNMP se muestra en la figura siguiente e incluye 3 componentes básicos.

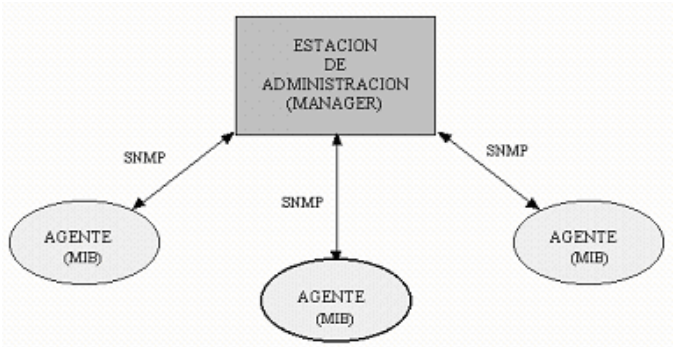


Figura I-2 – Arquitectura de un sistema SNMP

1. *MIB (Management Information Base)*: contiene los objetos, es decir las variables, que pueden ser monitoreadas o modificadas. Las variables MIB se identifican unívocamente mediante un código OID (object identifier), por ejemplo, 1.3.6.1.2.1.4.3.
2. *Agente*: software residente en el equipo a ser gestionado. Cada agente almacena datos de gestión y responde a las peticiones por parte del manager. Los agentes ejecutan dos funciones básicas: monitoreo y modificación de variables MIB. El monitoreo significa examinar los valores de contadores, umbrales, estados y otros parámetros, mientras que modificar significa cambiar los valores de las variables. Los agentes se configuran para pertenecer a ciertos grupos o "comunidades" y así mismo los managers están configurados para monitorear y recibir mensajes SNMP de determinadas comunidades. El nombre de la comunidad es parte de un mensaje SNMP.
3. *Manager (Gestor*): software residente en la estación de gestión la red. El gestor hace solicitudes al agente utilizando mensajes SNMP. Los managers corren en una estación de administración y usualmente proveen una interfaz gráfica con el usuario, mostrando por ejemplo el mapa de la red y gráficos de la variación en el tempo de las variables MIB.

SNMP es un protocolo orientado a datagrama que, al igual que Syslog, utiliza UDP como mecanismo de transporte y así se elimina la necesidad de establecer una conexión antes de la operación del protocolo. Además, por ser orientado a datagrama, no tiene conexión que pueda fallar bajo condiciones adversas. Utiliza dos puertos UDP: el puerto 161 lo abren los agentes para escuchar las peticiones del manager (mensajes Get, GetNext y Set) y también los abre el manager para recibir las respuestas de los agentes (Response). El manager también abre el puerto 162 para recibir los traps de los agentes.

Un trap es un mensaje especial generado por un agente para notificar al manager la ocurrencia de algún evento significativo. El mensaje incluye la identificación del agente que generó el trap, cuándo se generó y de qué tipo de evento se trata.

SNMP tiene varios problemas de seguridad. Por ejemplo, no existe la posibilidad de asegurar que los mensajes SNMP recibidos por un agente provengan realmente de la

estación de gestión y no de otra estación que haya falsificado su dirección IP. Por tal razón en principio es posible alterar las variables MIB de una máquina desde cualquier estación a través de un mensaje SetRequest, averiguando el nombre de la comunidad. Por otro lado SNMP no define el mecanismo por el cual un trap debe ser enviado ni explica qué información debe enviar el agente como parte del trap; sólo se especifica que debe incluir “información interesante”. Por ello los traps son específicos a cada implantación. Además sólo se reportan en eventos pre-programados: cuando ocurre una falla diferente, si el trap la reporta, lo hará incorrectamente.

I.2 Objetivos de la Investigación

I.2.1 Objetivo General

Evaluación de los mecanismos de seguridad en los sistemas de notificación y registro de eventos para la gestión de redes.

I.2.2 Objetivos Específicos

- Analizar el funcionamiento de los protocolos Syslog y SNMP como se usan actualmente.
- Realizar pruebas en una red experimental para comprobar las debilidades de dichos protocolos en lo que a seguridad de refiere
- Proponer soluciones para mejorar la seguridad de Syslog y SNMP.
- Evaluar y comparar las distintas soluciones y recomendar la mejor solución.

I.3 Metodología

Para realizar este trabajo de grado se utilizó una metodología basada en técnicas, instrumentos y procedimientos propios de la investigación científica, ya que se trata básicamente de un proyecto de investigación y en tal sentido se distingue de la metodología basada en proyectos factibles, típicos de la ingeniería.

Diferencias entre “proyecto de investigación” y “proyecto factible”	
Proyecto de Investigación	Proyecto factible
Plantea un problema de conocimiento (algo que se desconoce).	Plantea un problema de tipo práctico, generalmente determinado por una necesidad.
Se plantea objetivos de investigación, lo que refleja los aspectos a conocer.	Se traza objetivos de acción: tareas, actividades, procesos.
Requiere un marco teórico que fundamente la investigación a realizar.	No necesariamente requiere de postura teórica. Hace mucho énfasis en la justificación de proyecto.
Puede formular hipótesis.	Formula propuestas de acción y/o modelos operativos como alternativa de solución.

La metodología utiliza técnicas, instrumentos y procedimientos propios de la investigación científica.	La metodología varía según la fase y naturaleza del proyecto.
Los elementos básicos que se incluyen en un proyecto de investigación son: − Planteamiento del problema − Objetivos − Justificación − Marco Teórico − Metodología	Los elementos básicos que se incluyen en un proyecto factible son: − Objetivos − Justificación − Diagnóstico de necesidades − Formulación del modelo o propuesta − Análisis de su factibilidad
En un proyecto de este tipo se investiga.	En un proyecto de este tipo se planifica.

Tabla I -1 – Diferencia entre ”proyecto de investigación” y “proyecto factible”

I.4 Estructura del trabajo

La estructura del presente trabajo especial de grado está organizada de la siguiente manera:

- Capítulo I. Tema de investigación: Se presenta el tema de investigación y se establecen los objetivos que se buscan alcanzar con el desarrollo del mismo.
- Capítulo II. Marco Teórico: La base para el desarrollo del presente trabajo está constituido por los conceptos, conocimientos y tecnologías que fue necesario dominar para lograr los objetivos planteados.
- Capítulo III. Fase Experimental: En este capítulo se expone cada una de las experiencias que se llevaron a cabo durante el desarrollo del trabajo
- Capítulo IV. Conclusiones y recomendaciones: En esta parte se discuten los resultados obtenidos y se propone una solución para mejorar la seguridad en los sistemas actuales de notificación y registro de eventos.

El presente capítulo tiene como finalidad sentar las bases teóricas de la investigación, a través de los diferentes conceptos involucrados con los mecanismos de seguridad de los sistemas de notificación y registro de eventos para la gestión de redes.

II.1 Gestión de la Seguridad en Redes

La gestión de redes tiene como finalidad planificar el uso de los recursos disponibles y necesarios para mantener un servicio de red continuo y eficiente. Los recursos manejados por la gestión de redes incluyen el hardware y las aplicaciones respectivas, así como también consideraciones específicas acerca del personal, procedimientos, programas y sistemas. El propósito principal de la gestión de redes es monitorear y ajustar proactivamente el desempeño de las redes. Las actividades realizadas para asegurar el buen funcionamiento de la red pueden ser agrupadas en pequeñas áreas de administración, relacionadas con la configuración tanto física como lógica de los componentes de la red, el diagnóstico y la resolución de problemas, la contabilización de recursos y la seguridad.

La gestión de la seguridad se ha convertido en una de las áreas más importantes en la gestión de redes; entre sus objetivos principales está diseñar y mantener un buen sistema de seguridad tanto físico como lógico para proteger los componentes y la información manejada en la red, así como las otras áreas de la gestión de redes. La gestión de seguridad consta de dos niveles:

Seguridad Física: involucra consideraciones como la protección de todos los recursos de la infraestructura de la red como estructuras de apoyo, enlaces de comunicación, hosts, servidores importantes y máquinas claves de alteraciones y conexiones no autorizadas. Los equipos de red deben estar en un cuarto o en un lugar en el cual se pueda restringir la entrada a través de tarjetas magnéticas, limitar el número de personas con acceso y hasta ofrecer un registro de identidad y la hora en que las personas entran a la sala.

Seguridad Lógica: incluye la protección de los datos y el software de la red de posibles incidentes, que van desde la infección de virus hasta el robo o modificación de éstos,

mediante el uso de medidas y controles como passwords, logins y grupos de usuarios. La seguridad lógica implica también el establecimiento de estrategias de respaldo y recuperación de datos que permitan minimizar el tiempo de restablecimiento de los servicios de la red.

Cuando la seguridad de datos comenzó a surgir como una necesidad en la gestión de redes, la reacción inicial de muchos gerentes del área de tecnología de información y de muchos profesionales del área de sistemas de información consistió en la adquisición de herramientas sofisticadas, descuidando la adopción de buenos y sólidos controles gerenciales, a través de la implantación de políticas y procedimientos de seguridad. Para lograr un buen nivel de protección en las redes es necesario diseñar e implantar políticas de seguridad que incluyan aspectos tecnológicos y gerenciales.

La gestión de redes ha adquirido actualmente un lugar importante en el desarrollo exitoso de las actividades diarias de la mayoría de las organizaciones. Estas dependen del buen funcionamiento de los sistemas, la disponibilidad de los servicios y de los datos. Hoy en día, las empresas necesitan un equipo de trabajo dedicado a la gestión de la red y cada vez más aumenta la necesidad de protegerla, colocando a la seguridad entre las prioridades principales de cualquier empresa.

En una red, la seguridad implica reforzar cuatro aspectos básicos: confidencialidad, integridad, disponibilidad y autenticidad.

Confidencialidad

La confidencialidad permite proteger la información del acceso por parte de personas no autorizadas. Este objetivo de la seguridad busca asegurar que únicamente las personas que requieren acceso a cierta información sean las que la posean. En algunas situaciones, cuando se maneja información secreta y confidencial, las personas deben tener acceso sólo a la información necesaria para realizar su trabajo, protegiendo de esta forma la confidencialidad de dicha información.

La principal amenaza en una red de computadoras viene de personas no autorizadas que consiguen, de alguna manera, acceder a alguno de los elementos de la red violando de esta forma su confidencialidad. Por lo tanto, un objetivo básico de un sistema de seguridad es impedir los accesos no autorizados.

El control de acceso es una de las medidas de protección más utilizada para proteger la confidencialidad, ya que permite que personas específicas tengan acceso a la información o a determinados recursos. Comúnmente, el control de acceso se realiza a través del uso de passwords, los cuales restringen la entrada a personas no autorizadas. Uno de los principios fundamentales en la seguridad de la información es la protección de estos passwords, ya que la debilidad más explotada es su violación. La utilización de passwords fuertes, tarjetas inteligentes o tokens de acceso, representa el primer nivel de defensa en el control de acceso.

Otro aspecto relacionado con el control de acceso es la restricción de recursos, ya que una vez que las personas han sido correctamente identificadas, se debe verificar qué autorizaciones de acceso poseen. Normalmente los empleados del departamento de Recursos Humanos tienen acceso a información del empleado, como su cumpleaños y dirección, pero únicamente personas autorizadas pueden tener acceso a la información sobre las compensaciones y bonos recibidos; a su vez, sólo ciertos individuos pueden realizar modificaciones a dicha información. El control de acceso puede ser implementado en forma paralela brindando acceso a cierta información y negando el acceso a otra.

Integridad

La integridad asegura que la información no ha sido alterada, es decir que los datos almacenados son exactamente los mismos a los introducidos inicialmente o modificados por última vez. La pérdida de la integridad puede ser causada por errores humanos, actitudes intencionadas o simplemente por eventos catastróficos. Las consecuencias de utilizar la información incorrecta en un momento determinado pueden ser desastrosas, en la mayoría de los casos la modificación inapropiada de ésta puede inutilizarla o, en el peor de los casos, causar daños irreparables. Es por ello que se deben realizar esfuerzos para asegurar la exactitud y propiedad de la información en todo momento.

En situaciones en las cuales la validez de la información es vital, es necesario diseñar controles y chequeos que aseguren su exactitud y veracidad.

Disponibilidad

La disponibilidad de la información asegura que la información no será negada a los usuarios autorizados, previene la desaparición o inaccesibilidad de recursos, brindando protección y recuperación en caso de calamidades.

La "negación de servicios" es la imposibilidad de acceder los recursos requeridos. La mayoría de los ataques intencionados a los sistemas informáticos persiguen imposibilitar el acceso a los datos o el robo de la información; sus razones son diversas, y van desde simples motivaciones políticas a intereses económicos. En algunos casos, las cuentas de correo electrónico son cargadas con mensajes no solicitados, conocidos como “spams”, con la idea de afectar el servicio. En otros casos, estos ataques pueden formar parte integral de esfuerzos coordinados con el objetivo de hacer que el sistema central falle.

Reforzar la seguridad física de una red o sistema es una forma de proteger la disponibilidad. Al limitar el acceso físico y restringir el contacto con las máquinas vitales o con los recursos de información, se pueden reducir considerablemente incidentes no deseados, accidentes y actitudes mal intencionadas. También es necesario proteger electrónicamente los recursos, ya que la presencia de dominios públicos como Internet implica la existencia de varios puntos de acceso los cuales deben ser custodiados fuertemente.

El cortafuego (o firewall) es uno de los controles de seguridad más utilizados; actúa como un guardia entre dos redes regulando y restringiendo la información que fluye entre ellas.

Otro aspecto importante es asegurar que los recursos estén disponibles cuando y donde se necesitan. Los respaldos de información, los suplidores de energía ininterrumpibles (UPS) y la implementación de sistemas redundantes aseguran la disponibilidad. El almacenamiento remoto de los datos vitales asegura la recuperación de ésta si la seguridad local es violada. Por otro lado, el respaldo de los servidores permite asegurar la continuidad del trabajo, si la seguridad de la red principal se ve afectada. Así como estas medidas protegen la disponibilidad de la información, también es importante cuidarla de intrusos y mantener su confidencialidad.

Autenticidad

La autenticidad también permite proteger la información del acceso por parte de personas no autorizadas. Con ésta se busca asegurar que la persona quien dice ser el que está requiriendo el acceso sea la persona verdadera. Una amenaza muy importante en una red de computadoras viene dada por personas mal intencionadas que intentan hacerse pasar por las personas que tienen autorización de entrada a la red violando de esta forma la seguridad de la información. Es por ello que, otro objetivo imprescindible de un sistema de seguridad es impedir ese tipo de falsificación.

El control de autenticidad es una de medida de protección necesaria para proteger la veracidad de los usuarios. Comúnmente, el control de autenticidad se realiza a través del uso de servidores de autenticación, los cuales evitan la entrada a personas que intenta falsificar la identidad de otra. Las estrategias de seguridad deben ser enfocadas hacia estos cuatro objetivos, la confidencialidad, integridad, disponibilidad y autenticidad.

La formulación y planificación de la seguridad debe basarse en las necesidades del negocio u organización, para así determinar el énfasis a dar a cada uno de los objetivos de la seguridad. Por ejemplo, las políticas de seguridad de un sistema de defensa nacional brindarán mayor énfasis a la confidencialidad, ya que la información estratégica y clasificada debe ser protegida. Por lo contrario, el sistema de transferencia de un banco tiene como necesidad principal la integridad, ya que las cuentas monetarias deben ser exactas. Por último, un sistema de emergencia médica se enfocaría a la disponibilidad, ya que la información y los recursos deben estar listos para usar en cualquier lugar y momento.

II.2 Amenazas y Riesgos

Los datos y la información están constantemente expuestos a situaciones de peligro, representadas por amenazas que buscan alterar los objetivos de la seguridad de la información. Una amenaza es todo evento adverso que puede afectar al activo que se está protegiendo; en los sistemas de seguridad la amenaza representa cualquier circunstancia que potencialmente puede causar pérdidas o daños. Las amenazas accidentales son resultado de desastres naturales, fallas de equipos o errores

humanos. Los mecanismos de seguridad previstos en la mayoría de los ambientes computacionales han sido tradicionalmente dirigidos hacia estos tipos de riesgos. Actualmente, la amenaza más significativa para la propiedad intelectual de una organización son los empleados - actuales, nuevos y temporales - contratistas, consultores y proveedores. Mucha información en las organizaciones es divulgada o vendida a la competencia por empleados que se consideraban confiables. Otros empleados son seducidos o engañados para que entreguen los secretos de la organización. En la siguiente figura, que muestra la frecuencia de incidentes de seguridad, y se puede observar que las mayores amenazas están dadas por las fallas de hardware y la actitud de los empleados.

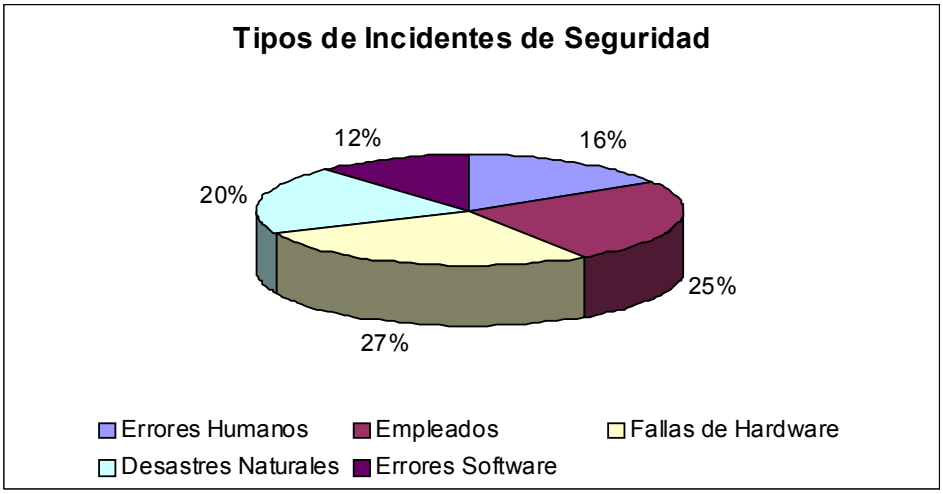


Figura II-1 – Incidentes de seguridad

Fuente: Farley, M., Stearms, T. y Hsu, J. (1997)
Guía de Seguridad e Integridad de Datos. (p.232)

Las amenazas, según Broder (1984), se pueden materializar a través de las siguientes acciones:

Manipulación de Información:

Este es uno de los aspectos más importantes y delicados en la seguridad de la información, ya que ataca la propia integridad. La utilización indebida de la información puede generar fraude o malversación de fondos, pérdidas de ingreso, pérdida de

activos, uso indebido de ingresos, paralización de actividades, entre otros. Una persona o empleado, en su intención de tomar provecho personal, puede realizar cualquiera de las actividades mencionadas anteriormente al modificar la información sensible. Lo más delicado es detectar la ocurrencia de un evento de este tipo y las consecuencias que podría generar la colocación de datos incorrectos en los sistemas.

Revelación de Información:

La revelación de la información consiste en la acción de dar a conocer cierta información importante para la organización. Esto puede ser realizado de manera intencional o simplemente por descuido al manejar ciertos documentos, reportes o datos de la misma. Esto también implica que cualquier persona podría realizar consultas indebidas a la información, usar indebidamente reportes o programas no autorizados, llegando a causar la pérdida de una posición competitiva en el mercado, problemas legales y pérdida de la confianza en la organización.

Pérdida o Interrupción de Operaciones:

Actualmente los sistemas de computación y las redes son parte fundamental de las operaciones del negocio y funcionan como repositorios principales de información. La pérdida de información o una pequeña interrupción en las operaciones de dichos sistemas podrían desencadenar situaciones de mucho riesgo para la organización. Por ello es importante prever posibles desastres, siniestros, sabotajes, errores, omisiones y virus. Cualquiera de estas eventualidades causaría retardo en los servicios a los usuarios, pérdida indirecta de activos, a través de oportunidades desaprovechadas en los negocios, pérdida o modificación de datos irremplazables, inclusive fallas en la detección de actividades no autorizadas en los sistemas.

Acciones Legales:

Básicamente, las acciones legales en contra de una organización se podrían resumir en demandas por derechos de autor sobre algún programa o aplicación, por copia ilegal de software, revelación de secretos profesionales, demandas por patente de invención. Una acción legal en contra de una empresa podría causar perturbaciones en sus

funciones, reducción de la confianza de usuarios y público en general, publicidad negativa, pérdida de activos, entre otros.

Las acciones realizadas para comprometer la seguridad de la información pueden ser clasificadas en:

- Fabricación: cuando una persona no autorizada introduce o construye información falsa.
- Intercepción: cuando una persona o programa no autorizado ha logrado el acceso a la información.
- Modificación: cuando se ha alterado o forjado la información.
- Interrupción: cuando la información se ha perdido, no está disponible o ha quedado inutilizada.

La siguiente figura muestra cómo las acciones realizadas para comprometer la seguridad actúan sobre el flujo normal de información.

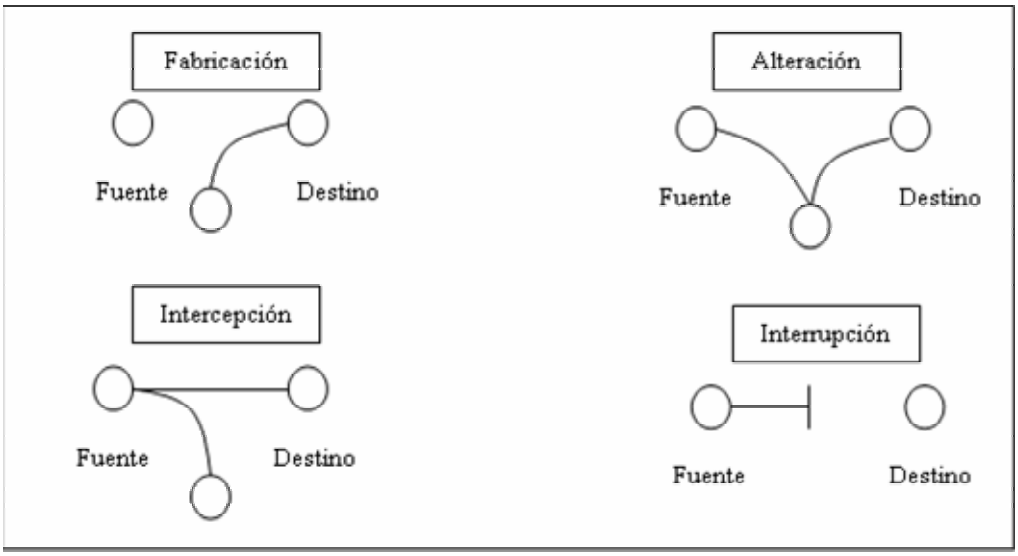


Figura II-2 – Amenazas para la seguridad

Fuente: Stallings,William. (1999). Crytography and Network Security. New Jersey: Editorial Prentice/Hall. (p. 7)

Las amenazas y los riesgos que éstas producen pueden ser atacados de tres maneras, tal como lo expone Martin (1983) en su libro Security, Accuracy and Privacy in

Computer:

1. Minimizando la probabilidad de que ocurran: En este caso lo que se busca es evitar o prevenir la materialización de la amenaza. Para ello es necesario realizar un análisis preliminar que permita identificar cuáles son los posibles riesgos, para así establecer los mecanismos de control de seguridad preventivos.

2. Minimizando el daño si ocurre el riesgo o la amenaza: Se busca limitar el daño o las consecuencias una vez que la amenaza ha ocurrido. Se establecen medidas y controles que permitan actuar mientras ocurren los daños, con el fin de aislarlos ya que es erróneo suponer que las medidas preventivas siempre funcionan.

3. Diseñando un método para recuperarse del daño: Es imprescindible para cualquier empresa o actividad contar con un método de recuperación que permita mantener el funcionamiento de todos los procesos cuando ha ocurrido alguna eventualidad.

Al crear planes de seguridad para establecer medidas y controles de protección, es necesario pensar en estas tres formas de atacar los incidentes inesperados. Un buen plan de seguridad establece medidas y controles que buscan no sólo prevenir los daños sino también enfrentarlos, restringiendo de alguna forma las consecuencias de estos, y define los procedimientos para restaurar el buen funcionamiento de los procesos en casos extremos.

II.3 Monitoreo de Redes y Sistemas

Una actividad fundamental de la gestión de redes es la utilización de software y hardware para monitorear el estado de los equipos de la red y de los medios de transmisión, optimizando el desempeño de la red y tomando acciones para solucionar anomalías en el funcionamiento. La gestión de red atiende a la sinergia entre múltiples equipos. Este enfoque unificador proporciona al usuario la perspectiva de cómo funciona la red en su totalidad y hace posible configurar servicios sobre múltiples equipos. En este nivel, entre las prestaciones básicas se incluyen localización

automática de todos los equipos en la red (descubrimiento), la capacidad para gestionar bloqueos y alarmas, y la capacidad para suministrar servicios como calidad de servicio (QoS) sobre múltiples equipos.

II.4 Syslog

Una de las tareas comunes del los administradores de redes y sistemas es recibir notificaciones vía consola y analizar los archivos de registro de eventos (logs). Estas tareas deben ser realizadas para determinar, por ejemplo, si ha ocurrido una falla o una intrusión. En muchas organizaciones esta información de los eventos es generada y almacenada usando Syslog.

Este protocolo fue introducido por Computer Science Research Group (CSRG) de la Universidad de California en Berkeley como parte del software de de Distribución Berkeley de Unix (BSD). Syslog fue diseñado para reportar eventos del sistema Unix. Estos eventos son almacenados por un proceso y registrados en los archivos de logs en el sistema local, en el sistema remoto o en ambos.

Componentes de Syslog

- *Dispositivo*: genera los mensajes.
- *Colector*: recibe y opcionalmente almacena los mensajes. Comúnmente conocido como demonio de Syslog o servidor.
- *Receptor*: un dispositivo que recibe mensajes Syslog.
- *Relay*: un dispositivo que reenvía mensajes Syslog.

Formato de los Mensajes Syslog

Los mensajes Syslog son transportados generalmente por UDP (*User Datagram Protocol*), aunque algunos dispositivos y colectores pueden utilizar TCP para mayor confiabilidad, debido a que UDP es solamente un servicio de “mejor esfuerzo”. El puerto de destino asignado a Syslog es 514. Cuando se usa TCP, el puerto de destino es usualmente 1468.

Un mensaje Syslog no puede exceder 1024 octetos y contiene tres partes: 1) PRI 2) HEADER 3) MSG.

La parte PRI (*priority*) indica la prioridad del mensaje Syslog y consiste de un número entre 0 y 191 en delimitadores <>, por ejemplo: < 1 >, < 23 > y < 203 >. Este número se forma a partir de dos valores: un código de tipo de servicio, llamado facilidad (facility) y un código de nivel de la severidad (*severity*). Existen códigos estándares para la facilidad para diferentes servicios (e-mail, impresora, red) y que derivan del entorno Unix (por ejemplo "0" es para mensajes del kernel del procesador, "1" para mensajes a nivel del usuario, "2" para mensajes del sistema de correo, etcétera). También hay códigos de severidad: "0" es para emergencia (el sistema está caído), "1" es para alarma (se debe tomar inmediatamente una acción), etcétera. El valor de PRI se obtiene multiplicando el valor de código de la facilidad por ocho y agregando el valor del código de severidad de error (Priority = Facility * 8 + Level). El valor de la facilidad provee una manera de determinar qué proceso en la máquina generó el mensaje.

Debido a que syslog originalmente se creó para sistemas Unix, los nombres de las facilidades reflejan los nombres de procesos y demonios Unix. Local0 - Local7 no se usan en Unix y en cambio se usa en equipos de red. Por ejemplo, los routers Cisco usan Local6 o Local7. La siguiente es la lista de los códigos de la facilidad:

0 kernel messages
1 user-level messages
2 mail system
3 system daemons
4 security/authorization messages
5 messages generated internally by Syslogd
6 line printer subsystem
7 network news subsystem
8 UUCP subsystem
9 clock daemon
10 security/authorization messages
11 FTP daemon
12 NTP subsystem
13 log audit

14 log alert
15 clock daemon
16 local use 0 (local0)
17 local use 1 (local1)
18 local use 2 (local2)
19 local use 3 (local3)
20 local use 4 (local4)
21 local use 5 (local5)
22 local use 6 (local6)
23 local use 7 (local7)

La siguiente es la lista de los códigos o niveles de severidad. La práctica recomendada es usar los niveles “Notice” o “Informational” para mensajes normales:

0 *Emergency:* el sistema esta deshabilitado (Una condición de “pánico” – notificar a todo el grupo técnico con una llamada? (tornado?) – afecta múltiples aplicaciones/servidores/sitos).
1 *Alert*: una acción debe ser tomada inmediatamente (deberá ser corregida inmediatamente – notificar al grupo que puede resolver el problema – por ejemplo si es perdida de la conexión ISP de backup).
2 *Critical*: condiciones críticas (deberá ser corregida inmediatamente, pero indica falla en un sistema primario - corregir el problema CRÍTICO antes de ALERTAR – como por ejemplo perdida de la conexión primaria de ISP.).
3 *Error*: condiciones de error (fallas no urgentes – estas pueden retransmitidas a desarrolladores o administradores; cada item debe ser resuelto en un momento dado)
4 *Warning*: condiciones de alerta (No es un error, pero indica que un error podría ocurrir si una acción no es tomada, ejemplo, el sistema de almacenamiento esta 85% lleno – cada ítem podría ser resulto sin dar tiempo).
5 *Notice*: normal pero es una condición significativa (Hay Eventos inusuales pero no son condiciones de error – podrían ser sumariados en un correo a los

desarrolladores o administradores para problemas potenciales en el site – no requiere de una acción inmediata).

6 *Informational*: mensajes informacionales (Mensajes de operación normal puedes ser recogidos para repórtalo, medir el caudal de proceso y transferencia, etc. - no requiere una acción).

7 *Debug*: mensajes de depuración de niveles (la información útil para los desarrolladores para depurar la aplicación, no es útil durante las operaciones).

La segunda parte (HEADER) de un mensaje Syslog consiste de dos campos: TIMESTAMP y HOSTNAME. El primero (ajustado al formato "Mm. dd hh:mm:ss") sigue inmediatamente a PRI y después de HOSTNAME debe venir un carácter de espacio. HOSTNAME debe ser el nombre del dispositivo o en su defecto la dirección IP. Ejemplo de HEADER: Jul 10 12:00:00 192.168.1.1

La parte MSG (*message*) de un mensaje Syslog es un texto que explica o clarifica el código PRI. Tiene dos subpartes: la etiqueta (TAG) de hasta 32 caracteres (con el nombre del proceso que generó el mensaje Syslog) y el contenido (CONTENT), que contiene el texto en sí. Cualquier carácter no alfanumérico se asume que finaliza el campo TAG y que es el carácter que comienza el campo CONTENT. Ese carácter típicamente es un corchete izquierdo ([), dos puntos (:) o un espacio.

Los siguientes son 2 ejemplos de mensajes Syslog válidos:

<123>Jul 10 12:00:00 192.168.1.1 SyslogGen Este es un mensaje de prueba

<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8

II.5 Kiwi Syslog

Kiwi Syslog y WinSyslog son ejemplos de productos que permiten montar un servidor syslog sobre una PC corriendo el sistema operativo Windows. Kiwi Syslog es un producto de Kiwi Enterprises (*http://www.kiwisyslog.com*) y aunque su función primaria es la notificación de eventos, brinda funciones adicionales, tal como filtrado y otras facilidades que ayudan a localizar averías, monitorear actividades específicas y realizar una variedad de otras funciones con una cantidad mínima de esfuerzo.

Los mensajes syslog se muestran en una tabla o rejilla. Se dispone de 10 display virtuales, y se pueden crear reglas para enviar mensajes seleccionados a una display específico. Por ejemplo, las alarmas y las emergencias se pueden mostrar en el Display 00 y los avisos en el Display 01. Por medio de reglas se controla cómo, donde y cuáles mensajes se procesan.

Los filtros especifican cómo manejar los atributos y los valores del mensaje. Por ejemplo, si el campo de la prioridad se refiere a una notificación del servicio de correo que se reciba durante las horas de trabajo y es de un dispositivo dentro de una gama específica de direcciones IP, entonces se ejecutan las acciones asociadas a esa regla.

Las acciones pueden consistir en tocar una alarma audible, enviar un trap SNMP, enviar un mensaje por e-mail, reenviar el mensaje a otra máquina, guardar el mensaje en un archivo de registro o a un log de eventos de Windows NT/2000/XP.

Kiwi Syslog puede recibir mensajes syslog vía UDP o TCP y también entiende los traps SNMP. Los logs que se crean pueden ser en base horaria, diaria, semanal o mensual.

También pueden ser por prioridad, nombre de las máquinas o direcciones IP.

En la figura siguiente se muestran varios mensajes syslog, incluyendo los de un equipo ADSL Cisco 677.

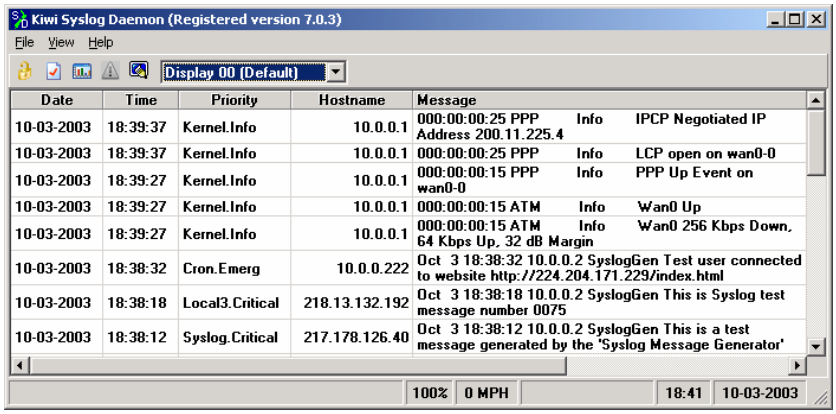


Figura II-3 – Kiwi Syslog Daemon

Para probar Kiwi Syslog en la fase experimental, se requieren algunas otras utilidades. Por ejemplo, *Kiwi Syslog Message Generator* permite efectuar pruebas, enviando mensajes syslog con la dirección IP de origen igual a la de su propia PC u otras direcciones IP. Además se puede utilizar un puerto de destino distinto al 514. Se pueden crear ráfagas de mensajes válidos o inválidos para poner bajo stress al servidor syslog y así ver si reporta correctamente.

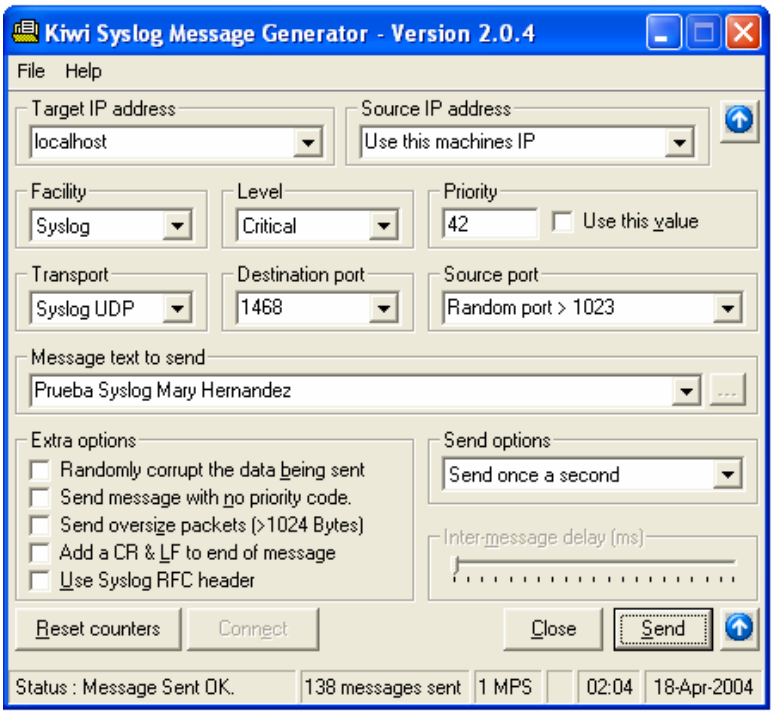


Figura II-4 – Kiwi Syslog Message Generator

Kiwi Secure Tunnel

El túnel seguro de Kiwi es un producto para usar junto con Kiwi Syslog. Recibe, comprime, encripta y asegura los mensajes Syslog.

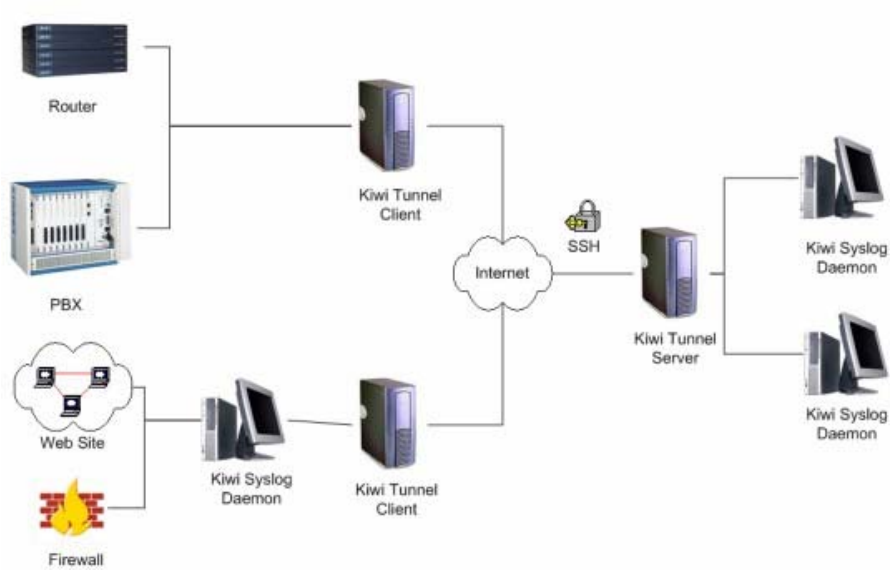


Figura II-5 – Kiwi Secure Tunnel

El Kiwi Secure Tunnel dispone de un cliente y un servidor. El cliente recibe los mensajes de uno o más dispositivos en una red y envía los mensajes en forma segura al servidor, quien a su vez los remite, ya desencriptados, al servidor Syslog.

II.6 SNMP

El protocolo de gestión de red Simple (SNMP) es un protocolo del conjunto TCP/IP diseñado para facilitar la gestión de dispositivos de red, tales como servidores, estaciones de trabajo, routers, switches y otros recursos de la red.

La versión original de SNMP (ahora conocida como SNMPv1) se convirtió rápidamente en el esquema de gestión de red más usado, sin embargo sus deficiencias se pusieron inmediatamente en evidencia:

- *Falta de mecanismos de seguridad:*

  No existe la posibilidad de asegurar que las PDUs SNMP recibidas por un agente provengan de la estación de gestión y no de cualquier otra estación. Por ello es posible alterar las variables MIB de cualquier agente desde cualquier estación a través de una PDU SetRequest.

- *El procedimiento para obtención de tablas es mediante peticiones repetidas, lo que genera demasiado tráfico por la red:*
  SNMP no posee la facilidad de obtener bloques de información en una sola petición a los agentes
- *No es posible la gestión distribuida:*
  SNMP no permite la existencia de varias estaciones de gestión en un solo sistema. Es imposible intercambiar información de gestión entre estaciones gestoras.
- *Limitaciones en el comando Trap:*
  SNMP no define el mecanismo por el cual un trap debe ser enviado ni explica qué información debe enviar el agente como parte del trap; sólo se especifica que debe incluir "información interesante". Por ello los traps son específicos a cada implantación. Además sólo se reportan en eventos pre-programados y cuando ocurre una falla diferente, si el trap la reporta lo hará incorrectamente.

El grupo encargado de desarrollar las especificaciones de SNMP reconoció estas limitantes en el protocolo y poco tiempo después de la estandarización de SNMP, la IETF comenzó las labores para mejorarlo. De este esfuerzo surgió en julio de 1992 un conjunto de documentos referidos como SNMP Seguro (S-SNMP, *Secure SNMP*).

Ese mismo mes, un grupo formado por cuatro de los principales participantes en el desarrollo de SNMP, propuso SMP (*Simple Management Protocol*). SMP incorporaba mejoras funcionales a SNMP incluyendo, con menores modificaciones, las mejoras de seguridad de S-SNMP. Además, SMP incorporaba algunos conceptos de RMON (*Remote Monitoring MIB*), incluyendo las especificaciones de alarmas y eventos, y una técnica simple para crear y eliminar líneas en una tabla. Tomando como base las propuestas S-SNMP y SMP, la IETF formó en otoño de 1992 dos grupos de trabajo para definir un protocolo que sería llamado SNMPv2 (SNMP versión 2).

El grupo conocido como Grupo de Trabajo de SNMPv2 (*SNMPv2 Working Group*) fue el encargado de definir todos los aspectos diferentes al de seguridad, incluyendo SMI, MIB y protocolo. Este trabajo se basó principalmente en SMP y en diciembre de 1992 el grupo publicó un conjunto de nueve documentos propuestos como estándares de Internet. El otro grupo, Grupo de Trabajo de Seguridad de SNMPv2 (*SNMPv2*

Security Working Group), fue encargado de desarrollar los aspectos de seguridad de SNMPv2. El trabajo fue basado sustancialmente en S-SNMP y en enero de 1993 se publicó un documento borrador con los resultados de los trabajos. La figura muestra la evolución de SNMPv2 a partir de SNMP:

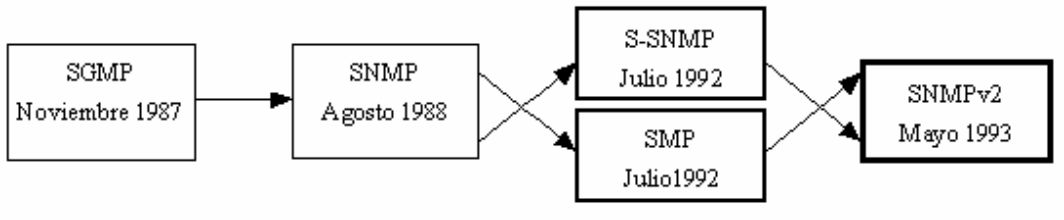


Figura II-6 – Evolución de SNMP

Los mensajes SNMPv2 pueden transportar siete tipos de PDU: aquellas clásicas soportadas por SNMPv1 (GetRequest, GetNextRequest, SetRequest, GetResponse y Trap) y dos nuevas: GetBulkRequest e InformRequest.

GetBulkRequest permite obtener múltiples filas de una tabla con una única petición, mientras que InformRequest permite a una estación administradora enviar información de gestión a otra estación administradora, sin que exista una petición previa.

Con estas dos nuevas PDUs, SNMPv2 elimina dos de las serias limitantes de SNMPv1: la imposibilidad de obtener eficientemente grandes bloques de información y la imposibilidad de implantar esquemas de gestión distribuida.

En cuanto a seguridad se refiere, SNMPv2 incorpora diferentes mecanismos para proteger la información de gestión transportada por los mensajes SNMP. La sinopsis de mensajes MD5 (*Message Digest 5*) crea un extracto (digesto) de los mensaje y verifica el origen del mismo y estándar de Cifrado de Datos (DES, *Data Encryption Standard*) encripta los mensajes SNMP para proteger su contenido.

Desafortunadamente, SNMPv2 no tuvo mucho éxito y sólo se popularizó parcialmente una variante conocida como SNMPv2c, que no incorpora mecanismos de seguridad.

Finalmente en 1999 salió oficialmente a la luz SNMPv3, especificado en las RFC 2570-2575, cuya arquitectura es mucho más robusta desde el punto de vista de seguridad, pero todavía no está muy extendido.

Arquitectura y Componentes Básicos de SNMP

La siguiente figura muestra la arquitectura de SNMP y sus funciones, y cómo estas funciones están relacionadas al modelo OSI.

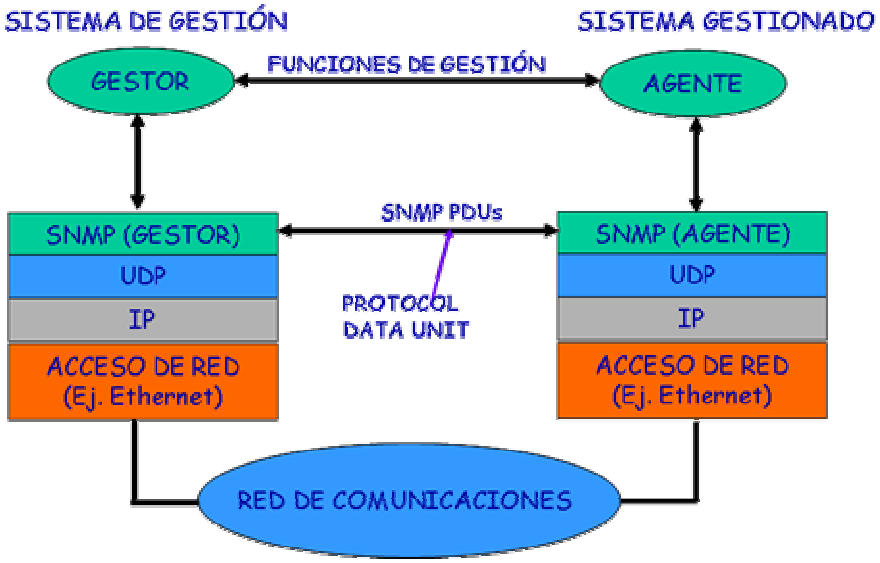


Figura II-7 – Arquitectura de SNMP

Como se puede apreciar en la figura, SNMP corre encima de UDP, por lo que si dispositivo no responde a una solicitud, simplemente se reenvía la solicitud de nuevo. La red física subyacente, es irrelevante y podría ser Ethernet o Frame Relay.

El modelo de gestión de redes que es usado por SNMP incluye los siguientes elementos básicos:

- Manager (Gestor).
- Agent (Agente).
- Base de información de Gestión (MIB - *Management Information Base).*

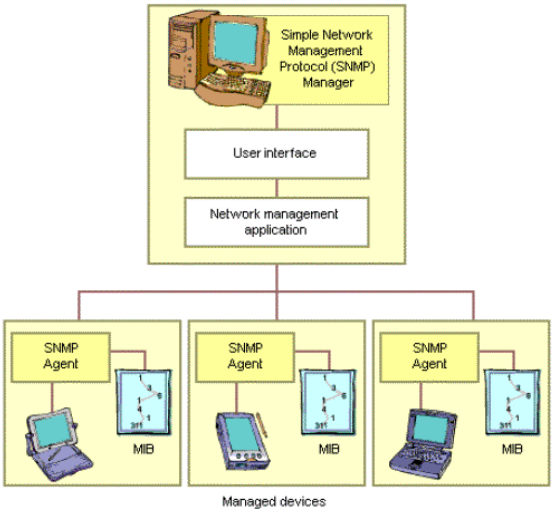


Figura II-8 – Elementos del modelo SNMP

El manager es un software residente en la estación de gestión la red. El manager hace solicitudes al agente utilizando los comandos de SNMP. Los managers ejecutan las funciones de gestión de la red y usualmente proveen una interfaz gráfica con el usuario, presentando un mapa de la red.

El agente es un software residente en el equipo a ser gestionado (PC, bridge, router, hub, etc.). Cada agente almacena datos de la gestión y responde a las peticiones de datos por parte de la estación de gestión.

Los agentes ejecutan dos funciones básicas: inspección y modificación de variables MIB. Usualmente, la inspección de variables significa examinar los valores de contadores, umbrales, estados y otros parámetros, mientras que modificar significa cambiar los valores de las variables que inspecciona.

El manager y el agente se comunican mediante los siguientes comandos:

- *Get*: permite al manager interrogar al agente para obtener las variables monitoreadas. Con *GetRequest* se obtienen variables sencillas, mientras que *GetNextRequest* permite obtener variables almacenadas en tablas. Esto es debido a que los agentes no pueden acceder todos los elementos de una tabla de una sola vez y por eso utilizan *GetNextRequest*, que les permite moverse en la tabla en orden lexicográfico. El agente reporta los resultados a las

peticiones del gestor por medio del mensaje *GetResponse*. En el caso de tablas, se envía una respuesta *GetResponse* por cada *GetNextRequest.* El agente envía un mensaje *GetResponse* al gestor para indicarle si tuvo éxito o no.

- *Set*: permitir al manager solicitar al agente que haga cambios en alguna variable. Aquí también el agente envía un mensaje *GetResponse* al gestor para indicarle si tuvo éxito o no.
- *Trap*: permitir al agente que notifique al manager de eventos significativos. No hay mensaje de confirmación por parte del manager.

En SNMPv2 la comunicación entre el agente y el manager permite también otros tipos de mensajes, tal como se muestra en la figura:

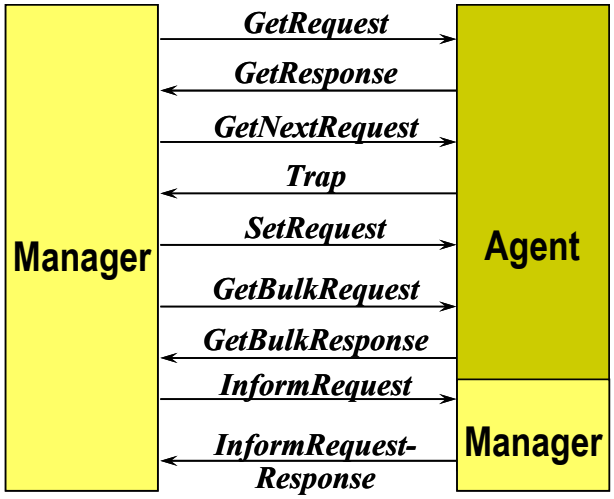


Figura II-9 – Interacción en el modelo SNMPv2

- *GetBulkRequest*: permite el acceso a múltiples variables en la MIB.
- *InformRequest*: permite la comunicación de manager a manager.

SNMP utiliza dos puertos, el puerto 161 se utiliza para recibir todos los mensajes, excepto para los traps que llegan al puerto UDP 162. Los agentes reciben sus mensajes del gestor a través del puerto UDP 161.

Base de Información de Gestión (MIB)

La primera MIB desarrollada para la gestión de redes TCP/IP, fue definido en el RFC 1066 en agosto de 1988. Luego fue actualizada en el RFC 1156 en mayo del año 1990. La versión 2 de la MIB (MIB-II) fue publicada en el RFC 1213 en Mayo de 1991 y tenía algunas mejoras que han probado su efectividad en la gestión de redes TCP/IP.

Una estación manager depende de un agente instalado en un dispositivo para obtener o actualizar la información disponible en ese elemento de red. La MIB especifica la estructura de datos que debe manejar un nodo o dispositivo para almacenar información relativa a la gestión del mismo, independientemente del protocolo que se utilice. Esto permite que los fabricantes diseñen el software sin tener que escoger un protocolo particular, o que los usuarios cambien de protocolos de gestión sin necesidad de cambiar el software en los equipos.

La MIB puede ser considerada como parte un árbol jerárquico. Las hojas del árbol están formadas por las variables y están identificadas por un OID (*Object Identifier*).

Los OID representan a cada variable u objeto administrable con una secuencia única de números a lo largo de la trayectoria desde la raíz hasta el objeto. Son como los números telefónicos; organizados jerárquicamente con dígitos específicos asignados por diferentes organizaciones. SNMP usa el número como una forma abreviada del nombre, para hacer solicitudes y para enviar la respuesta.

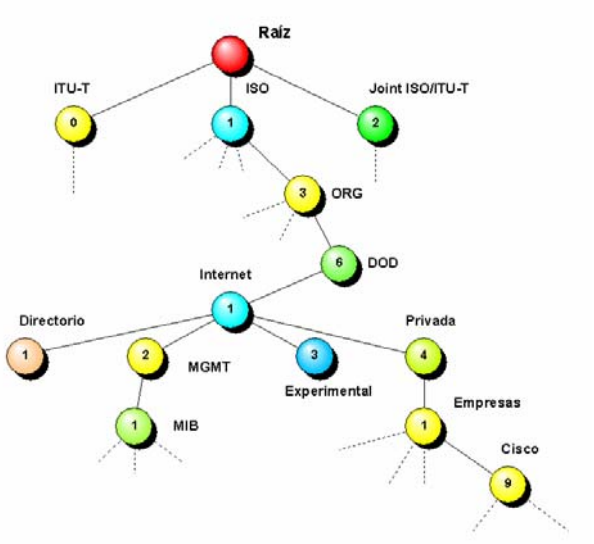


Figura II-10 – El árbol de la MIB

Las variables MIB se agrupan en grupos o categorías (Ej. System, Interfaces…). Cada categoría corresponde a un sub-árbol del nodo MIB en el árbol jerárquico de nombres. La figura muestra parte del sub-árbol por debajo del nodo MIB. Las variables MIB versión 2 (MIB-2) se encuentran ubicadas en el sub-árbol MIB bajo la secuencia 1.3.6.1.2.1.

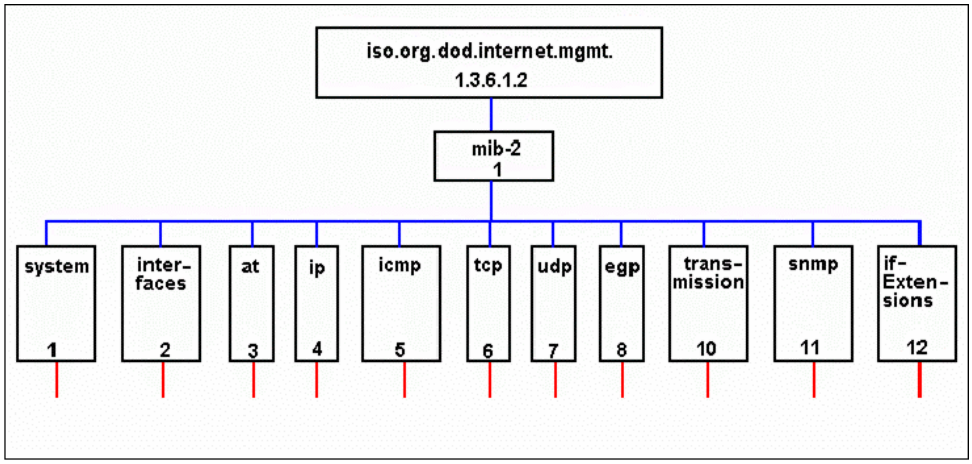


Figura II-11 – Grupos de variables MIB

La MIB se amplía en SNMPv3, para contemplar las nuevas informaciones necesarias para la gestión (RFC 3418).

A diferencia de la mayoría de los protocolos del conjunto TCP/IP, SNMP no tiene campos fijos. Un mensaje SNMP consiste de tres partes principales:

- Número de versión del protocolo
- Nombre de la comunidad
- Área de datos

En la figura que se muestra a continuación, se detalla el formato que toman los mensajes en el protocolo de SNMP:

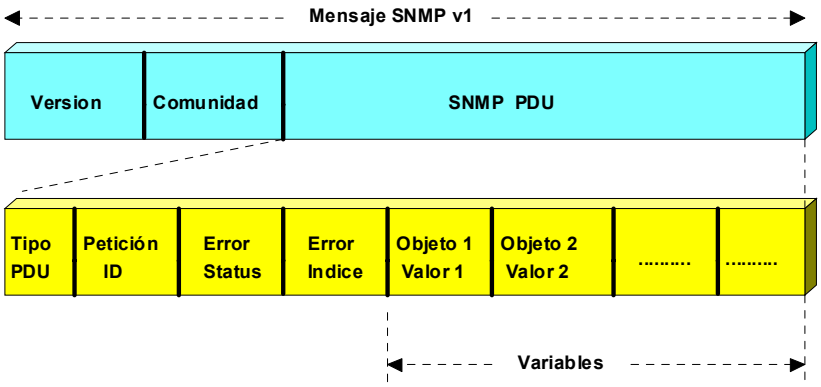


Figura II-12 – Formato de mensajes SNMPv1

El campo versión es para que todos los elementos de la red estén seguros de manejar la misma versión del SNMP.

Un sistema de gestión de red basado en SNMP consiste de *comunidades.* Los agentes pertenecen a un subconjunto de esas comunidades, permitiendo a comunidades específicas el acceso a un subconjunto de sus variables MIB. El campo nombre de comunidad es utilizado por SNMP para las funciones siguientes:

- *Autenticación/privacidad:* para implementar esta función, los mensajes recibidos pasan un proceso de autenticación junto con el nombre de comunidad del mensaje y las direcciones fuente y destino. El objetivo del proceso de autenticación es determinar si un mensaje es auténtico, realizar cualquier operación relacionada con este proceso y devolver el mensaje resultante. Si se requiere privacidad, el mensaje pasado al proceso de autenticación se encontraría encriptado. El procesamiento continúa con el mensaje en su forma revisada.
- *Control de acceso:* provee diferentes capacidades de gestión a diferentes estaciones de gestión. El nombre de comunidad especifica el subconjunto de MIB a los cuales una petición tiene acceso y el tipo de acceso permitido. Los diferentes tipos de acceso son: lectura/escritura, solo lectura, solo escritura, no accesible.

El área de datos de un mensaje SNMPv1 lleva una de la las siguientes PDU (Protocol Data Unit): GetRequest, GetNextRequest, GetResponse, Set Request, Trap. Los mensajes trap son muy utilizados para notificar eventos. Hay siete campos en un mensaje trap:

1. *PDU Type*: debe contener el valor 4, lo cual indica que es un PDU tipo Trap.
2. *Enterprise*: contiene cualquiera de los dos valores de 0.0.0.0 si el transporte UDP no es usado, o el valor de la variable del agente sysObjects o la identidad parcial del trap. Si el valor del campo "Generic Trap type" es 6 entonces el valor está definido en la macro TRAP-TYPE definido en el trap.
3. *Agent Address*: contiene la dirección IP del agente que genera el trap.
4. *Generic Trap* Type: datos del tipo de trap:

Tipo de trap	Valor	Descripción
ColdStart	0	Arranque en frió
WarmStart	1	Arranque en caliente
LinkDown	2	Interfaz caída
LinkUp	3	Interfaz levantada
AuthenticationFailure	4	Nombre de la comunidad Incorrecto
EgpNeighborLoss	5	Falla de enlace hacia un router vecino
EnterpriseSpecific	6	Evento específico del equipo o sistema del fabricante

Tabla II-1 – Códigos para los tipos de Traps de SNMP

5. *Specific Trap Type*: indica el número del trap si el campo Generic Trap Type fue asignado el valor de 6 (Enterprise Specific). Para todos los otros traps genéricos, este campo es cero.
6. *Time Stamp*: Contiene el valor de la variable sysUpTime, es decir el tiempo de ocurrencia del evento a partir de la inicialización del equipo.
7. *Variable Bindings*: Contiene el valor de la variable o de las variables que el agente reporta al manager.

Para SNMPv3 el formato del mensaje SNMP es más complejo:

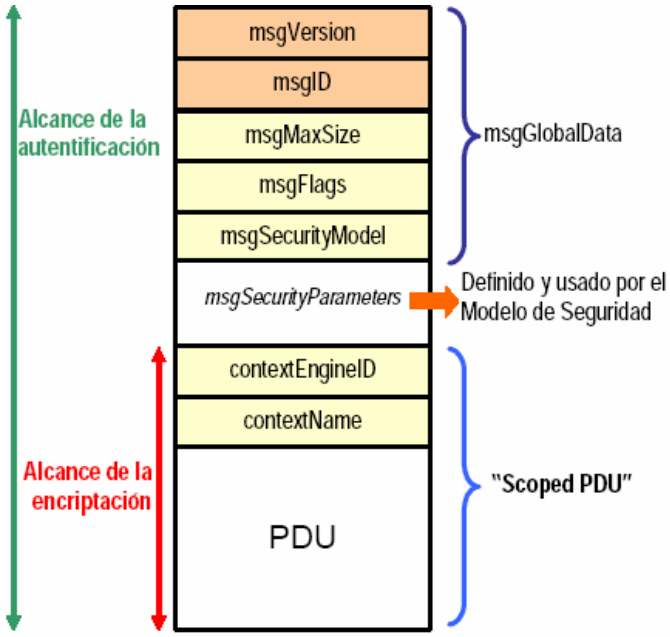


Figura II-13 – Formato de mensajes SNMPv3

Donde:

- msgVersion, msgID: como en las versiones 1 y 2.
- msgMaxSize: tamaño máximo de mensaje (bytes) que soporta el emisor.
- msgFlags: contiene 3 flags en los bits menos significativos.
- reportableFlag: igual a 1 si hay que generar una PDU de respuesta a la recepción de este mensaje.
- privFlag: aplicar encriptación al mensaje.
- authFlag: aplicar autenticación al mensaje.
- Niveles de seguridad: noAuthNoPriv, authNoPriv, authPriv.
- msgSecurityModel: identificador que indica qué modelo de seguridad empleó el emisor al preparar el mensaje.
- Valores reservados: 1 (SNMPv1), 2 (SNMPv2c), 3 (USM).

- msgSecurityParameters: parámetros del subsistema de seguridad.
- contextEngineID: identificador único de la entidad SNMP que ha de procesar el mensaje entrante.
- contextName: nombre único de un contexto en la entidad SNMP.
- Contexto: conjunto nombrado de instancias de objetos en la MIB local
- PDU: una PDU SNMPv3.

II.7 Generación y Captura de Traps

Para poder estudiar y evaluar las características de los mensajes trap utilizados para notificar eventos, se dispone de varias herramientas y productos.

TrapGen es un programa muy sencillo que permite el envío de traps usando la línea de comandos (DOS):

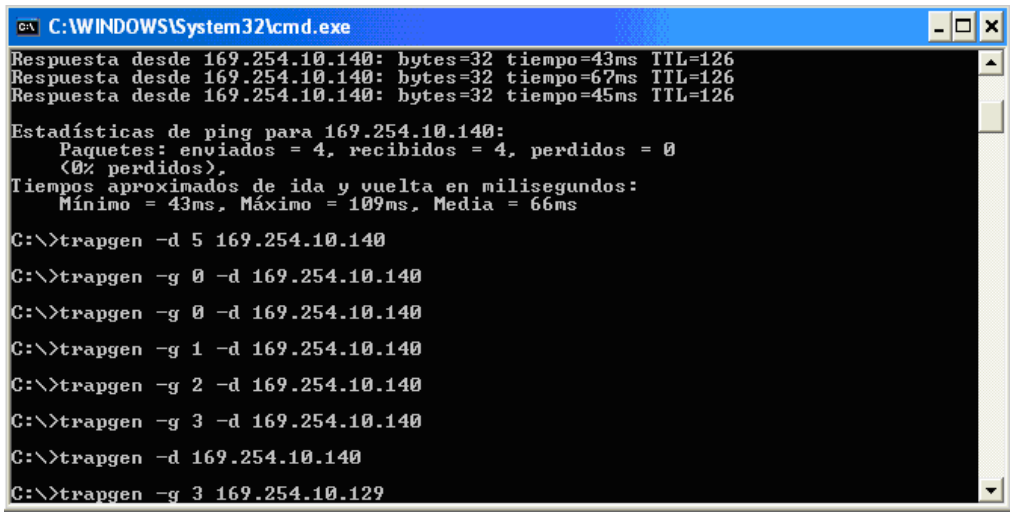


Figura II-14 – Envío de Traps a través de TrapGen

Trapgen posee las siguientes opciones para generar traps:

[v[1|2] | inform] – especifica el tipo de trap

-f <filename> - archivo que contiene los parámetros de la línea de comandos

-h - llama a la ayuda de TrapGen

-c <community string> - nombre de la comunidad a la que se envía el trap.

-d <destinationIpOrHost[:portnumber]>: dirección IP o nombre de host con el puerto adonde va dirigido el trap

-v <varbind OID> <varbind type> <varbind data>

OID es el ID de la variable objeto. Estas variables pueden tomar los siguientes valores:

STRING
COUNTER
GAUGE
INTEGER
ADDRESS
OID
TIMETICK
HEX

<varbind type> es:

S|s – para cadenas varbind
A|a - para Ip Address varbind
O|o - para OID varbind
C|c – para contador varbind
G|g – para indicador varbind
I|i – para un valor entero varbind
T|t – para un valor de tiempo varbind
H|h – para un valor octal varbind

-o envía OID´s

-i enviar direcciones

-l para especificar el nombre del archivos de log

-g tipo genérico

-s tipo específico

-r requiere id - para V2 o informes

-m <timeout> - para recibir informes de la respuesta

-t <timestamp>

-p a - descargar los traps en formato ASCII para la pantalla

-p h - descargar los traps en formato hex para la pantalla

-p b - dumps descargar los traps en ambos formatos (ASCII y hex)

-z para que no aparezca la ventana de consola

SNMP Trap Watcher es un programa que permite mostrar los traps recibidos por el puerto UDP 162. Esos traps pueden sean filtrados por palabras (string) o por tipo (específica o genérica).

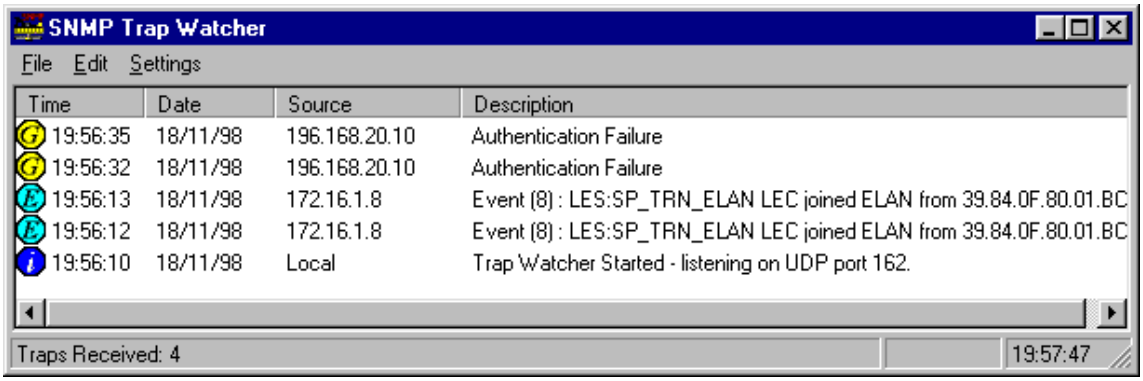


Figura II-15 – Capturador Trap Watcher

SNMPc Network Manager es un NMS (*Network Management System*) para la gestión de redes pequeñas, medianas y grandes. Permite generar traps y también recibirlos y notificar en la consola.

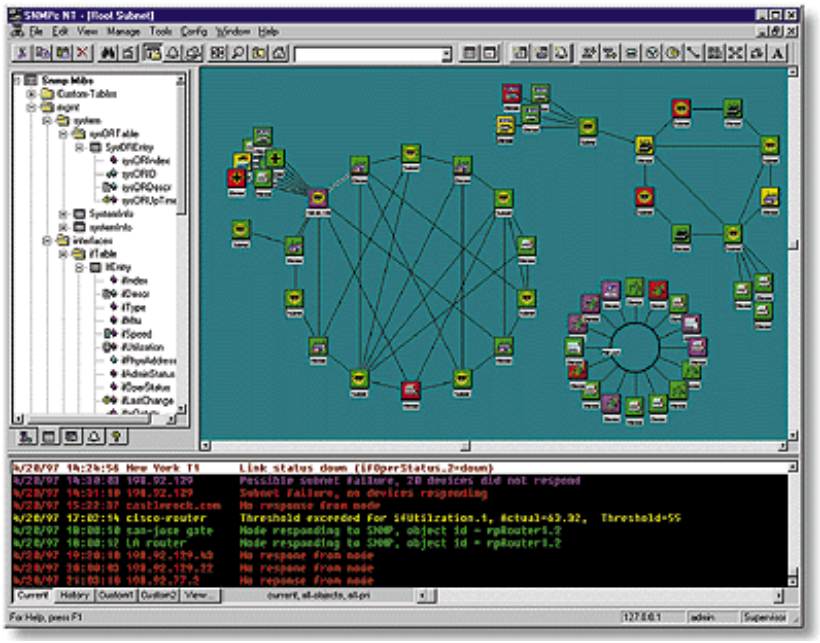


Figura II-16 – SNMPc Network Manager

En la figura siguiente se muestran pantallas de algunas de las herramientas utilizadas para el envío y recepción de mensaje traps y syslog (SNMPc Server, TrapGen, Trap Watcher, Kiwi Syslog).

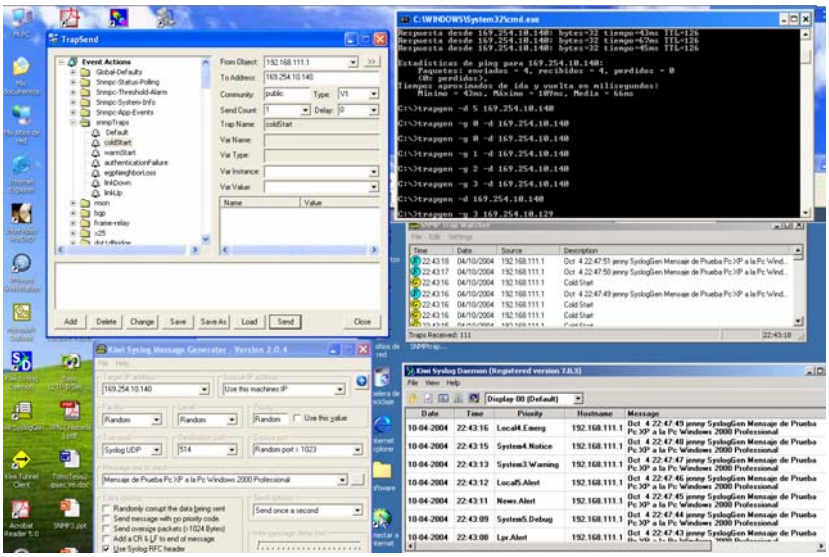


Figura II-17 – Generación y recepción de Traps

II.8 Redes Privadas Virtuales (VPN)

Una manera de hacer más seguros los mensajes SNMP y Syslog en utilizando la tecnología de Redes Privadas Virtuales (VPN, *Virtual Private Network*). Las VPN se comportan como túneles encriptados a través de medios compartidos para transmitir información privada entre sitios. Proporcionan un modo de construir una red de área extendida a escala global con un costo muy inferior a hacerlo con redes privadas.

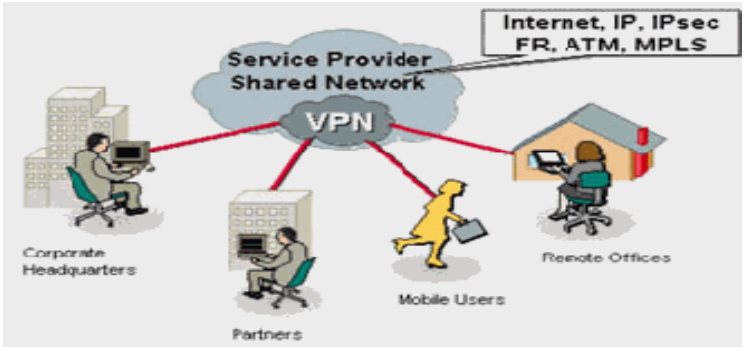


Figura II-18 – Modelo de una VPN

Básicamente, la tecnología VPN conforma un canal de comunicaciones encriptadas seguro a través del medio compartido para oficinas remotas, usuarios móviles y socios comerciales. En lugar de alquilar una línea dedicada (circuito) entre dos sitios, es a menudo mucho mejor crear un circuito virtual a través de la red de conmutación pública.

Todo aquel que use la red, comparte los costos, en oposición a las líneas alquiladas dedicadas para las cuales la organización paga todos los costos, aunque pudiera no utilizarla el 100% del tiempo. En todo caso, si se transmite información sensible al retardo o urgente, VPN sobre Internet no es la mejor solución porque puede encontrar problemas de rendimiento debido a los retardos.

El costo de la línea dedicada se incrementa con la distancia, y es ahí donde la Internet puede usarse para suministrar parte de la conexión de larga distancia y reducir dramáticamente el costo de los enlaces WAN. Sin embargo, debe considerarse la seguridad cuando se usa Internet. Las transmisiones ya nunca más van a estar confinadas a circuitos privados; van a viajar a través de Internet en un terreno desconocido. Aunque puede parecer imposible que alguien esté monitoreando una

línea y consiga capturar parte de la transmisión y hacer uso de ella, la posibilidad existe. Por eso la encriptación es importante. Cuando la información está encriptada, se requiere una clave para desencriptarla. Los dispositivos de cada parte de un túnel deben tener las claves adecuadas para encriptar y desencriptar (el mismo conjunto de datos). Si se está configurando un enlace con una sucursal, es fácil administrar este intercambio de claves. Sin embargo, si un usuario remoto accede a la red corporativa, se necesita un modo de verificar quién es y un modo de intercambiar las claves para la encriptación. Las claves públicas y las firmas digitales son lo que más se utiliza para este propósito.

Antecedentes de las VPN

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de correo, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad.

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services (RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un abono mensual más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas y, además, tiene

sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos. Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan.

Las VPN son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

Una VPN necesita proveer cuatro funciones críticas para garantizar la seguridad de los datos:

- Autenticación, asegurando que el usuario que desea conectarse a la red es quien dice ser.
- Control de acceso ó autorización, restringiendo el acceso a la red y a los recursos de los usuarios no autorizados.
- Confidencialidad, previniendo que alguien copie los datos que viajan a través de la Internet.
- Integridad, asegurando que los datos no han sido alterados durante la transferencia.

Debido a la carencia de estándares de interoperabilidad, usualmente era necesario utilizar routers y firewalls del mismo fabricante para implementar una VPN. Pero el grupo de trabajo IETF (Grupo de trabajo de ingeniería Internet) ha desarrollado un grupo de estándares para la identificación, encriptación e intercambio de claves entre productos de distintos fabricantes que trabajan con los protocolos IP a nivel de la capa de red del modelo OSI.

El estándar IPSec (*IP Secure*) define una cabecera de un paquete IP para que tenga integridad de identificación y de datos y una cabecera de encriptación. La primera proporciona seguridad de que el paquete es de quien pretende ser y que no ha sido alterado. Una asociación de seguridad mantiene el acuerdo mutuo sobre la información que se requiere para la identificación y la encriptación. Un método para administrar las claves se llama ISAKMP (Protocolo de administración en clave y Asociación de

seguridad Internet). Además, Microsoft y otros fabricantes han desarrollado un protocolo similar llamado protocolo punto a punto canalizado (PPTP) que permite la creación de redes virtuales privadas por Internet entre Microsoft Windows NT Server.

Específicamente, PPTP utiliza líneas de comunicaciones analógicas o ISDN, para crear un túnel directamente a un Servidor NT/2000 específico de una red. Los usuarios remotos y los sistemas remotos en sucursales se conectan con Internet desde cualquier sitio y establecen conexión a un proveedor de servicios Internet (ISP) que trata su tráfico PPTP; el ISP instala plataformas capaces de operar con PPTP o procesadores finales (FEP) en el sitio del usuario.

Un ISP no necesita ser parte del túnel PPTP. Muchas organizaciones querrán conectarse directamente a Internet a través de su propio software y hardware. PPTP trabaja también con este modelo y proporciona la misma seguridad que a las conexiones ISP. Los usuarios de los sistemas operativos Windows 95/98/XP y de Windows NT/2000 pueden utilizar esta tecnología.

Para que los ISP proporcionen PPTP, deben añadir o actualizar el software de sus servidores de acceso remoto. Estas actualizaciones están ya disponibles por parte de un grupo de fabricantes que aceptan PPTP. Una vez que se hacen las actualizaciones, sus clientes/compradores pueden iniciar el uso de VPN sobre PPTP sin necesitar cambiar ninguna propiedad de clientes o servidores.

PPTP puede usarse junto a un firewall (cortafuego). Mientras un cortafuego regula los datos que entran en la red corporativa desde Internet, PPTP se ha diseñado para asegurar las sesiones de comunicación entre usuarios remotos identificados y la red corporativa. Si tanto el cortafuego como un servidor RAS son desplegados, el servidor RAS se coloca fuera del cortafuego y envía todos los paquetes que recibe de los usuarios remotos al cortafuego. El cortafuego simplemente proporciona la misma seguridad que daría si no existiese PPTP.

Uno de los defectos de PPTP es que se sufre retrasos temporales y se puede reducir dramáticamente el rendimiento de las conexiones. Además, el tráfico sobre Internet podría no hacerlo útil porque algunas operaciones necesitan respuesta inmediata entre el cliente y el servidor. A pesar de ello, el protocolo tiene ventajas en muchas situaciones, especialmente si las sucursales están situadas en sitios remotos en

cualquier parte del mundo.

Desde luego, la identificación de inicio de sesión es vital para el acceso remoto. Si se usa el método no PPTP para el acceso remoto, en el que los usuarios llaman directamente al sitio, puede identificarles usando Microsoft CHAP, suponiendo que son clientes Windows. Pero si se trasladan los servicios de acceso remoto a un ISP externo por las razones antes descritas, es necesario identificar adecuadamente a los usuarios y esto es lo que hace PPTP. Proporciona las prestaciones de seguridad que se necesitan para las transmisiones encriptadas de datos y para identificar de manera segura a los usuarios.

Estructura de una VPN

Una VPN es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura siguiente, la idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada. Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

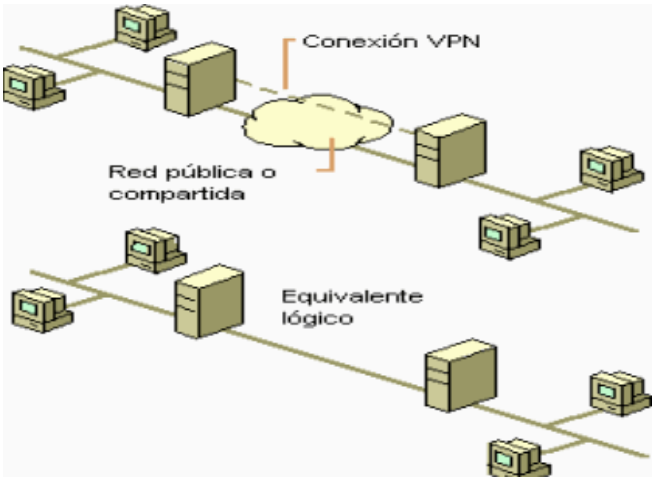


Figura II-19 – Estructura de una VPN

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos, para lo cual se negocian esquemas de encriptación y autenticación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autenticación.

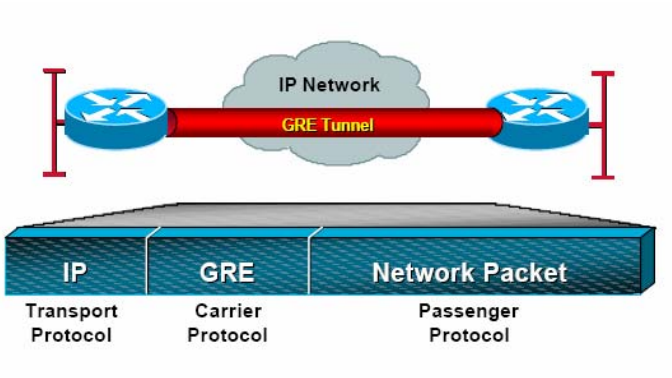


Figura II-20 – Formato de la comunicación en la VPN

La tecnología de túneles ("tunneling") es básicamente un modo de transferir datos encapsulando un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados y/o autenticados.

Autenticación

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPN es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

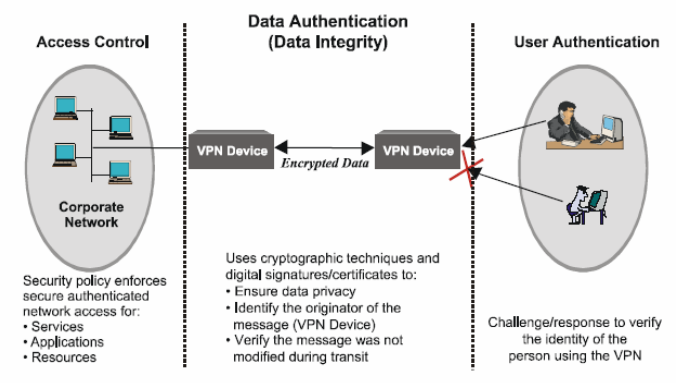


Figura II-21 – Sistema de autenticación en la VPN

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos están dañados en la transmisión o interceptados y modificados en el camino. Ejemplos de sistemas de autenticación son Challenge Handshake Authentication Protocol (CHAP) y RSA.

Encriptamiento

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de la poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada

y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

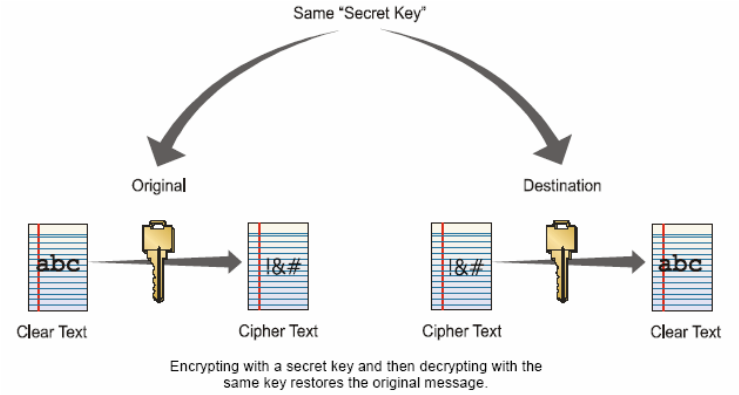


Figura II-22 – Proceso de encriptación en la VPN con clave secreta

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la comunicación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

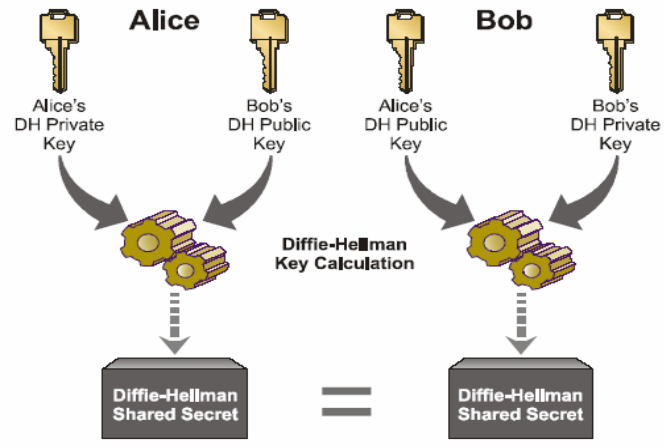


Figura II-23 – Proceso de encriptación en la VPN con clave pública

En las VPN la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPN es IPSec, que consiste en un conjunto de estándares del IETF que delinean un protocolo IP seguro para IPv4 e IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrita anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec.

IP Seguro - IPSec

IPSec es un grupo de estándares abiertos para asegurar comunicaciones privadas seguras sobre redes IP. Basado en estándares desarrollados por el Internet Engineering Task Force (IETF), IPSec asegura confidencialidad, integridad y autenticidad de los datos que se encuentran sobre la red IP pública.

La encriptación y el control de autenticación pueden ser implementados en distintas capas dentro del modelo de infraestructura de comunicación. Antes de IPSec, se desarrollaron soluciones parciales que se enfocaron en la resolución de una porción del problema. Por ejemplo, SSL provee encriptación para Web browsers y otras aplicaciones. SSL protege la confidencialidad de los datos enviados desde cada aplicación que lo usa, pero no protege los datos enviados desde otras aplicaciones. Por lo tanto, cada aplicación debe trabajar con SSL para obtener una protección completa.

Instituciones, como los militares, han estado utilizando enlaces encriptados por años. En este sentido, cada enlace de comunicación es protegido con un par de dispositivos encriptando en ambos extremos del enlace. Este método ofrece una excelente protección de los datos, pero requiere que cada extremo cuente con un dispositivo de encriptación, debido que los datos viajan en texto en claro.

IPSec implementa encriptación y autenticación en la capa de red, permitiendo una solución de seguridad de extremo a extremo en la arquitectura de red misma. De esta

forma las aplicaciones y los sistemas finales no deben ser modificados para obtener las ventajas de un medio seguro.

Debido a que los paquetes encriptados lucen como paquetes IP ordinarios, pueden ser fácilmente enrutados en las redes IP, sin realizar cambios en los equipos de red intermedios en el enlace. Únicamente los dispositivos finales conocen sobre la encriptación, reduciendo así los costos de implementación y administración.

El protocolo IPSec define un nuevo grupo de encabezados que se adicionan al datagrama IP; estos encabezados se ubican después del encabezado IP y antes del Protocolo de capa 4 (típicamente Transmisión Control Protocol [TCP] o User Datagram Protocol [UDP]). Estos nuevos encabezados proveen información para asegurar la carga del paquete IP, como se describe a continuación:

- *Authentication Header (AH):* este encabezado, cuando es añadido al datagrama IP, asegura la integridad y autenticidad de los datos incluyendo los campos invariables del encabezado IP. Esta facilidad no provee protección a la confidencialidad. AH usa una función Hash con clave, en vez de firmas digitales, dado que la tecnología de firmas digitales es muy lenta y puede reducir el desempeño de la red.
- *Encapsulation Security Payload (ESP):* este encabezado, cuando es añadido al datagrama IP, protege la confidencialidad, integridad y autenticidad de los datos. Si ESP es utilizado para validar la integridad de los datos en el canal no se incluyen los campos invariables del encabezado IP.

AH y ESP puede ser usado independientemente o juntos, sin embargo para la mayoría de las aplicaciones sólo uno de los encabezados es suficiente. Para ambos protocolos IPSec no define un algoritmo específico de seguridad a utilizar, pero provee un grupo de protocolos abiertos para implementar algoritmos estándar de la industria.

Inicialmente, la mayoría de las implementaciones de IPSec soporta MD5 de RSA Data Security o el Secure Hash Algorithm (SHA). El algoritmo Data Encryption Standard (DES) y triple DES (3DES) son actualmente los algoritmo más comunes.

El protocolo IPSec provee dos modos de operación: modo transporte y modo túnel. En el *modo transporte*, solo la porción de carga del paquete es encriptada y el

encabezado IP original permanece intacto. Este modo tiene la ventaja de adicionar sólo unos pocos bytes a cada paquete. Permite a los dispositivos en la red pública ver la dirección fuente y destino del paquete. Esta capacidad facilita el habilitar procesamiento especial, tal como calidad de servicio, en la red intermedia. Sin embargo, el encabezado de capa 4 se encripta, limitando la posibilidad de examinar a fondo el paquete.

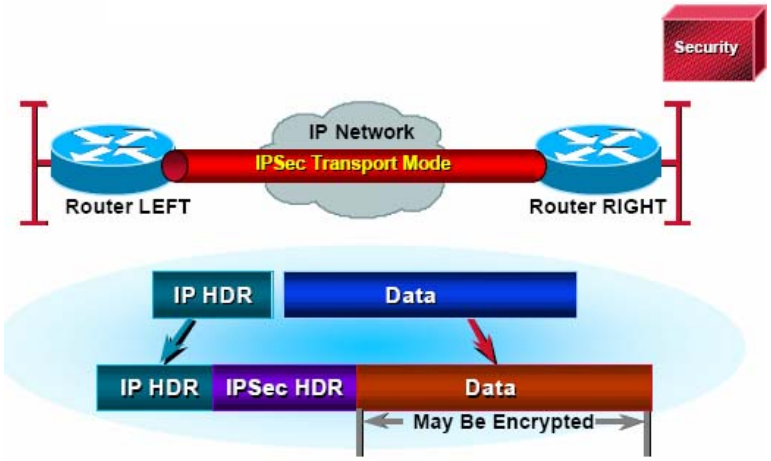


Figura II-24 – Modo transporte del protocolo IPSec

Desafortunadamente, el transmitir el encabezado IP en claro, permite a algún atacante realizar análisis de parte del paquete en tráfico. Sin embargo, lo único que el atacante puede conocer es que un paquete IP fue enviado, junto con su dirección fuente y destino, pero no puede determinar si el paquete es de correo o cualquier otra aplicación.

En *modo túnel*, el datagrama IP completo es encriptado y viene a formar la porción de carga del nuevo datagrama IP. Este modo permite que un dispositivo de red, tal como un router, actúe como un IPSec Proxy. En este caso se debe contar con dos dispositivos de red, uno fuente y otro destino, quienes ejecutan las funciones de encriptación y desencriptación.

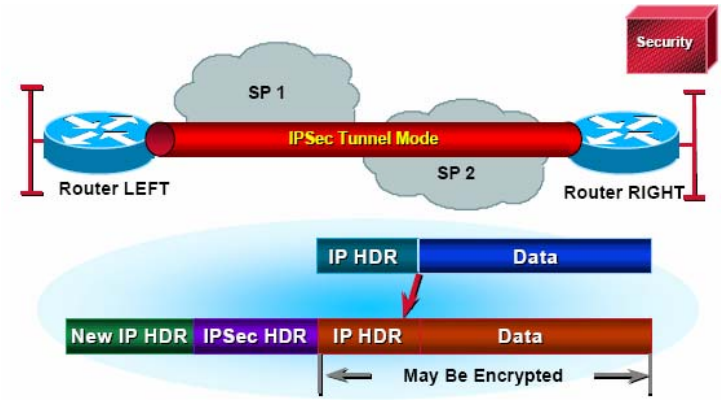


Figura II-25 – Modo túnel del protocolo IPSec

La principal ventaja del modo túnel es que los sistemas finales no requieren ser modificados para disfrutar de los beneficios de la seguridad IP. El modo túnel también protege del análisis del tráfico, debido a que el atacante sólo puede determinar los puntos finales del túnel y no puede conocer las direcciones fuentes y destino reales del paquete.

Como fue definido por el IETF, IPSec en modo transporte puede ser usado sólo cuando el sistema fuente y destino soportan IPSec. En la mayoría de los casos se implanta IPSec en modo túnel, dado que esta modalidad no requiere modificar el sistema operativo o alguna aplicación en la estación de trabajo o servidor.

IPSec provee varias opciones para ejecutar la encriptación y autenticación en la red mediante las Asociación de Seguridad (SA). Cuando el servicio de seguridad es habilitado, los nodos a comunicar deben determinar exactamente cuales algoritmos van utilizar, por ejemplo: DES o IDEA para encriptación; MD5 o SHA para asegurar la integridad. Después de definido los algoritmos, los dispositivos deben compartir una clave de sesión. La Asociación de Seguridad es el método que usa IPSec para verificar toda la información particular concerniente a una comunicación de una sesión IPSec. Una Asociación de Seguridad es una relación entre dos o más entidades que describe como éstas usarán los servicios de seguridad para establecer una comunicación segura.

La Asociación de Seguridad es unidireccional, significa que al menos dos conexiones

de seguridad deben establecerse durante una comunicación, una de A a B y otra de B a A; las asociaciones de seguridad son identificadas por un número único seleccionado aleatoriamente denominado Security Parameter Index (SPI) y la dirección IP destino. Cuando un sistema envía un paquete que requiere protección IPSec, busca la asociación de seguridad en su base de datos, aplica el procesamiento específico y entonces inserta el SPI obtenido desde la asociación de seguridad en el encabezado IPSec. Cuando el puerto IPSec recibe el paquete, éste busca la asociación de seguridad en su base de datos por dirección IP destino y SPI y entonces procesa el paquete como requiera. En resumen, la Asociación de Seguridad es simplemente una instrucción de la política de seguridad negociada entre dos dispositivos.

IPSec asume la ubicación de la Asociación de Seguridad, pero no tiene un mecanismo para crear esta asociación. El IETF describe el proceso en dos etapas: IPSec provee el procesamiento a nivel de paquete, mientras que el Internet Key Management Protocol (IKMP) negocia las asociaciones de seguridad. Después de considerar distintas alternativas el IETF seleccionó ISAKMP/Oakley como el método estándar para configurar las asociaciones de seguridad en IPSec.

ISAKMP/Oakley crea un túnel seguro; entre las dos entidades que se autentican una con la otra y establecen la clave compartida. A continuación se describen los dos procesos ejecutados:

- *Autenticación:* ambas partes en la comunicación se deben autenticar. El protocolo ISAKMP/Oakley es muy flexible y soporta múltiples métodos de autenticación. Las dos entidades deben acordar un protocolo de autenticación común obtenido del proceso de negociación. En este momento los siguientes mecanismos son generalmente implementados:
- *Claves pre-compartidas:* con este método una clave es pre-instalada en cada host. Los puertos ISAKMP/Oakley se autentican uno con otro, calculando y enviando una porción de datos que incluye la clave pre-compartida encriptada con una función hash. Si el puerto receptor puede crear el mismo extracto con la misma función hash y utilizando su clave pre-compartida, entonces ambas partes poseen la misma clave y de esta forma se autentican uno con el otro.

- *Criptografía de clave pública:* cada parte genera un número seudo aleatorio el cual encripta con la clave pública de la otra parte. La habilidad de cada parte para desencriptar utilizando la función hash con su clave privada, es el proceso que permite autenticar cada parte. El sistema provee de procedimientos para la negación de las transacciones. Esto quiere decir, que cualquier dispositivo en el intercambio de información para el inicio de la sesión, puede negarse a tomar parte de la comunicación. Actualmente, sólo el algoritmo RSA público es soportado.
- *Firma digital:* en este método cada dispositivo firma digitalmente una porción de datos y lo envía a la otra parte. Este método es similar al de criptografía de clave pública, excepto que este provee no repudiación. Actualmente, son soportados: el algoritmo RSA público y el Digital Signature Standar (DSS).

Ambos métodos, el de criptografía de clave pública y el de firma digital, requieren del uso de certificados digitales para validar el par de claves pública/privada. ISAKMP/Oakley permite que el certificado sea accedido independientemente, por ejemplo desde DNSSEC, o que ambos dispositivos posean explícitamente el certificado a intercambiar como parte de ISAKMP/Oakley.

Para el Intercambio de clave ambas partes de la comunicación deben contar con una clave para encriptar el túnel ISAKMP/Oakley. El protocolo Diffie-Hellman es usado para acordar una clave de sesión común. El intercambio es autenticado para protegerse de los ataques denominados “hombre en el medio”.

Usando ISAKMP/Oakley con IPSec, los pasos de autenticación e intercambio de clave crea la asociación de seguridad SA de ISAKMP/Oakley, en otras palabras, un túnel seguro entre los dispositivos. Seguidamente, uno de los dispositivos ofrece un grupo de algoritmos para la encriptación y el otro dispositivo debe aceptar uno de los algoritmos ofrecidos o rechazar la conexión completa. Cuando ambos lados acuerdan el algoritmo a utilizar, se debe decidir la clave a utilizar para IPSec con AH, ESP o ambos.

IPSec usa una clave compartida diferente a la de ISAKMP/Oakley. La clave compartida de IPSec puede ser obtenida usando el algoritmo Diffie-Hellman de nuevo para asegurar la seguridad o refrescar la clave secreta derivada desde el intercambio

original. El algoritmo Diffie-Hellman genera la SA de ISAKMP/Oakley con la ejecución de la función hash y un número pseudo aleatorio.

El primer método provee mayor seguridad pero es más lento. En la mayoría de las implementaciones es utilizada una combinación de ambos métodos. Esto es que el algoritmo Diffie-Hellman es utilizado para el primer intercambio de claves y entonces la política local determina cuando usar de nuevo el algoritmo Diffie-Hellman o ejecutar un refrescamiento de la clave. Después que este procedimiento culmina, es cuando finalmente se ha establecido una Asociación de Seguridad. A continuación se presenta un ejemplo para la mejor comprensión del procedimiento:

- A está intentando comunicarse con B de una forma segura. A envía sus datos a B.
- Cuando el router donde se encuentra conectado A analiza el paquete, éste chequea su política de seguridad y determina que la comunicación debe ser encriptada.
- La política de seguridad preconfigurada indica que el router donde se encuentra conectada B es el punto final del túnel IPSec.
- El router donde se encuentra conectado A también verifica si está establecido un IPSec SA con el router donde se encuentra conectada B. Si no es así, entonces este requiere establecer un SA con el protocolo ISAKMP/Oakley. Si los dos routers ya tienen establecido un SA ISAKMP/Oakley, la SA IPSec puede ser generada rápida e inmediatamente. Si los dispositivos no comparten la SA ISAKMP/Oakley, ésta debe ser creada antes de iniciar la negociación de la SA IPSec.
- Los dos routers intercambian los certificados digitales, los cuales deben ser firmados de antemano por una autoridad de certificados de confianza para ambos routers.
- Cuando la sesión ISAKMP/Oakley activa, los dos routers pueden negociar la SA IPSec.
- Cuando la SA IPSec es establecida, ambos routers deben negociar el algoritmo de encriptación (por ejemplo DES) y el algoritmo de autenticación

(por ejemplo MD5) y contar con una clave compartida de sesión.

- Ahora, el router donde se encuentra conectado A puede encriptar el paquete IP, lo encapsula en un nuevo paquete IPSec y lo envía al router donde está conectada B.
- Cuando éste recibe el paquete IPSec, busca la SA IPSec, procesa apropiadamente el paquete, desempaquete el datagrama original y lo envía a B.

Protocolo de Túnel Punto a Punto (PPTP)

Point-to-Point Tunneling Protocol fue desarrollado por Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser enrutado a través de una red IP, como Internet.

Figura II-26 – Modelo del Protocolo de Túnel Punto a Punto (PPTP)

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP. Existen dos escenarios comunes para este tipo de VPN:

- El usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header IP, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, Frame Relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.

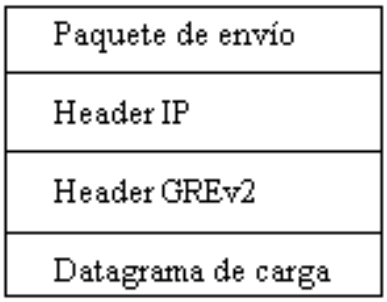


Figura II-27 – Capas del encapsulamiento PPTP

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto en claro. Si se utiliza CHAP, standard en el que se intercambia un número secreto y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT/2000, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (*Password Autenthication Protocol*), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 o 128 bits.

Protocolo de Túnel Capa 2 (L2TP)

Layer-2 Tunneling Protocol (L2TP) facilita el “entunelamiento” de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran. El escenario típico L2TP, cuyo objetivo es la creación de “entunelar” tramas PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:

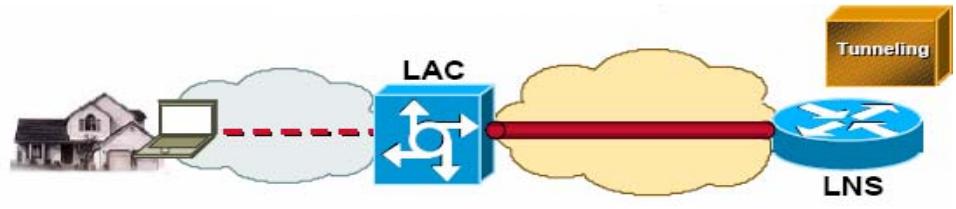


Figura II-28 – Modelo del Protocolo de Túnel Capa 2 (L2TP)

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan las tramas PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre las tramas PPP y los mensajes de control a través de los canales de control y datos de L2TP.

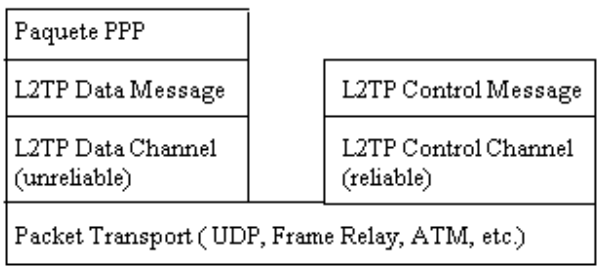


Figura II-29 – Relación entre las tramas PPP y los mensajes de control en L2TP

Las tramas PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

II.9 Protocolo SSH (Secure Shell)

Otra forma de crear túneles seguros para el tráfico SNMP y Syslog es usando SSH, que fue desarrollado por un programador finlandés, Tatu Ylönen, quien publicó su trabajo bajo una licencia libre. Pronto el éxito de su programa lo llevó a patentar la marca registrada "SSH™" y crear una empresa con fines comerciales. Las siguientes versiones dejaron de ser libres y se permitió su empleo únicamente para usos no

comerciales. Los desarrolladores de OpenBSD se dieron cuenta de que su sistema operativo, centrado en la criptografía y seguridad, se quedaba "cojo" sin SSH. Además, las encuestas afirmaban que lo primero que la mayoría de usuarios de OpenBSD añadía después de instalar el sistema, era SSH. Con estas ideas en la cabeza y bastante buenas intenciones, surgió el proyecto OpenSSH, cuyo principal objetivo consistió en desarrollar una implementación totalmente libre de SSH. Los primeros pasos de este proyecto estuvieron centrados en utilizar solamente código libre y portable. Tanto es así que pusieron especial empeño en evitar problemas con patentes y restricciones gubernamentales: la mayoría de los desarrolladores residían fuera de Estados Unidos, a excepción de Niels Provos, un alemán afincado en Michigan, que cruzó la frontera a Canadá para enviar su código desde una pequeña tienda local de informática en Ontario. Todos estos esfuerzos no fueron vistos con tan buenos ojos por el desarrollador inicial de SSH, que veía como su proyecto comercial se iba al traste. Después de varias demandas judiciales y muchas discusiones, OpenSSH pudo mantener el "SSH" en su nombre y seguir con el trabajo que estaban realizando.

SSH permite que usuarios entren en forma segura a un sistema remoto. Además, como cifra todo lo que se envía y recibe, puede ser usado para hacer seguros otros protocolos usando una técnica llamada *port forwarding* (reenvío de puerto). SSH está constituido por tres componentes principales:

- El protocolo de capa de transporte [SSH - TRANS] suministra al servidor la autenticación, la confidencialidad, y la integridad. Puede opcionalmente también proveer la compresión. La capa de transporte se ejecuta típicamente en una conexión de TCP/IP, pero también puede ser usado en lo más alto de cualquier otro flujo de datos confiable.
- El usuario de protocolo de Autenticación [SSH - USERAUTH] autentica el usuario del cliente en el servidor. Se ejecuta sobre la capa de transporte del protocolo.
- El protocolo de conexiones [SSH - CONNECT] multiplexa al cifrar.

II.10 Protocolo SSL

Otro protocolo interesante es SSL (*Secure Socket Layer*) o Capa de Conector Seguro. Fue diseñado en 1994 por Netscape Communications Corporation y es un protocolo

que provee tres niveles distintos de protección:

- Autenticación de las entidades (cliente y servidor) involucradas en la comunicación utilizando criptografía de clave pública, como RSA, Diffie-Hellman y DSS.
- Confidencialidad de la información a través del uso de criptografía de clave secreta, como DES, Triple-DES, RC4, RC2.
- Integridad de la información a través del uso de códigos de autenticación de mensajes, como MD5 y SHA.

SSL es un protocolo de seguridad en tiempo real, por lo que los nodos involucrados negocian interactivamente para autenticarse y establecer los parámetros de seguridad de la sesión. Se ubica en el modelo de capas de Internet entre el nivel de transporte y de aplicación, suministrando un canal seguro de comunicación a nivel de socket (conector), de allí su nombre.

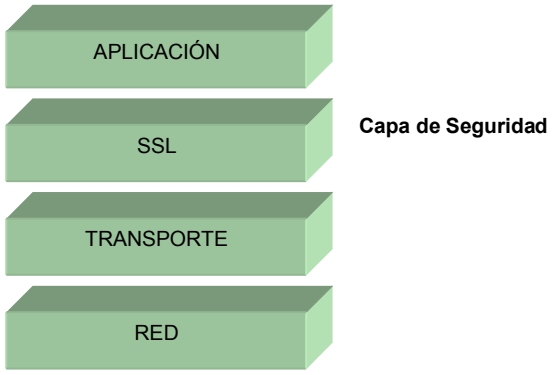


Figura II-30 – Capa de operación del protocolo SSL

SSL fue originalmente implementado en el navegador Netscape. Luego que la versión dos fue publicada, Microsoft mejoró algunos de sus problemas de seguridad e introdujo un protocolo similar denominado PCT (Private Communications Technology). Luego Netscape mejoró notablemente el protocolo desarrollando la versión tres, la cual es la más usada hoy en día.

SSL fue desarrollado principalmente para permitir transacciones comerciales seguras sobre la Web, por lo que el protocolo que más lo usa es HTTP, sin embargo SSL ha sido diseñado para ser independiente de la capa de aplicación, por lo que también es usado para hacer seguros otros protocolos de este nivel, como FTP para transferencia de archivos, SMTP para correo electrónico, Telnet para conexión a máquinas remotas, etc.

Protocolo	**Puerto TCP asignado**	**Protocolo protegido por SSL**	**Puerto TCP asignado**
https	80	HTTPS	443
smtp	25	SSMTP	465
pop3	110	SPOP3	995
telnet	23	TELNET	992
ftp	21	FTP	989 (Datos), 990 (Control)
nntp	119	NNTP	563
ldap	389	SSL-LDAP	646

Tabla II-2 – Puertos TCP tradicionales y puertos TCP al usar SSL

Por funcionar sobre la capa de transporte, SSL no altera el sistema operativo sino que es implementado en un proceso de usuario.

SSL normalmente requiere a TCP como protocolo de la capa de transporte, en vez de UDP. Este requisito fue impuesto para que la estructura de este protocolo resultara más simple, ya que no tiene que encargarse del control de flujo ni de la retransmisión de los datos perdidos que TCP realiza.

Al usar SSL se establece el equivalente de una red privada virtual (VPN) entre el servidor y el cliente. Como los datos de la aplicación viajan encriptados, esto crea un túnel o canal de comunicación seguro sobre redes públicas, abiertas, con recursos de transmisión y conmutación compartidos.

SSL utiliza criptografía de clave pública para autenticar los nodos y para establecer una clave de sesión simétrica que es usada para cifrar y proteger la integridad de la

información cursada entre ellos.

En SSL se llevan a cabo dos fases, una inicial denominada fase de *handshake* en la que se negocian los parámetros de seguridad que regirán la sesión, se autentica el servidor y opcionalmente, se autentica el cliente. Una segunda fase que es en la que se transmiten los datos de la aplicación que esta utilizando SSL, bajo los parámetros de seguridad que se hayan negociado.

A continuación se muestra una forma simplificada del protocolo, en la que se asume el uso de RSA como algoritmo de clave pública y autenticación solo del servidor:

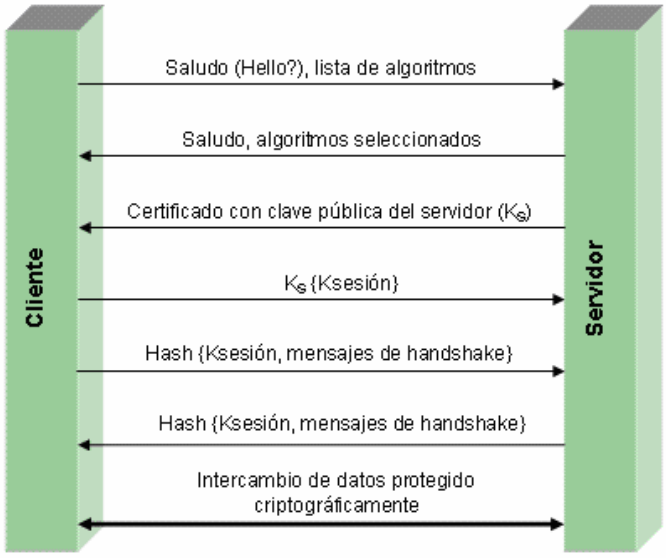


Figura II-31 – Modelo de Operación del protocolo SSL

1. El cliente inicia la conexión enviando un mensaje de saludo al servidor en el que proporciona una lista de los algoritmos de cifrado, autenticación y compresión que soporta.
2. El servidor envía un mensaje de saludo en el que responde con uno de los algoritmos de cifrado, autenticación y compresión que soporta, de los del grupo provisto por el cliente.
3. A continuación el servidor envía al cliente su certificado con su clave pública.
4. Luego el cliente genera la clave de sesión, la cifra con la clave pública del servidor y se la envía.

5. Adicionalmente el cliente envía un extracto cuyos argumentos son la clave de sesión y todos los mensajes anteriores intercambiados entre él y el servidor. El propósito de este mensaje es probar que el cliente conoce la clave de sesión y garantizar la integridad de la información cursada entre él y el servidor.
6. El servidor con su clave privada descifra la clave de sesión. Ahora, tanto cliente como servidor disponen de una clave secreta con la cual proteger criptográficamente la comunicación entre ambos.
7. Al igual que lo hizo el cliente, el servidor envía un extracto cuyos argumentos son la clave de sesión y todos los mensajes, anteriores a este, intercambiados entre ambos. Este mensaje permite probar que el servidor conoce la clave de sesión y garantiza la integridad de la información cursada entre él y el cliente.
8. Finalmente, comienza el intercambio de data protegida criptográficamente entre cliente y servidor. La data es fragmentada, se le agrega un código de autenticación y se cifra, antes de transferirse.

SSL actualmente se encuentra implementado tanto en Java (IAIK: iSaSiLk, Phaos Technology: SSLava, DSTC: JCSI) como en lenguaje C (Netscape Communication: SSLRef, Consensus Development: SSLPlus, OpenSSL). La implementación más popular de código abierto de este protocolo es el proyecto OpenSSL (www.openSSL.org), mantenido por una comunidad de voluntarios a nivel mundial y que está basado en la librería SSLeay desarrollada por Eric A. Young y Tim J. Hudson. Existen varias debilidades detectadas en las versión 2 del protocolo:

- Truncado de sesión (*Truncation Attack*). Para cerrar una sesión, SSL v2 dependía del cierre de la conexión TCP. Sin embargo, como los comandos TCP no están criptográficamente protegidos por SSL, por lo que un atacante podía finalizar la sesión enviando un mensaje de cierre de sesión TCP, y SSL no tenía forma de detectar que dicha sesión había terminado anormalmente. Para subsanar esta falla, en la versión tres del protocolo se agregó un mensaje de alerta, Notificación de cierre (Close_notify).
- Ataque de degradación (*Downgrade attack*). En SSL v2, no se protegía la integridad del handshake inicial, así que un atacante activo podía sustituir los

algoritmos criptográficos más robustos de la lista que el cliente le envía al servidor, forzando así que el servidor seleccionara algoritmos poco seguros para la sesión. Para corregir esta falla, en SSL v3 se incorporó el mensaje Fin de Handshake (Handshake Finished), para cerrar la fase de handshake. En este se incluye un hash de los mensajes de handshake y la clave simétrica que comparten servidor y cliente, por tal razón permite verificar la integridad de la información cursada entre ambos.

II.11 OpenVPN

OpenVPN es una aplicación de SSL de código abierto, fácil de usar y robusta para crear un túnel seguro entre 2 sitios.

OpenVPN soporta PKI (infraestructura de clave pública) para la autenticación de sesión, el protocolo de TLS para el intercambio de clave, diferentes algoritmos de cifrado y de autenticación. Permite encriptación convencional que usa una clave pre-compartida (modo de clave estático) o encriptación de contraseña pública (modo TLS) usado certificados para el cliente y el servidor.

II.12 Máquinas Virtuales

Para llevar a cabo las pruebas y experiencias con los protocolos explicados anteriormente, se pueden utilizar máquinas virtuales. Normalmente las computadoras corren un solo sistema operativo a la vez. Esos sistemas operativos utilizan drivers para comunicarse con el hardware instalado (teclado, mouse, controladores de disco duro, adaptadores de red, etc.). Una máquina virtual usa el hardware instalado en el equipo y lo comparte con cada uno de los sistemas operativos que corren dentro de ella. Algunos componentes de hardware son virtualizados, es decir, emulados por software. Estos componentes incluyen controladores de interrupciones, controladores de DMA, controladores de dispositivos IDE/ATA, de teclado, de mouse, buses, de memoria, etc. De esta manera pueden convivir diversos sistemas operativos dentro de un mismo equipo, ya que gran parte del hardware es emulado por la máquina virtual para cada uno de ellos. Lo que comparten entre todos son los dispositivos de entrada / salida, tal como unidades de diskette, de CD-ROM y por supuesto la memoria del sistema y el

CPU. Por tal motivo, cuanta más memoria tenga la PC, más sistemas operativos se pueden correr simultáneamente. Con respecto al espacio en disco duro, cada máquina virtual posee su propio disco duro virtual, que no es más que un archivo en el disco duro real. Este archivo parte de un tamaño establecido (típicamente 4 GB) y crece conforme se vayan agregando aplicaciones a la máquina virtual. Las aplicaciones que corren desde las máquinas virtuales no se distinguen en absoluto de las instaladas en una máquina física. Por convención, se usa el término host para referirse a la máquina física que sirve de soporte y el término guest para referirse a la máquina virtual. Las características de la máquina host deben ser bastantes elevadas, sobre todo en lo que concierne a memoria, ya que cada sistema operativo que corre ocupa una buena parte de los recursos.

Para probar cómo funcionan los protocolos de comunicación se puede utilizar una LAN virtual, todo en una sola máquina. La interfaz virtual se comporta como un adaptador o tarjeta física de red con su propia dirección IP, máscara de red, puerta de enlace, etc. Puede asignársele una dirección válida en Internet o una dirección interna en la red virtual. Se pueden crear complejas redes virtuales para probar túneles IPSec, SSH, SSL.

El concepto de *virtualización* lo introdujo IBM en su sistema operativo VMS para mainframe hace varias décadas, pero es sólo en los años recientes que se ha ido popularizando para computadoras personales mediante productos como VMware (*http://www.vmware.com*) y Virtual PC (*http://www.microsoft.com/windows/virtualpc*). Recientemente han ido surgiendo muchos otros proyectos (especialmente en el mundo del software libre) que siguen la estela marcada por VMware, como por ejemplo Bochs (*http://bochs.sourceforge.net*).

VMware fue el primer software para máquina virtual que se difundió ampliamente. VMware Wokstation 4 es la versión más liviana. Para aplicaciones pesadas existe VMware GSX Server y VMware ESX Server. VMware corre bajo Windows NT, 2000, 2003 o XP. También existe una versión para Linux que corre sobre diversas distribuciones, como SuSE, Mandrake, Red Hat.

VMware Workstation 4 es una potente herramienta que permite tener varios sistemas operativos instalados sin necesidad de particiones. Es poco menos que asombroso

poder abrir un sistema operativo dentro del propio y ejecutarlo en una ventana, sin necesitar ningún reinicio, como si de un programa más se tratase o a pantalla completa, como si el anterior sistema operativo hubiese desaparecido. Se puede así tener simultáneamente, por ejemplo, Windows XP con Linux, sin ningún problema. Otra de sus ventajas es que una vez instalados los sistemas operativos adicionales a través de VMware, se pueden trasladar a otro PC o a otra partición, sin dificultad. Los requerimientos para VMware son los siguientes:

- Procesador: 400 MHz mínimo, 1 GB o más recomendado. Soporta multiprocesamiento.
- Tipo de procesador: Celeron, Pentium, Xeon, Athlon, Duron, Opteron.
- Memoria: 128 MB mínimo, 256 MB recomendado.
- Espacio en disco: 100 MB para el host y al menos 1 GB para cada máquina guest.
- Monitor: SVGA con resolución recomendada de 800 x 600.

VMware soporta los siguientes sistemas operativos guest:

- MS-DOS 6.x
- Windows 3.1, 3.11 for Workgroups, 95, 98, 98SE, Me
- Windows NT y sus variantes
- Windows 2000 y sus variantes
- Windows XP Professional y Home Edition
- Windows 2003 y sus variantes
- Linux en algunas de sus distribuciones como Mandrake, Red Hat, SuSE
- FreeBSD
- Novell Netware 5.1 y 6
- Otros sistemas operativos

Bajo una plataforma Windows XP Professional se ha probado Sun Solaris 9 junto a Red Hat Linux 9 y Windows 2000 Professional, y los tres corren satisfactoriamente. La única desventaja para los sistemas operativos que no se listan arriba, es que VMware

Workstation no brinda soporte a través de VMware Tools. Por ejemplo, al instalar Solaris 9, la resolución de vídeo no puede fácilmente ajustarse, pero existen sitios en Internet que explican cómo hacerlo. Algunas de las especificaciones para la máquina virtual son las siguientes:

- Procesador: El mismo de la máquina host.
- Tarjeta madre: Emula Intel 440BX con chipset NS338 SIO y 82093AA IOAPIC.
- BIOS: PhoenixBIOS 4.0 Release 6 con VESA BIOS.
- Memoria: Hasta 1GB, dependiendo la memoria física.
- Gráficos: VGA y SVGA.
- Sonido: Emula Creative Labs Sound Blaster AudioPCI.
- Adaptador Ethernet: Emula hasta 3 adaptadores virtuales tipo AMD PCnet-PCI II.
- Redes virtuales: Hasta 9 switchs virtuales Ethernet.

II.13 Redes Virtuales

Con las máquinas virtuales se pueden crear *redes virtuales* que se comportan prácticamente como redes reales. De esta forma se pueden realizar pruebas y experiencias sin añadir componentes físicos. Con VMware se pueden "instalar" hasta 3 adaptadores virtuales Ethernet (NIC: *Network Interface Card*) en cada máquina virtual. Esos adaptadores se conectan a la red virtual mediante un *switch virtual*. Se dispone de 9 switches virtuales con los cuales se pueden crear hasta 9 redes virtuales (VMnet0…VMnet8). Además se dispone de servidores DHCP (*dynamic host configuration protocol*) y dispositivo NAT (*network address translation*). Una máquina virtual también puede conectarse a la red Ethernet real a través de un *puente virtual*.

Durante el proceso de creación o de modificación de una máquina virtual, VMware permite seleccionar 3 tipos de conexiones de red (o ninguna), como se ilustra a continuación.

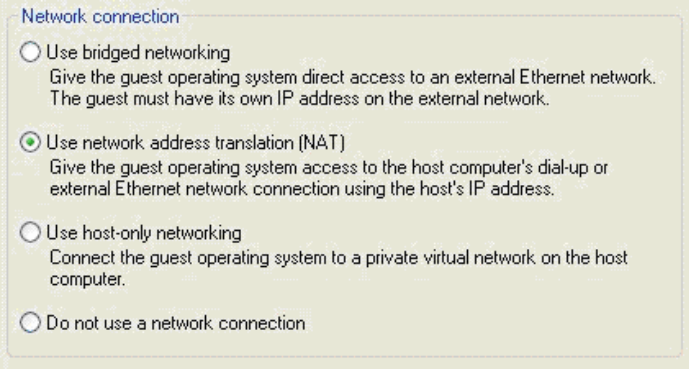


Figura II-32 – Tipos de conexión de red de una Maquina Virtual VMWare

A) *Bridged networking* hace que la máquina virtual se conecte a la red externa a través del virtual bridge, tal como si fuese una máquina más. Si uno está conectado a una LAN (o WLAN) en su casa o oficina, ahora dispone de 2 o más computadoras conectadas directamente a la red. Por supuesto que hay asignarle a cada máquina virtual una dirección IP diferente de la máquina física y además su máscara de red, puerta de enlace, etc. Esto se puede hacer manualmente o a través de un servidor DHCP externo.

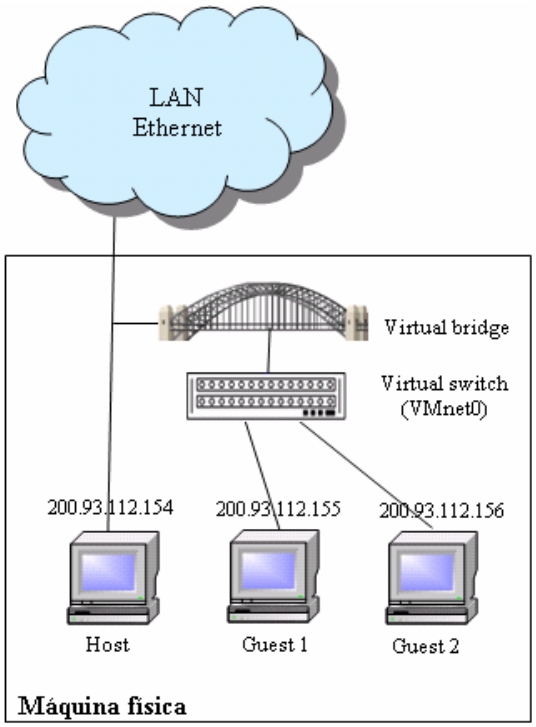


Figura II-33 – Conexión de red puenteada (bridged) en VMWare

B) *Network address translation* (NAT) permite que la máquina virtual utilice la dirección IP de la máquina física para conectarse a la red, usando la conocida técnica de traducción de direcciones. Esto es útil en el caso de que en la casa o oficina uno disponga de una sola dirección IP y desea que también las máquinas virtuales se conecten al mundo exterior (pero no son accesibles desde afuera).

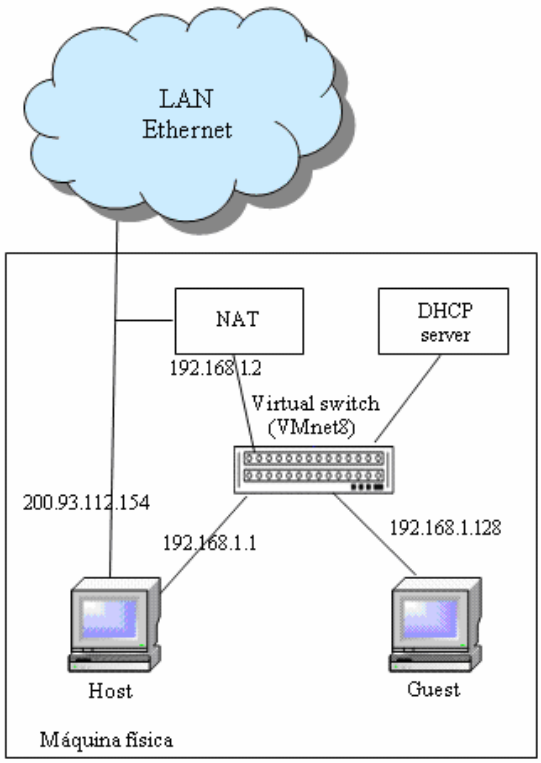


Figura II-34 – Conexión de red mediante NAT en VMWare

C) *Host-only networking* hace que sólo la máquina física (host) se conecte a la red externa, pero las máquinas virtuales pueden comunicarse entre ellas y con la máquina real, pero no hacia fuera. Puede que ni exista red externa. Esta configuración es conveniente cuando se vayan a hacer pruebas o experiencias en ambiente aislado, que no requieran, por ejemplo, acceso a Internet.

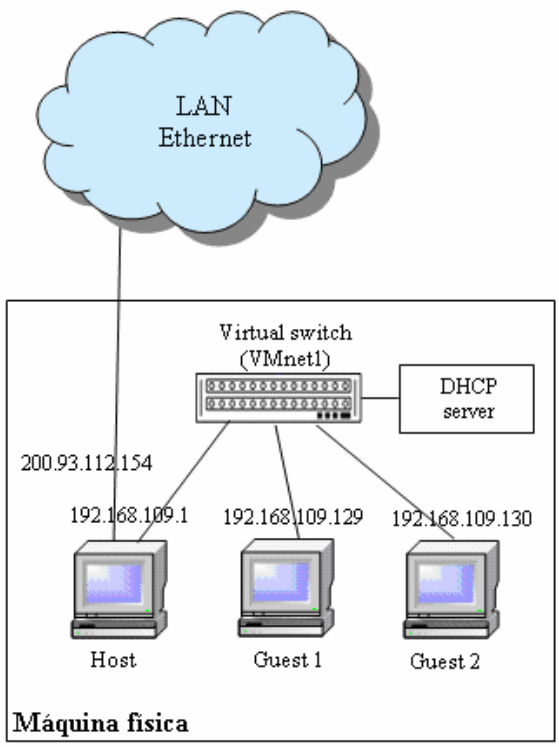


Figura II-35 – Conexión de red Host-only en VMWare

II.14 Analizadores de Tráfico

Estos dispositivos son muy útiles para los trabajos de investigación en redes, ya que permiten encontrar y solucionar variados problemas. También son una excelente ayuda didáctica para entender cómo funcionan los protocolos de las redes modernas.

Uno de los productos comerciales más conocidos es Sniffer Pro (www.nai.com), de Network Associates. Otro es Ethereal (http://www.ethereal.com), que es un producto de distribución gratuita, al contrario de Sniffer.

Ethereal es quizás uno de los mejores capturadores de paquetes, de fuente abierta, disponible actualmente. Ethereal (*www.ethereal.com*), es una analizador de protocolos rápido, simple y gratuito, al contrario de Iris, Agilent Advisor o Sniffer Pro, que son productos comerciales.

Las características más interesantes de Ethereal son:

- ✓ Disponibles para Windows y UNIX.

- ✓ Captura y despliega los paquetes desde cualquier interfaz en un sistema de UNIX.
- ✓ Muestra los paquetes capturados bajo un numero capturados de otros programas:
    - o TCPDUMPC.
    - o Network Associates Sniffer and Sniffer Pro.
    - o NetXray.
    - o LANalyzer.
    - o Shomiti.
    - o AIX's iptrace.
    - o RADCOM's WAN/LAN Analyzer.
    - o Productos de acceso Lucent/Ascend.
    - o HP-UX's nettl.
    - o Enrutadores Toshiba's ISDN.
    - o Utilidad ISDN4BSD i4btrace.
    - o Microsoft Network Monitor.
    - o Sun snoop.

- ✓ Salvar lo capturado en varios formatos:
    - o Libpcap (tcpdump).
    - o Sun snoop.
    - o Microsoft Network Monitor.
    - o Network Associates Sniffer.

- ✓ Filtrar los paquetes en muchos criterios.
- ✓ Búsqueda por paquetes utilizando filtros.
- ✓ Muestra en olores los paquetes basados en filtros.

Iris es un analizador de tráfico desarrollado por EEye Digital Security (www.eeye.com). Si bien es parecido a otros productos como Agilent Advisor, Sniffer

Pro y Ethereal, su tecnología avanzada permite reconstruir totalmente los datos tal como lo ven los usuarios. Las características más interesantes de Iris son:

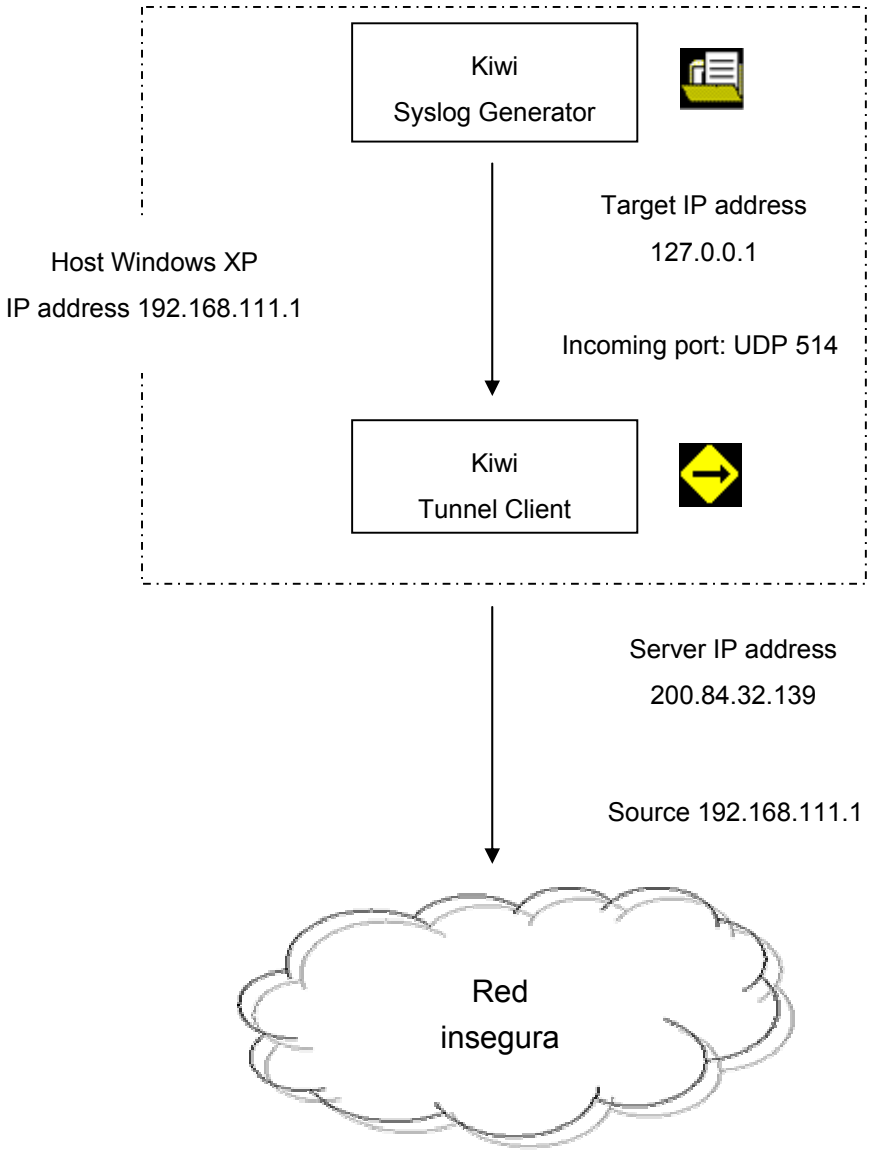
- *Decodificación de protocolos*: Se puede analizar el tráfico en la red en un formato simple de entender y se pueden producir distintos reportes gráficos.
- *Reconstrucción de paquetes:* Se pueden reconstruir las sesiones Web y se pueden simular cookies para entrar en sitios Web protegidos con contraseña, para así evaluar la seguridad de la red de una organización.
- *Supervisión del correo y mensajería electrónica:* Esta facilidad puede complementar los procedimientos para que se haga un uso correcto y racional de los medios electrónicos de comunicación por parte de los empleados.
- *Filtrado de tráfico:* Se pueden usar reglas o criterios para filtrar los paquetes que se van a capturar, por ejemplo dirección MAC, dirección IP, palabra clave, puerto, capa del protocolo, etc. Los filtros permiten buscar un tipo de contenido específico y rastrear patrones de tráfico que puedan corresponder a un virus o a información confidencial de la empresa.
- *Manipulación y forjado de paquetes (spoofing):* Se pueden crear paquetes a la medida o modificar paquetes previamente capturados para luego enviarlos a la red. Esta facilidad se puede utilizar para probar un firewall y asegurarse de que bloquea y filtra los paquetes correctamente. También permite evaluar la capacidad de soportar una carga elevada por parte de un sistema o de un servidor y simular ataques de negación de servicio (DoS).
- *Registro de intentos de conexión:* Se puede capturar y registrar la evidencia de intrusiones en la red, reconstruyendo cada movimiento que un atacante haya hecho.

CAPITULO III - FASE EXPERIMENTAL

En este capítulo se describen las experiencias que se llevaron a cabo para probar las diferentes soluciones a fin de establecer un canal seguro para la notificación de eventos generados por Syslog y Traps SNMP.

III.1 Kiwi Secure Tunnel

Se empezó por experimentar con Kiwi Secure Tunnel, por ser un producto diseñado específicamente para el envío seguro de mensajes Syslog entre 2 máquinas. La figura siguiente ilustra el arreglo utilizando una máquina real (host) y una máquina virtual (guest), ambas conectadas a Internet.



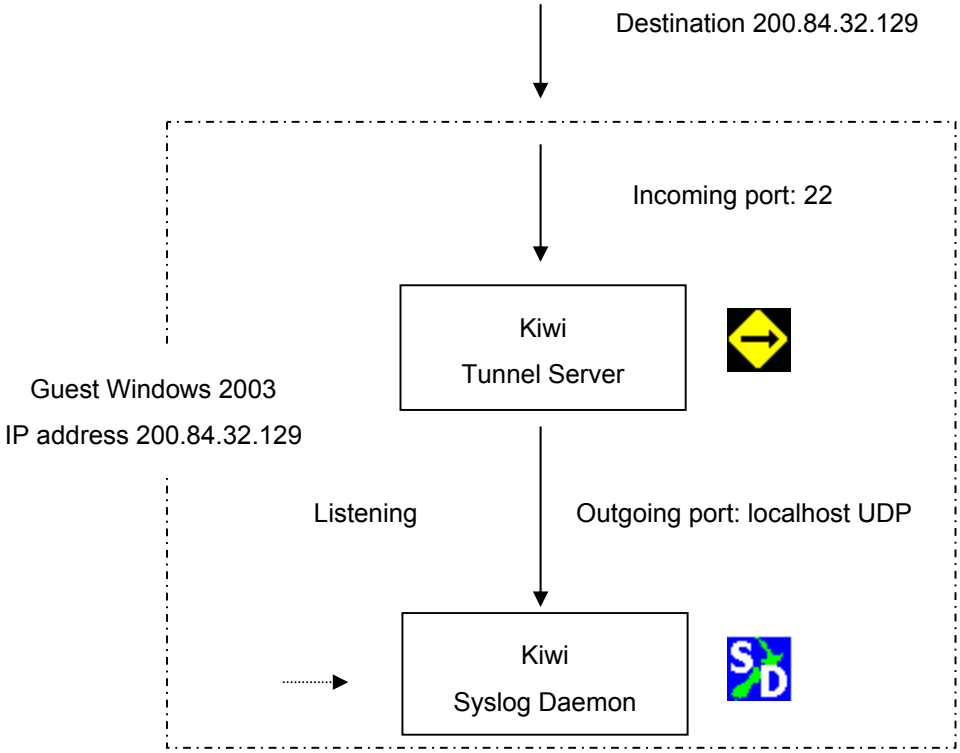


Figura III-1 – Arreglo experimental del túnel Kiwi

En primer lugar se procedió a la instalación del módulo cliente en un extremo del túnel. Luego se configuró en base a los siguientes pasos:

- Colocar la dirección IP del Kiwi Tunnel Server al que se va a conectar (200.84.32.129).
- Colocar el login y el password (deben ser los mismos que en el Kiwi Tunnel Server).
- Colocar el puerto del servidor (usualmente 22, el mismo de SSH).
- Seleccionar el método de encriptación.
- Activar o no la compresión de datos.
- Agregar un puerto entrante, usualmente el 514, que es el predefinido para Syslog.

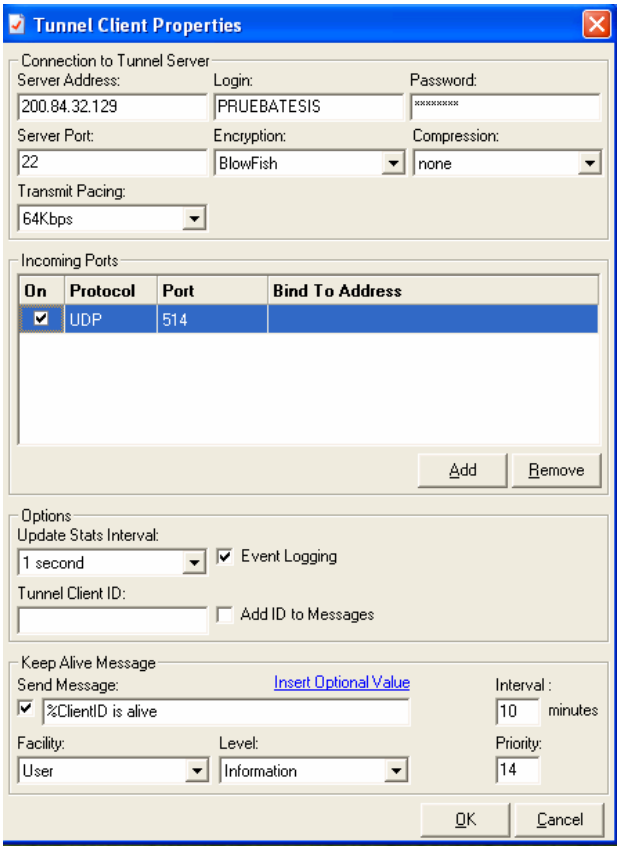


Figura III-2 – Configuración de Kiwi Tunnel Client

Luego de esos pasos, se instaló y se activó el servicio.

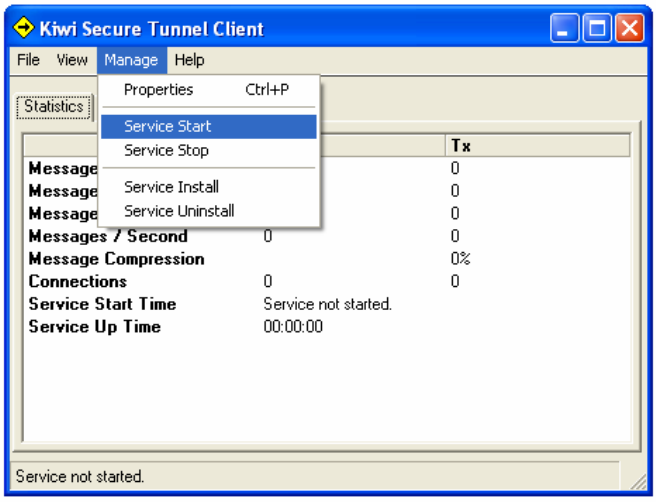


Figura III-3 – Instalación e inicio del servicio de Kiwi Tunnel Client

La instalación y configuración del módulo servidor en el otro extremo del túnel es similar al del cliente.

La opción *Bind to:* permite que los mensajes entrantes sean aceptados sólo desde la interfaz especificada (en el caso de que la máquina posea varias interfaces de red). Si se deja en blanco (lo usual), acepta los mensajes desde cualquier interfaz.

La opción *Bind to Address:* permite que los mensajes salientes sean enviados sólo por la interfaz especificada.

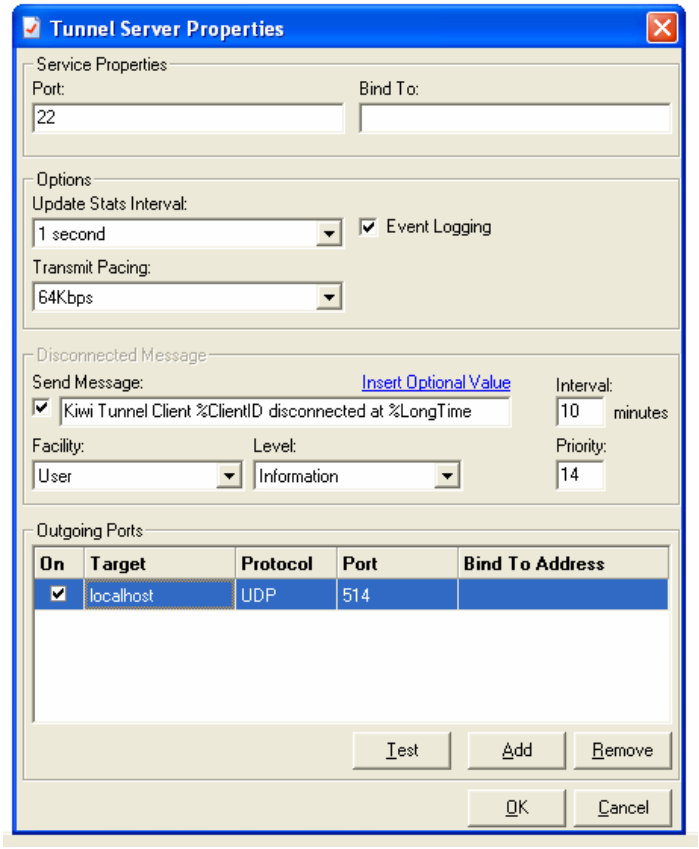


Figura III-4 – Configuración de Kiwi Tunnel Server

Si en vez de local host se pone una dirección IP, a la salida del túnel el mensaje desencriptado es reenviado a esa dirección IP. Esto es útil en el caso de que el servidor Syslog resida en una máquina distinta a la que reside el Kiwi Tunnel Server.

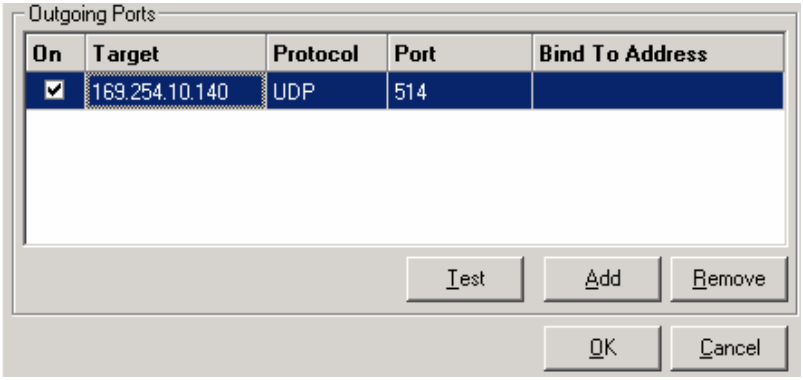


Figura III-5 – Configuración de Kiwi Tunnel Server para reenvío de mensajes

Además se debe crear un Login y Password para cada conexión de cliente entrante.

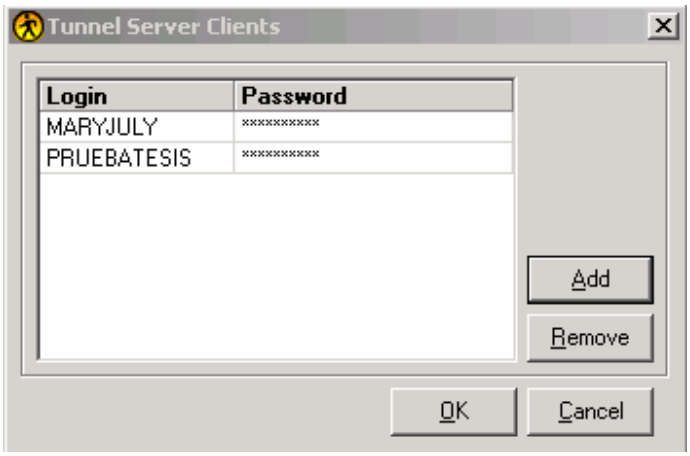


Figura III-6 – Creación de clientes autorizados para Kiwi Tunnel Server

Luego de completar esos pasos, se instaló y se activó el servicio.

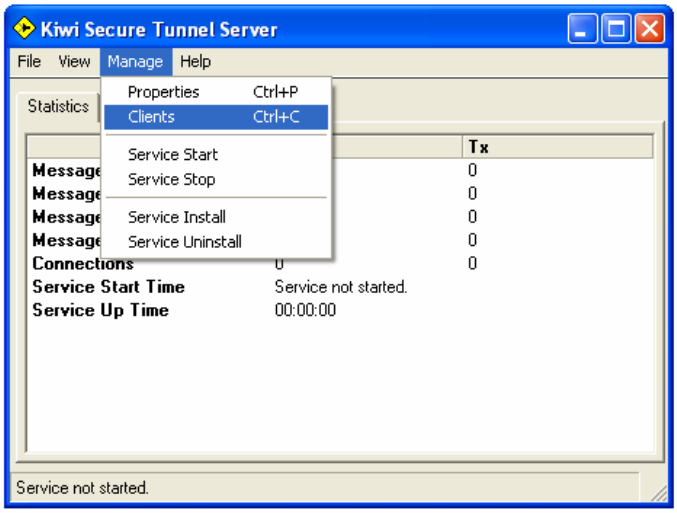


Figura III-7 – Instalación e inicio del servicio de Kiwi Tunnel Server

Finalmente se estableció automáticamente el túnel entre ambas máquinas, lo cual se pudo verificar en la ventana de status, así como en el log.

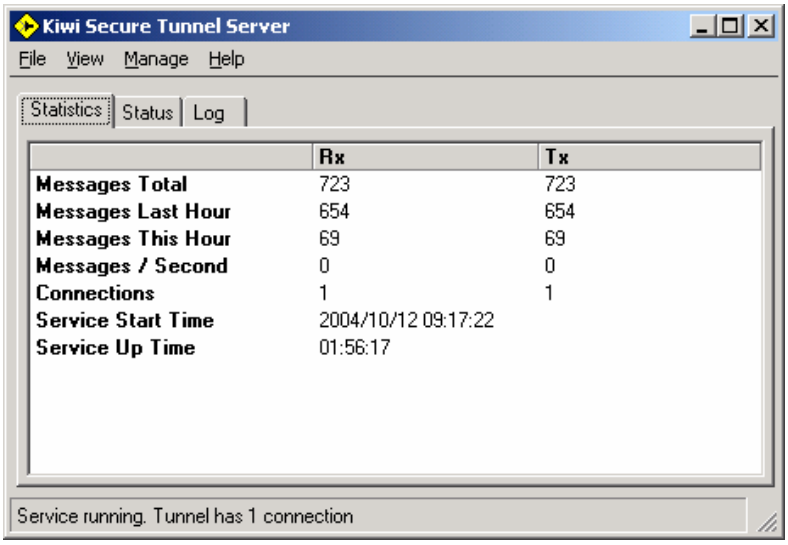


Figura III-8 – Ventana de estado del Kiwi Tunnel Server

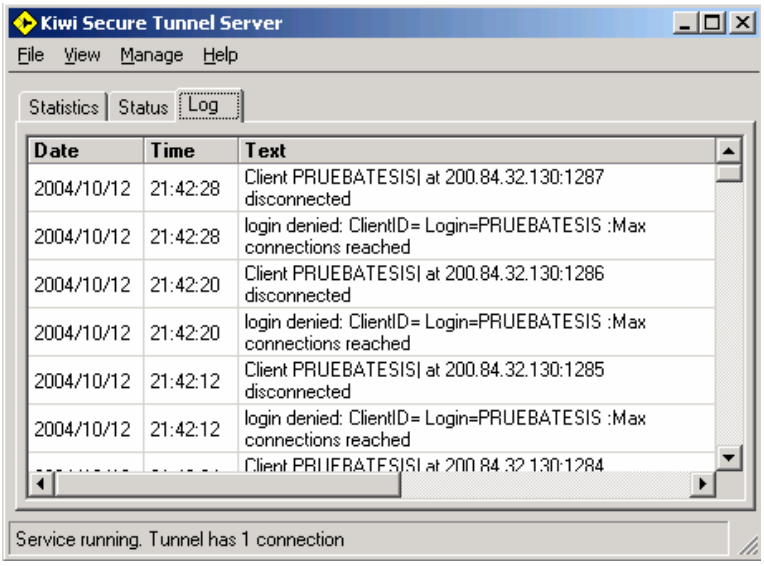


Figura III-9 – Ventana de log de Kiwi Tunnel Server

Del lado del cliente también se pudo verificar que el túnel efectivamente está establecido.

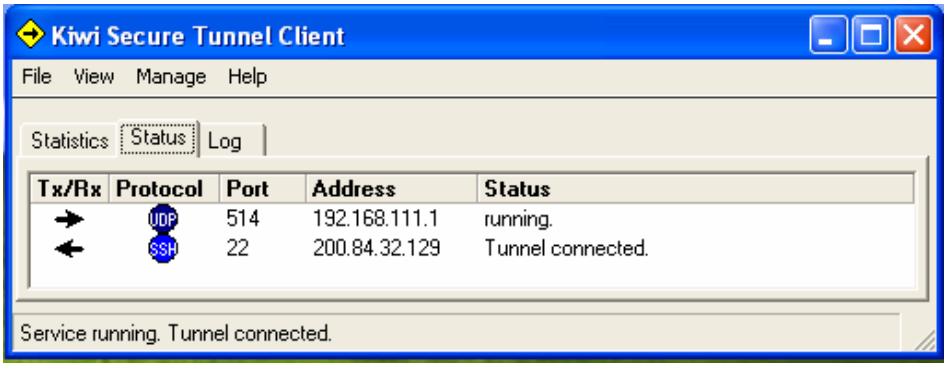


Figura III-10 – Verificación del establecimiento del túnel

Captura de tráfico

Para verificar que los mensajes Syslog efectivamente estaban encriptados, se utilizó el analizador de tráfico Ethereal, el cual además de ser de código abierto, posee la ventaja con respecto a Iris que también decodifica el tráfico en la interfaz virtual y se generaron mensajes de prueba Syslog.

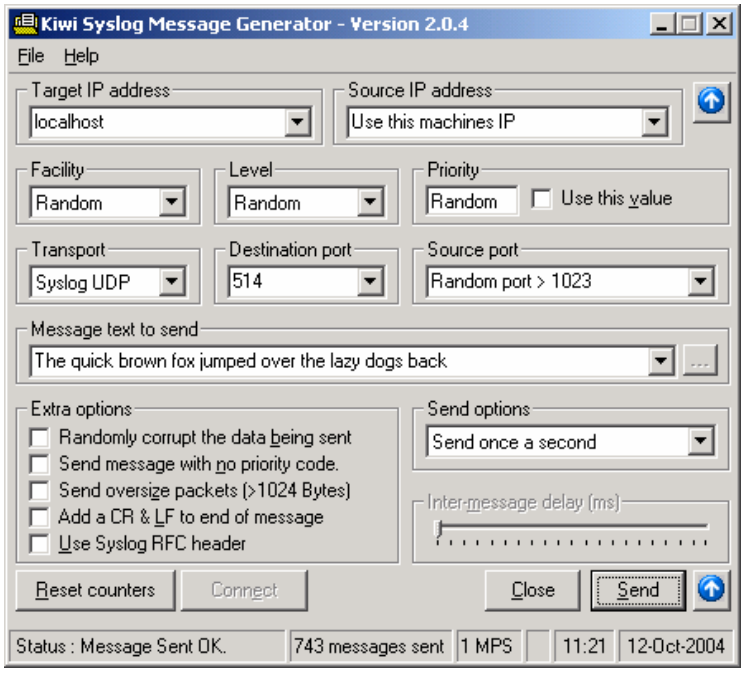


Figura III-11 – Configuración del generador de mensajes Syslog

Como se puede notar en la siguiente figura, el tráfico aparece como protocolo SSH, ya que usa el puerto 22, que es el puerto predefinido para ese protocolo. Además todo está encriptado.

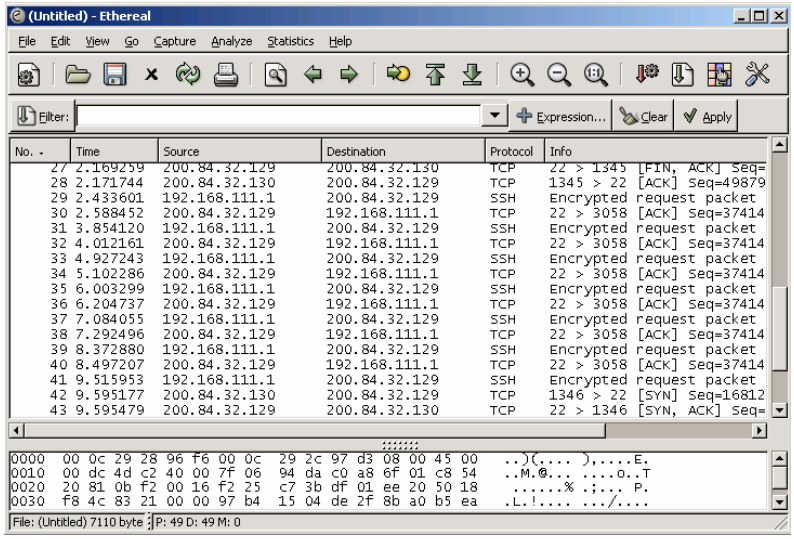


Figura III-12 – Mensajes Syslog encriptados a través de la red

En cambio, si no usa el túnel y los mensajes Syslog se envían directamente al servidor (200.84.32.129) en vez que a la entrada del túnel (127.0.0.1), el tráfico evidentemente no viaja encriptado.

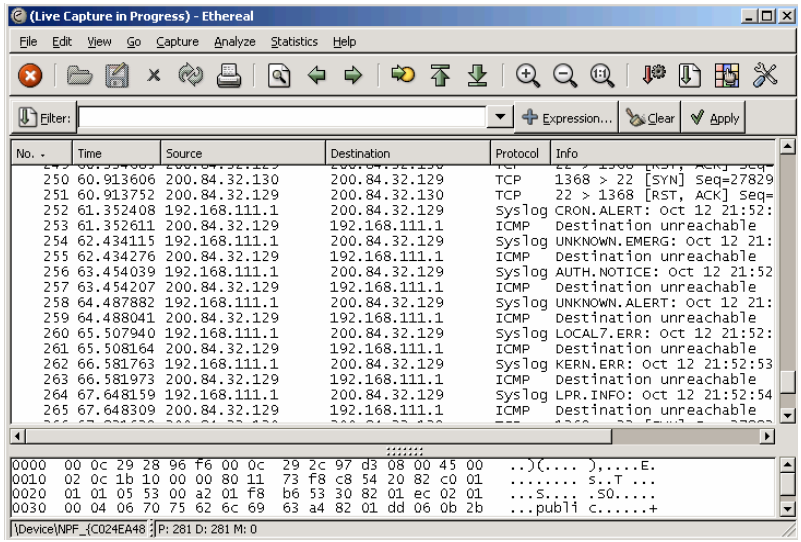


Figura III-13 – Mensajes Syslog desencriptados.

III.2 Túnel VPN con PPTP

Para experimentar con otra posible solución en relación a la seguridad de los mensajes Syslog y trap SNMP, se configuró un túnel VPN utilizando un servidor Windows 2003.

Se instalo localmente un laboratorio virtual VPN sin necesidad de estar conectado a Internet, utilizando VMware, tal como se ilustra en la figura siguiente. El servidor VPN posee Windows Server 2000/2003. Con Windows Server 2000 se encontraron problemas en la expedición de certificados para VPN con IPSec. La conexión entre el cliente VPN y el servidor VPN se hizo utilizando las interfaces virtuales VMnet1, VMnet2 y VMnet3.

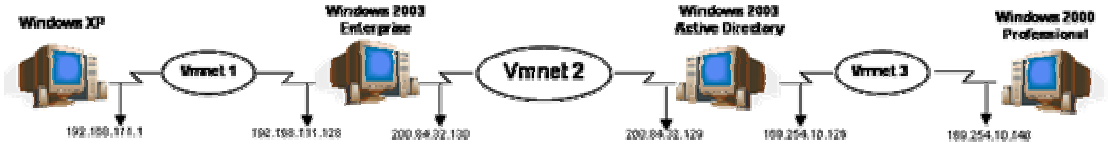


Figura III-14 – VPN con PPTP

Se configuraron VMnet1, 2 y 3 con sus respectivas direcciones IP, través del menú *Edit | Virtual Network Settings | Host Virtual Network Mapping* y luego llenando las casillas de la subred.

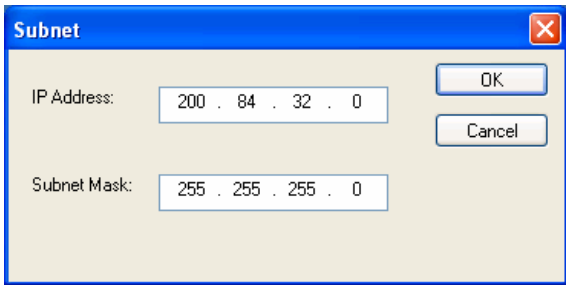


Figura III-15 – Configuración de adaptador virtual de red

Luego se añadió y activó un servidor DHCP para VMnet2. (Nota: De haber ya un servidor DHCP en la red privada, esto no hace falta).

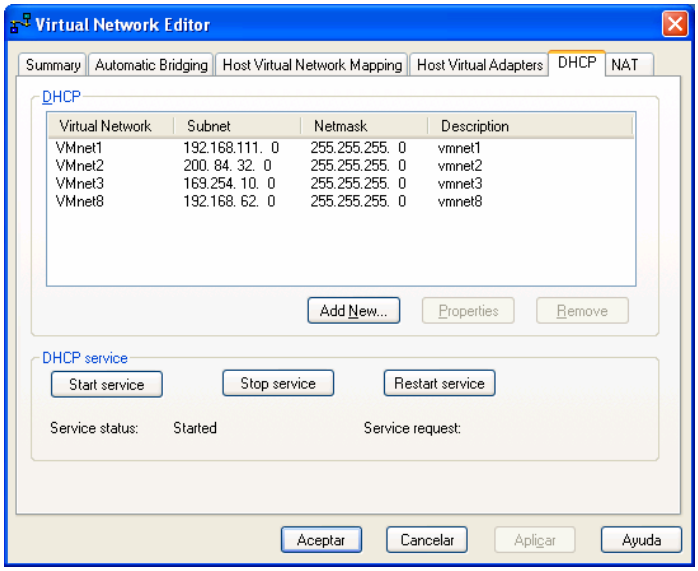


Figura III-16 – Configuración DHCP

Se procedió a añadir los adaptadores de red Ethernet necesarios para el servidor VPN. El NIC 2 va conectado a VMnet2.

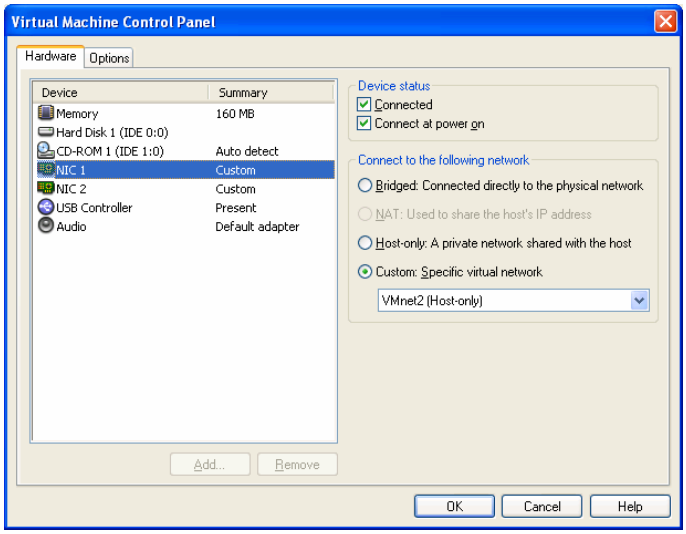


Figura III-17 – Ventana de configuración de la Máquina Virtual

Se inicio el servidor Windows 2003 (sistema host) y luego se procedió a activar el servicio VPN a través del menú *Inicio* | *Herramientas administrativas* | *Enrutamiento y acceso remoto*.

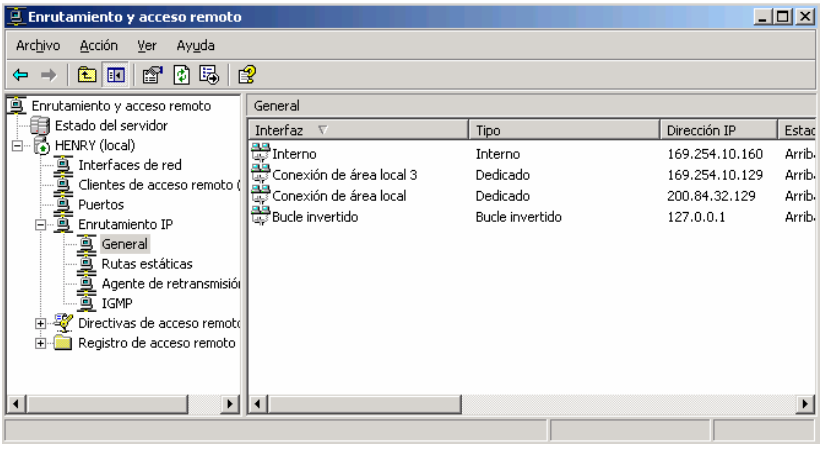


Figura III-18 – Configuración de enrutamiento y acceso remoto

Se creó y activó una cuenta de usuario para conexión remota.

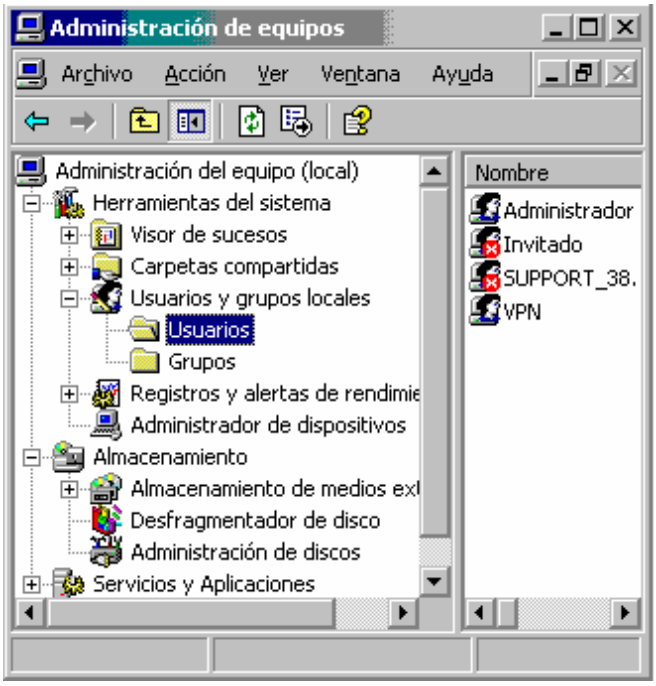


Figura III-19 – Ventana de creación de cuenta de usuario

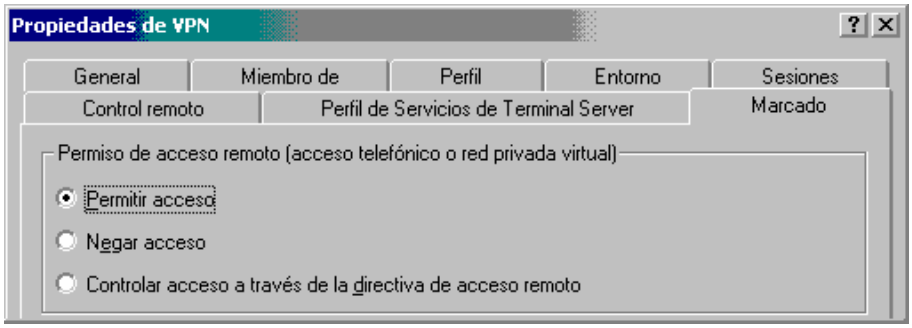


Figura III-20 – Activación de permiso de acceso remoto

Establecimiento del túnel PPTP

Una vez completada las fases anteriores, del lado del sistema host se procedió a crear una conexión nueva de red para establecer un túnel PPTP, de acuerdo a los pasos que se ilustran a continuación.

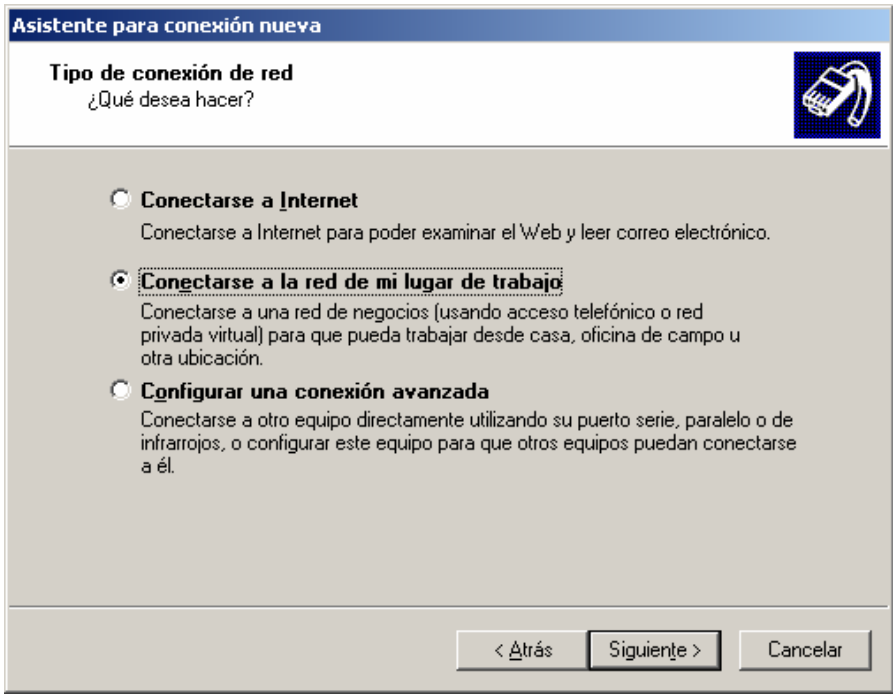


Figura III-21 – Selección del tipo de conexión de red

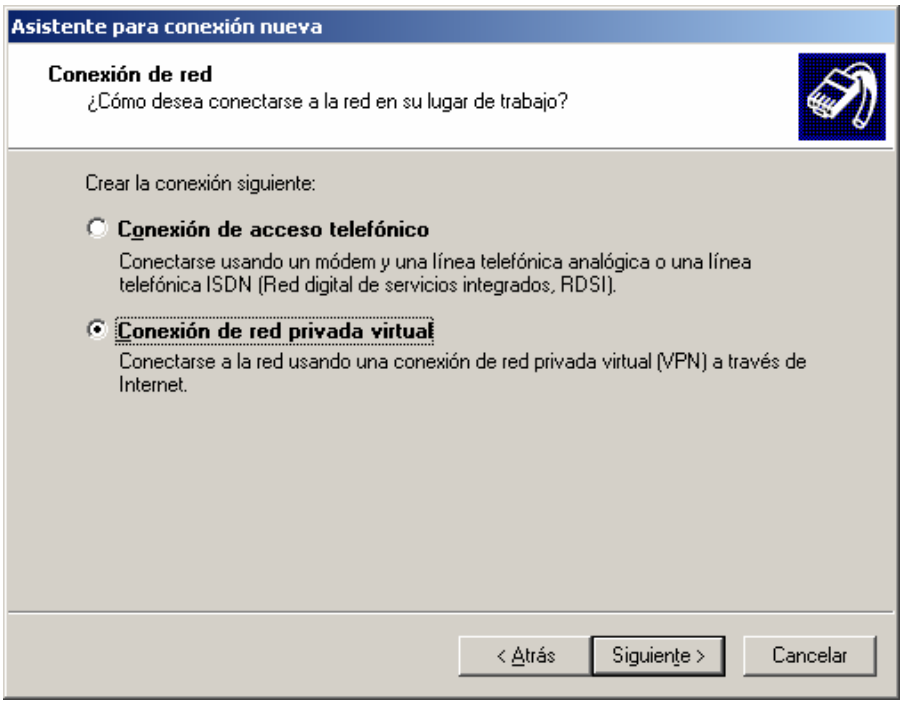


Figura III-22 – Selección modo de conexión del tipo de red

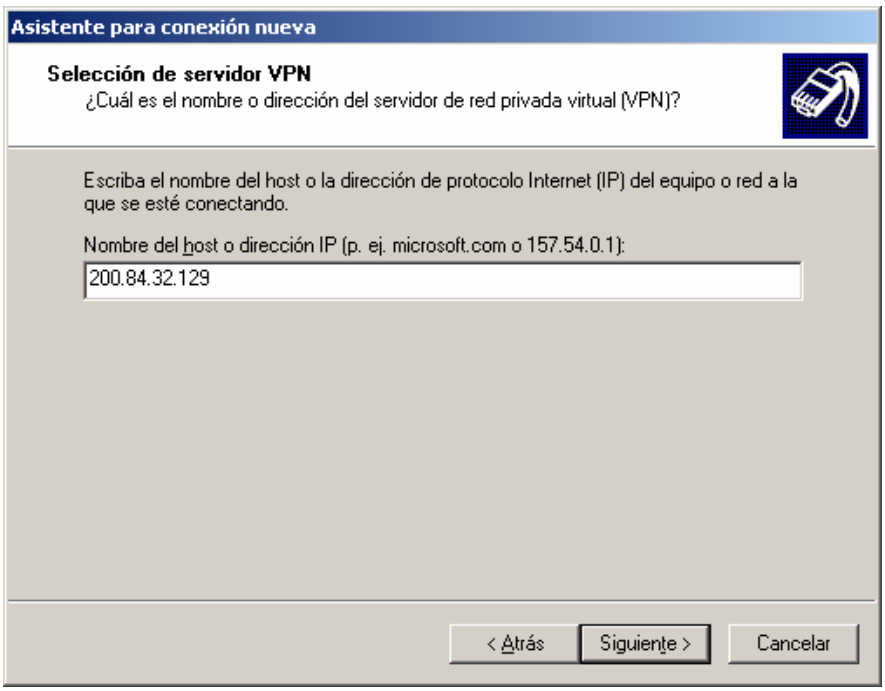


Figura III-23 – Selección del nombre o dirección del servidor VPN

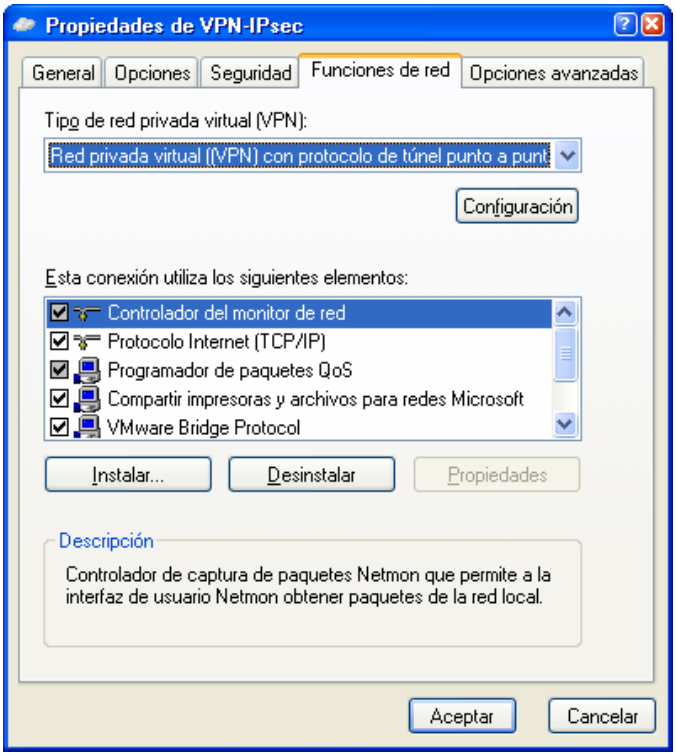


Figura III-24 – Selección de tipo de VPN en el cliente

Usando el login y la contraseña correcta, la conexión VPN mediante PPTP se estableció rápidamente.

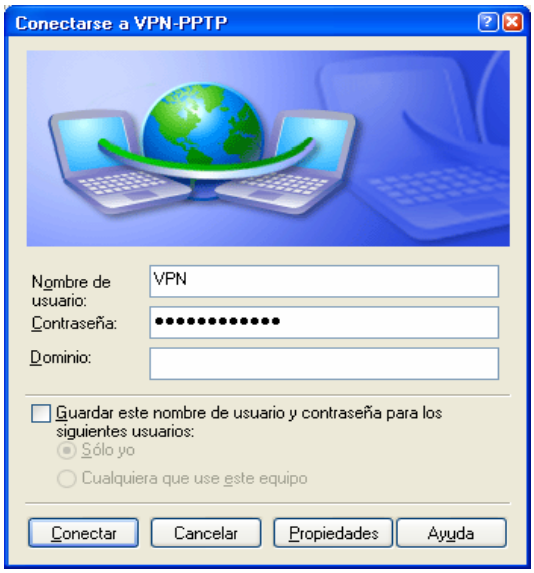


Figura III-25 – Solicitud de credenciales

Haciendo clic sobre la conexión, se pudieron observar detalles interesantes sobre el túnel PPTP.

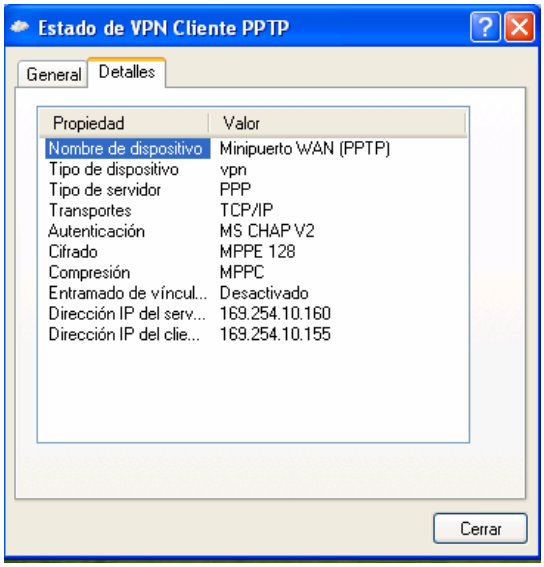


Figura III-26 – Detalles de la conexión VPN vía PPTP

Del lado del cliente VPN se ejecutó IPconfig y se pudo así notar la existencia de un nuevo adaptador PPP temporal con su dirección IP correspondiente a un extremo del túnel.

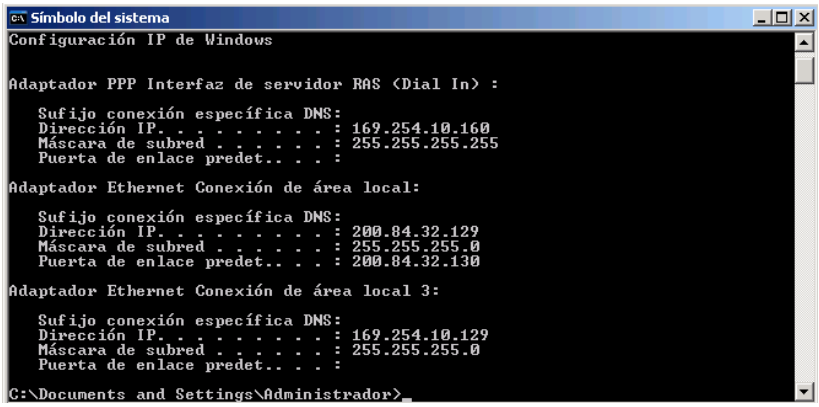


Figura III-27 – Configuración IP de la conexión VPN vía PPTP

Captura de tráfico

Para verificar que los mensajes Syslog y traps SNMP efectivamente viajaban encriptados, se utilizó el analizador de tráfico Ethereal y se capturó el tráfico en varias partes de la red. Los resultados se muestran en las siguientes figuras.

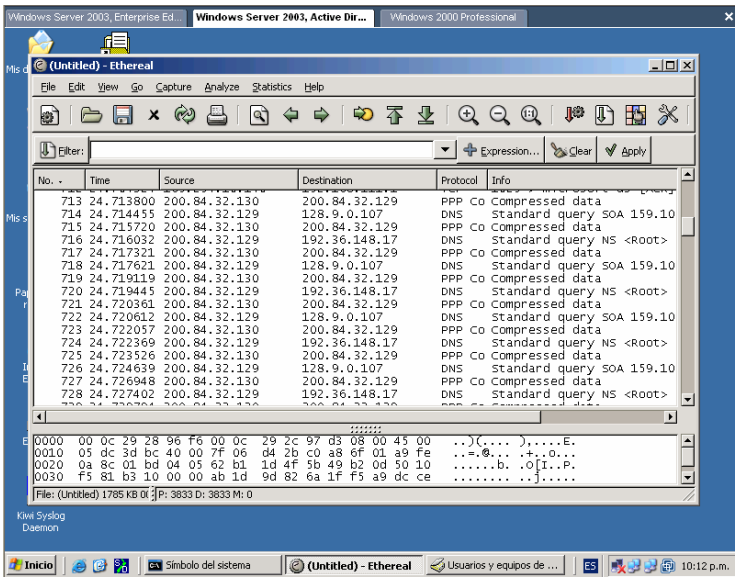


Figura III-28 – Mensajes Syslog encriptados y comprimidos por el túnel PPTP

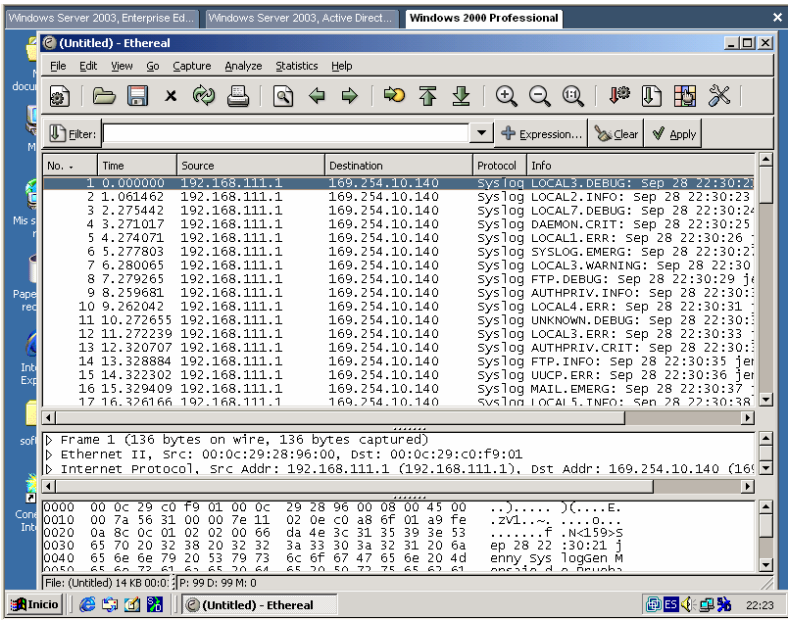


Figura III-29 – Mensajes desencriptados fuera del túnel PPTP

III.3 Túnel VPN con L2TP/IPSec

Esta experiencia resultó ser mucho más complicada que las anteriores debido a problemas con los certificados digitales. El sistema operativo Windows admite dos métodos de autenticación para las conexiones VPN basadas en L2TP/IPSec: clave secreta compartida o certificados digitales. El primer método es débil, por lo que sólo se recomienda como medida transitoria mientras se implementa la infraestructura de claves públicas (PKI) para obtener certificados digitales

Instalación de servidor de certificados digitales

Para disponer del servicio de emisión de certificados en un servidor Windows 2000/2003, se debe instalar primero el servidor Web conocido como IIS (*Internet Information Services*). Luego mediante el procedimiento de *Agregar o quitar componentes de Windows*, es que se instala el servicio de Certificate Server.

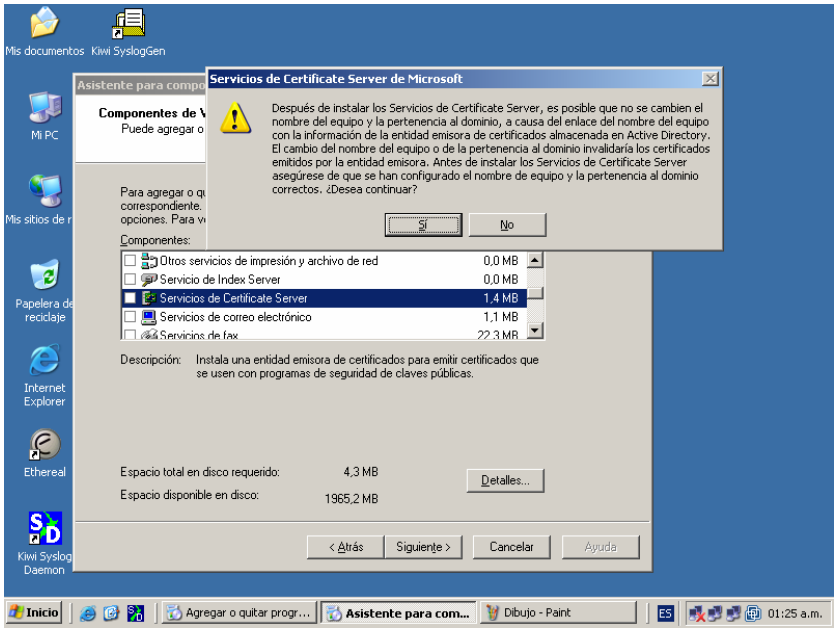


Figura III-30 – Instalación de servicio de Servidor de Certificados

La instalación de entidad emisora de certificados raíz de empresa requiere que el servidor sea miembro de un dominio y que se utilice el servicio de directorio de Active Directory. Por simplicidad, se utilizó la entidad emisora raíz independiente.

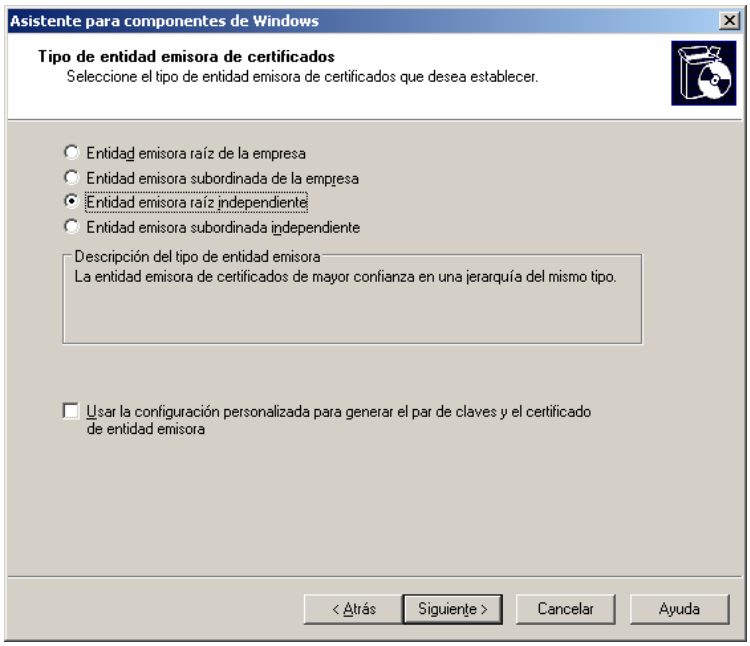


Figura III-31 – Creación de entidad emisora raíz del Servidor de Certificados

En *Nombre común para esta entidad emisora de certificados*, se puso un nombre descriptivo (*Autoridad VPN*). Se rellenó también la casilla *Sufijo de nombre completo,* separando los campos con coma.

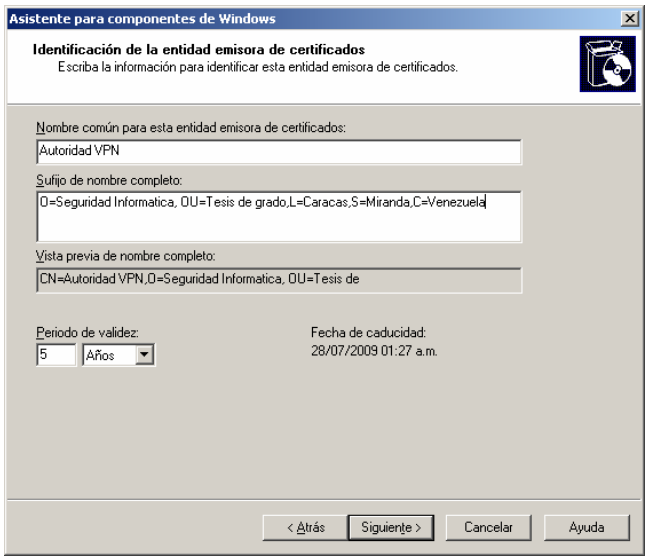


Figura III-32 – Características de la entidad emisora de certificados

Una vez instalado el servicio, se procedió a administrarlo mediante *Configuración* | *Herramientas Administrativas* | *Entidad Emisora de Certificados.*

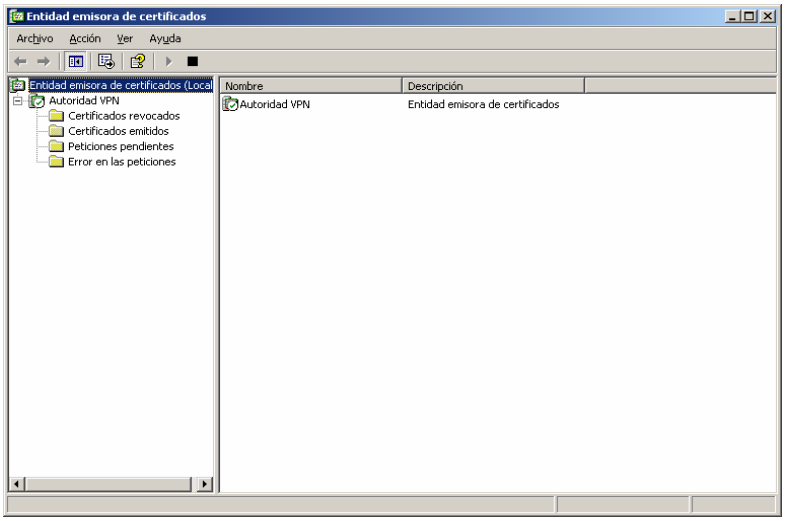


Figura III-33 – Administración de la Entidad Emisora de Certificados

Se configuró para que el certificado se expida automáticamente cuando un usuario lo solicita vía Web.

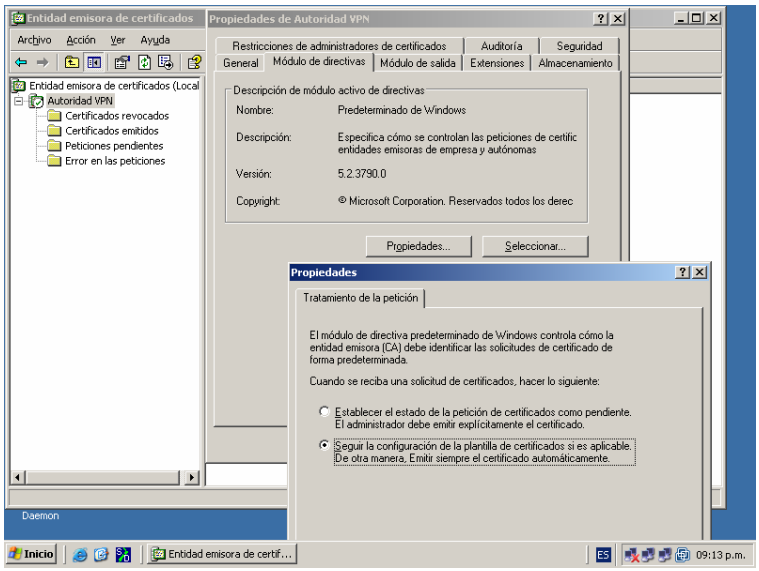


Figura III-34 – Expedición automática de certificados

Una vez instado el servicio de certificados, se pasó a instalar el servicio VPN mediante *Inicio* | *Herramientas administrativas* | *Enrutamiento y acceso remoto,* seleccionando la primera opción en el Asistente.

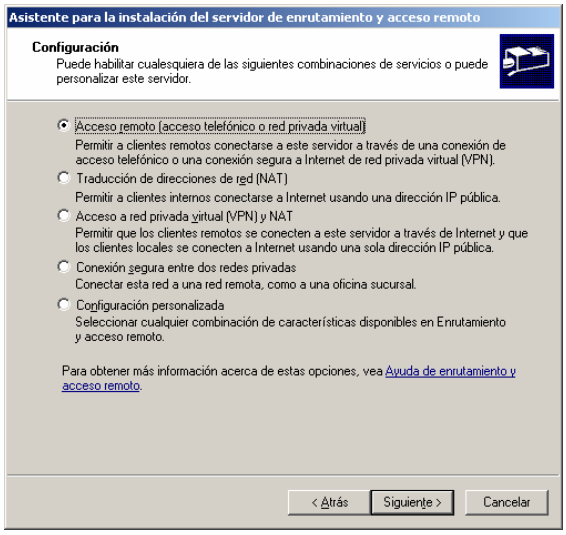


Figura III-35 – Asistente de instalación de Servidor de Enrutamiento

Aquí se escogió la opción de acceso remoto para VPN:

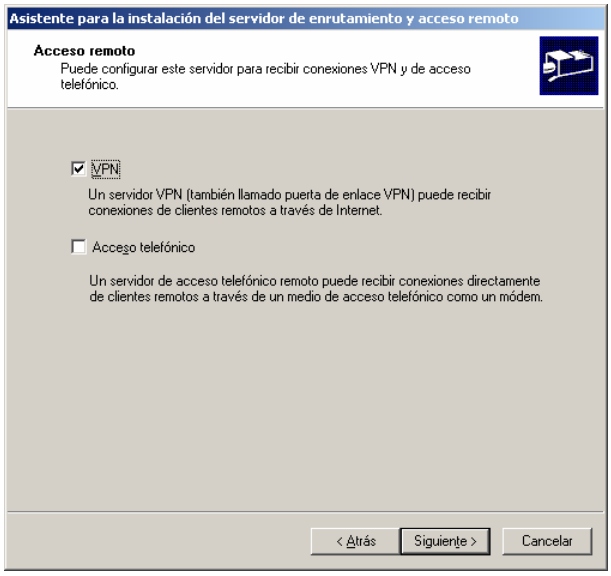


Figura III-36 –Tipo de conexión para acceso remoto

Además debió seleccionarse cuidadosamente la interfaz externa e interna. También se desactivó la casilla *Habilitar seguridad* para tener menos problemas en las pruebas.

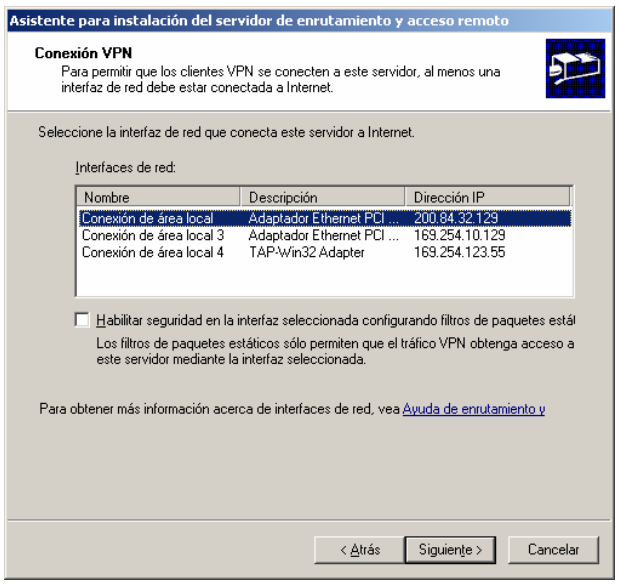


Figura III-37 – Selección de la interfaz del servidor de certificados

Al finalizar el Asistente, se pudieron ver los detalles del servicio (Interfaces de red, Clientes de acceso remoto, Puertos, Enrutamiento IP). En particular se pudo notar que parte de los minipuertos WAN son del tipo PPTP y el resto L2TP.

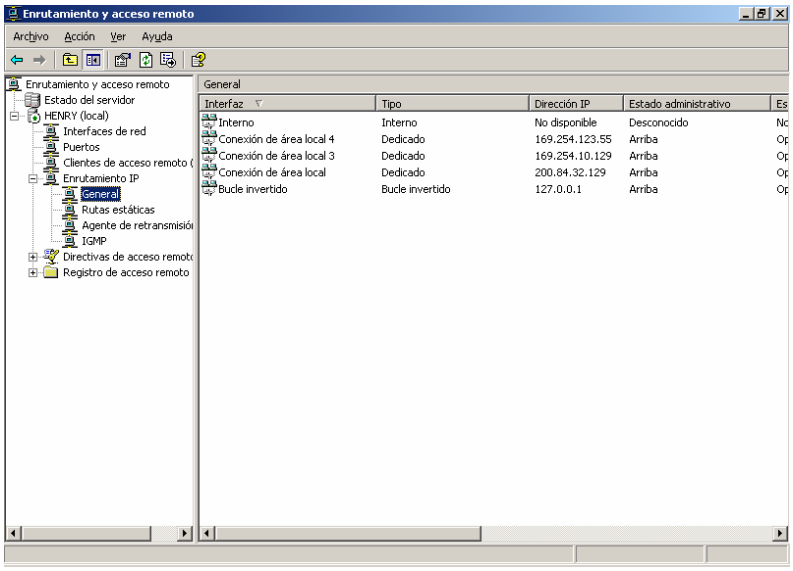


Figura III-38 – Detalles del servicio de enrutamiento y acceso remoto

Certificado para el servidor VPN

El siguiente paso fue la obtención e instalación de un certificado digital para el servidor VPN. Hay que tomar en cuenta que al intentar establecer una conexión VPN L2TP/IPSec, la autenticación de equipos no se produce si el certificado del servidor VPN no tiene configurado el propósito *Autenticación del servidor* en las extensiones en las extensiones de Uso mejorado de claves (EKU: *Enhanced Key Usage*) del certificado. Pero aunque los servidores VPN que finalizan las conexiones de usuarios remotos sólo necesitan un certificado que tenga configurado el propósito *Autenticación del servidor* en las extensiones EKU, un servidor VPN que se utilice como extremo de una conexión VPN con otro servidor VPN, origina (como cliente) y termina (como servidor) las conexiones VPN. Por este motivo, el certificado de estos servidores debe contener tanto el propósito Autenticación del servidor como el propósito *Autenticación del cliente* en las extensiones EKU. Además, debido a la forma en la que funciona la selección automática de certificados, ambos propósitos (Autenticación del servidor y

autenticación del cliente) deben estar contenidos en el mismo certificado.

Desde la máquina donde se instaló el servidor VPN (que es la misma máquina donde está instalado el servidor de certificados), mediante Internet Explorer se hizo una conexión a http://servername/certsrv, donde servername es el nombre del servidor de certificados, por ejemplo, *http:/localhost/certsrv*, tal como se muestra en la figura:

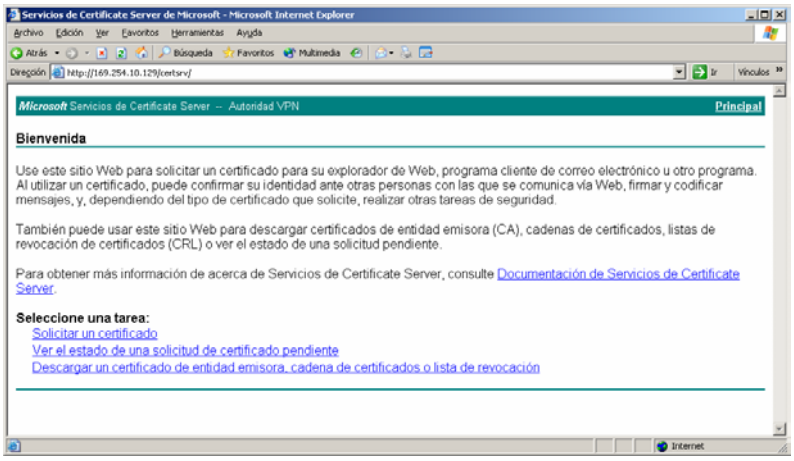


Figura III-39 – Solicitud de certificados vía http

Aquí se seleccionó *Solicitar un certificado* y luego *Solicitud avanzada*.

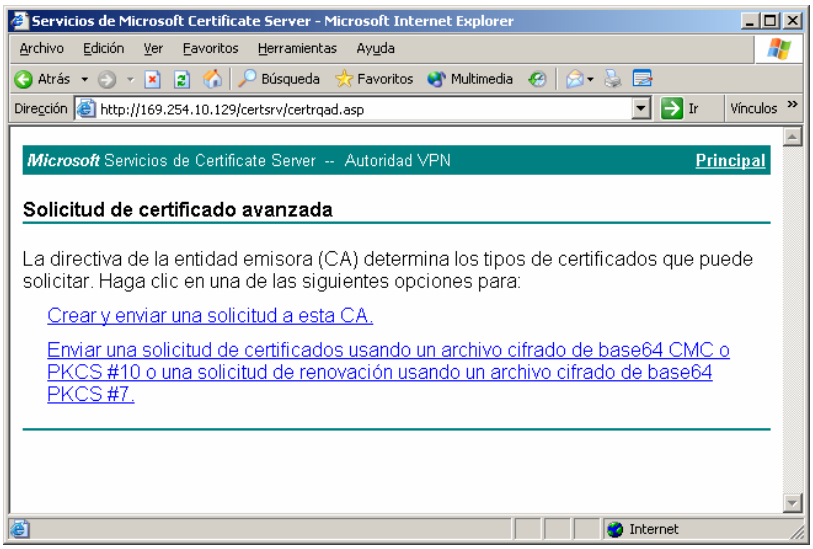


Figura III-40 – Ventana de solicitud de certificado avanzada

En la ventana siguiente, se seleccionó la primera opción: *Crear y enviar una solicitud a esta CA*. Se llenó la planilla con los datos solicitados. En Tipo de certificado necesario, se seleccionó *Otro…* con OID 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, que corresponde a Autenticación del servidor y Autenticación de cliente. Se activó *Marcar claves como exportables* y además *Almacenar el certificado en el almacén de certificados del equipo local*.

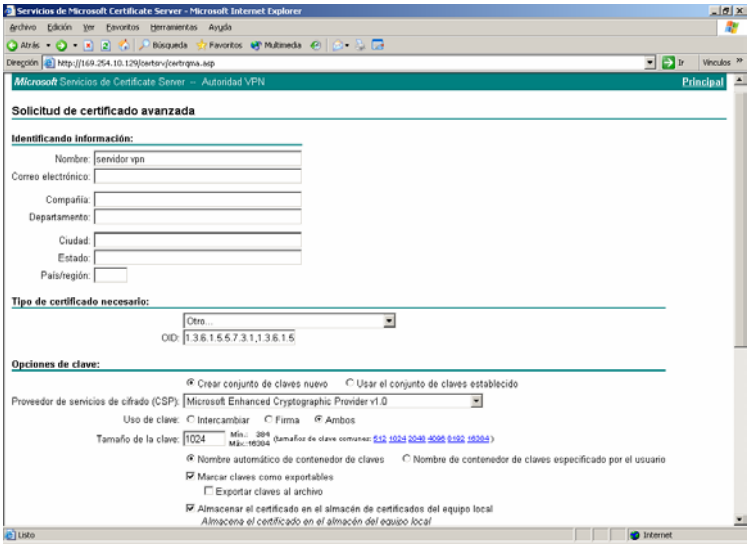


Figura III-41 – Planilla de solicitud de certificado

Al enviar la solicitud, se otorgó inmediatamente el certificado y se procedió a su instalación.

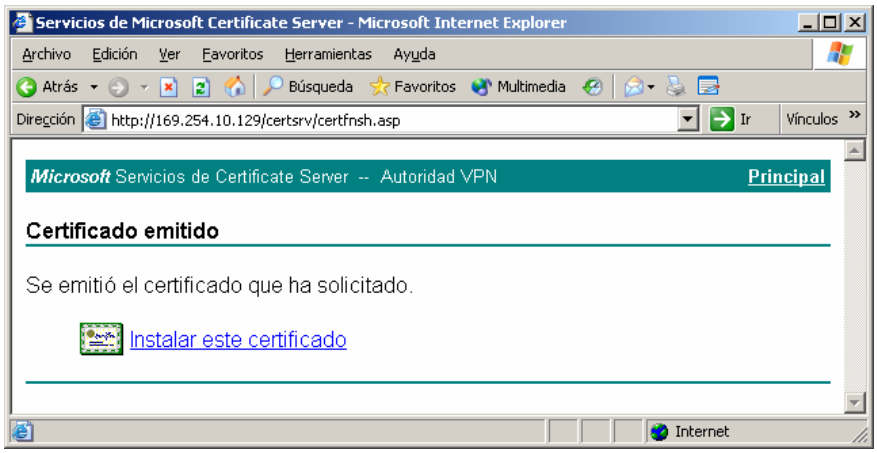


Figura III-42 – Emisión e instalación del certificado

Para administrar los certificados, se utilizó la consola de Windows MMC (*Microsoft Management Console*).

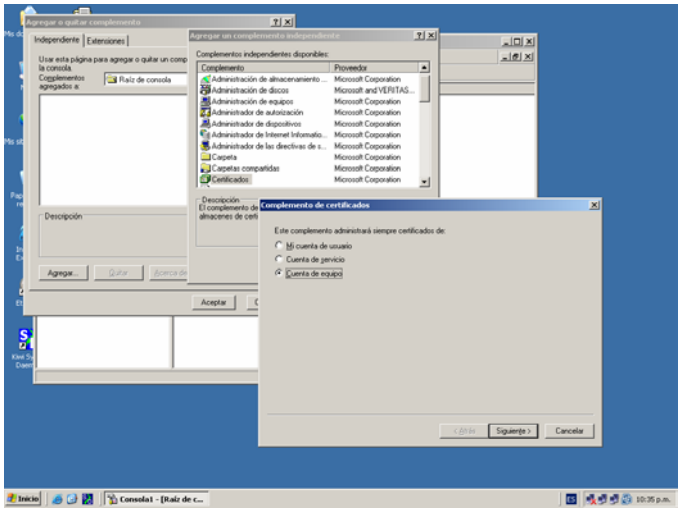


Figura III-43 – Administración de certificados mediante MMC

Mediante MMC se verificó que el certificado aparecía bajo *Certificados (equipo local)*, ya que de otra forma no podría establecer un túnel IPSec. Haciendo doble clic sobre el certificado se comprobó que en el campo *Uso mejorado de claves* aparecía *Autenticación del servidor y Autenticación del cliente* con sus respectivos OID.

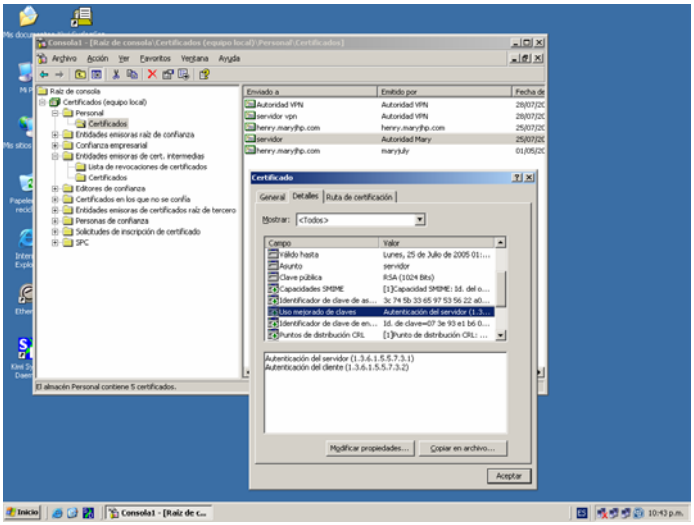


Figura III-44 – Comprobación de instalación correcta del certificado

Se verificó si bajo *Entidades emisoras raíz de confianza*, aparecía el certificado de la entidad emisora de ese certificado. Como no fue así, se buscó bajo *Entidades emisoras de certificados intermedias,* de donde se copió y se pegó a *Entidades emisoras raíz de confianza*, ya que si no, IPSec no iba a funcionar.

Certificado para el cliente VPN

Al intentar establecer una conexión VPN L2TP/IPSec entre un cliente Windows y un servidor VPN basado en Windows 2000/2003 Server, la autenticación falla si el certificado del cliente VPN ubicado en el almacén de certificados del equipo local, no tiene configurado el propósito *Autenticación del cliente* en las extensiones en las extensiones de Uso mejorado de claves (EKU: Enhanced Key Usage) del certificado.

Desde una PC equipada con Windows XP y mediante Internet Explorer se repitió el mismo procedimiento que se describió previamente para el servidor VPN, sólo que en el tipo de certificado necesario, se seleccionó *Certificado de autenticación de cliente*.

Se comprobó que el certificado aparecía bajo *Certificados (equipo local)*, de otra forma no podría establecer un túnel IPSec.

Se verificó si bajo *Entidades emisoras raíz de confianza*, aparecía el certificado de la entidad emisora de ese certificado. Como no fue así, se buscó bajo *Entidades emisoras de certificados intermedias,* de donde se copió y se pegó a *Entidades emisoras raíz de confianza*, ya que si no, IPSec no iba a funcionar.

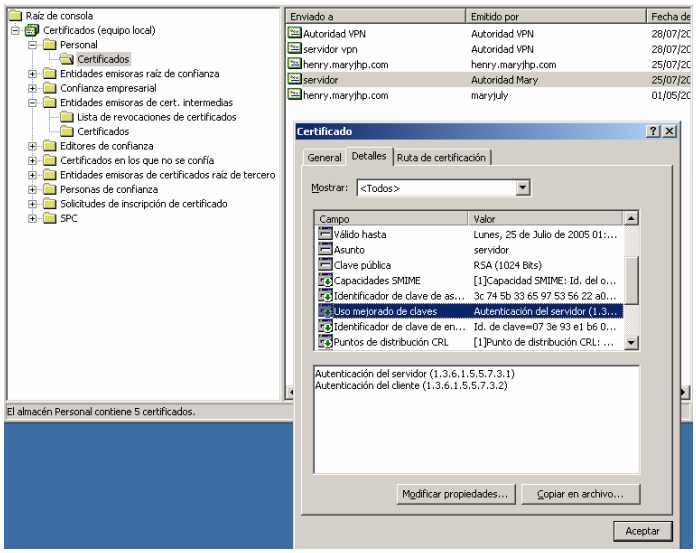


Figura III-45 – Validación de instalación de certificado

Establecimiento del túnel L2TP/IPSec

Una vez instalado el certificado, se procedió a crear una conexión nueva de red para establecer un túnel con IPSec, siguiendo los mismos pasos que para crear una conexión PPTP, excepto que en tipo de red, se seleccionó L2TP/IPSec.

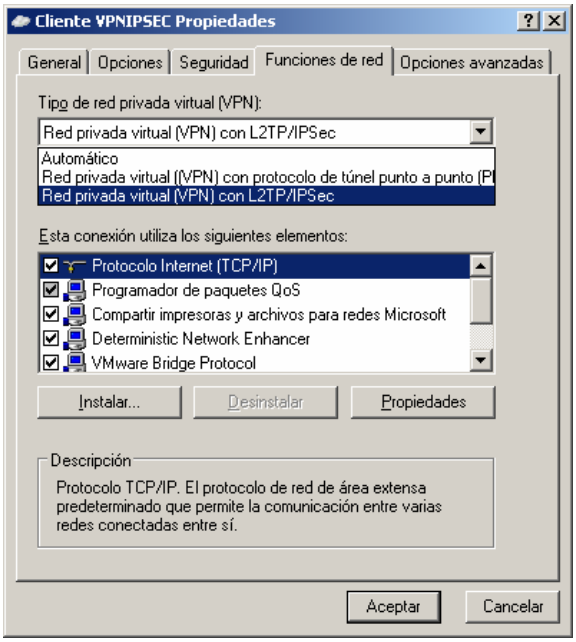


Figura III-46 – Selección de tipo de VPN en el cliente

Usando el login y la contraseña correcta, la conexión VPN mediante PPTP se estableció no tan rápidamente como en el caso PPTP, aunque en ciertas oportunidades no se logró establecer a causa de problemas con los certificados o las direcciones IP. Haciendo clic sobre la conexión, se pudieron observar detalles interesantes, como el tipo de cifrado (IPSec, ESP, 3DES) y la dirección IP del servidor y del cliente. Esas direcciones virtuales internas son temporales y son suministradas por el servidor VPN conjuntamente con el servidor DHCP.

Captura de tráfico

Para verificar que los mensajes Syslog y Traps SNMP efectivamente viajan encriptados, se utilizó el analizador de tráfico Ethereal y se capturó el tráfico en varias partes de la red. Los resultados se muestran en las siguientes figuras. Se pudo observar que los paquetes IPSec son del tipo ESP (*Encapsulated Security Payload*).

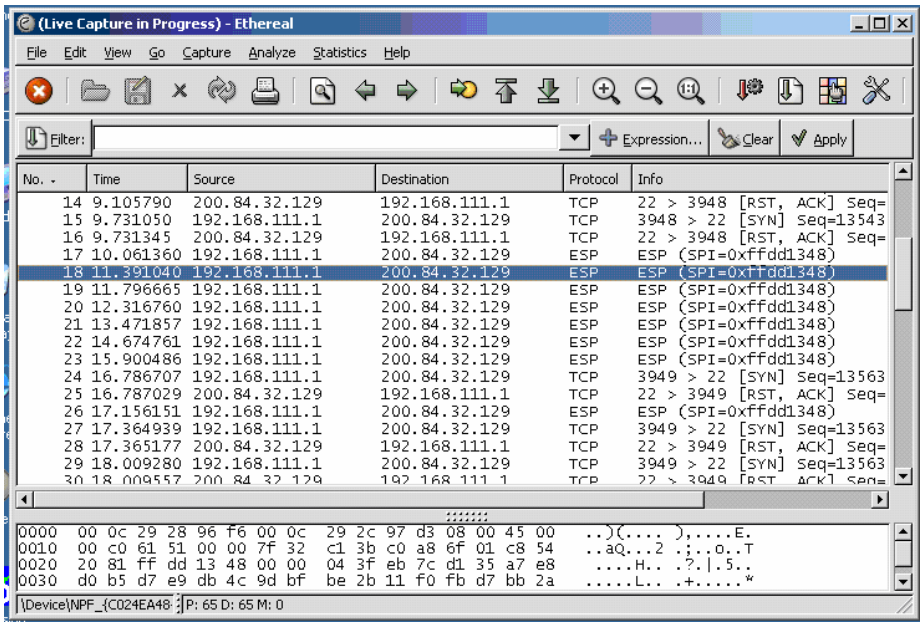


Figura III-47 – Mensajes encriptados dentro del túnel L2TP/IPSec

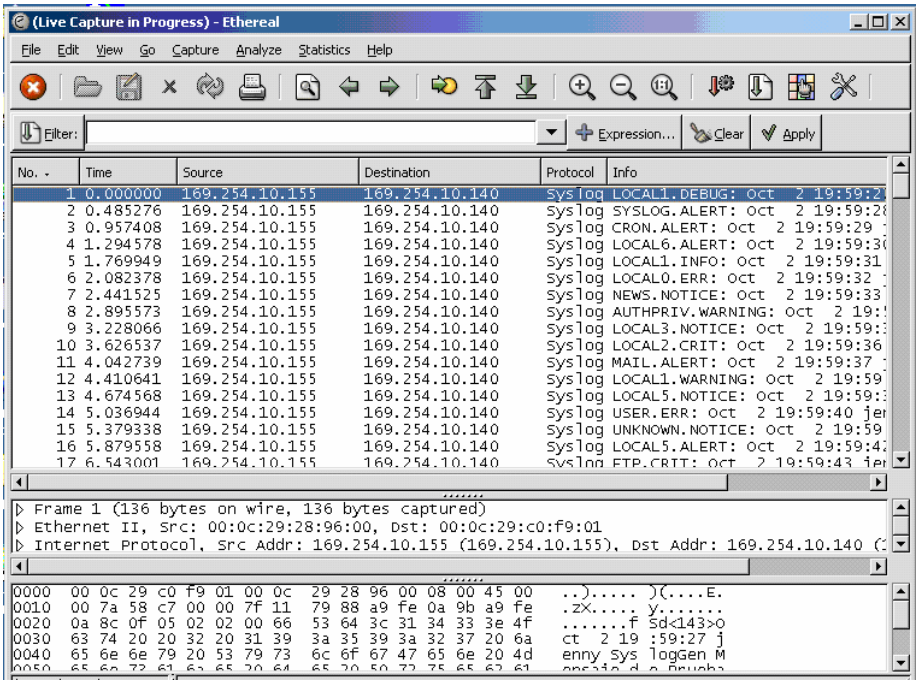


Figura III-48 – Mensajes desencriptados fuera del túnel L2TP/IPSec

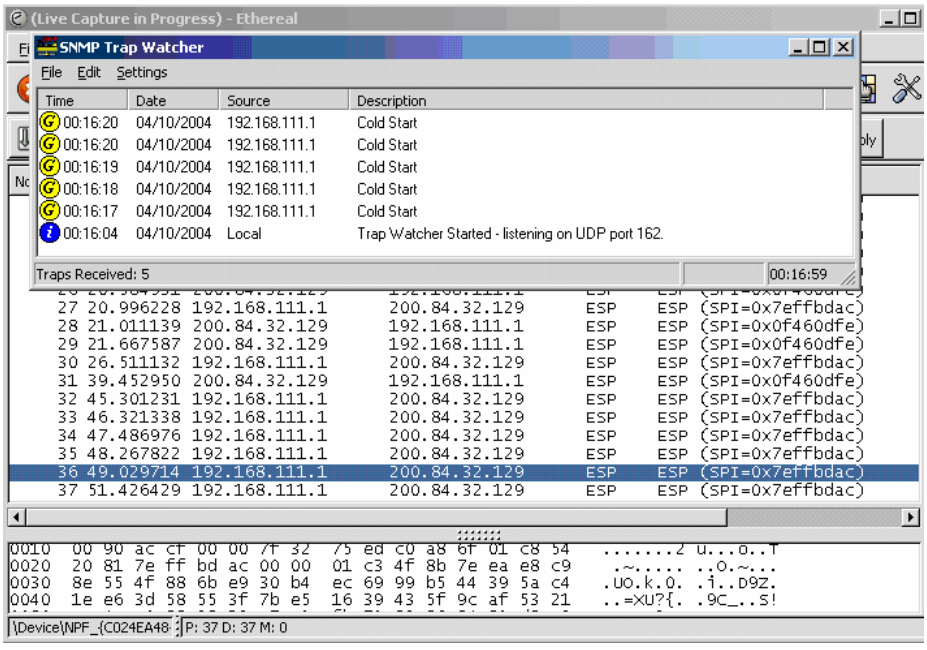


Figura III-49 – Mensajes Trap encriptados dentro de Tunel IPSec/L2TP

III.4 Túnel VPN con OpenVPN

Una tercera solución que se probó para mejorar la seguridad de los mensajes Syslog y SNMP, fue mediante OpenVPN.

El primer paso para crear un túnel fue verificar que las dos máquinas lograban verse a través de sus direcciones IP reales. Luego se generó una clave estática común para ser usada por ambas máquinas, tal como se muestra en la figura:

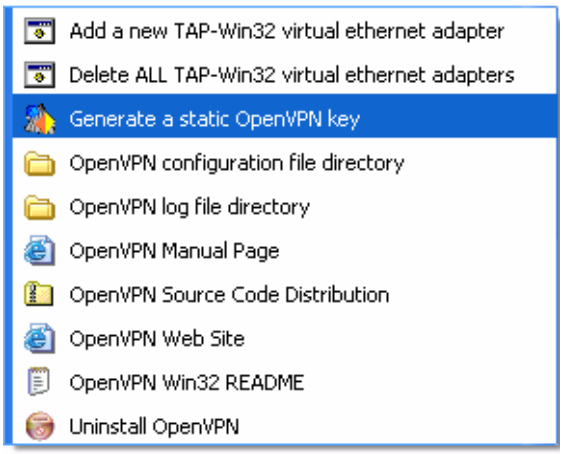


Figura III-50 – Opción para generar la clave común para OpenVPN

Esta clave se guarda en un archivo *key.txt* en la carpeta donde se instaló OpenVPN y ese mismo archivo se copia luego en la otra PC.

A continuación se procedió a editar el archivo de configuración *config.ovpn*, el cual contiene los parámetros del túnel:

Detalles del archivo config.ovpn de la PC A

```
# Edit this file, and save to a .ovpn extension
# so that OpenVPN will activate it when run as a service.
# Change 'myremote' to be your remote host,
# or comment out to enter a listening
# server mode.
remote 200.84.32.129
```

En el parámetro **remote** se coloca la dirección IP de la PC a la cual se quiere hacer la conexión.

Uncomment this line to use a different
port number than the default of 5000.
; port 5000
ifconfig 10.3.0.1 255.255.255.0
10.3.0.1 is the local VPN IP address and
10.3.0.2 is the remote VPN IP address.
secret key.txt

En el parámetro **ifconfig** se coloca la dirección que tendrá la PC en el túnel con su respectiva máscara de subred.

El parámetro **secret** contiene el nombre del archivo con la clave secreta compartida.

Detalles del archivo config.ovpn de la PC B

Edit this file, and save to a .ovpn extension
so that OpenVPN will activate it when run as a service.
Change 'myremote' to be your remote host,
or comment out to enter a listening
server mode.
remote 192.168.111.1
Uncomment this line to use a different
port number than the default of 5000.
; port 5000
ifconfig 10.3.0.2 255.255.255.0
secret key.txt

Una vez configurado OpenVPN se procedió a activar el túnel a través del menú rápido *Start OpenVPN* que aparece al presionar el botón derecho del mouse sobre el archivo config.ovpn. Esta operación se debe realizar en ambas máquinas.

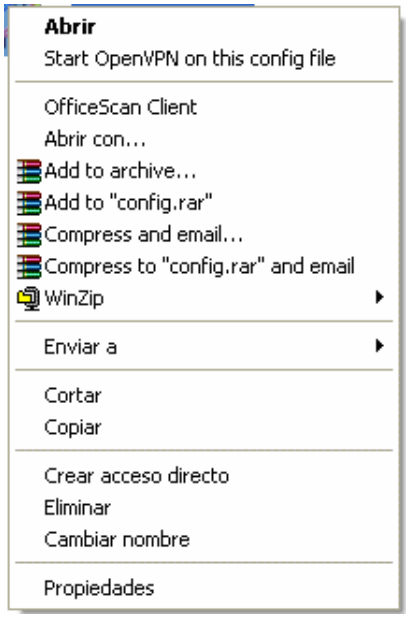


Figura III-51 – Inicio de sesión en OpenVPN

Luego de esta acción, se abrió automáticamente una ventana DOS mostrando cómo se va estableciendo la conexión y los distintos parámetros de la misma.

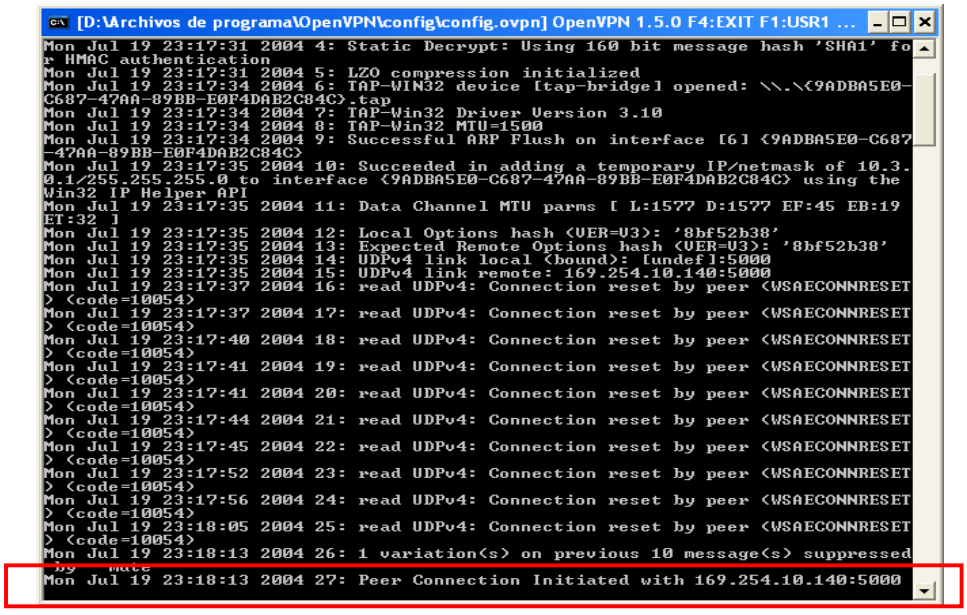


Figura III-52 – Ventana de estado de conexión de OpenVPN

Captura de tráfico

Para verificar que los mensajes Syslog y Traps SNMP efectivamente viajaban encriptados, se utilizó el analizador de tráfico Ethereal en varios puntos de la red. Los resultados se muestran en las siguientes figuras. Pudo notarse el uso del puerto 5000 y del protocolo UDP.

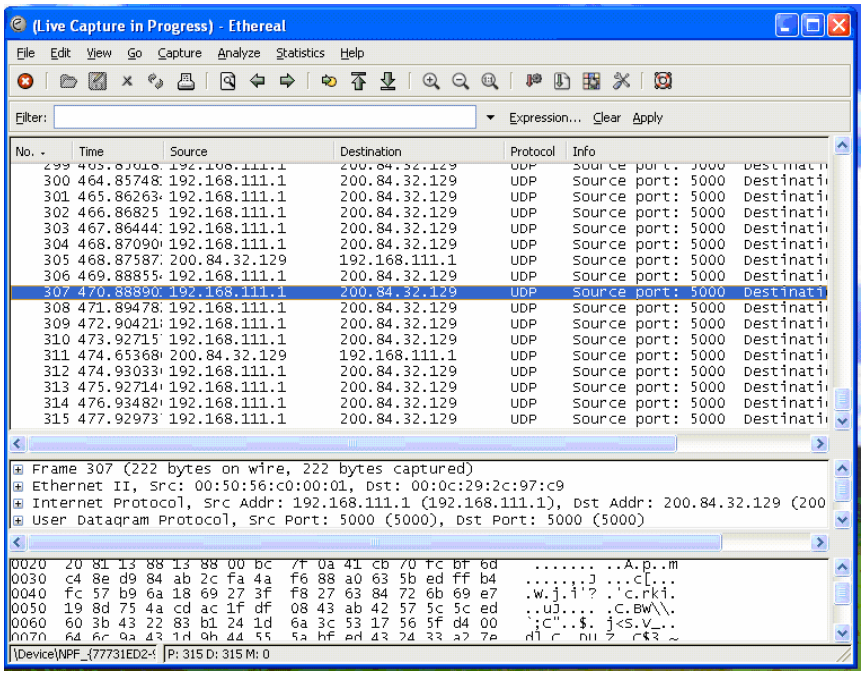


Figura III-53 – Mensajes Syslog encriptados en el túnel OpenVPN

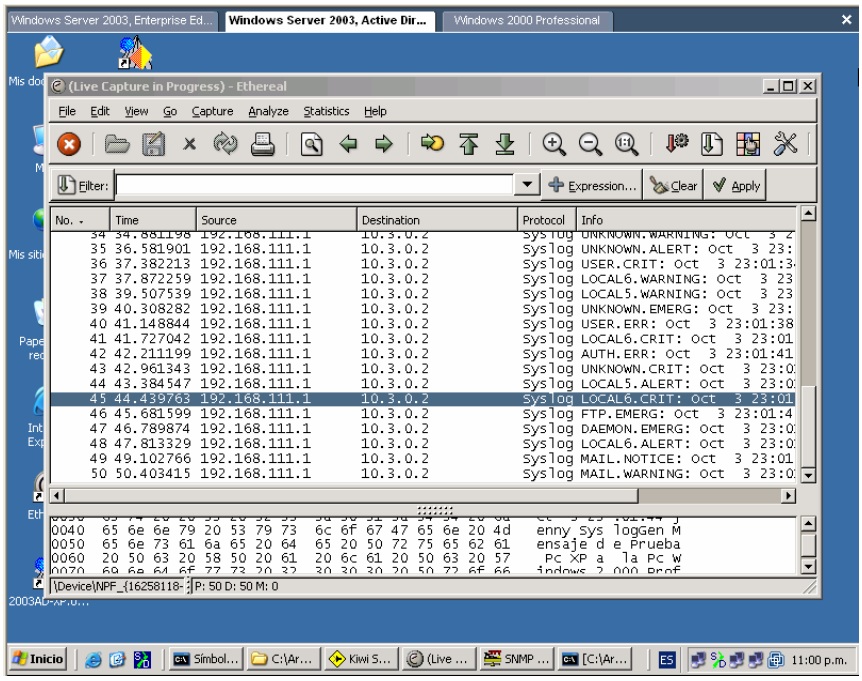


Figura III-54 – Mensajes Syslog desencriptados fuera de túnel OpenVPN

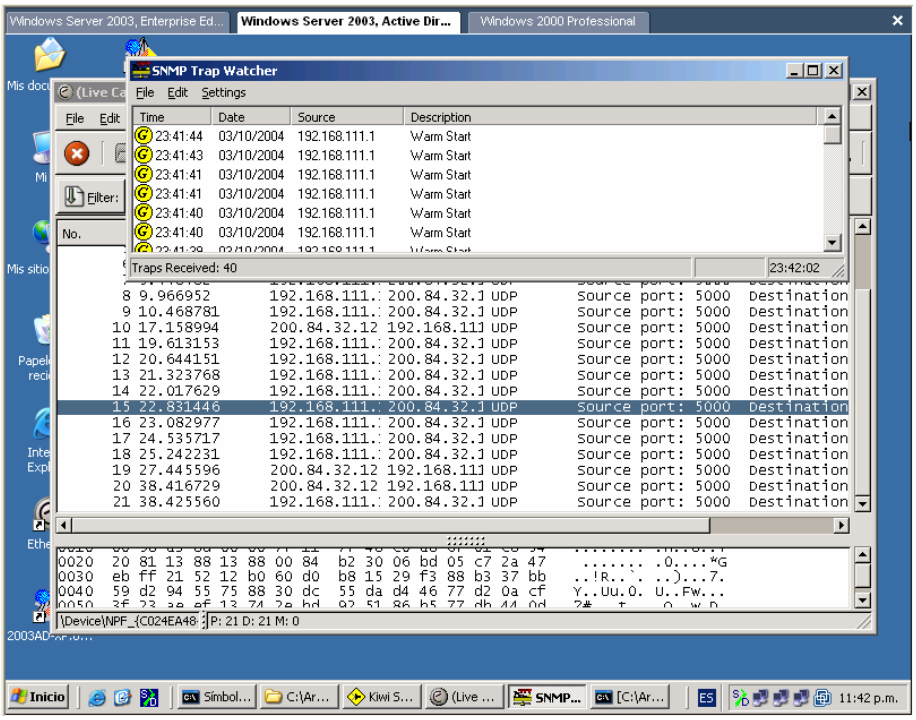


Figura III-55 – Mensajes Trap encriptados dentro del túnel OpenVPN

CAPITULO IV - CONCLUSIONES Y RECOMENDACIONES

Las organizaciones modernas dependen cada vez más del buen funcionamiento de los sistemas de comunicaciones y de sus recursos informáticos para la realización de su actividad diaria. Cada vez es menos justificable la expresión “la red está caída” o “la red está lenta” y en tal sentido se debe disponer de un buen sistema de gestión para supervisar su correcta operación.

La utilización de mecanismos de notificación de eventos como Syslog y traps SNMP es vital para determinar situaciones críticas, por ejemplo congestión, falla o ataque de hackers. Sin embargo esos mecanismos adolecen de una serie de debilidades desde el punto de vista de la seguridad, como se comprobó durante el desarrollo de este trabajo. De hecho, no se encriptan ni se autentican los mensajes de notificación, por lo que son relativamente fáciles de forjar o adulterar (por ejemplo capturando un mensaje auténtico y luego modificándolo y reenviándolo).

Con el fin de buscar posibles mejoras de seguridad que fueran relativamente fáciles de implantar, se probaron y evaluaron varias tecnologías comerciales y de código abierto, las cuales básicamente establecen un canal seguro (“túnel”) entre la fuente y el destino de los mensajes de notificación. A estas tecnologías se les denomina a veces VPN (*Virtual Private Network*).

A continuación se resumen las fortalezas y debilidades de las soluciones estudiadas en este trabajo.

Protocolo de Túnel de Punto a Punto (PPTP)

Es un protocolo que sólo funciona bajo ambiente Windows y además requiere un Windows Server 2000 o 2003 como servidor VPN. Es relativamente fácil de utilizar y transporta perfectamente tanto Syslog como SNMP.

Protocolo de Túnel Capa 2 (L2TP) con IPSec

IPSec es más complicado de utilizar, ya que requiere certificados digitales en ambos extremos del túnel, además usualmente no funciona detrás de un NAT (*Network Address Traslation*). Transporta perfectamente tanto syslog como SNMP. Al usarlo con

L2TP bajo ambiente Windows, se requiere un Windows Server 2000 o 2003, como servidor VPN.

Kiwi Syslog Tunnel

Es un producto comercial optimizado para el transporte seguro de syslog y puede funcionar como gateway, llevando el tráfico de múltiples clientes syslog. Además el Kiwi Tunnel Client puede servir para concentrar el tráfico de distintas máquinas y equipos que requieren enviar mensajes syslog a un servidor remoto syslog, pero no transporta otros protocolos que no sean syslog, por ejemplo traps SNMP.

Como conclusión final, entre las diferentes tecnologías evaluadas, la que representa la mejor alternativa para la mejora de la seguridad en los mensajes de notificación y registros de eventos es el Protocolo de Túnel de Punto a Punto (PPTP), debido a su facilidad de uso y transparencia a los protocolos trasportados.

Para trabajos futuros se recomienda probar y evaluar la nueva versión 3 de SNMP, la cual incorpora fuertes mecanismos de seguridad, aunque todavía no están fácilmente disponibles agentes SNMPv3.

También se recomienda probar y evaluar las distintas propuestas de syslog seguro, tales como SDSC Secure Syslog, syslog-ng y msyslog, entre otros, las cuales ofrecen la posibilidad de utilizar el protocolo TCP para la transmisión de los mensajes, funciones avanzadas de filtrado y el registro de los mensajes directamente en una base de datos tipo SQL.

CAPITULO V - INDICE DE SIMBOLOS, ABREVIATURAS Y TERMINOS

A

- ALGORITMO DE CIFRADO: Proceso lógico matemático que permite codificar y decodificar el texto en base a una *"clave".*
- AP: *Access Point*. Punto de Acceso.
- ARP: *Address Resolution Protocol*. Protocolo de resolución de dirección.
- ACCESO REMOTO: conexión de un cliente desde un punto remoto de una red o desde Internet a la red interna de una empresa.
- AUTENTICACIÓN: Con respecto a la seguridad, la verificación de la identificación de una persona o proceso.

B

- BRIDGE: Puente. Dispositivo de almacenamiento y reenvío de datos.
- BUFFER: Área del almacenamiento temporal usado para datos que se transmiten entre dos dispositivos, para compensar para las diferencias en la proporción a que cada dispositivo funciona o la disponibilidad del dispositivo receptor.

C

- CLAVE DE CIFRADO: contraseña para establecer una comunicación segura, la cual es transformada a cifras, esto es números, para que hacerlo ininteligible.
- CERTIFICADO DIGITAL: Un certificado digital (también llamado identificador digital o en inglés digital ID) consta principalmente de los datos del titular, su clave pública y la firma digital de la autoridad certificadora.
- CIFRADO, CODIFICADO: método para proteger los datos de un acceso no autorizado a los mismos. Se utiliza en Internet para proteger el correo electrónico.
- CPU: Unidad central de procesos.
- CONFIABILIDAD: Proporción entre los mensajes de actividad esperados y recibidos de un enlace; si la relación es alta, la línea es confiable. Utilizado como métrica de enrutamiento.

D

- DATAGRAMAS: Conjunto de datos de características específicas. Paquetes de datos que viajan por una red.
- DIAL-UP: Término actualmente utilizado como sinónimo de dial-in. Conexión a Internet que se establece a través de un módem y una línea telefónica.

E

- ENCAPSULAMIENTO: colocación en los datos de un encabezado de un protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de enviar el tráfico a la red. Además, al puentear redes que no son similares, toda la trama de una red, se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red.
- ETHEREAL: Es un analizador de tráfico de red, o "sniffer", para los sistemas operativos Unix, Unix-like y Windows. Usa GTK+, una interfaz del usuario gráfica, la biblioteca, y libpcap, una captura del paquete y biblioteca de filtros.
- ETHERNET: Esta red fue desarrollada originalmente por Xerox y Dec como forma de solucionar el problema del cableado de redes. Sus inventores fueron Robert Metcalfe y David Boggs. Según Robert Metcalfe, el nombre Ethernet proviene de la palabra Ether (éter), la cual denomina poéticamente a un material inexistente que, según algunas antiguas teorías, llenaba el espacio y actuaba como soporte para la propagación de la energía a través del universo.

F

- FRAME: Trama. Estructura utilizada para encapsular los paquetes IP.
- FIREWALL: Router o servidor de acceso, o varios router o servidores de acceso, designados para funcionar como buffer entre redes de conexión publica y una red privada. Un router usado como firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

H

- HTTP: *Hyper Text Transfer Protocol*. Servicio orientado a conexión que ofrece la posibilidad de manejar documentos de Hyper Texto o Texto Enriquecido (Hyper Text Markup Language, HTML) ubicados en un servidor remoto.
- HOST: termino en inglés que define a un computador principal.

I

- IEEE: Institute of Electrical and Electronics Engineers, Inc. Autoridad que se encarga de establecer ciertos estándares en el ámbito de ingeniería de computación, tecnología biomédica, telecomunicaciones, energía eléctrica, ingeniería aerospacial y electrónica, entre otros.
- IETF: Internet Engineering Task Force. Comunidad internacional de diseñadores de red, operadores, vendedores e investigadores que tienen relación con la evolución de la arquitectura y el funcionamiento de Internet.
- IIS (Internet Information Service): Producto de Microsoft que permite la publicación de páginas web en Internet e Intranet.
- INTERFAZ: Medio de interacción o presentación entre el usuario y el computador.
- IP: Un número binario de 32 cifras que se divide en cuatro subgrupos. Cada uno de los subgrupos puede ser representado como número decimal y de ahí resulta el número IP.
- IPSec: Internet Protocol Security. Seguridad de Protocolo de Internet. IPSec es un grupo de estándares abiertos para asegurar comunicaciones privadas seguras sobre redes IP. Basado en estándares desarrollados por el Internet Engineering Task Force (IETF), IPSec asegura confidencialidad, integridad y autenticidad de los datos que se encuentran sobre la red IP pública
- ISP: Internet Service Provider. Proveedor de Servicios de Internet.

K

- KERNEL: Núcleo de comandos esenciales para inicializar cualquier sistema operativo.

- KEY: Clave. Conjunto de dígitos encadenados.

L

- LAN: *Local Area Network*. Red de Área Local de datos que se utiliza para dar servicio a un área de pocos kilómetros cuadrados y consiste en una red única privada. Se usan para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir recursos (por ejemplo, impresoras) e intercambiar información.
- L2TP (Layer-2 Tunneling Protocol): Creado como combinación de los protocolos L2F de Cisco y PPTP de Microsoft, permite la creación de túneles a través de una gran variedad de redes (IP, SONET, ATM) para el transporte de tráfico PPP.

M

- MAC: *Media Access Control*. Control de Acceso al Medio. Contienen 48 bits de longitud y son únicas, es un componente superior de la Capa de Enlace de Datos (OSI).
- MAN: *Metropolitan Area Network*. Redes de Área Metropolitana.
- MBPS: *Megabits por segundo*. Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.
- MÓDEM: Codificador y decodificador de señales digitales en señales analógicas susceptibles de trasladarse por una línea de telecomunicaciones.

N

- NAT (Network addressees translation): traducción de direcciones de red. Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a Internet transformando esas direcciones en espacio de direccionamiento enrutable global. También denominado traductor de dirección de red.

- NIC: *Network Interface Card*. Tarjetas de interfaz de red.

O

- OpenVPN: es una aplicación de SSL de código abierto, fácil de usar y robusta para crear un túnel seguro entre 2 sitios.
- OSI: Open Systems Interconnection. Modelo que estandariza la representación de las redes a través de capas.

P

- PDA: *Personal Digital Assistants*. Asistente Personal Digital.
- PGP: *Pretty Good Privacy*. Un sistema de encriptación por clave pública y sirve para que nadie, salvo uno mismo y el destinatario o destinatarios a los que vaya dirigido el mensaje puedan leerlo, al ir el mensaje codificado.
- PING (búsqueda de direcciones de Internet): mensaje de echo ICMP y su respuesta. A menudo se usa en redes IP para probar el alcance de un dispositivo de red.
- POP: *Post Office Protocol*. Servicio orientado a conexión que permite al usuario obtener su correo electrónico entrante.
- PPP: *Point-to-Point Protocol*. Protocolo Punto-a-Punto. Es un protocolo que permite un enlace por línea serial, es muy utilizado por los usuarios de un PC doméstico con acceso a Internet mediante módem y línea telefónica.
- PPTP (Point-to-Point Tunneling Protocol): Protocolo de túnel Punto-a-Punto, fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP
- PROTOCOLO: Se denomina protocolo a un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (emisor y receptor). Estos protocolos "gobiernan" formatos, modos de acceso, secuencias temporales,

etc.

Q

- QoS: *Quality of Service*. Calidad de Servicio.

R

- RADIUS: *Remote Authentication Dial-In User Service*. Servicio de usuario de acceso telefónico de autenticación remota. Suministra servicios de autenticación, autorización y cuentas al acceso telefónico a redes distribuidas.
- RARP: *Reverse Ardes Resolution Protocol*. Protocolo de resolución de dirección inverso.
- RFC (Request for Comments): requerimiento de comentario
- ROUTER: Dispositivo de capa de red que usa una o mas métricas para determinar cual es la ruta optima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se esta volviendo obsoleta).

S

- SMTP: Simple Mail Transfer Protocol. Servicio que permite la transmisión de Correo Electrónico saliente desde el computador origen hasta el servidor destino.
- SNMP: *Simple Network Management Protocol*. Protocolo Simple de Manejo de Redes.
- SNMPc: es un sistema de administración para la gestión de redes pequeñas, medianas y grandes. Permite generar Traps SNMP y también recibirlos y notificar en la consola.
- SPAM: correo basura que es distribuido a través de Internet.
- SSH: desarrollado por SSH Communications Security Ltd., Secure Shell es un programa para permitir la entrada a otro computador sobre una red de datos, para ejecutar comandos en una máquina remota, y mover los archivos de una

computadora a la otra. Provee una robusta autenticación y comunicación segura sobre canales con poca seguridad reemplazan los conocidos comandos: rlogin, rsh, rcp y rdist de UNIX. SSH protege a la red de ataques como IP spoofing, IP source routing y DNS spoofing ya que su sesión es protegida mediante la encriptación de la misma. SSH está disponible para Windows, Unix, Macintosh y OS2.

- SSL (Secure Sockets Layer): desarrollado por Netscape para la transmisión de documentos privados vía Internet. SSL trabaja a través del uso de clave pública para encriptar la data que es transferida sobre una conexión SSL. Tanto como el navegador de Netscape como el Explorer soportan SSL y muchos sitios WEB usan el protocolo para obtener información confidencial, como saldos de cuentas y tarjetas de créditos. Por convención los URL que requieren una conexión SSL comienzan con https en vez de http.
- SYSLOG: es un protocolo de comunicación que proporciona un medio de transporte para permitir que una máquina envíe mensajes de notificación de sucesos a través de redes IP. Estos mensajes son enviados a servidores Syslog.

T

- TCP/IP: *Transmission Control Protocol / Internet Protocol*.: protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de duplex completo. TCP es parte de la pila de protocolo TCP/IP
- TRAP: es un mensaje especial generado por un agente para notificar al manager la ocurrencia de algún evento significativo. El mensaje incluye la identificación del agente que generó el trap, cuándo se generó y de qué tipo de evento se trata.

U

- UDP: *User Data Protocol*. Permite a las aplicaciones enviar datagramas IP sin establecer una conexión. Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagrama sin confirmación o garantía de entrega y que requiere

que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768.

V

- VPN (*Virtual Private Network*.): Red Privada Virtual. Una red privada virtual, o *Virtual Private Network*, VPN permite establecer una conexión segura a través de una red publica, o Internet. Una VPN permite que el trafico IP viaje seguro a través de una red pública TCP/IIP al encriptar el trafico desde una red hasta la otra. Una VPN usa tunneling para encriptar toda la información en el nivel IP.
- VMWare: VMware es una máquina virtual (VM) para Intel Pentium o una máquina superior y está disponible para los sistemas operativos Windows NT, Windows 2000, Windows XP y Linux. El software de la máquina virtual se ejecuta en una máquina real y suministra una máquina virtual con la misma arquitectura básica de una maquina real.

W

- WAN: *Wide Area Network*. Red de Área Amplia que cubre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas (hosts) dedicada a ejecutar programas de usuario (aplicaciones).

CAPITULO VI - REFERENCIAS BIBLIOGRAFICAS

- COMER, D. (1996). Redes Globales de Información con Internet y TCP/IP. Tercera Edición. México. Editorial Prentice-Hall Hispanoamericana, S.A.
- CRAIG, H. (1997).TCP/IP Network Administration, Eyrolls, Ediciones Gestión 2000 S.A.
- Enciclopedia Temática de Informática. (1987). Maveco de Ediciones, S.A.
- GONZALES, N. (1980). Comunicaciones y Redes de Procesamiento de Datos. Mc Graw Hill. Segunda Edición. México.
- KARANJIT, S. (1995). Internet y Seguridad en Redes. Prentice Hall.
- STALLINGS, W. (1997). Data and Computer Communications. Fifth Edition. Prentice Hall.
- TANENBAUM, A. (1997). *Redes de Computadoras*. México, Prentice-Hall Hispanoamericana, S.A.
- MENDILLO, V (2004). Gestión de Redes, (en CD-ROM).
- MENDILLO, V. (2004). Seguridad en Informática y Comunicaciones. (en CD-ROM).
- WILLIAM STALLINGS, (1999), SNMP, SNMPv2, SNMPv3, and RMON, Addison Wesley.
- ED WILSON, (1999) Network Monitoring and Analysis: A Protocol Approach to Troubleshooting, Prentice Hall.
- DAVID ZELTSERMAN, (1999) A Practical Guide to SNMPv3 and Network Management, Prentice Hall.
- PAUL SIMONEAU, (1999) SNMP Network Management, McGraw-Hill.
- JEFFREY CASE AND ROB FRYE, (1999) SNMP V3 Survival Guide: Practical Strategies for Integrated Network Management, John Wiley & Sons.
- STEVE MAXWELL, (1999) Unix Network Management Tools, McGraw-Hill.

- MARK A. MILLER, (1997) Managing Internetworks With SNMP: The Definitive Guide to the Simple Network Management Protocols, SNMPv2, RMON, and RMON2, IDG Books.
- NEAL ALLEN, (1997) Network Maintenance and Troubleshooting Guide, Fluke Corporation.

REFERENCIAS BIBLIOGRAFICAS EN INTERNET

Kiwi Syslog Home Page. En

http://www.kiwisyslog.com

Security Issues in Network Event Logging (Syslog) En

http://www.ietf.org/html.charters/Syslog-charter.html

SDSC Secure Syslog Home Page. En

http://security.sdsc.edu/software/sdsc-Syslog/

SDSC Secure Syslog. En

http://slashdot.org/article.pl?sid=02/12/05/1554209

BEEP, a new Internet standards-track protocol framework for new Internet Applications. En

http://www.beepcore.org/

Reliable Delivery for Syslog. En

http://www.ietf.org/rfc/rfc3195.txt y ftp://ftp.rfc-editor.org/in-notes/rfc3195.txt

The BSD Syslog Protocol. En

ftp://ftp.rfc-editor.org/in-notes/rfc3164.txt

Syslog-ng. En

http://www.balabit.hu/en/downloads/Syslog-ng/

MSyslog. En

http://sourceforge.net/projects/mSyslog/

Metalog. En

http://metalog.sourceforge.net/

Network Management. En

http://smurfland.cit.buffalo.edu/NetMan/

Tools for Network Management. En

http://ermis.cc.duth.gr/InfoBase/noc.html

SNMP++ Web Site. En

http://rosegarden.external.hp.com/snmp++/

Network Management. En

http://www.dallas.net/~jwill/html/networks.html

Network Management Tools. En

http://jaring.nmhu.edu/net-tool.htm

ETHEREAL Web Site. En

http://www. Ethereal.com