ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación (FIEC)

“Seguridad Aplicada a un Carrier transaccional”

TOPICO DE GRADUACION

Previo la obtención del Título de:

INGENIERO EN ELECTRICIDAD ESPECIALIZACION ELECTRONICA

Presentado por:

Larry Segundo Medina Aguirre

GUAYAQUIL – ECUADOR

AÑO 2006

AGRADECIMIENTO

A DIOS, por hacer posible la realización del Proyecto, a mi hijo Larry Adrián. A mis padres por su comprensión y apoyo brindado.

DEDICATORIA

A MI HIJO, A MIS PADRES Y HERMANOS

TRIBUNAL DE GRADUACION

_____	_____
Ing. Holger Cevallos SUBDECANO DE LAFIEC PRESIDENTE	Ing. José Escalante DIRECTOR DEL TOPICO
_____	_____
Ing. Germán Vargas. MIEMBRO PRINCIPAL	Ing. Gomer Rubio MIEMBRO PRINCIPAL

DECLARACION EXPRESA

“La responsabilidad del contenido de esta tesis de grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL

_____

Larry Segundo Medina Aguirre

RESUMEN

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

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

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

INDICE GENERAL

ABREVIATURAS

WAN	Red de área amplia
RDSI	Red digital de servicios integrados
HDLC	Control de enlace de datos de alto nivel
DLCI	Data link connection identifier
DE	Discard eligibility
FCN	Forward explicit congestion notification
BECN	Bacward explicit congestion notification
TCP/IP	Trasmission control protocol /protocolo de Internet
FRAD	Frame relay assambler/dessambler
VC	Circuito virtual
LAN	Red de área local
IPSec	Protocolo de seguridad
DARPA	Defense advanced research proyects agency
DOD	Departament of defense
UDP	User datagram protocol
SNMP	Protocolo básico de gestión de red
SMTP	Simple mail transfer protocol
FTP	File transfer protocol
NAT	Traductor de direcciones de red

ICMP	Protocolo Internet de mensajes de control
NIC	Centro de información de red
RIP	Protocolo de enrutamiento interior
ISPs	Proveedor de servicios de Internet
IKE	Internet security association and key management protocol
IETF	Internet engineering task force
SA	Asociaciones de seguridad
DOI	Dominio de interpretación
SPI	Security parameter index
PMTU	Protocol maximun transfer unit
SPD	Security polity database
IANA	Internet assigned numbers authority
ICV	Integrity check value
PRTG	Pessler router traffic grapher
IGRP	Interior gateway routing protocol
OSPF	Open shortest path first
EGEP	Exterior gateway protocol
ITU	International telecommunication union
SNA	Arquitectura de sistemas en red
ATM	Modo de transferencia asíncrono
CCITT	Comité consultivo internacional para telegrafía y telefonía
OSI	Interconexión de sistemas abiertos

DES	Norma de cifrado de datos
ARP	Protocolo de resolución de direcciones
SLIP	Protocolo Internet de línea serie
PPP	Protocolo punto a punto
VPN	Red privadas virtuales
IPX	Intercambio de paquetes entre redes
DNS	Servicios de nombres de dominio
LSP	Link state packet

INDICE DE FIGURAS

Pàgina

Página

Página

Página

Página

INDICE DE TABLAS

INTRODUCCION

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

A continuación se realizará una descripción de cada capítulo.

Capítulo I

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

Capítulo II

Describe los problemas y falencias de la red del cliente y del carrier. Realizando una evaluación de dichas redes y solución a la inseguridad informática.

Capítulo III

Describe la implementación del proyecto, el hardware y software utilizado, los pasos para la instalación del Firewall, instalación del software de administración, creación de reglas y políticas de seguridad.

Capítulo IV

Se refiere al análisis económico del software a utilizar, costos de instalación, licenciamiento y actualizaciones de licencias.

Capítulo V

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

CAPITULO 1

1. TECNOLOGIAS CONCEPTOS Y PROTOCOLOS

1.1 TECNOLOGIAS Y CONCEPTOS

1.1.1 REDES DE DATOS

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

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y

procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

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

pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

1.1.2 REDES WAN

Generalmente, se considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público, y utilizan parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Típicamente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo a los situados en los contornos) no les concierne el contenido de los datos, al contrario su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

Tradicionalmente, las WAN se han implementado usando una de las tecnologías siguientes: conmutación de circuitos y conmutación de paquetes.

1.1.2.1 CONMUTACION DE CIRCUITOS

En las redes de conmutación de circuitos se establece a través de los nodos de la red un camino dedicado a la interconexión de dos estaciones. El camino es una secuencia conectada de enlaces físicos entre nodos. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino dedicado tan rápido como se pueda. En cada nodo, los datos de entrada se encaminan y conmutan o conmutan por el canal apropiado de salida de sin retardos. El ejemplo más ilustrativo de la conmutación de circuitos es la red telefónica.

1.1.2.2 CONMUTACION DE PAQUETES

Un enfoque diferente al anterior es el adoptado en redes de conmutación de paquetes. En este caso, no es necesario hacer una reserva a priori de recursos (capacidad de transmisión) en el camino (o sucesión de nodos). Por el contrario, los datos se envían en secuencias de pequeñas unidades llamadas paquetes. Cada paquete se pasa de nodo a nodo en la red siguiendo algún camino entre la estación origen y la de destino. En cada nodo, el paquete se recibe completamente, se almacena durante

un intervalo breve y posteriormente se trasmite al siguiente nodo. Las redes de conmutación de paquetes se usan fundamentalmente para comunicaciones Terminal-computador y computador-computador.

1.1.2.3 RDSI y RDSI DE BANDA ANCHA

La sinergia y evolución entre las comunicaciones y las tecnologías de la computación, junto con la creciente demanda de servicios eficaces de captación, procesamiento y diseminación de la información, está desembocando en el desarrollo de sistemas integrados que transmiten y procesan todo tipo de datos. Una consecuencia significativa de esta tendencia ha sido el desarrollo de la Red Digital de Servicios Integrados (RDSI).

La RDSI se ha diseñado para sustituir a las redes públicas de telecomunicaciones existentes, proporcionando una gran variedad de servicios. La RDSI se define mediante la estandarización de las interfaces de usuario, y se ha implementado como un conjunto de conmutadores digitales y enlaces que proporcionan una gran variedad de tipos de tráfico, a la vez que servicios de valor añadido. En la práctica, se trata de múltiples redes, implementadas dentro de los límites nacionales, pero desde el

punto de vista del usuario se considera como una única red mundial, uniformemente accesible.

A pesar de que la RDSI tiene todavía que conseguir la cobertura mundial para la que fue diseñada, está en su segunda generación. La primera generación, a veces denominada como RDSI de banda estrecha, se basa en el uso de canales de 64 Kbps como unidad básica de conmutación, presentando una clara orientación hacia la conmutación de circuitos. Técnicamente hablando, la principal contribución de la RDSI de banda estrecha ha sido el frame relay. La segunda generación, denominada RDSI de banda ancha, proporciona velocidades de transmisión muy elevadas (cientos de Mbps) y tiene una clara orientación hacia la conmutación de paquetes. La contribución técnica principal de la RDSI de banda ancha ha sido el modo de transferencia asíncrono (ATM), también denominado retransmisión de celdas cell relay.

1.1.3 FRAME RELAY, HDLC

La conmutación de paquetes se desarrolló en la época en la que los servicios de transmisión a larga distancia sufrían una tasa de error relativamente elevada, comparada con los servicios de los que se dispone actualmente. Por tanto, para compensar esos

errores relativamente frecuentes, en los esquemas de conmutación de paquetes se realiza un esfuerzo considerable, que se traduce en añadir información redundante en cada paquete, así como la realización de un procesamiento extra, tanto en el destino final como en los nodos intermedios de conmutación, necesario para detectar los errores y corregirlos.

Con los modernos sistemas de comunicaciones de alta velocidad, este esfuerzo adicional es innecesario y contraproducente. Es innecesario debido a que la tasa de error se ha reducido drásticamente y en los escasos errores que aparecen se pueden tratar en el sistema final mediante dispositivos que operan por encima del nivel de la lógica dedicada a la conmutación de paquetes. A su vez es contraproducente debido a que los bits redundantes significan un desperdicio de parte de la capacidad proporcionada por la red.

La retransmisión de tramas (frame relay) se ha desarrollado teniendo presente las mayores velocidades de transmisión que actualmente se disponen, así como las bajas tasas de error. Mientras que las redes originales de conmutación de paquetes se diseñaron para ofrecer una velocidad de transmisión al usuario final de 64 kbps, las redes (frame relay) están diseñadas para

operar eficazmente a velocidades de transmisión de usuario de 2 Mbps. La clave para conseguir estas velocidades reside en eliminar la mayor parte de la información redundante y el procesamiento asociado para el control de errores.

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI: El ITU (entonces CCITT). Sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los conmutadores, en cada "salto" de la red. X.25 tiene el grave inconveniente de su importante "overhead" producido por los mecanismos de control de errores y de flujo.

Hasta hace relativamente poco tiempo, X.25 se ha venido utilizando como medio de comunicación para datos a través de redes telefónicas con infraestructuras analógicas, en las que la norma ha sido la baja calidad de los medios de transmisión, con una alta tasa de errores. Esto justificaba los abundantes controles de errores y sus redundantes mecanismos para el control de flujo, junto al pequeño tamaño de los paquetes. En resumen, se trataba de facilitar las retransmisiones para obtener una comunicación segura.

Frame Relay, por el contrario, maximiza la eficacia, aprovechándose para ello de las modernas infraestructuras, de mucha mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información.

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps., aunque nada le impide superarlas.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, debido a que todas siguen el mismo camino a través de la red.

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay como se visualiza en la figura 1.1.3.1. También incorporan los nodos que conmutan las tramas Frame Relay en función del

identificador de conexión, a través de la ruta establecida para la conexión en la red.

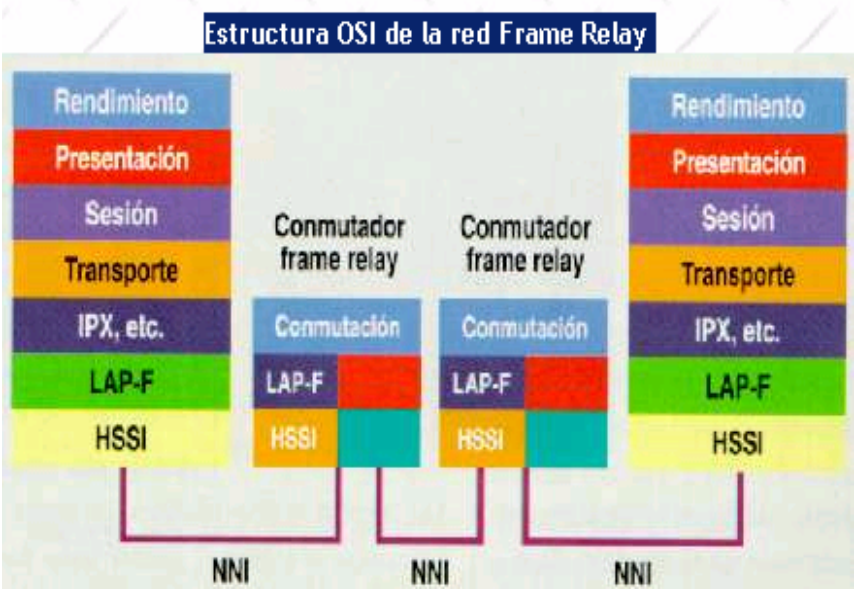


FIGURA 1.1.3.1 ESTRUCTURA FRAME RELAY

Este equipo se denomina FRAD o "Ensamblador/Desensamblador Frame Relay" (Frame Relay Assembler/Disassembler) y el nodo de red se denomina FRND o "Dispositivo de Red Frame Relay"

Las tramas y cabeceras de Frame Relay figuras 1.1.3.2 y 1.1.3.3, pueden tener diferentes longitudes, debido a que hay una gran variedad de opciones disponibles en la implementación, conocidos como anexos a las definiciones del estándar básico.

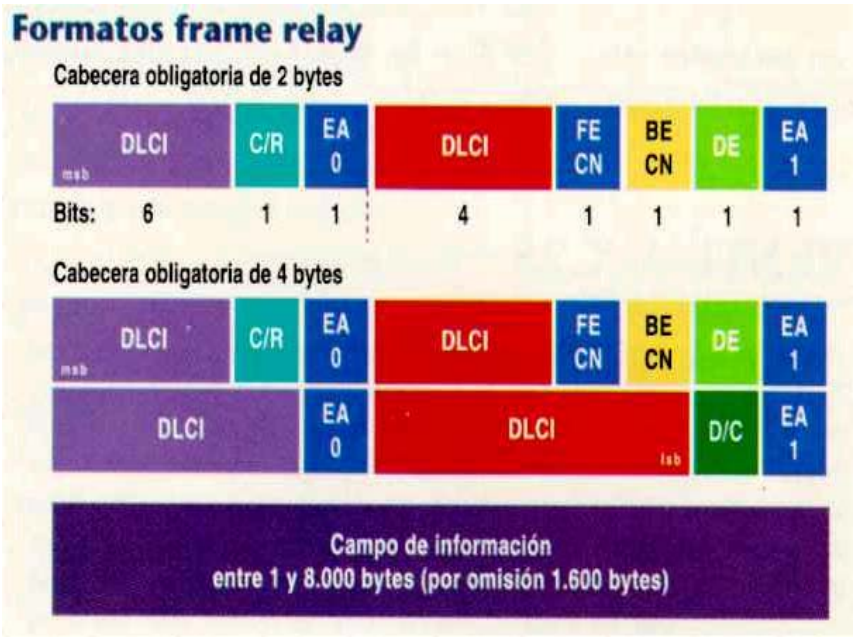


FIGURA 1.1.3.2 CABECERAS DE FRAME RELAY

La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8.250 bytes, aunque por defecto es de 1.600 bytes.

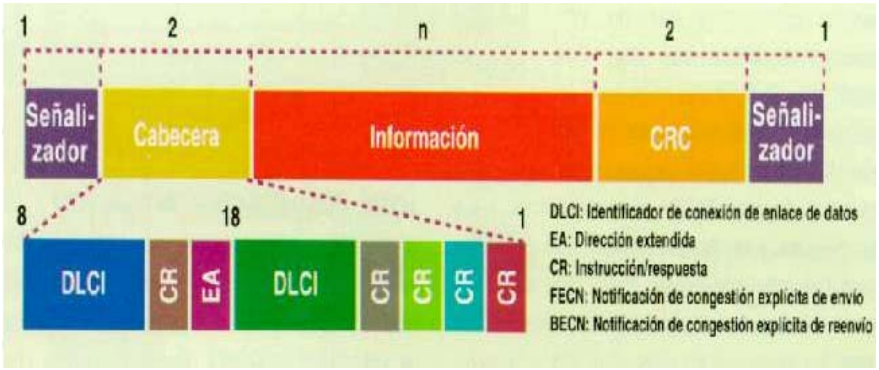


FIGURA 1.1.3.3 TRAMA DE FRAME RELAY

Lo más increíble de todo, es que, a pesar del gran número de formas y tamaños Frame Relay funciona perfectamente, y ha demostrado un muy alto grado de interoperatibilidad entre diferentes fabricantes de equipos y redes. Ello es debido a que, sean las que sean las opciones empleadas por una determinada implementación de red o equipamiento, siempre existe la posibilidad de "convertir" los formatos de Frame Relay a uno común, intercambiando así las tramas en dicho formato.

En Frame Relay, por tanto, los dispositivos del usuario se interrelacionan con la red de comunicaciones, haciendo que sean aquellos mismos los responsables del control de flujo y de errores. La red sólo se encarga de la transmisión y conmutación de los datos, así como de indicar cual es el estado de sus recursos. En el caso de errores o de saturación de los nodos de la red, los equipos del usuario solicitarán el reenvío (al otro extremo) de las tramas incorrectas y si es preciso reducirán la velocidad de transmisión, para evitar la congestión.

Las redes Frame Relay son orientadas a conexión, como X.25, SNA e incluso ATM. El identificador de conexión es la concatenación de dos campos HDLC (High-level Data Link

Control), en cuyas especificaciones originales de unidad de datos (protocolo de la capa 2), se basa Frame Relay. Entre los dos campos HDLC que forman el "identificador de conexión de enlace de datos" o DLCI (Data Link Connection Identifier) se insertan algunos bits de control (CR y EA).

A continuación se añaden otros campos que tienen funciones muy especiales en las redes Frame Relay. Ello se debe a que los nodos conmutadores Frame Relay carecen de una estructura de paquetes en la capa 3, que por lo general es empleada para implementar funciones como el control de flujo y de la congestión de la red, y que estas funciones son imprescindibles para el adecuado funcionamiento de cualquier red.

Los tres más esenciales son DE o "elegible para ser rechazada" (Discard Eligibility), FECN o "notificación de congestión explícita de envío" (Forward Explicit Congestion Notification), y BECN o "notificación de congestión explícita de reenvío" (Backward Explicit Congestion Notification). El bit DE es usado para identificar tramas que pueden ser rechazadas en la red en caso de congestión. FECN es usado con protocolos de sistema final que controlan el flujo de datos entre en emisor y el receptor, como el mecanismo

"windowing" de TCP/IP; en teoría, el receptor puede ajustar su tamaño de "ventana" en respuesta a las tramas que llegan con el bit FECN activado. BECN, como es lógico, puede ser usado con protocolos que controlan el flujo de los datos extremo a extremo en el propio emisor.

Según esto, la red es capaz de detectar errores, pero no de corregirlos (en algunos casos podría llegar tan solo a eliminar tramas).

No se ha normalizado la implementación de las acciones de los nodos de la red ni del emisor/receptor, para generar y/o interpretar estos tres bits. Por ejemplo, TCP/IP no tiene ningún mecanismo que le permita ser alertado de que la red Frame Relay está generando bits FECN ni de cómo actuar para responder a dicha situación. Las acciones y funcionamiento de las redes empleando estos bits son temas de altísimo interés y actividad en el "Frame Relay Forum" (equivalente en su misión y composición al "ATM Forum").

Frame Relay también ha sido denominado "tecnología de paquetes rápidos" (fast packet technology) o "X.25 para los 90´", y esto es cierto en gran medida.

El protocolo X.25 opera en la capa 3 e inferiores del modelo OSI, y mediante la conmutación de paquetes, a través de una red de conmutadores, entre identificadores de conexión. En cada salto de la red X.25 se verifica la integridad de los paquetes y cada conmutador proporciona una función de control de flujo. La función de control de flujo impide que un conmutador X.25 envíe paquetes a mayor velocidad de la que el receptor de los mismos sea capaz de procesarlos. Para ello, el conmutador X.25 receptor no envía inmediatamente la señal de reconocimiento de los datos remitidos, con lo que el emisor de los mismos no envía más que un determinado número de paquetes a la red en un momento dado.

Frame Relay realiza la misma función, pero partiendo de la capa 2 e inferiores. Para ello, descarta todas las funciones de la capa 3 que realizaría un conmutador de paquetes X.25, y las combina con las funciones de trama. La trama contiene así al identificador de conexión, y es transmitida a través de los nodos de la red en lugar de realizar una "conmutación de paquetes".

Para una mejor comprensión veamos la figura. 1.1.3.4, en la que primero se observa una comparación entre una Red x.25 y Red Frame Relay y luego se visualiza como operan las dos redes y en la que resaltamos la operación del frame relay, así :

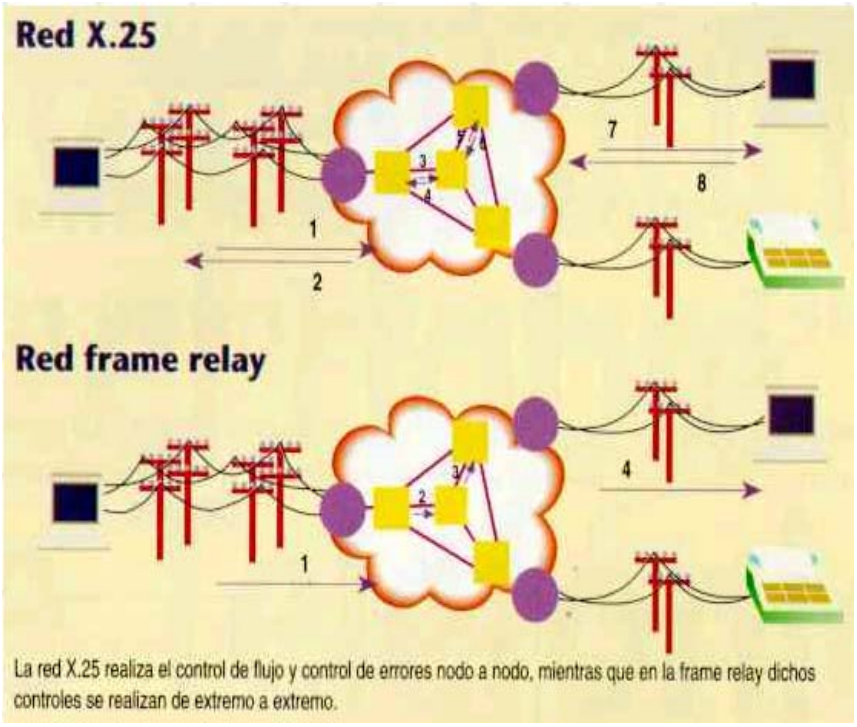


FIGURA 1.1.3.4 COMPARACION Y OPERACION DE RED X.25

Si el usuario "A" desea una comunicación con el usuario "B", primero establecerá un Circuito Virtual (VC o Virtual Circuit), que los una. La información a ser enviada se segmenta en tramas a las que se añade el DLCI.

1.1.4 REDES LAN

Al igual que las redes de área amplia, una red de área local es una red de comunicaciones que interconecta varios edificios y proporciona un medio para el intercambio de información entre ellos. No obstante, hay algunas diferencias entre las LAN y las WAN que se enumeran a continuación:

1. La cobertura de una LAN es pequeña, típicamente un edificio o como mucho un conjunto de edificios próximos. Como se verá más adelante, esta diferencia en cuanto a la cobertura geográfica, condicionará la solución técnica finalmente adoptada.

2. Es común que la LAN sea propiedad de la misma entidad que es propietaria de los dispositivos conectados a la red. En WAN, esto no es tan corriente, o al menos una fracción significativa de recursos de la red son ajenos. Esto tiene dos implicaciones. La primera es que se debe cuidar mucho la elección de la LAN, debido a que evidentemente, lleva acarreado una inversión substancial de capital (comparado con los gastos de conexión o alquiler de líneas en redes de área amplia) tanto en la adquisición como en el

mantenimiento. La segunda, la responsabilidad de la gestión de la red local recae solamente en el usuario.

3. Las velocidades de transmisión internas en una LAN son mucho mayores.

Tradicionalmente, en LAN se utiliza la difusión en lugar de utilizar técnicas de conmutación. En una red de difusión, no hay nodos intermedios. En cada estación hay un transmisor/receptor que se comunica con las otras estaciones a través de un medio compartido. Una transmisión desde cualquier estación se recibirá por todas las otras estaciones. Los datos se transmiten en forma de paquetes. Debido a que el medio es compartido, una y sólo una estación en cada instante de tiempo podrá transmitir el paquete.

1.1.5 TOPOLOGIAS

Las topologías usuales en LAN son bus, árbol, anillo y estrella (figura 1.1.5.1). El bus es un caso especial de la topología en árbol, con un solo tronco y sin ramas.

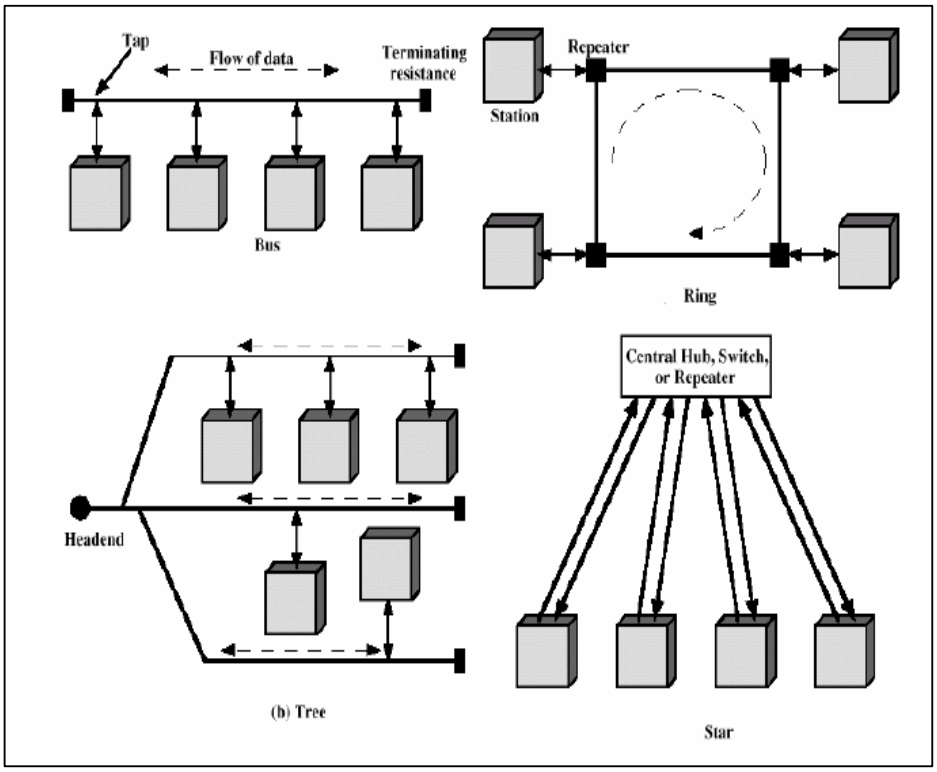


FIGURA 1.1.5.1 TOPOLOGIAS

1.1.5.1 TOPOLOGIAS EN BUS Y EN ARBOL

Ambas topologías se caracterizan por el uso de un medio multipunto. En el caso de la topología en bus, todas las estaciones se encuentran directamente conectadas, a través de interfaces físicas apropiadas conocidas como tomas de conexión (taps), a un medio de transmisión lineal o bus. El funcionamiento full-duplex entre la estación y la toma de conexión permite la transmisión y

recepción de datos. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de estaciones. En cada extremo del bus existe un terminador que absorbe las señales, eliminándolas del bus.

La topología en árbol es una generalización de la topología en bus. El medio de transmisión es un cable ramificado sin bucles cerrados, que comienza que comienza en un punto conocido como raíz o cabecera (headend). Uno o más cables comienzan en el punto raíz , y cada uno de ellos pueden presentar ramificaciones. Las ramas pueden disponer de ramas adicionales, dando lugar a esquemas más complejos. De nuevo, la transmisión desde una estación se propaga a través del medio y puede alcanzar al resto de las estaciones.

Existen dos problemas en esta disposición. E primer lugar, dado que la transmisión desde una estación se puede recibir en las demás estaciones, es necesario algún método para indicar a quien va dirigida la transmisión. En segundo lugar, se precisa un mecanismo para regular la transmisión. Para ver la razón de este hecho hemos de comprender que si dos estaciones intentan transmitir simultáneamente, sus señales se superpondrán y serán erróneas; también se puede considerar la situación en que una

estación decide transmitir continuamente durante un largo período de tiempo.

Para solucionar estos problemas las estaciones trasmiten datos en bloques pequeños llamados tramas. Cada trama consta de una porción de datos que una estación desea transmitir además de una cabecera de trama que contiene información de control. A cada estación en el bus se le asigna una dirección, o identificador, única, incluyéndose en la cabecera la dirección destino de la trama.

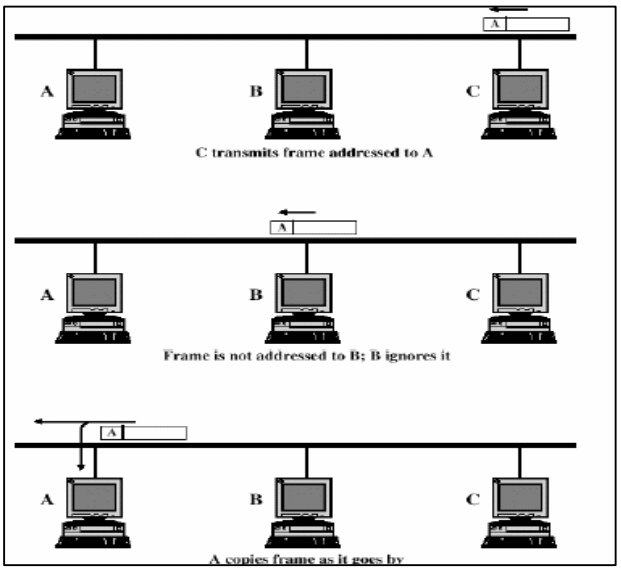


FIGURA 1.1.5.1.1 ESQUEMA PARA LA TRANSMISION DE TRAMA DE DATOS

En la figura 1.1.5.1.1 se ilustra este esquema. En este ejemplo, la estación C desea transmitir una trama de datos a A, de modo que la cabecera de la trama incluirá la dirección de A. En la propagación de la trama a lo largo del bus, ésta atraviesa B, quien observa la dirección de destino e ignora la trama A, por su parte, observa que la trama va dirigida a ella y copia los datos de ésta mientras que pasa.

La estructura de la trama resuelve el primer problema mencionado anteriormente: proporciona un mecanismo para indicar al receptor de los datos. También proporciona una herramienta básica para resolver el segundo problema, el control e acceso. En particular, las estaciones transmiten por turnos en forma cooperativa, lo que implica, como se verá mas adelante, el uso de información de control adicional en la cabecera de las tramas.

1.1.5.2 TOPOLOGIA EN ANILLO

En la topología en anillo, la red consta de un conjunto de repetidores unidos por enlaces punto a punto formando un bucle cerrado. El repetidor es un dispositivo relativamente simple, capaz de recibir datos a través del enlace y de transmitirlos, bit a bit, a través del otro enlace tan rápido como son recibidos.

Los enlaces son unidireccionales, es decir, los datos se transmiten solo en un sentido, de modo que estos circulan alrededor del anillo en el sentido de las agujas del reloj o en el contrario.

Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él.

Como en los casos de las topologías en bus y en árbol, los datos se transmiten en tramas. Una trama que circula por el anillo pasa por las demás estaciones, de modo que la estación de destino reconoce su dirección y copia la trama, mientras ésta la atraviesa, en una memoria temporal local. La trama continúa circulando hasta que alcanza de nuevo la estación origen, donde es eliminada del medio como se ilustra en la figura 1.1.5.2.1

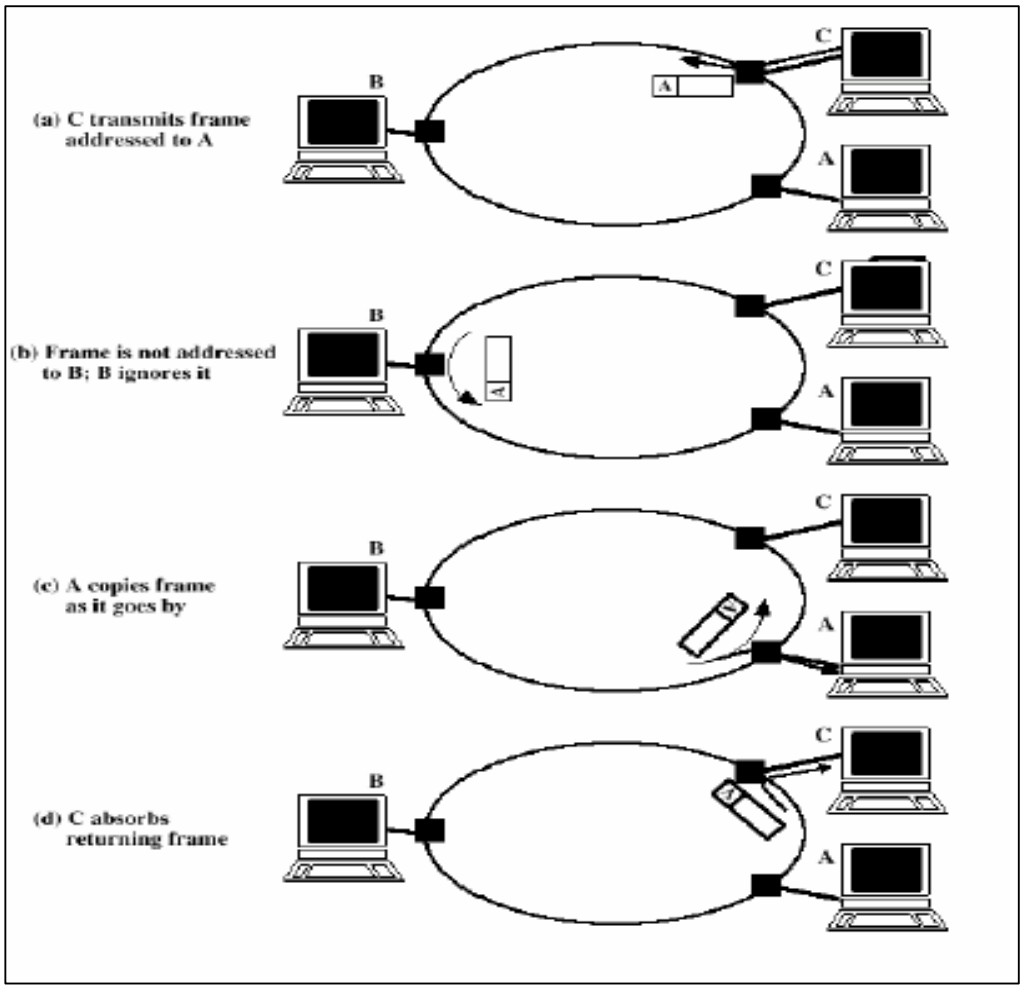


FIGURA 1.1.5.2.1 TOPOLOGIA EN ANILLO

1.1.5.3 TOPOLOGIA EN ESTRELLA

En redes LAN con topología en estrella cada estación está directamente conectada a un nodo central figura 1.1.5.3.1,

generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción.

En general existen dos alternativas para el funcionamiento del nodo central. Una es el funcionamiento en modo de difusión. En el que la transmisión de una trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central.

En este caso, aunque la disposición física es una estrella, lógicamente funciona como un bus: una transmisión desde cualquier estación es recibida por el resto de las estaciones, y sólo puede transmitir una estación en un instante de tiempo dado.

Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino.

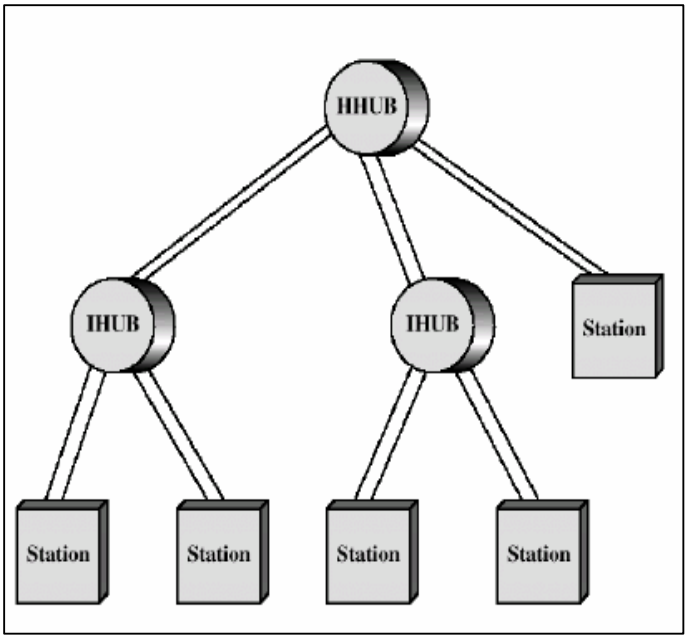


FIGURA 1.1.5.3.1 TOPOLOGIA EN ESTRELLA

1.1.6 REDES PRIVADAS

Una red privada es una red de comunicaciones privada construida, mantenida y controlada por la organización a la que sirve. Como mínimo una red privada requiere sus propios equipos de conmutación y de comunicaciones. Puede también, emplear sus propios servicios de comunicación o alquilar los servicios de una red pública o de otras redes privadas que hayan construido sus propias líneas de comunicaciones.

Aunque una red privada es extremadamente cara, en compañías donde la seguridad es imperante así como también lo es el control sobre el tráfico de datos, las líneas privadas constituyen la única garantía de un alto nivel de servicio. Además, en situaciones donde el tráfico de datos entre dos puntos remotos excede de seis horas al día, emplear una red privada puede ser más rentable que utilizar la red pública.

1.1.7 SEGURIDADES EN LAS REDES

Las amenazas a la seguridad de red se dividen en dos categorías: amenazas pasivas, llamadas a veces escuchas y que suponen el intento de un atacante de obtener información relativa a una comunicación; y amenazas activas que suponen alguna modificación de los datos transmitidos o la creación de transmisiones falsas.

Hasta ahora la herramienta automática más importante para la seguridad en red y de la comunicación es el cifrado. Con el cifrado convencional, dos partes comparten una clave de cifrado/descifrado. El principal reto del cifrado convencional es la distribución y protección de las claves. Un esquema de cifrado de clave pública implica dos claves, una para el cifrado y otra para el

descifrado. Una de las claves es privada de la parte que genera el par de claves y la otra se hace pública.

El cifrado convencional y el cifrado de clave pública se suelen combinar en aplicaciones de red seguras. El cifrado convencional se utiliza para cifrar los datos transmitidos, con una clave utilizada una sola vez o clave de sesión temporal. La clave de sesión la puede distribuir un centro de distribución de claves de confianza o ser transmitida cifrada utilizando un cifrado de clave pública. El cifrado de clave pública también se utiliza para crear firmas digitales, que pueden autentificar la fuente de los mensajes transmitidos.

Una mejora en la seguridad utilizada con IPV4 e IPV6, llamada IPSec, proporciona mecanismos de confidencialidad y autentificación.

Los requisitos en la seguridad de la información dentro de un organismo han sufrido principalmente dos cambios en las últimas décadas. Antes de que se extendiera la utilización de los equipos de procesamiento de datos, la seguridad de la información, que era de valor para una institución se conseguía fundamentalmente por medios físicos y administrativos. Como ejemplo del primer

medio es el uso de cajas fuertes con combinación de apertura para almacenar documentos confidenciales. Un segundo ejemplo es el uso de procedimientos de investigación de personal durante la fase de contratación.

Con la introducción de las computadoras, fue evidente la necesidad de herramientas automáticas para proteger ficheros y otra información almacenada en las computadoras. Este es especialmente el caso de los sistemas multiusuario, como con los sistemas de tiempo compartido, y la necesidad es más aguda para sistemas a los que se puede acceder desde teléfonos públicos o redes de datos.

El segundo cambio relevante, que ha afectado a la seguridad, es la introducción de sistemas distribuidos y la utilización de redes y facilidades de comunicación para transportar datos entre terminales de usuario y computadoras y de computador a computador. Las medidas de seguridad en red son necesarias para proteger los datos durante su transmisión y garantizar que los datos transmitidos sean auténticos.

Virtualmente la tecnología esencial subyacente en todas las redes automáticas y las aplicaciones de seguridad en computadoras es

el cifrado. Existen dos técnicas fundamentales en uso: cifrado convencional, también conocido como cifrado simétrico, y el cifrado con clave pública, también conocido como cifrado asimétrico.

1.1.7.1 REQUISITOS Y AMENAZAS A LA SEGURIDAD

Para ser capaz de entender los tipos de amenazas a la seguridad que existen, conviene definir los requisitos en seguridad. La seguridad en computadoras y en redes implica tres requisitos:

Secreto: requiere que la información en un computador sea accesible para lectura sólo por los entes autorizados. Este tipo de acceso incluye la impresión, mostrar en pantalla y otras formas de revelación que incluye cualquier forma de dar a conocer la existencia de un objeto.

Integridad: requiere que los recursos de un computador sean modificados solamente por entes autorizados. La modificación incluye escribir, cambiar de estado, suprimir y crear.

Disponibilidad: requiere que los recursos de un computador estén disponibles a los entes autorizados.

1.1.7.2 ATAQUES PASIVOS

Las agresiones pasivas son del tipo de las escuchas, o monitorizaciones, de las transmisiones. La meta del oponente es obtener información que está siendo transmitida. Existen dos tipos de agresiones: divulgación del contenido de un mensaje y análisis de tráfico.

La divulgación del contenido de un mensaje se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico, un fichero transferido puede contener información sensible o confidencial. Así sería deseable prevenir que el oponente se entere del contenido de estas transmisiones.

El segundo tipo de agresión pasiva, el análisis del tráfico, es más sutil. Suponga que tenemos un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección del cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y

observar la frecuencia y la longitud de los mensajes intercambiados.

Los ataques pasivos son muy difíciles de detectar pues no implican la alteración de los datos. Sin embargo, es factible prevenir el éxito de estas agresiones. Así, el énfasis para tratar estas agresiones está en la prevención antes que la detección.

1.1.7.3 ATAQUES ACTIVOS

Los ataques activos suponen alguna modificación del flujo falso y se subdividen en 4 categorías: enmascaramiento, repetición, modificación de mensajes y denegación de un servicio.

Un enmascaramiento tiene lugar cuando una entidad pretende ser otra entidad diferente. Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa. Por ejemplo, se puede captar una secuencia de autentificación y reemplazarla por otra secuencia de autentificación válida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.

La repetición supone la captura pasiva de unidades de datos y su retransmisión subsecuente para producir un efecto no autorizado.

La modificación de mensajes significa sencillamente que alguna porción de un mensaje legítimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular (por ejemplo, al servicio de vigilancia de seguridad). Otro tipo de denegación de servicio es la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de forma que se degrade su rendimiento.

1.1.7.4 PRIVACIDAD CON CIFRADO CONVENCIONAL

CIFRADO CONVENCIONAL

El cifrado convencional, también llamado cifrado simétrico o de clave única, era el único tipo de cifrado en uso antes de la introducción del cifrado de clave pública a finales de la década de los 70. El cifrado convencional ha sido utilizado para las comunicaciones secretas por incontables individuos y grupos. Es todavía el cifrado más utilizado mundialmente de los dos tipos de cifrado.

Un esquema de cifrado convencional tiene cinco ingredientes.

Texto nativo: es el mensaje original o datos que actúan como entrada al algoritmo.

Algoritmo de cifrado: el algoritmo de cifrado lleva a cabo varias substituciones y transformaciones en el texto nativo.

Clave secreta: la clave secreta es también una entrada al algoritmo de cifrado. Las substituciones y transformaciones exactas realizadas por el algoritmo dependen de la clave.

Texto cifrado: es el mensaje aleatorio que se produce en la salida. Depende del texto nativo y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos cifrado diferentes.

Algoritmo de descifrado: es esencialmente el algoritmo de cifrado ejecutando al revés. Toma como entradas el texto cifrado y la clave secreta y produce el texto nativo original.

Existen dos requisitos para la utilización segura del cifrado convencional:

1. Se necesita un algoritmo de cifrado robusto. Como mínimo, es de desear un algoritmo tal que si el oponente conoce el algoritmo y tiene acceso a más de un texto cifrado, sea incapaz de descifrar el texto o descubrir la clave incluso si él o ella posee un determinado número de texto cifrados junto a los textos nativos que producen cada texto cifrado.

2. El emisor y el receptor deben haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y conoce el algoritmo, todas las comunicaciones que utilicen esta clave pueden ser leídas.

Existen dos enfoques generales para atacar el esquema de cifrado convencional. El primer ataque se conoce como criptoanálisis. El ataque de criptoanálisis se basa en la naturaleza del algoritmo más quizás algún conocimiento de las características generales del texto nativo o incluso de algunos pares de texto nativo-texto cifrado. Este tipo de ataque explota las características del algoritmo para intentar deducir un texto nativo específico o deducir la clave que se está utilizando. Si el ataque tiene éxito en deducir la clave, el efecto es catastrófico: todos los

mensajes cifrados antiguos y futuros con esa clave están comprometidos.

El segundo método, conocido como ataque de fuerza bruta, es intentar cada clave posible en un trozo de texto cifrado hasta que se obtenga una traducción inteligible del texto nativo.

ALGORITMOS DE CIFRADO

Los algoritmos de cifrado usados más comúnmente son los cifradores de bloque. Un cifrador de bloque procesa una entrada de texto nativo en bloques de tamaño fijo y produce un bloque de texto cifrado de igual tamaño para cada bloque de texto nativo. Los dos algoritmos convencionales más importantes cifradores de bloques, son el DES y el TDEA.

1.1.8 ARQUITECTURA TCP/IP

Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de comunicación: el conjunto de protocolos TCP/IP y el modelo de referencia OSI. TCP/IP es la arquitectura más adoptada para la interconexión de sistemas, mientras que OSI se ha convertido en el modelo estándar para clasificar las funciones de comunicación.

TCP/IP es el resultado de la investigación y desarrollo llevados a cabo en la red experimental de conmutación de paquetes ARPANET, financiada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA, Defense Advanced Research Proyects Agency), y se denomina globalmente como la familia de protocolos TCP/IP. Esta familia consiste en una extensa colección de protocolos que se han erigido como estándares de internet.

Al contrario que en OSI, no hay un modelo oficial de referencia TCP/IP. No obstante, basándose en los protocolos estándar que se han desarrollado, todas las tareas involucradas en la comunicación se puede organizar en cinco capas relativamente independientes:

- Capa de aplicación.
- Capa origen-destino o de transporte.
- Capa Internet.
- Capa de acceso a la red.
- Capa física.

La capa física define la interfaz física entre el dispositivo de transmisión de datos (por ejemplo, la estación de trabajo o el

computador) y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos, y cuestiones afines.

La capa de acceso a la red es responsable del intercambio de datos entre el sistema final y la red a la que se está conectando. El emisor debe proporcionar a la red la dirección del destino, de tal manera que la red pueda encaminar los datos hasta el destino apropiado. El emisor puede requerir ciertos servicios, como por ejemplo solicitar una determinada prioridad, que pueden ser proporcionadas por el nivel de red. El software en particular que se use en esta capa dependerá del tipo de red que se disponga; se han desarrollado diversos estándares para conmutación de circuitos, conmutación de paquetes (por ejemplo, X.25), redes de área local (por ejemplo ethernet), entre otros.

La capa de acceso a la red está relacionada con el acceso y encaminamiento de los datos a través de la red. En situaciones en las que los dos dispositivos estén conectados a redes diferentes, se necesitarán una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas. Esta es la función de la capa Internet. El protocolo Internet (IP, Internet

Protocol) se utiliza en esta capa para ofrecer el servicio de encaminamiento a través de varias redes. Este protocolo se implementa tanto en los sistemas finales como en los routers intermedios. Un router es un dispositivo con capacidad de procesamiento que conecta dos redes y cuya función principal es retransmitir datos desde una red a otra siguiendo la ruta adecuada para alcanzar el destino.

Independientemente de la naturaleza de las aplicaciones que están intercambiando datos, es usual requerir que los datos se intercambien de forma segura. Esto es, sería deseable asegurar que todos los datos llegan a la aplicación destino y el mismo orden en el que fueron enviados. Los procedimientos que garantizan una transmisión segura están localizados en la capa origen-destino, o capa de transporte. El protocolo TCP (Transmission Control Protocol) es el mas utilizado para proporcionar esta funcionalidad.

Finalmente, la capa de aplicación contiene la lógica necesaria para posibilitar las distintas aplicaciones de usuario. Para cada tipo particular de aplicación, como por ejemplo la transferencia de ficheros, se necesitará un módulo bien diferenciado.

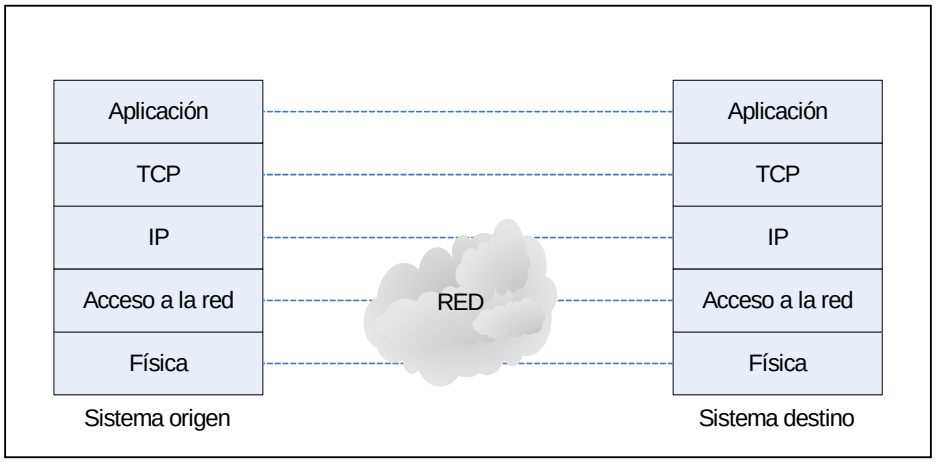


FIGURA 1.1.8.1 IMPLEMENTACION DE PROTOCOLOS TCP/IP

La figura 1.1.8.1 muestra como se implementan los protocolos TCP/IP en los sistemas finales. Nótese que las capas físicas y de acceso a la red proporcionan la interacción entre el sistema final y la red, mientras que las capas de aplicación y transporte albergan los protocolos denominados extremo a extremo, y facilitan la interacción entre los sistemas finales. La capa Internet tiene algo de las dos aproximaciones anteriores. En esta capa, los sistemas origen y destino proporcionan a la red la información necesaria para realizar el encaminamiento, pero a la vez, deben proporcionar algunas funciones adicionales de intercambio entre los dos sistemas finales.

1.1.8.1 EL MODELO OSI

El modelo de OSI (Open Systems Interconection) se desarrolló por la Organización Internacional de Estandarización ISO (International Organization for Standarization) como la arquitectura para comunicaciones entre computadores, con el objetivo de ser el marco de referencia en el desarrollo de protocolos estándares. OSI considera siete capas:

- Aplicación
- Presentación
- Sesión
- Transporte
- Red
- Enlace de datos
- Física

La intención del modelo OSI es que los protocolos se desarrollen de forma tal que realicen las funciones de cada una de las capas.

Existe una serie de razones que justifican el éxito de los protocolos TCP/IP sobre OSI. A continuación enumeramos las siguientes:

1. Los protocolos TCP/IP se especifican y se utilizaron de una forma generalizada antes de la normalización ISO. Así en los años ochenta las instituciones que tenían necesidades apremiantes de intercambio de información se enfrentaron al dilema de esperar a la disponibilidad del paquete siempre prometido y nunca entregado de OSI, o por el contrario utilizar el conjunto TCP/IP de disponibilidad inmediata y operatividad cada vez mas contrastada. Una vez hecha la elección de TCP/IP, el coste y los riesgos de la migración a un nuevo entorno, inhibió la aceptación d e ISO.

2. Los protocolos TCP/IP se desarrollaron inicialmente como resultado del esfuerzo investigador en el entorno militar de los EE.UU., financiado por el Departamento de Defensa (DOD, Department of Defense). Aunque el DOD, como el resto del gobierno de los EE.UU., estaba involucrado en los procesos internacionales de normalizaciones, el DOD tenía una necesidad imperiosa e inmediata de conectividad, tal que no le permitía esperar hasta los años ochenta o incluso

principios de los noventa a productos basados en OSI. Por consiguiente, el DOD exigió el uso de los protocolos TCP/IP en todas sus adquisiciones de software.

3. Internet está construida sobre el conjunto de protocolos TCP/IP.

El conjunto de protocolos TCP/IP reconoce que la tarea de la comunicación es lo suficientemente compleja y diversa como para realizarla en una única unidad. Consecuentemente, la tarea se descompone en diversos módulos o entidades, que se pueden comunicar con sus entidades pares del sistema remoto. Una entidad dentro de un sistema proporciona servicios a otras entidades y, a su vez, utiliza los servicios de otras entidades. Las reglas de diseño del software de calidad dictan que estas entidades se deben agrupar en una forma modular y jerárquica.

El modelo OSI se basa en el mismo razonamiento, pero introduce un paso más. El siguiente paso en OSI está en reconocer que, en muchos aspectos, los protocolos en el mismo nivel de la jerarquía tienen algunas características comunes. Esto desemboca ineludiblemente en el concepto del nivel o capa, así como en el

intento de describir de una forma abstracta las características comunes de los protocolos en un nivel dado.

Como herramienta didáctica, un modelo en capas tiene un valor significativo.

En el modelo TCP/IP, el uso estricto de todas las capas no es obligatorio. Por ejemplo, hay protocolos de aplicación que operan directamente sobre IP.

- **Capa de aplicación:** proporciona la comunicación entre procesos o aplicaciones de computadores separados.

- **Capa de transporte o extremo-a-extremo:** proporciona un servicio de transferencia de datos extremo-a-extremo. Esta capa puede incluir mecanismos de seguridad. Oculta los detalles de la red, o redes subyacentes, a la capa de aplicación.

- **Capa Internet:** relacionada con el encaminamiento de los datos del computador origen al destino a través de una o más redes conectadas por dispositivos de encaminamiento.

- **Capa de acceso a la red:** relacionada con la interfaz lógica entre un sistema final y una subred.

- **Capa física:** define las características del medio de transmisión, la tasa de señalización y el esquema de codificación de las señales.

1.1.8.2 FUNCIONAMIENTO DE TCP/IP

La figura 1.1.8.2.1 muestra como se configuran los protocolos TCP/IP. Para conectar un computador a una subred se utiliza algún tipo de protocolo de acceso como, por ejemplo, Ethernet. Este protocolo permite al computador enviar datos a través de la subred a otro computador o, en caso de que el destino final esté en otra subred, a un dispositivo de encaminamiento. IP se implementa en todos los sistemas finales y dispositivos de encaminamiento. Actúa como un porteador que transportará bloques de datos desde un computador hasta otro, a través de uno o varios dispositivos de encaminamiento. TCP se implementa solamente en los sistemas finales: guarda un registro de los bloques de datos para asegurar que todos se entregan de forma segura a la aplicación apropiada.

Para tener éxito en la transmisión, cada entidad en el sistema global debe tener una única dirección. En realidad, se necesitan dos niveles de direccionamiento. Cada computador en la red debe tener una única dirección Internet que permita enviar los datos al computador adecuado. Además, cada proceso que se ejecute dentro de un computador en red debe tener a su vez una dirección que sea única dentro del mismo; esto permite al protocolo extremo-a-extremo (TCP) entregar los datos al proceso adecuado. Estas últimas direcciones se denominan puertos.

A continuación, se va a describir paso a paso el funcionamiento de la figura 1.1.8.2.1. Así, un proceso asociado al puerto 1 en el computador A, desea enviar un mensaje a otro proceso, asociado al puerto 2 del computador B. El proceso en A pasa el mensaje al TCP con la instrucción de enviarlo al puerto 2 del computador B. El TCP pasa el mensaje al IP con instrucciones de que lo envíe al computador B. Obsérvese que no es necesario comunicarle al IP la identidad del puerto destino. Todo lo que necesita saber es que los datos van dirigidos al computador B. A continuación, IP pasa el mensaje al la capa de acceso a la red (por ejemplo, a la lógica ethernet) con el mandato expreso de enviarlo al dispositivo de encaminamiento X (el primer salto en el camino a B).

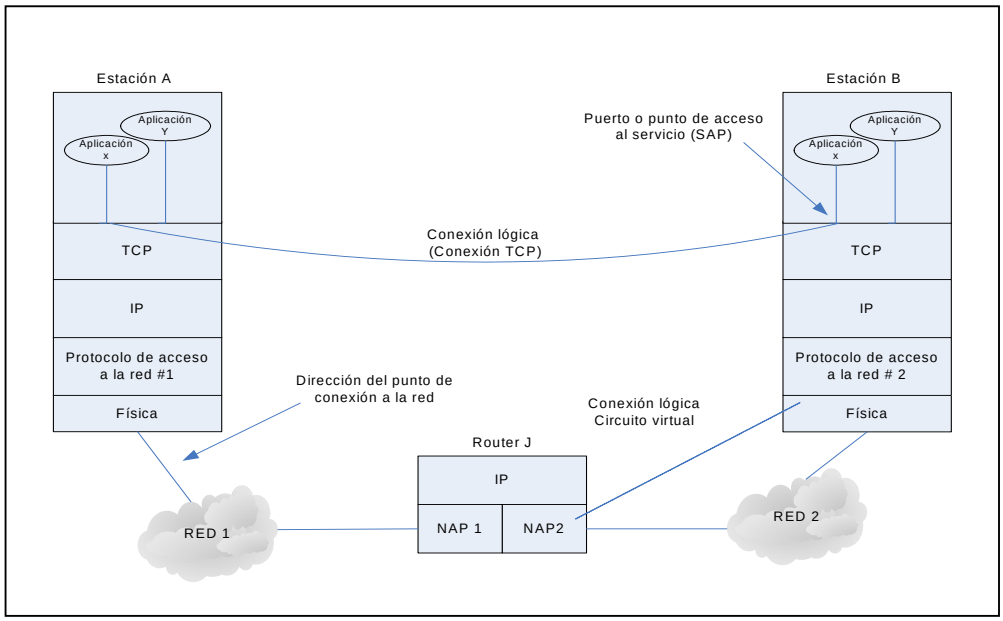


FIGURA 1.1.8.2.1 CONFIGURACION DE PROTOCOLOS TCP/IP

Para controlar esta operación se debe transmitir información de control junto con los datos de usuario, como así se sugiere en la figura 1.1.8.2.2. Supongamos que el proceso emisor genera un bloque de datos y lo pasa al TCP. El TCP puede que divida este bloque en fragmentos más pequeños para hacerlos más manejables. A cada uno de estos fragmentos le añade información de control, denominada cabecera TCP, formando un segmento TCP. La información de control la utilizará la entidad TCP en el computador B. Entre otros, en la cabecera se incluyen los siguientes campos:

- **Puerto destino:** cuando la entidad TCP en B recibe el segmento, debe conocer a quién se le deben entregar los datos.
- **Número de secuencia:** TCP numera secuencialmente los segmentos que envía a un puerto destino dado, para que si llegan desordenados la entidad TCP en B pueda reordenarlos.
- **Suma de comprobación:** la entidad emisora TCP incluye un código calculado en función del resto del segmento. La entidad receptora TCP realiza el mismo cálculo y compara el resultado con el código recibido. Si se observa alguna discrepancia implicará que ha habido algún error en la transmisión.

A continuación, TCP pasa cada segmento al IP con instrucciones para que los transmita a B. Estos segmentos se transmitirán a través de una o varias subredes y serán retransmitidos en uno o mas dispositivos de encaminamientos intermedios. Esta operación también requiere el uso de información de control. Así, el IP añade una cabecera de información de control a cada segmento para formar un datagrama IP. En la cabecera IP, además de otros campos, se incluirá la dirección del computador destino.

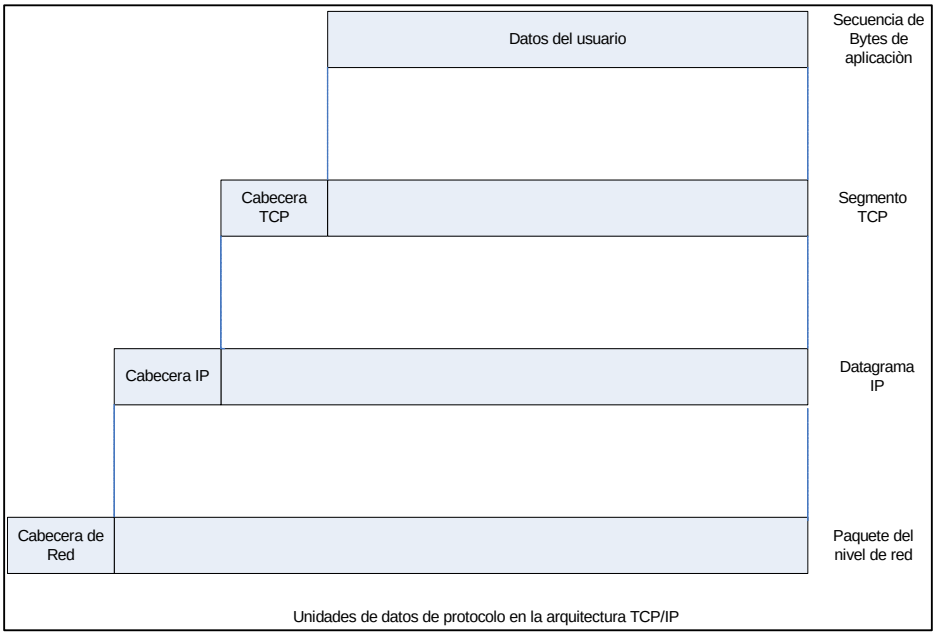


FIGURA 1.1.8.2.2 UNIDADES DE PROTOCOLO DE DATOS

Finalmente, cada datagrama IP se pasa a la capa de acceso a la red para que se envíe a través de la primera subred. La capa de acceso a la red añade su propia cabecera. Creando un paquete, o trama. El paquete se transmite a través de la red al dispositivo de encaminamiento J. La cabecera del paquete contiene la información que la red necesita para transferir los datos. La cabecera puede contener, entre otros, los siguientes campos:

Dirección de la red destino: la red debe conocer a qué dispositivo conectado se debe entregar el paquete.

Funciones solicitadas: el protocolo de acceso a la red podría solicitar la utilización de ciertas funciones que ofrezca la red, como, por ejemplo, la utilización de prioridades.

En el dispositivo de encaminamiento J se elimina la cabecera del paquete y se examina la cabecera IP. El módulo IP del dispositivo de encaminamiento direcciona el paquete a través de la red 2 hacia B basándose en la dirección destino que contenga la cabecera IP. Para hacer esto, se le añade al datagrama una cabecera de acceso a la red.

Cuando se reciben los datos en B, ocurre el proceso inverso. En cada capa se elimina la cabecera correspondiente y el resto se pasa a la capa inmediatamente superior, hasta que los datos de usuario alcancen al proceso destino.

1.1.8.3 INTERFACES DE PROTOCOLO

En la familia de protocolos TCP /IP cada capa interacciona con sus capas adyacentes. En el origen, la capa de aplicación utilizará los servicios de la capa extremo-a-extremo y la capa Internet, e igualmente en la interfaz entre la capa Internet y la capa de

acceso a la red. En el destino, cada capa entrega los datos a la capa superior adyacente.

La arquitectura de TCP/IP no exige que se haga uso de todas las capas. Como así se sugiere en la figura 1.1.8.3.1, es posible desarrollar aplicaciones que invoquen directamente los servicios de cualquier capa. La mayoría de las aplicaciones requieren un protocolo extremo-a-extremo seguro y por tanto utilizan TCP. Algunas de estas aplicaciones, como el protocolo sencillo de gestión de red (SNMP, Simple Network Management Protocol), Utilizan un protocolo extremo-a-extremo alternativo denominado protocolo de datagrama de usuario (UDP, User Datagram Protocol); otras, en cambio, pueden hacer uso de IP directamente. Las aplicaciones que no necesiten interconexión de redes y que no necesiten TCP pueden invocar directamente los servicios de la capa de acceso a la red

La figura 1.1.8.3.1 muestra la organización de los protocolos más importantes de la familia de TCP/IP.

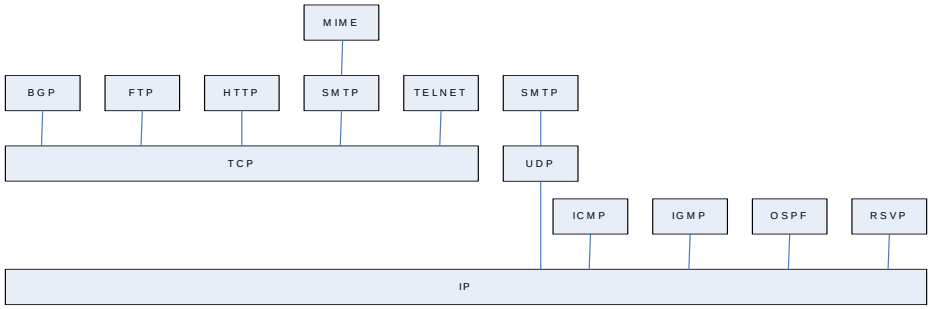
El protocolo sencillo de transferencia de correo (SMTP, Simple Mail Transfer Protocol) proporciona una función básica de correo electrónico. Proporciona un mecanismo para transferir mensajes

entre computadores remotos. Entre las propiedades del SMTP cabe destacar la utilización de listas de mensajería, la gestión de acuses de recibo y el reenvío de mensajes. El protocolo SMTP no especifica cómo se crean los mensajes, para este fin se necesita un programa de correo electrónico nativo o un editor local. Una vez que se ha creado el mensaje, SMTP lo acepta y hace uso del TCP para enviarlo al módulo SMTP en el conmutador remoto. En el receptor, el módulo SMTP utilizará su aplicación de correo electrónico local para almacenar el mensaje recibido en el buzón de correo del usuario destino.

El protocolo de transferencia de ficheros (FTP, File Transfer Protocol) se utiliza para enviar ficheros de un sistema a otro bajo el control del usuario. Se permite transmitir ficheros tanto de texto como en binario, además el protocolo permite controlar el acceso de los usuarios. Cuando un usuario solicita la transferencia de un fichero, el FTP establece una conexión TCP con el sistema destino para intercambiar mensajes de control. Esta conexión permite al usuario transmitir su identificador y contraseña, además de la identificación del fichero junto con las acciones a realizar sobre el mismo. Una vez que el fichero se haya especificado y su transferencia haya sido aceptada, se establecerá una segunda conexión TCP a través de la cual se materializará la transferencia.

El fichero se transmite a través de la segunda conexión, sin necesidad de enviar información extra, o cabeceras generadas por la capa de aplicación. Cuando la transferencia finaliza, se utiliza la conexión de control para indicar el fin, además esta misma conexión estará disponible para aceptar nuevas órdenes de transferencia.

TELNET facilita la posibilidad de conexión remota, mediante la cual el usuario en un Terminal o computador personal se conecta a un computador remoto y trabaja como si estuviera conectado directamente a ese computador. El protocolo se diseñó para trabajar con terminales poco sofisticados en modo scroll (avance de pantalla). En realidad, TELNET se implementa en dos módulos: el usuario TELNET interactúa con el módulo de E/S para comunicarse con Terminal local. Este convierte las particularidades de los terminales reales a una definición normalizada de Terminal de red, y viceversa. El servidor TELNET interactúa con las aplicación, actuando como un sustituto del gestor del Terminal, para que de esta forma el Terminal remoto le parezca local a la aplicación. El tráfico entre el Terminal del usuario y el servidor TELNET se transmite sobre una conexión TCP.



BGP = Protocolo de pasarela frontera
FTP = Protocolo de transferencia de Ficheros
HTTP = Protocolo para la transferencia de hipertexto
ICMP = Protocolo de control de mensajes en Internet
IP = Protocolo Internet
Mime = Extensiones multipropósito de correo electrónico en internet

OSPF = Protocolo abierto del primer camino mas corto
RSVP = Protocolo de reserva de recursos
SMTP = Protocolo sencillo de correo electrónico
SNMP = Protocolo sencillo de control de mensajes en Internet
TCP = Protocolo de control de transmisión
UDP = Protocolo de datagramas de usuarios

FIGURA 1.8.3.1 DE PROTOCOLOS DE LA FAMILIA TCP/IP

1.2 CONCEPTO Y FUNCIONES DE FIREWALL

1.2.1 CONCEPTO DE FIREWALL

Un firewall o cortafuegos es una herramienta de hardware o software utilizado en una red para prevenir algunas comunicaciones prohibidas por las políticas de seguridad de la red, como se ilustra

en la figura 1.2.1. Un firewall es también llamado un filtro de paquetes

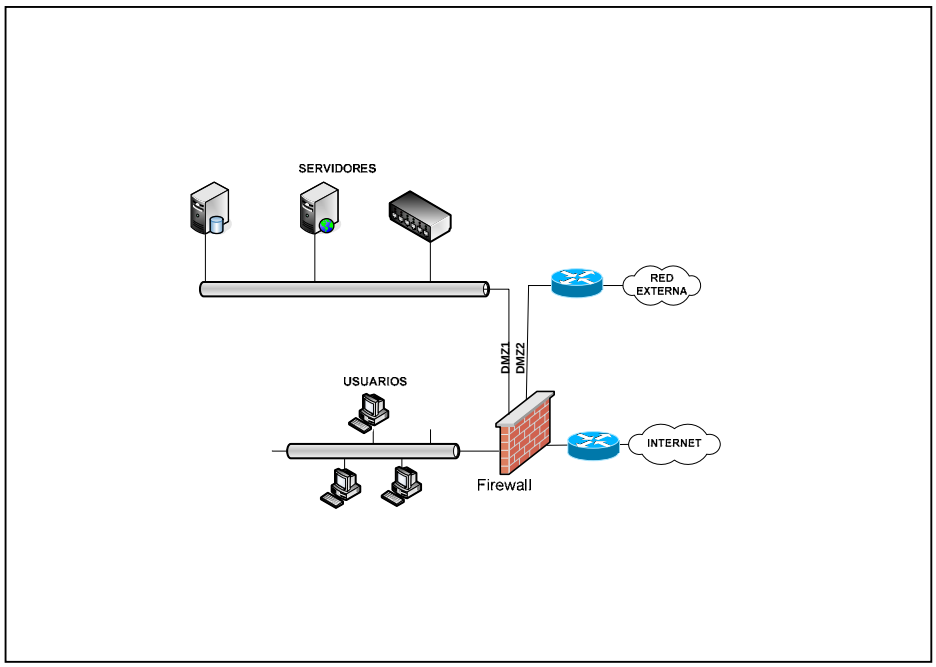


FIGURA 1.2.1 ESQUEMA DE UN FIREWALL

Un firewall nos garantiza que si nuestra red tiene algún tipo de conexión hacia el mundo exterior, o hacia otras redes, ésta sea segura, evitando violaciones, y permitiendo pasar sólo los paquetes de red autorizados, por lo que se deben configurar los firewalls para lograr que sean transparente a los usuarios normales de nuestra red, y totalmente sólido para los "otros usuarios". En muchos casos, la posibilidad de destrucción de la

información existente en nuestra red, por medio de los llamados "hackers" (en realidad, el término correcto es el de crackers), lleva a implementar la necesidad de, en caso de conectarnos con redes externas, loguearse primero en un ordenador firewall, y luego ir al exterior.

Esta política no es la más acertada, ya que el sólo hecho de saber que hay un firewall, lleva a usuarios más avezados en el mundo de las redes a intentar crackearlos, muchas veces con éxito por tener más datos de la red que los crackers externos.

No olvidemos que en el año 1997, el 85% de los problemas de seguridad fueron ocasionados por usuarios internos, desde la propia red en la que se estaba trabajando, que intentaban, como meta personal, lograr destruir la seguridad interna.

Sin duda el mejor firewall es el que no genera una huella visible en una red. Es el que posee un sistema operativo que es totalmente desconocido, o que no posee un sistema operativo en el concepto completo que todos poseemos del mismo. Hoy en día, existen productos que permiten, a través de algoritmos muy avanzados,

generar redes privadas virtuales en Internet. El mismo se basa en el concepto de la creación de un "túnel" dentro de Internet.

La ventaja de estos sistemas, es que el cracker no encuentra qué es lo que debe crackear, ya que estos sistemas no permiten el sniff (sniff es la acción de "oler" los paquetes de red, filtrándolos para obtener algún tipo de información).

La desventaja es que sólo se puede generar la comunicación si de los dos lados de la red existe un sistema con estas características. Sin embargo, se puede armar un sistema bastante seguro utilizando un sistema operativo robusto, el software adecuado, y las configuraciones necesarias para tales fines.

1.2.2 TIPOS DE FIREWALL

Conceptualmente hay dos tipos de firewalls, nivel de red y nivel de aplicación.

Los firewalls de nivel de red toman sus acciones en función del origen, la dirección de destino y el port en cada paquete IP. Los modernos firewalls de este tipo se han sofisticado y mantienen información respecto del estado de las conexiones que están

activas a través de él, etc.. Este tipo de firewall tienden a ser muy rápidos y son transparentes al usuario.

Los firewalls de nivel de aplicación por lo general son hosts corriendo proxy servers, que no permiten el tráfico directo entre redes, manteniendo una elaborada auditoria y logeo del tráfico que pasa a través de él. Este tipo de firewall puede ser utilizado para realizar las tareas relativas al NAT, debido a que como las comunicaciones van de un lado hacia el otro se puede enmascarar la ubicación original. Este tipo tiende a proveer una auditoría más detallada y un mayor grado de seguridad que los de nivel de red.

Los routers de filtro de paquetes, que corresponden al primer grupo, realizan una decisión del tipo pasa no pasa para cada paquete que recibe. El router examina cada datagrama para determinar si se aplican sus reglas de filtrado. Las reglas de filtrado se basan en la información contenida en el header del paquete. Esta información consiste en el IP de origen, la IP de destino, el protocolo encapsulado (TCP, UDP, ICMP), el port TCP/UDP de origen y de destino, etc. Toda esta información es controlada contra las reglas de filtrado definidas, pudiendo ser enrutada si existe una regla que lo permite, descartada si una

regla así lo indica y si no existe regla comparable un parámetro previamente configurado determinará si el paquete pasa o no.

Dentro de este tipo están los que filtran en función del servicio involucrado. Esto es posible pues hay muchos servicios para los cuales están normalizados los ports en los que escuchan, por lo cual se pueden definir reglas que involucren el port, definiendo la aceptación o el rechazo.

Por otro lado frente a diferentes ataques que se fueron produciendo surgieron otros firewalls cuyas reglas son independientes del servicio; estas reglas exigen un análisis más detallado que involucra el ruteo, las opciones de IP, verificación de los fragmentos de desplazamiento y puntos por el estilo.

La mayoría de los firewalls implementados sobre Internet están desarrollados sobre el concepto de filtrado de paquetes. Este tipo de firewalls no son difíciles de configurar debido a que su software contiene una serie de reglas previamente configuradas y fundamentalmente son transparentes al usuario y no exigen instalar ningún software adicional en los hosts.

Por otro lado cuando se debe customizar de manera tal de adaptarlo a aplicaciones específicas de cada empresa la tarea se puede hacer algo compleja pues exige una figura de administrador que debe conocer los servicios de Internet, los distintos encabezados de los paquetes, los distintos valores que se espera encontrar en los campos a analizar. Si se requiere un filtrado complejo, las reglas pueden volverse demasiado largas con la consecuencia de una difícil administración y seguimiento.

Los filtros a nivel de aplicación permiten aplicar un esquema de seguridad más estricto. En estos firewalls se instala un software específico para cada aplicación a controlar (un proxy server); de hecho si no se instala los servicios relativos a la aplicación las comunicaciones no podrán ser enrutadas, punto que no se convierte en trivial pues de esta forma estamos garantizando que todas aquellas nuevas aplicaciones desconocidas no podrán acceder a nuestra red. Otra ventaja que trae el uso de este tipo de firewall es que permite el filtrado del protocolo, por ejemplo se podría configurar el proxy server que atiende el FTP para que pueda aceptar conexiones pero denegar el uso del comando put asegurando de esta forma que no nos puedan escribir ningún archivo o que impida navegar por el FS; esto es lo que hay se conoce como un FTP anónimo.

Este tipo de configuración incrementa los costos de la plataforma sobre la cual funcionará el filtro. Algunos autores reconocen otro nivel de aplicación de firewall que es nivel de circuito, que en realidad no procesa ni filtra el protocolo, sino que simplemente establece un circuito entre origen y destino.

1.2.3 ARQUITECTURA DE UN FIREWALL

Las tecnologías de filtrado de paquetes que se emplean en los firewalls constituyen una manera eficaz y general para controlar el tráfico en la red. Tales tecnologías tienen la ventaja de no realizar ningún cambio en las aplicaciones del cliente y el servidor, pues operan en las capas IP y TCP, las cuales son independientes de los niveles de aplicación según se establece en el modelo OSI. Por otro lado, los enfoques de la filtración de paquetes no han declarado muchos requerimientos de seguridad, por la información incompleta con la que trabajan. Sólo la información de las capas de transporte y red, como las direcciones IP, los números de puerto y las banderas TCP están disponibles para las decisiones de filtración. En muchas implementaciones de los filtros de paquete, el número de reglas puede ser limitado; además, mientras mayor sea este número, habrá una alta penalización en

el desempeño, a causa del proceso adicional necesario para las reglas complementarias.

En vista de la falta de información de contexto, ciertos protocolos como el UDP y RPC no pueden filtrarse con efectividad. Además, en muchas implementaciones, faltan los mecanismos de intervención y alerta. Muchas de estas implementaciones de filtros pueden requerir un alto nivel de comprensión de los protocolos de comunicación y su comportamiento, cuando se utilizan por diferentes aplicaciones.

Los dispositivos de filtración de paquetes, casi siempre se mejoran mediante otros tipos dispositivos llamados barreras de protección. Las barreras de protección se llaman así porque operan en las capas superiores del modelo OSI y tienen información completa sobre las funciones de la aplicación en la cual basan sus decisiones. Estos constituyen la mayoría de los firewalls tal cual hoy los conocemos.

Existen varios métodos para construir una barrera de protección. Las organizaciones con talento en la programación y recursos financieros suficientes, en general prefieren usar un método personalizado de barreras de protección para proteger la red de la

organización. Si se ejecuta de manera adecuada, tal vez éste sea el método más eficaz y por supuesto el más costoso.

Otras organizaciones prefieren usar los productos comerciales existentes, así como personalizarlos y configurarlos para cumplir la política de seguridad de red de esas organizaciones.

De aquí en adelante iremos describiendo las distintas arquitecturas con las cuales se puede implementar una barrera de protección para nuestra red

- **De dos bases**

  Es un firewall con dos interfaces de red, que permite asilar una red interna de una red externa no confiable figura 1.2.3.1. Como este firewall no envía ningún tráfico TCP/IP, bloquea por completo cualquier tráfico IP entre las redes no confiables interna y externa.

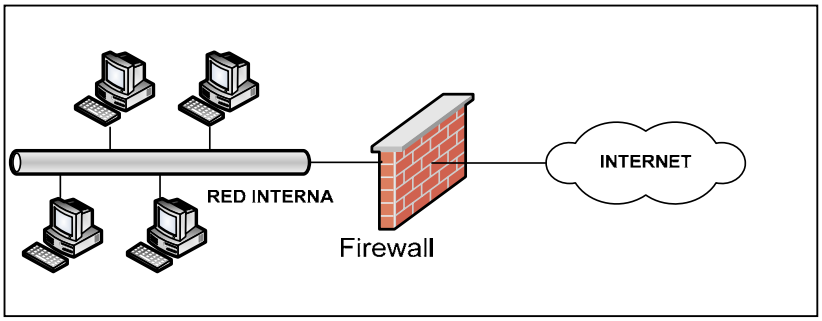


FIGURA 1.2.3.1 FIREWALL DE DOS BASES

Muchos servicios Internet son en esencia de almacenaje y envío. Si estos servicios se ejecutan en el firewall, pueden configurarse para transmitir servicios de aplicación desde una red hacia la otra. Si los datos de aplicación deben cruzar la barrera, es factible configurar los agentes emisores de aplicación para hacer la ejecución en el anfitrión. Estos agentes son programas especiales, utilizados para enviar solicitudes de aplicación entre dos redes conectadas. Otro método es permitir que los usuarios se conecten al firewall de dos bases y después tengan accesos a los servicios externos desde la interfaz de red externa del firewall.

Si se usan los emisores de aplicación, el tráfico de la aplicación no puede cruzar la barrera, a menos que el emisor de aplicación se ejecute y se configure en el servidor de barrera de protección. Esta acción es la implementación de la política “si no está permitido de manera expresa, está prohibido”. Si se autoriza a los usuarios conectarse en forma directa a la barrera de protección, puede comprometerse la seguridad de ésta porque la barrera es el punto central de la conexión entre la red externa y la interna. Por definición, la barrera de este tipo está en zona

de riesgo. Si el usuario selecciona una contraseña débil o compromete su cuenta de usuario (al proporcionar la contraseña), la zona de riesgo quizá se extienda a la red interna y por lo tanto eliminará el objetivo de la barrera.

Si se mantienen registros adecuados de las conexiones de usuarios, es posible rastrear las conexiones no autorizadas a la barrera, en el momento que se descubra una brecha de seguridad. En cambio si se impide que los usuarios se conecten en forma directa a la barrera, cualquier intento de conexión directa se registrará como algo notorio y como una brecha potencial de seguridad.

Este tipo de firewall, con una interfaz mirando a cada red, es la configuración básica usada en las barreras de protección. Los aspectos delicados son que el enrutamiento se encuentra inhabilitado y que la única ruta entre los segmentos de red es a través de una función de capa de aplicación. Si el enrutamiento se ha configurado de manera errónea por accidente (o por diseño) para permanecer activo, se ignorarán las funciones de la capa de aplicación de las barreras de protección.

La mayoría de estas configuraciones están montadas sobre máquinas UNIX. En algunas implementaciones de este sistema operativo, las funciones de enrutamiento se activan de manera predeterminada, por lo cual es importante verificar que dichas funciones están inhabilitadas.

La mayor amenaza ocurre cuando el intruso obtiene el acceso directo de conexión al firewall. La conexión siempre se da mediante una aplicación apoderada del servidor. Las conexiones desde redes externas requieren una autenticación más rigurosa.

Si el usuario obtiene acceso al servidor, la red interna puede ser inválida. Estas invasiones pueden tener cualquiera de las siguientes fuentes:

1. Autorizaciones débiles en el sistema de archivos.
2. Volúmenes montados en NFS en la red interna.
3. Programas de respaldo de red que puedan restituir autorizaciones excesivas.
4. El uso de scripts administrativos que no se hayan asegurado de manera adecuada.

5. Comprensión del sistema a partir de antiguos niveles de revisión del software y notas que no se hayan asegurado de manera adecuada.
6. La instalación de antiguos kernels de sistema operativo que activen el envío IP o la instalación de versiones de antiguos kernels de sistema operativo con problemas de seguridad conocidos.

Si el servidor firewall falla, la red interna no tendrá defensa ante futuros intrusos, a menos que el problema se detecte y corrija con rapidez.

La variable ipforwarding del kernel de UNIX controla el desempeño del enrutamiento IP. Si el intruso obtiene suficiente privilegios del sistema, podrá cambiar el valor de esta variable y habilitar el envío IP, con lo cual se ignorará el mecanismo de la barrera.

- **Firewall como servidor bastión**

  Un firewall es un servidor de barrera de protección que es determinante para la seguridad en la red. Es el servidor central para la seguridad en la red de una organización y, por su función, debe estar en una buena fortaleza. Esto significa que el firewall lo monitorean con detenimiento los administradores de la red. La seguridad del sistema y del software del servidor debe revisarse con regularidad. Asimismo, es preciso observar los registros de acceso en busca de cualquier brecha potencial de seguridad y de un intento de asalto al servidor, figura 1.2.3.2.

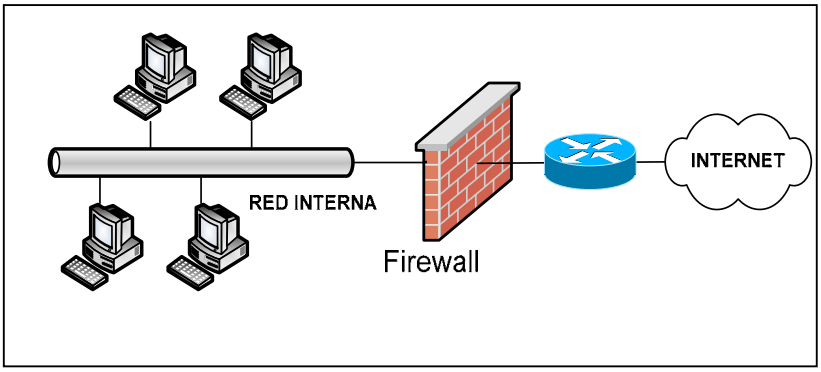


FIGURA 1.2.3.2 FIREWALL COMO SERVIDOR DE BASTION

La configuración antes comentada es un caso especial del firewall. Como los firewalls actúan como un punto de interfaz para una red externa no confiable, casi siempre están sujetos a invasiones. La distribución más simple es aquella en la que el servidor constituye el primer y único punto de entrada para el tráfico de una red externa.

En vista de que el firewall es determinante para la seguridad de la red interna, por lo regular se coloca otra primera línea de defensa entre la red externa no confiable y la red interna. Esta línea casi siempre la proporciona un router de selección. En este esquema el firewall tiene una sola interfaz de red conectada a la red interna y el enrutador de selección tiene dos, una a Internet y la otra a la red interna enrutando todo el tráfico hacia el bastión.

Se debe configurar el router para que envíe primero hacia el firewall todo el tráfico recibido de las redes externas para la red interna. Antes de enviar el tráfico hacia este servidor, el router aplicará sus reglas de filtro en el tráfico del paquete. Sólo el tráfico de red que pase tales reglas será dirigido hacia el firewall; el resto del tráfico será rechazado. Esta arquitectura da un mayor nivel de confianza en la seguridad

de la red. Un intruso necesita penetrar primero en el router de selección y, si lo logra, debe enfrentarse con el firewall.

El firewall utiliza funciones a nivel de aplicación para determinar si las solicitudes hacia y desde la red externa se aceptarán o negarán. Si la solicitud pasa el escrutinio del firewall, se enviará a la red interna para el tráfico de entrada. Para el tráfico de salida (tráfico hacia la red externa), las solicitudes se enviarán al router de selección.

Algunas organizaciones prefieren que su proveedor de acceso a Internet, IAP, proporcione las reglas de los filtros de paquetes para el tráfico en red enviado a la red de dicha organización. El filtro de paquetes aún actúa como la primera línea de defensa, pero se debe confiar al IAP el mantenimiento adecuado de las reglas del filtro de paquetes.

Otro punto a tener en cuenta es la seguridad del router de selección. Sus tablas de enrutamiento deben configurarse para enviar el tráfico externo al firewall. Dichas tablas necesitan estar protegidas contra las invasiones y los cambios no autorizados. Si la entrada a las tablas se

cambia para que el tráfico no se envíe al firewall sino en forma directa a la red conectada localmente, el firewall se ignorará.

Además si el router responde a los mensajes ICMP (protocolo Internet de mensajes de control) de redirección, será vulnerable a los falsos mensajes ICMP que envíe el intruso. Por lo tanto, debe inhabilitarse la respuesta a los mensajes ICMP de redirección. Se deben eliminar los servicios de red innecesarios y utilizar el enrutamiento estático. En especial, asegurarse que los demonios “routed” y “gated” no se encuentren en ejecución; de lo contrario, las rutas serán anunciadas al mundo exterior. Por otro lado, realizar entradas permanentes en la tabla de caché ARP para señalar al firewall.

Entre los servicios a inhabilitar se encuentran: ARP, redirecciones ICMP, ARP apoderado, MOP y mensajes ICMP no alcanzables, TELNET. En una operación ARP normal, las tablas ARP de entrada se construyen de manera dinámica y expiran después de un tiempo determinado. Inicializar en forma manual la tabla cache ARP para el router y el firewall. Las entradas ARP

realizadas en forma manual nunca expiran y actúan como entradas “estáticas”. Con el procesamiento ARP inhabilitado en el router, éste no proporcionará su dirección de hardware.

- **Firewall como servidor de bastión con dos interfaces de red**

  Bajo esta configuración una interfaz está conectada a la red “exterior” y la otra interfaz lo está a la red “interior”. Uno de los puertos del router (el de la primera línea de defensa) está conectado a la red “interior” y el otro lo está a Internet. Nótese que hablamos de red “interior”, “exterior” e Internet; aquí surge el nuevo concepto de red exterior que es la que se ubica entre el firewall y el router figura 1.2.3.3.

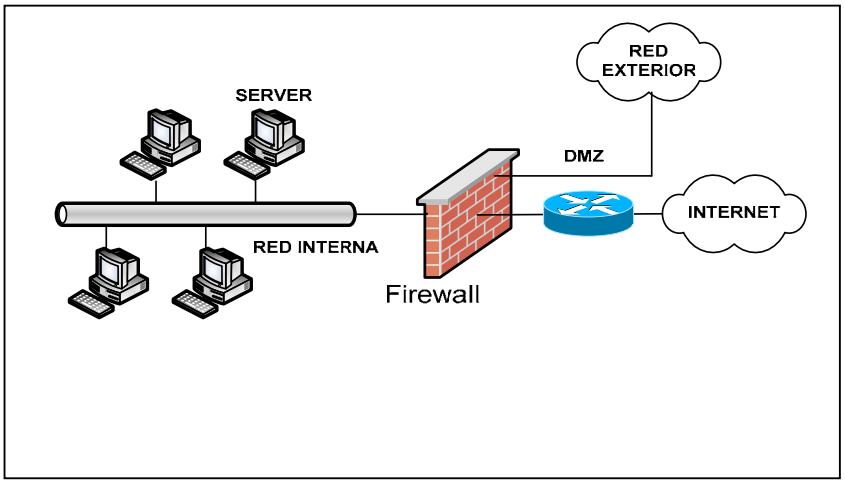


FIGURA 1.2.3.3 FIREWALL COMO SERVIDOR DE BASTION DE DOS INTERFACES

De nuevo el router debe configurarse para enviar todo el tráfico recibido de las redes externas para la red interna hacia la interfaz de red “interior” del bastión. Antes de enviar el tráfico, el router aplicará sus reglas de filtro de paquetes. Sólo el tráfico de red que pase estas reglas se dirigirá hacia el firewall; el resto habrá de rechazarse. Un intruso debe penetrar primero en el router y, si lo logra, se enfrentará al firewall.

No existen servidores en la red exterior más que el router y una de las interfaces de red del firewall. La red exterior forma una zona desmilitarizada DMZ. Ya que la DMZ sólo tiene dos conexiones de red, puede reemplazarla un enlace dedicado punto a punto. Este hecho dificultará más conectarse con este enlace mediante analizadores de protocolos. Si se utiliza una red Ethernet o token ring para la DMZ, una estación de trabajo que coloque su interfaz de red en el modo promiscuo puede capturar el tráfico de la red y tener acceso a los datos delicados. Por lo general, las interfaces de red sólo leen el paquete que se le dirija en forma directa. En el modo promiscuo, sin embargo, dichas interfaces leen todos los paquetes que ve la interfase de

red. Todos los servidores de la organización (excepto el firewall) están conectados a la red interior.

Esta configuración, tiene otra ventaja sobre esa configuración de red en la cual sólo se empleaba una interfase de red del firewall. Esta ventaja es que el firewall no se puede ignorar al atacar las tablas de enrutamiento de los routers. El tráfico de la red debe pasar por este firewall para llegar a la red interior.

- **Dos firewalls y dos DMZ**

  En este caso ambas interfaces de los firewalls se encuentran configuradas. Tres zonas de red están formadas en la red interna: la red exterior, la red privada y la red interior figura 1.2.3.4.

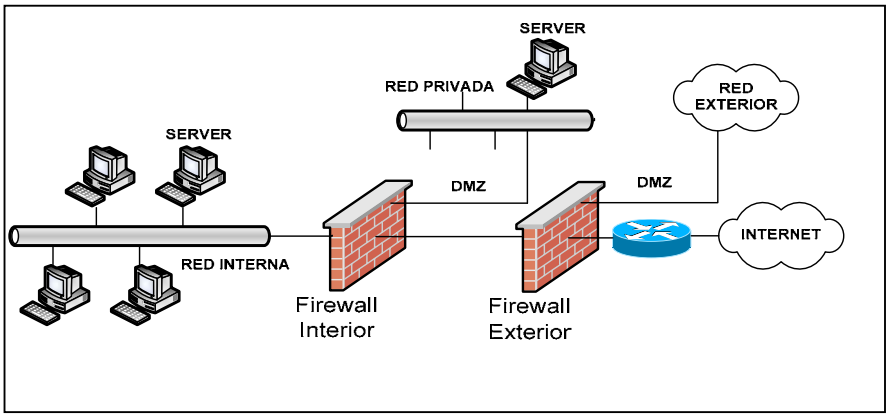


FIGURA 1.2.3.4 DOS FIREWALLS Y DOS DMZ

Existe una red privada entre los firewalls interior y exterior. Una organización puede colocar algunos servidores en la red privada y mantener los más delicados detrás del firewall interior. Por otra parte, una organización quizá desee una seguridad máxima y usar la red privada como una segunda zona de buffer o DMZ interior, además de mantener todos los servidores en la red interior.

Si una empresa quiere proporcionar acceso completo a una gran variedad de servicios, como FTP anónimo (protocolo de transferencia de archivos), Gopher y WWW (World Wide Web), puede proveer ciertos servidores de sacrificio en la DMZ exterior. Los firewalls no deben confiar en ningún tráfico generado desde estos servidores de sacrificio.

El router de selección debe estar configurado para enviar todo el tráfico recibido desde las redes externas para la red interna hacia el firewall interior. Antes de mandar el tráfico, el router aplicará las reglas de filtro de paquetes. Sólo el tráfico de la red que pasa esas reglas se dirigirá al firewall exterior; el resto será rechazado. Un intruso debe penetrar primero el router y, si lo hace, se enfrentará al firewall exterior.

Sin que le importe violar las defensas de la red exterior, el intruso penetra en el firewall interior. Por ello, si los recursos lo permiten, tal vez se desee dar a cada firewall la responsabilidad de un grupo administrativo diferente. Esto asegura que los errores de un grupo de administradores no los repitan los demás administradores. También se debe garantizar que los dos grupos compartan información acerca de debilidades descubiertas en los firewalls.

Otro tipo de configuración de red , se obtiene al utilizar dos firewalls, pero sólo una interfaz de red de cada anfitrión. Un segundo router llamado el ”ahogador” se agrega entre la DMZ y las redes interiores. Se debe asegurar que los firewalls no se ignoren y que los routers usen rutas estáticas.

A partir de estos elementos, firewalls con una o dos interfaces de red y routers, se pueden lograr diferentes configuraciones que surgen de la combinación de ellos. Cuando sólo esté en uso una interfaz de red del firewall, se deben utilizar rutas estáticas en los routers y configurar bien las entradas de las tablas de enrutamiento para asegurar que los firewalls no se ignoren.

1.2.4 COMPONENTES DEL FIREWALL

Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos:

- Ruteador Filtra-paquetes.
- Gateway a Nivel-aplicación.
- Gateway a Nivel-circuito.

1.2.4.1 EDIFICANDO OBSTACULOS: RUTEADOR FILTRA-PAQUETES

Este ruteador figura 1.2.4.1, toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interfase de entrada del

paquete, y la interfase de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

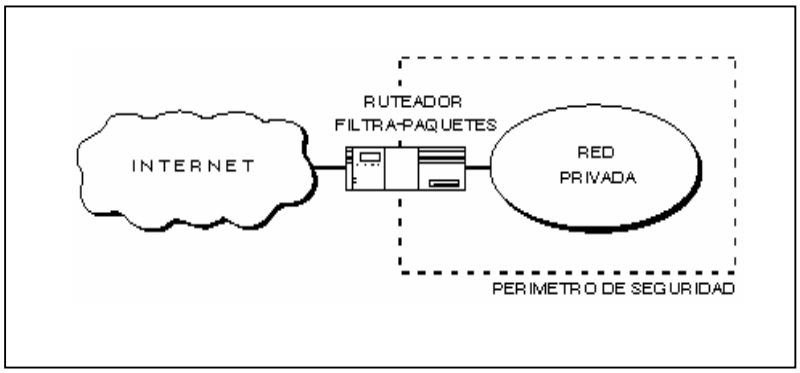


FIGURA 1.2.4.1 RUTEADOR FILTRA-PAQUETES

Servicio dependiente del filtrado

Las reglas acerca del filtrado de paquetes a través de un ruteador para rehusar/permitir el tráfico esta basado en un servicio especifico, desde entonces muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet esta a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMTP espera las conexiones de entrada en el puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el ruteador simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado numero de servidores internos, el ruteador podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 *y* que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfeccionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el trafico UDP.

Servicio independiente del filtrado

Este tipo de ataques ciertamente son difíciles de identificar usando la información básica de los encabezados debido a que estos son independientes al tipo de servicio. Los ruteadores pueden ser configurados para protegerse de este tipo de ataques pero son mas difíciles de especificar desde entonces las reglas para el filtrado requieren de información adicional que pueda ser estudiada y examinada por la tabla de ruteo, inspeccionando las opciones especificas IP, revisando fragmentos especiales de edición, etc. Algunos ejemplos de este tipo de ataques incluye:

Agresiones originadas por el direccionamiento IP.

Para este tipo de ataque, el intruso trasmite paquetes desde afuera pretendiendo pasar como servidor interno, los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema. El agresor espera que usando este impostor se pueda penetrar al sistema para emplearlo seguramente como dirección fuente donde los paquetes que trasmita sean autentificados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente

“interno” si el paquete arriba en una de las interfaces del ruteador “externo”.

Agresiones originadas en el ruteador.

En un ataque de ruteo, la estación de origen especifica la ruta que un paquete deberá de tomar cuando cruce a través del Internet. Este tipo de ataques son diseñados para cuantificar las derivaciones de seguridad y encauzan al paquete por un inesperado camino a su destino. Los ataques originados en el ruteador pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de ruteo opcionales.

Agresiones por fragmentación.

Por este tipo de ataques, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a separarse en paquetes. Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado de un ruteador examinando los primeros fragmentos y el resto pasa sin ser visto. Aunque si bien únicamente es explotado por sencillos decodificadores, una agresión pequeñísima puede ser frustrada si se descartan todos los paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

Beneficios del ruteador filtra-paquetes

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no, el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el tráfico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software específico que tenga que ser instalado en cada uno de los servidores.

Limitaciones del ruteador filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el

conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo mas difícil su administración y comprensión. Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Cualquier paquete que pasa directamente a través de un ruteador puede ser posiblemente usado como parte inicial un ataque dirigido de datos. Haciendo memoria este tipo de ataques ocurren cuando los datos aparentemente inocuos se desplazan por el ruteador a un servidor interno. Los datos contienen instrucciones ocultas que pueden causar que el servidor modifique su control de acceso y seguridad relacionando sus archivos facilitando al intruso el acceso al sistema.

Generalmente, los paquetes entorno al ruteador disminuyen conforme el numero de filtros utilizados se incrementa. Los ruteadores son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interfase apropiada de la transmisión. Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada

paquete, pero también sucede aun aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el tráfico. Un ruteador Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto/dato del servicio. Por ejemplo, un administrador de red necesita filtrar el tráfico de una capa de aplicación - limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateways a Nivel-aplicación.

1.2.4.2 GATEWAYS A NIVEL-APLICACION

Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de propósito-especial (un servicio

Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

Aun cuando, el código Proxy puede ser configurado para soportar únicamente las características especificas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras.

Un aumento de seguridad de este tipo incrementa nuestros costos en términos del tipo de gateway seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el gateway, y un decrecimiento en el nivel de los servicios que podrán obtener nuestros usuarios, dando como resultado un sistema carente de transparencia en el manejo de los usuarios en un ambiente “amigable”. Como en todos los casos el administrador de redes debe de balancear las necesidades propias en seguridad de la organización con la demanda de “fácil de usar” demandado por la comunidad de usuarios.

Es importante notar que los usuarios tienen acceso por un servidor Proxy, pero ellos jamás podrán seccionar en el Gateway a nivel-aplicación. Si se permite a los usuarios seccionar en el sistema de

firewall, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema.

Por ejemplo, el intruso podría obtener el acceso de root, instalar un caballo de troya para colectar las contraseñas, y modificar la configuración de los archivos de seguridad en el filrewall.

Servidor de defensa

Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el Gateway a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos.

Un Gateway a nivel-aplicación por lo regular es descrito como un “servidor de defensa” porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque. Hay

varias características de diseño que son usadas para hacer mas seguro un servidor de defensa:

La plataforma de Hardware del servidor de defensa ejecuta una versión “segura” de su sistema operativo. Por ejemplo, si el servidor de defensa es una plataforma UNIX, se ejecutara una versión segura del sistema operativo UNIX que es diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del firewall.

Únicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor.

El servidor de defensa podrá requerir de una autenticación adicional para que el usuario accese a los servicios Proxy. Por ejemplo, el servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización (tal como la tecnología “una-sola vez” de contraseña donde una tarjeta inteligente generaba un código de acceso único por medios criptográficos).

Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión.

Cada Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.

Cada Proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.

La figura 1.2.4.2 ilustra la operación de un Telnet Proxy en un servidor de defensa. Para este ejemplo, un cliente externo ejecuta una sesión Telnet hacia un servidor integrado dentro del sistema de seguridad por el Gateway a nivel-aplicación.

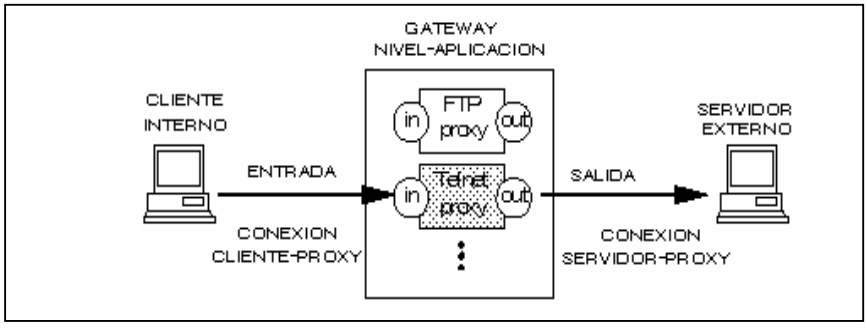


FIGURA 1.2.4.2 TELNET PROXY

El Telnet Proxy nunca permite al usuario remoto que se registre o tenga acceso directo al servidor interno. El cliente externo ejecuta un telnet al servidor de defensa donde es autorizado por la tecnología “una-sola vez” de contraseña. Después de ser autentificado, el cliente obtiene acceso a la interfase de usuario del Telnet Proxy. Este únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores son disponibles para el acceso vía Telnet.

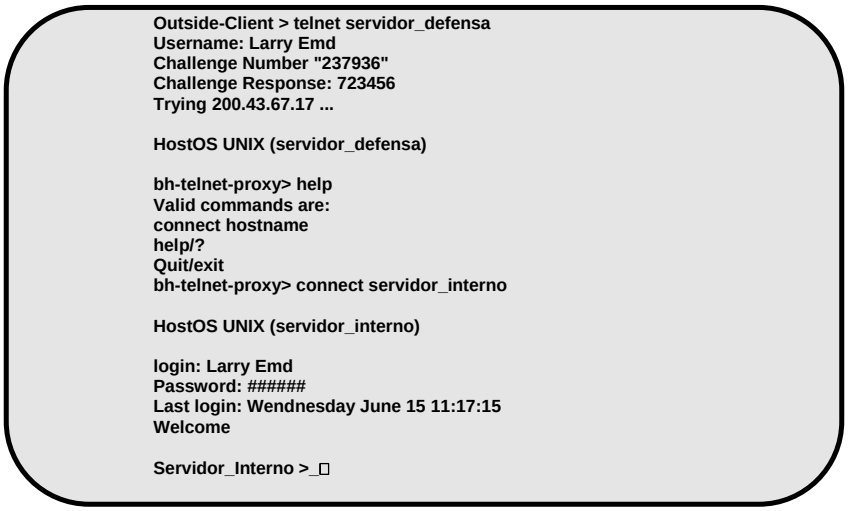


FIGURA 1.2.4.3 CONEXION CLIENTE SERVIDOR

Los usuarios externos especifican el servidor de destino y el Telnet Proxy una vez hecha la conexión, los comandos internos son desplazados hacia el cliente externo. El cliente externo cree que el Telnet Proxy es el servidor interno real, mientras el servidor interno cree que el Telnet proxy es un cliente externo.

El figura 1.2.4.3 muestra la salida en pantalla de la Terminal de un cliente externo como la “conexión” al servidor interno una vez establecida. Nótese que el cliente no se esta registrando al servidor de defensa - el usuario comienza su sesión autentificándose por el servidor de defensa e intercambia respuestas, una vez que se le ha permitido seccionar se comunica con el Telnet Proxy. Después de pasar el intercambio de respuestas, el servidor Proxy limita un conjunto de comandos y destinos que están disponibles para los clientes externos.

La autenticación puede basarse en “algo conocido por los usuarios” (como una contraseña) o “algo que tengan” que posean físicamente (como una tarjeta electrónica) cualquiera de las dos. Ambas técnicas están sujetas a plagio, pero usando una combinación de ambos métodos se incrementa la probabilidad del uso correcto de la autenticación. En el ejemplo de Telnet, el Proxy transmite un requerimiento de registro y el usuario, con la ayuda de su tarjeta electrónica, obtendrá una respuesta de validación por un número. Típicamente, se le entrega al usuario su tarjeta desactivada para que el introduzca un PIN y se le regresa la tarjeta, basada en parte como llave “secreta” de encriptación y con un reloj interno propio, una vez que se establece la sesión se obtiene un valor de respuesta encriptado.

Beneficios del gateway a nivel-aplicación

Son muchos los beneficios desplegados en un gateway a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede acceder a los servicios. Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado. Los gateways a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para un gateway de este tipo son mucho mas fáciles de configurar y probar que en un ruteador filtra-paquetes.

Limitaciones del gateway a nivel-aplicación

Probablemente una de las grandes limitaciones de un gateway a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accede a los servicios proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel-aplicación demanda modificar la conducta del usuario desde el momento en que se

requiere de dos pasos para hacer una conexión mejor que un paso. Como siempre, el software especializado podrá ser instalado en un sistema terminado para hacer las aplicaciones del gateway transparentes al permitir a los usuarios especificar el servidor de destino, mejor que el propio, en un comando de telnet.

1.2.4.3 EDIFICANDO OBSTACULOS: GATEWAY A NIVEL-CIRCUITO

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

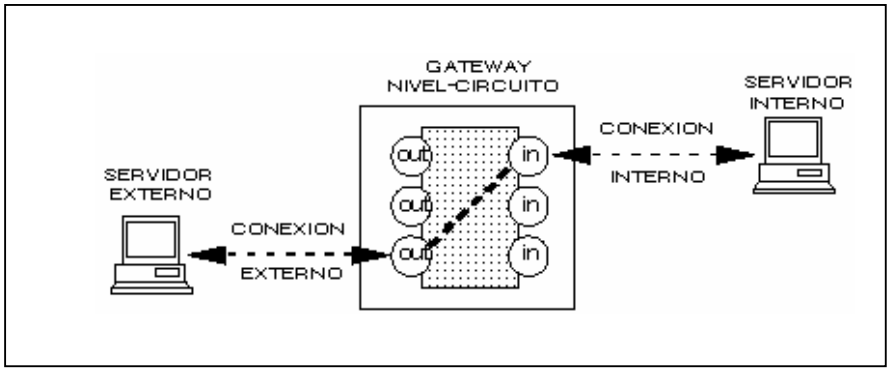


FIGURA 1.2.4.4 GATEWAY A NIVEL-CIRCUITO

La figura 1.2.4.4 muestra la operación de una conexión típica Telnet a través de un gateway a nivel-circuito. Tal como se mencionó anteriormente, este gateway simplemente transmite la

conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito acciona como un cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar el encubrir la información sobre la protección de la red.

El gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un gateway “híbrido” soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización.

1.2.5 VENTAJAS Y DESVENTAJAS

1.2.5.1 VENTAJAS

Los firewalls administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un embudo, manteniendo al margen los usuarios no-autorizados (tal, como, hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es “si” pero “cuando” ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

La figura 1.2.5.1 ilustra las ventajas de un sistema firewall de seguridad.

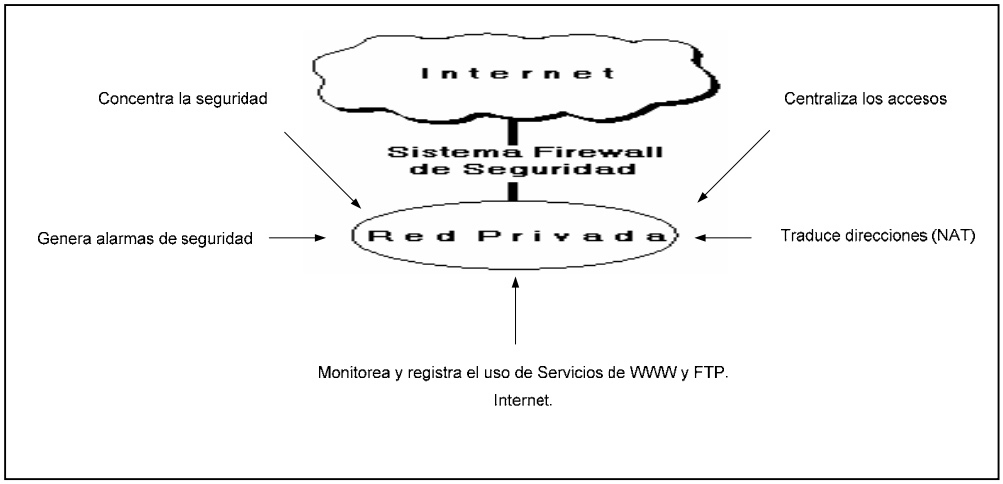


FIGURA 1.2.5.1 VENTAJAS DEL FIREWALL

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del proveedor de servicios de Internet (ISPs).

Un firewall es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando únicamente el acceso al Internet esta perdido.

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significan dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

1.2.5.2 DESVENTAJAS

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo como se ilustra en la figura 1.2.5.2, si existe una conexión dial-up sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen “irritarse” cuando se requiere una autenticación adicional requerida por un firewall

proxy server (FPS) lo cual puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar concientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.

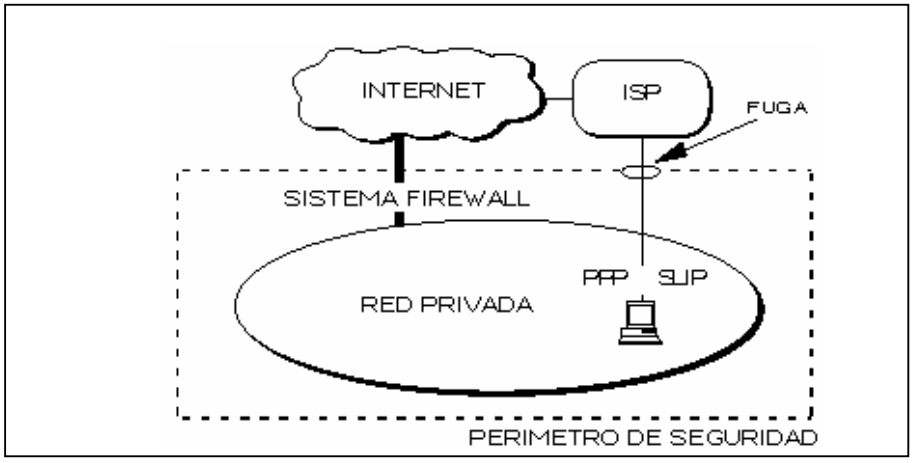


FIGURA 1.2.5.2 CONEXION CIRCUNVECINA AL FIREWALL DE INTERNET

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien

datos sensitivos en medios magnéticos y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la “Ingeniería Social”, por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso “temporal” a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución real esta en que la organización debe ser consciente en instalar software anti-viral en cada despacho para protegerse de los virus que llegan por medio de disquettes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo más fácil el acceso de un intruso al sistema.

Como nosotros podemos ver, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

1.3 CONCEPTO DE VPN

1.3.1 CONCEPTO DE VPN

Es una red privada que se extiende, mediante un proceso de encapsulación y de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Los paquetes de datos figura 1.3.1.1 de la red privada viajan por medio de un “túnel” definido en la red pública.

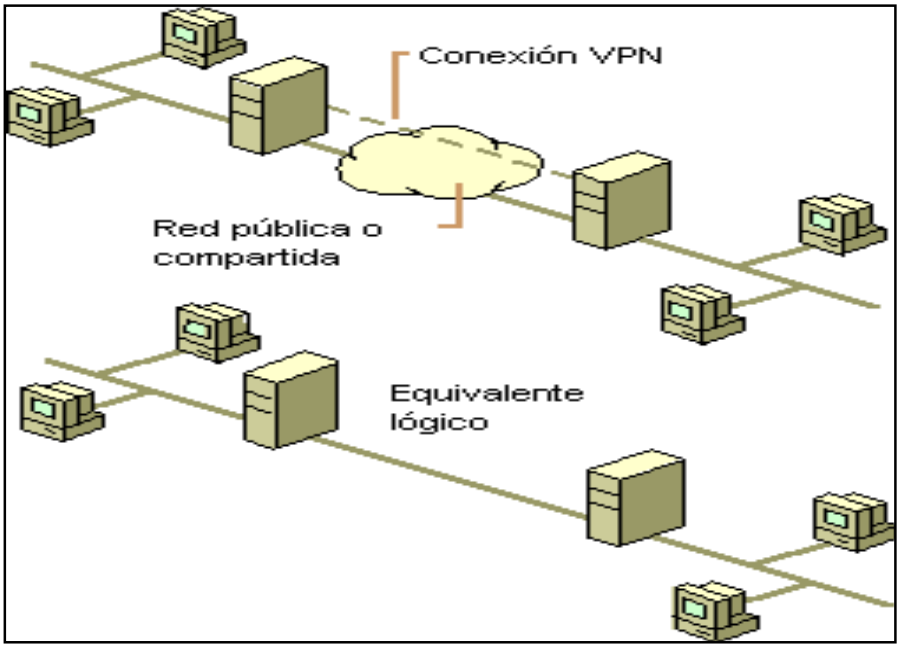


FIGURA 1.3.1.1 ESQUEMA DE UNA VPN

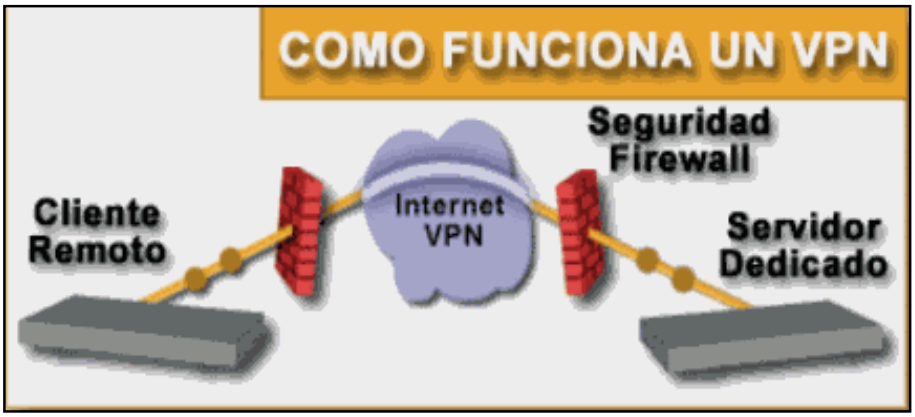


FIGURA1.3.1.2 DATOS A TRAVES DE UNA VPN

La figura 1.3.1.2 muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando al firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a la nube de internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar oficinas corporativas figura 1.3.1.3 con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como internet, IP, Ipsec, Frame Relay, ATM.

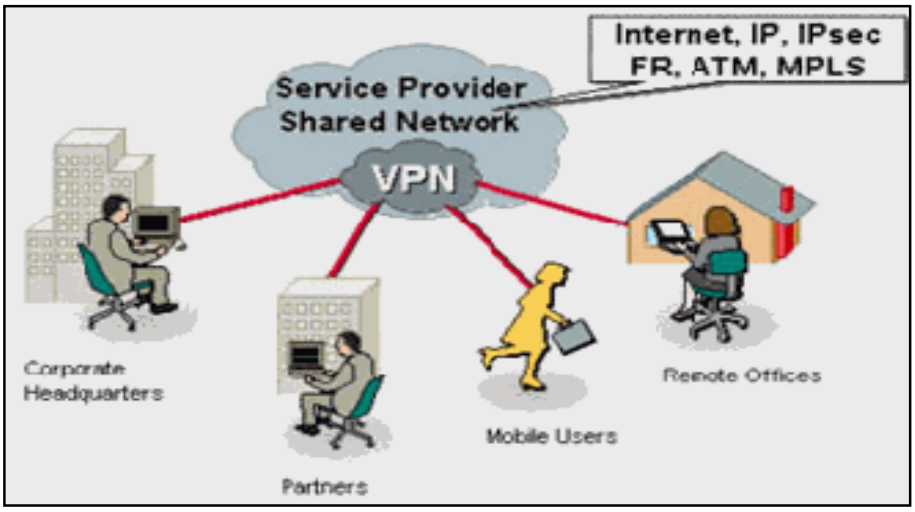


FIGURA 1.3.1.3 CONEXION CON OFICINAS CORPORATIVAS

Las redes privadas virtuales crean un túnel figura 1.3.1.4, o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

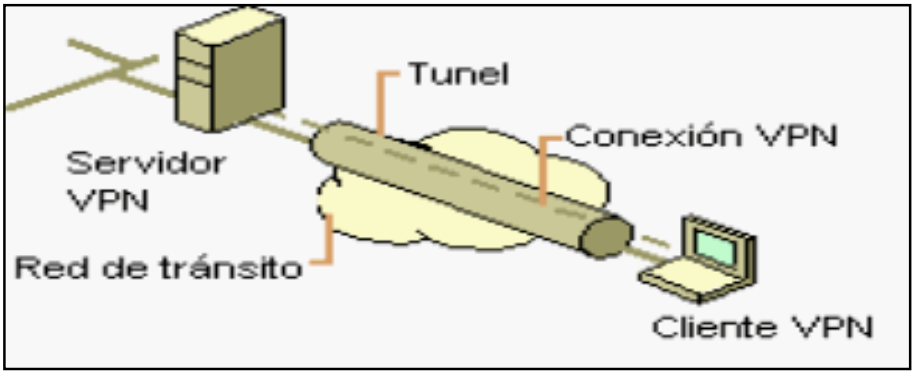


FIGURA1.3.1.4 TUNEL CONEXION VPN

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de tránsito se envían los datos sin problemas.

1.3.2 CLASES DE VPN

1.3.2.1 INTRANET

Son conexiones seguras entre segmentos de una misma compañía. Basadas en la tecnología de Internet, las intranets, han llegado a ser una parte esencial de los sistemas de información corporativos de hoy en día.

1.3.2.2 EXTRANET

Son construidas para manejar comunicación segura entre compañías y sus socios estratégicos, clientes y proveedores. Tienen control de tráfico para prevenir el bloqueo de redes a través de sus puntos de acceso. Manejan rápida entrega y respuesta en tiempos para datos críticos

1.3.2.3 ACCESO REMOTO

Comunicación remota con usuarios móviles.

Cuando se diseña un acceso remoto VPN se obtiene:

Autenticación fuerte para verificar usuarios remotos y móviles.

Administración centralizada.

1.3.3 IMPLEMENTACION DE VPN

Por lo general cuando se desea implementar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

Identificación de usuario

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet(IP), el intercambio de paquete de internet(IPX) entre otros.

1.3.3.1 HERRAMIENTAS DE UNA VPN

- VPN Gateway
- Software
- Firewall
- Router

VPN Gateway

Dispositivos con un software y hardware especial para proveer de capacidad a la VPN

Software

Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

1.4 PROTOCOLOS DE SEGURIDAD Y MONITOREO

1.4.1 PROTOCOLO IKE

Internet Key Exchange (IKE).

El protocolo IKE no es parte de IPSec, es una alternativa para crear las Asociaciones de Seguridad de forma dinámica, está definido en el RFC 2409. IKE es un protocolo híbrido basado en el marco definido por el Protocolo de manejo de llaves y asociaciones de seguridad de Internet (Internet Security Association and Key Management protocol, ISAKMP) definido en el RFC2408, y otros dos protocolos de manejo de llaves Oakley y SKEME. Las implementaciones de IPSec están forzadas a soportar el manejo manual y solo algunas de ellas consideran IKE, que ha resultado demasiado complejo e inapropiado.

1.4.2 PROTOCOLO IPSEC

IPSec (Internet Protocol Security) es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.

La arquitectura de IPSec.

La arquitectura de IPSec define la granularidad con la que el usuario puede especificar su política de seguridad. Permite que cierto tráfico sea identificado para recibir el nivel de protección deseado (Figura 1.4.2.1)

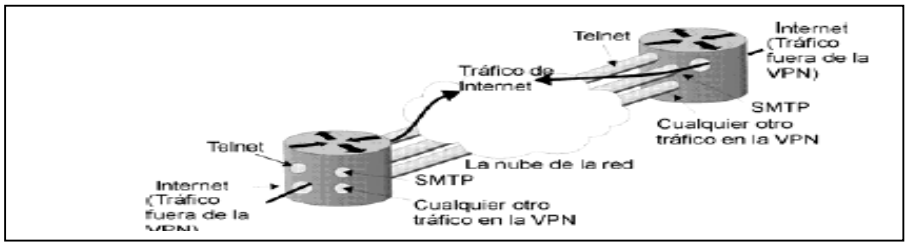


FIGURA 1.4.2.1 TUNELES DE COMUNICACION PROTEGIDOS POR IPSEC ENTRE REDES SEPARADAS.

IPSec está diseñado para proveer seguridad interoperable de alta calidad basada en criptografía, tanto para IPv4 como para IPv6. Está compuesto por dos protocolos de seguridad de tráfico, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), además de protocolos y procedimientos para el manejo de llaves encriptadas. AH provee la prueba de los datos de origen en los paquetes recibidos, la integridad de los datos, y la protección contra-respuesta. ESP provee lo mismo que AH adicionando confidencialidad de datos y de flujo de tráfico limitado.

En la figura 1.4.2.2, se aprecia la arquitectura de IPSec. Al utilizar el mecanismo de AH se aplican algoritmos de autenticación, con la aplicación del mecanismo ESP, además de autenticación, también algoritmos de encriptación. El esquema de interoperabilidad se maneja a través de Asociaciones de Seguridad (SA), almacenadas

en una base de datos. Los parámetros que se negocian para establecer los canales seguros se denominan Dominio de Interpretación IPSec (Domain of Interpretation, DOI), bajo políticas pre-establecidas dentro de un esquema de funcionamiento estático con valores fijos y previamente establecidos, o bien, en un esquema de funcionamiento dinámico utilizando un protocolo de manejo de llaves, Interchange Key Exchange (IKE).

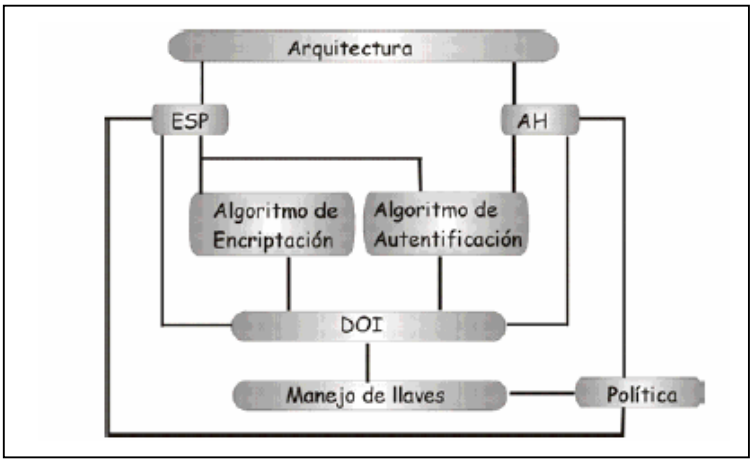


FIGURA 1.4.2.2 ARQUITECTURA DE IPSEC.

Modos de funcionamiento de IPSec.

El diseño de IPSec plantea dos modos de funcionamiento para sus protocolos: transporte y túnel, la diferencia radica en la unidad que se esté protegiendo, en modo transporte se protege la carga útil IP (capa de transporte), en modo túnel se protegen paquetes IP (capa de red) y se pueden implementar tres combinaciones: AH en

modo transporte, ESP en modo transporte, ESP en modo túnel (AH en modo túnel tiene el mismo efecto que en modo transporte).

El modo transporte se aplica a nivel de hosts. AH y ESP en este modo interceptarán los paquetes procedentes de la capa de transporte a la capa de red y aplicarán la seguridad que haya sido configurada. En la figura 1.4.2.3, se aprecia un esquema de IPSec en modo transporte, si la política de seguridad define que los paquetes deben ser encriptados, se utiliza ESP en modo transporte, en caso que solo haya sido requerida autenticación, se utiliza AH en modo transporte.

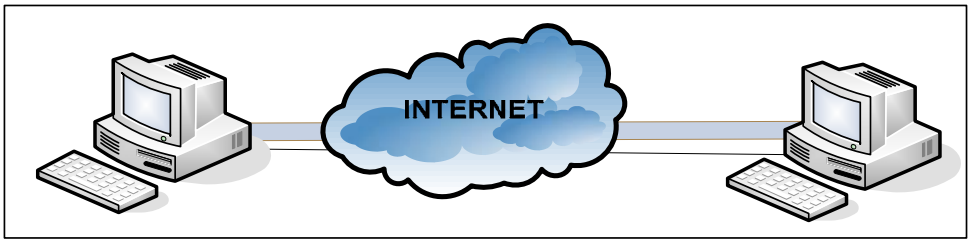


FIGURA 1.4.2.3. HOSTS A Y B IMPLEMENTANDO ESP EN MODO TRANSPORTE.

Los paquetes de la capa de transporte como TCP y UDP pasan a la capa de red, que agrega el encabezado IP y pasa a las capas inferiores; cuando se habilita IPSec en modo transporte, los paquetes de la capa de transporte pasan al componente de IPSec (que es implementado como parte de la capa de red, en el caso de sistemas operativos), el componente de IPSec agrega los

encabezados AH y/o ESP, y la capa de red agrega su encabezado IP. En el caso que se apliquen ambos protocolos, primero debe aplicarse la cabecera de ESP y después de AH, para que la integridad de datos se aplique a la carga útil de ESP que contiene la carga útil de la capa de transporte, esto se ilustra en la figura 1.4.2.4.

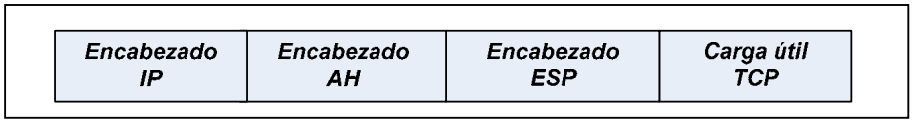


FIGURA 1.4.2.4 FORMATO DEL PAQUETE CON AH Y ESP.

El modo túnel se utiliza cuando la seguridad es aplicada por un dispositivo diferente al generador de los paquetes, como el caso de las VPN, o bien, cuando el paquete necesita ser asegurado hacia un punto seguro como destino y es diferente al destino final, como se ilustra en la figura 1.4.2.5, el flujo de tráfico es entre A y B, e IPSec puede aplicarse con una asociación de seguridad entre RA y RB, o bien, una asociación de seguridad entre A y RB.

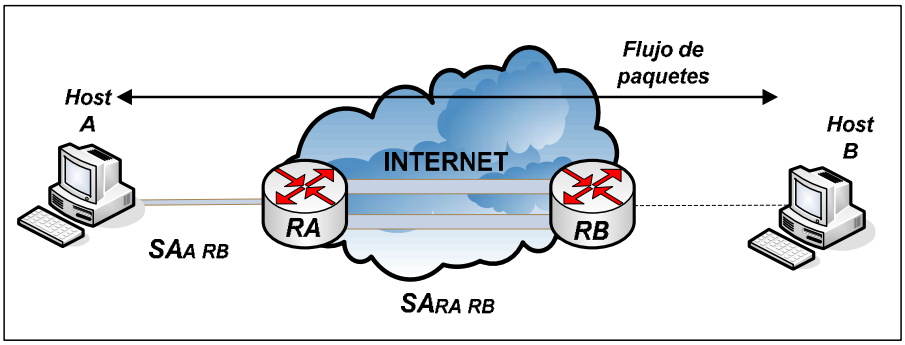


FIGURA 1.4.2.5 APLICACIÓN DE IPSEC EN MODO TÚNEL.

IPSec en modo túnel, tiene dos encabezados IP, interior y exterior. El encabezado interior es creado por el host y el encabezado exterior es agregado por el dispositivo que está proporcionando los servicios de seguridad. IPSec encapsula el paquete IP con los encabezados de IPSec y agrega un encabezado exterior de IP como se ilustra en la figura 1.4.2.6.

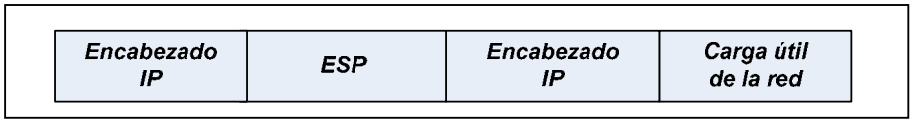


FIGURA 1.4.2.6 FORMATO DEL PAQUETE APLICANDO IPSECEN MODO TÚNEL.

IPSec también soporta túneles anidados, aunque no son recomendados por lo complicado de su construcción, mantenimiento y consumo de recursos de red. La figura 1.4.2.7, muestra dos túneles, A envía un paquete a B, la política indica que debe ser autenticado con el router RB, además existe una VPN entre RA y RB, de tal forma que el paquete que ve RB es el que se muestra en la figura 1.4.2.8, el encabezado exterior es un paquete ESP entunelado y contiene un paquete AH entunelado, el paquete AH contiene el paquete IP para el host B generado por el host A.

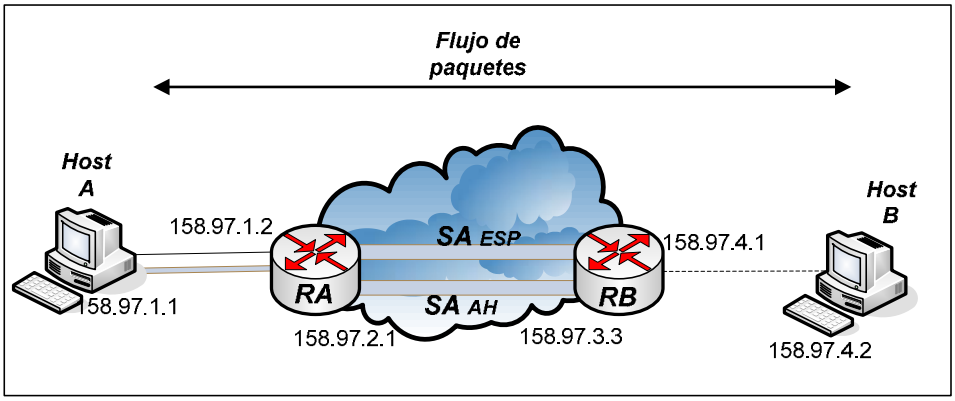


FIGURA 1.4.2.7 EJEMPLO DE TUNELES ANIDADOS.

Encabezado IP	ESP	Encabezado IP	AH	Encabezado IP	Datos
Fuente: 158.97.2.1		*Fuente: 158.97.1.1*		*Fuente: 158.97.1.1*	
Destino: 158.97.3.3		*Destino: 158.97.3.3*		*Destino: 158.97.4.2*	

FIGURA 1.4.2.8 FORMATO DEL PAQUETE DEL TUNEL ANIDADO.

Asociaciones de seguridad.

Una asociación de seguridad (SA) es la forma básica de IPSec, es el contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los protocolos a utilizar, las transformaciones, las llaves y la duración de validez de dichas llaves. Las SA son almacenadas en una base de datos (SADB), son de un solo sentido, es decir, cada entidad con IPSec tiene una SA para el tráfico que entra, y otra SA para el tráfico que sale.

Además de ser unidireccionales, también son específicas al protocolo, hay SA separadas para AH y para ESP.

Indice de parámetros de seguridad (Security Parameter Index, SPI).

El SPI es una entidad de 32 bits que identifica de manera única una SA. Es el mecanismo concebido para que en una comunicación segura, la fuente identifique cual SA utilizar para asegurar un paquete por enviar, y el destino identifique cual SA utilizar para verificar la seguridad del paquete recibido. El SPI se incluye en los encabezados ESP y AH, el destino utiliza la dupla <spi, dst protocol> para identificar de forma única la SA.

Gestión de las SA.

Para el manejo de SA se establecen dos tareas: creación y borrado; estas actividades pueden ser manuales o a través del protocolo de manejo de llaves (IKE).

La creación es un proceso de dos etapas: 1) negociación de parámetros de la SA, 2) actualización de la SADB. El manejo manual de llaves es obligatorio en toda implementación, el

proceso de definición de SPI y parámetros es totalmente manual, y permanecerán hasta que sean manualmente borrados. En el manejo dinámico de llaves, se utiliza un protocolo en Internet llamado IKE. El kernel con IPSec habilitado, invoca IKE si se trata de una comunicación segura y no encuentra una SA. IKE negocia la SA con el destino o con el siguiente salto (host o router), dependiendo de la política y crea la SA en la SADB.

Igualmente las SA pueden ser borradas manualmente o con IKE, los criterios de borrado pueden ser: tiempo de vida expirado, llaves comprometidas, solicitud explícita para borrarse, o el número de bytes utilizado excede un umbral especificado en la política.

Parámetros.

Los parámetros por negociar en una SA, tanto para AH como para ESP son los siguientes:

Número de secuencia: Un campo de 32 bits utilizado en el procesamiento de paquetes de salida, es parte de los encabezados de AH y/o ESP, su valor inicial es 0, se incrementa en uno cada vez que la SA es utilizada, se utiliza para detectar ataques del tipo “replay”.

Sobreflujo del número de secuencia: Campo utilizado en el procesamiento de paquetes de salida y se establece cuando hay sobreflujo del campo de número de secuencia. La política determina qué hacer si este campo está activado.

Ventana de antireply: Campo utilizado en el procesamiento de paquetes de entrada. Se activa si IPSec detecta paquetes retransmitidos por hosts sospechosos.

Tiempo de vida: El tiempo de validez de una SA, se especifica en términos de bytes asegurados con la SA, no se recomienda enviar más de 4Gb de paquetes utilizando la misma SA. Para evitar la pérdida de la conexión segura, se manejan dos límites, soft y hard. Al llegar al límite soft el kernel es notificado para que inicie una nueva negociación antes del límite hard que es cuando la SA expira.

Modo: Los valores son: túnel, transporte o indistinto. Si el valor es indistinto la SA puede ser utilizada para modo túnel o modo transporte.

Destino del túnel: Campo utilizado para el modo túnel, indica la dirección IP de destino del encabezado exterior.

Parámetros PMTU: IPSec no fragmenta o reensambla paquetes, sin embargo, agrega un encabezado IPSec y por lo tanto impacta

la longitud del PMTU. IPSec debe participar en la determinación del PMTU (Protocol Maximum Transfer Unit), una SA mantiene dos valores: el PMTU y el campo de edad.

Políticas de seguridad en IPSec.

La política es uno de los componentes más importantes de la arquitectura de IPSec, determina los servicios de seguridad que serán aplicados a un paquete. Las políticas de seguridad son también almacenadas en una base de datos (Security Policy Database, SPD) indexada por seleccionadores.

La SPD es consultada tanto para el procesamiento de salida como el de entrada, se propone un administrador de la SPD para agregar, borrar y modificar; no hay un estándar que lo defina, pero se propone que los seleccionadores contengan los siguientes campos:

Dirección fuente: Puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica. Indistinta en el caso de que sea la misma política para todos los paquetes con un mismo host de origen, el rango de direcciones y prefijo de red, para los gateways de seguridad y para VPNs, la dirección

específica para un host con varias direcciones, o en un gateway cuando los requerimientos de algún host sean específicos.

Dirección destino: Puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica (homologada o no). Los tres primeros para gateways de seguridad, la dirección específica como índice para la SPD.

Nombre: Nombre de un usuario o sistema sobre el cual se aplique la política de forma específica.

Protocolo: El protocolo de transporte.

Puertos de capas superiores: Los puertos fuente y destino sobre los que se aplica la política.

IP Encapsulating Security Payload (ESP).

ESP es un encabezado de protocolo insertado en el datagrama IP para proveer servicios de confidencialidad, autenticación del origen de los datos, antireplay e integridad de datos a IP. Es un estándar definido en el RFC 2406. El encabezado ESP se inserta después del encabezado IP y antes del encabezado del protocolo

de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel).

El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado ESP contendrá el valor 50 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6).

El formato de los paquetes ESP para una SA dada es fijo durante la duración de la SA. El encabezado ESP tiene la forma definida en la figura 1.4.2.9, el SPI y número de secuencia fueron definidos antes, la carga útil de datos son los datos protegidos, el relleno (de hasta 255 bytes) se utiliza en ESP por varias circunstancias: Algunos algoritmos criptográficos requieren que el elemento de entrada sea un múltiplo del tamaño de su bloque, si no se especifica confidencialidad en la SA, se utiliza el relleno para justificar los campos *longitud de relleno* y s*iguiente cabecera* del encabezado ESP, para esconder el tamaño real de la carga útil; el contenido del relleno es dependiente del algoritmo de criptografía, el algoritmo puede definir un valor de relleno que debe ser verificado por el receptor para el proceso de desencriptado. El campo de longitud de relleno define cuánto relleno se agregó, el campo de siguiente cabecera indica el tipo de dato contenido en la

carga útil de acuerdo al conjunto de números de Protocolo IP definidos por IANA (Internet Assigned Numbers Authority). El campo de datos de autenticación contiene el valor de verificación de integridad calculado sobre el paquete ESP menos los datos de autenticación.

ESP aplicado en modo transporte solo se utiliza en implementaciones del tipo host y provee protección a los protocolos de capas superiores, pero no al encabezado IP.

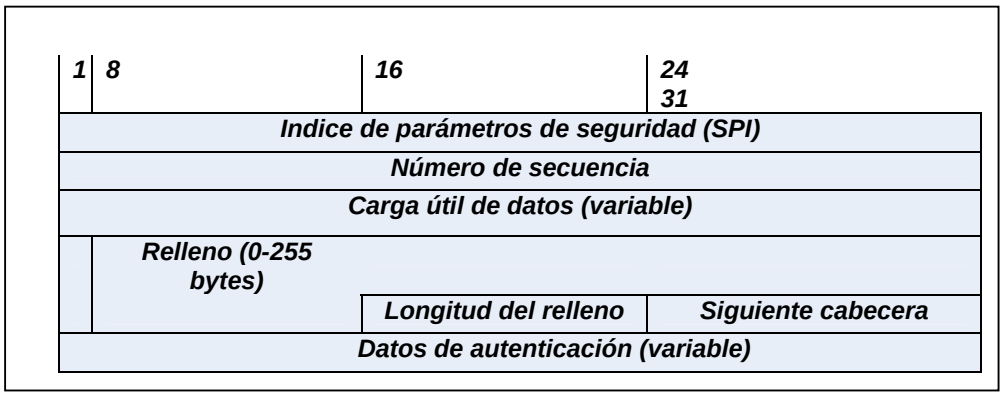


FIGURA 1.4.2.9. EL ENCABEZADO ESP.

El encabezado ESP se inserta después del encabezado IP y antes del protocolo superior (TCP, UDP, ICMP, etc.) o antes de cualquier encabezado IP que haya sido previamente insertado. En la figura 1.4.2.10, se ilustra la transformación del paquete IP al aplicar ESP en modo transporte para IPv4; en la figura 1.4.2.11, se muestra el caso para IPv6.

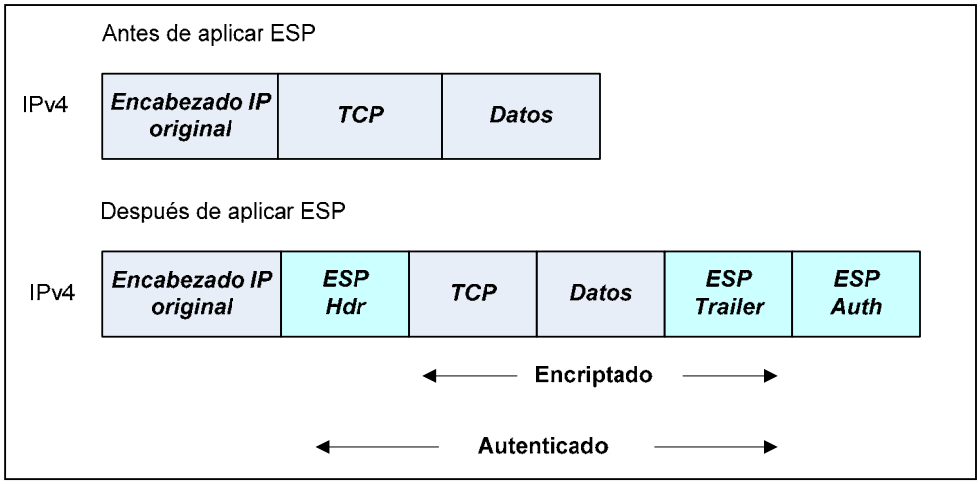


FIGURA 1.4.2.10 TRANSFORMACION DEL PAQUETE IPV4 AL APLICAR ESP EN MODO TRANSPORTE.

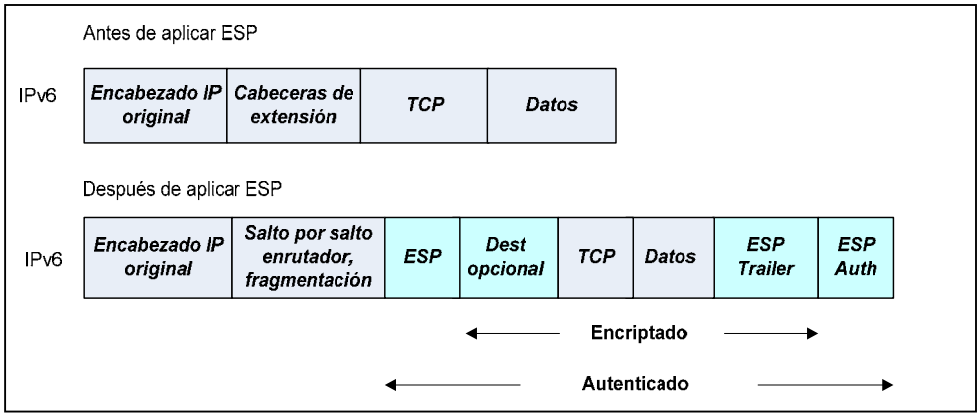


FIGURA 1.4.2.11 TRANSFORMACION DEL PAQUETE IPV6 AL APLICAR ESP EN MODO TRANSPORTE

En modo túnel, ESP puede ser empleado en hosts o en gateways. El encabezado IP interior contiene las direcciones del destino y origen del paquete, y el encabezado exterior puede contener direcciones diferentes, comúnmente direcciones de gateways de

seguridad en el camino entre el origen y destino. La posición de los encabezados ESP en modo túnel con respecto a los encabezados IP exteriores es igual que en modo transporte. En la figura 1.4.2.12, se muestran los encabezados ESP para IPv4 e IPv6.

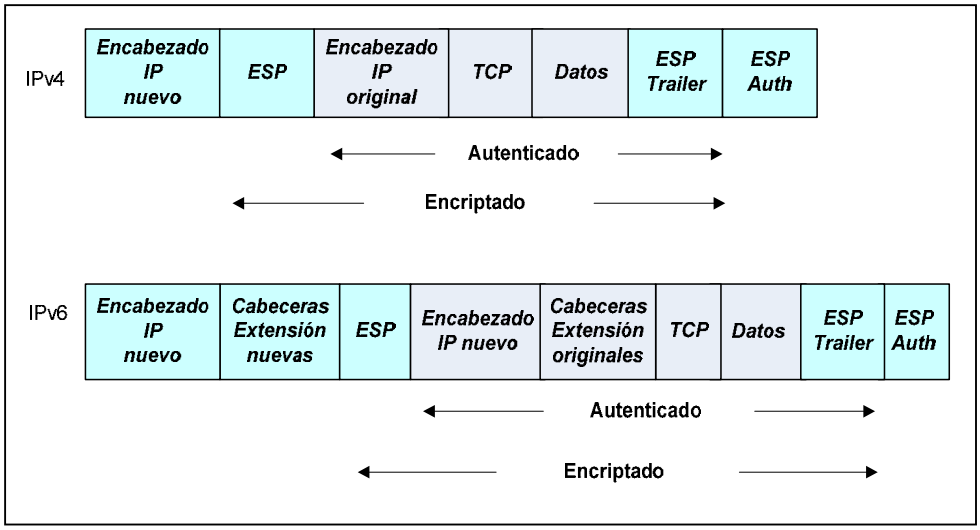


FIGURA 1.4.2.12. TRANSFORMACION DEL PAQUETE IP AL APLICAR ESP EN MODO TÚNEL.

En caso de no haberse indicado la confidencialidad en la SA, el algoritmo de criptografía es nulo, en caso de aplicar confidencialidad a un paquete que se envía, el proceso aplicado en general es el siguiente:

1. Encapsular en el campo de carga útil de ESP:

    - Para modo transporte, solo la información original del protocolo de capa superior.

- Para modo túnel, el datagrama IP original completo.

2. Agregar el relleno necesario.
3. Encriptar el resultado (carga útil de datos, relleno, longitud del relleno y la siguiente cabecera) usando la llave, el algoritmo de criptografía, el modo indicado en la SA y si existe, datos de sincronización criptográfica.

En la parte del receptor se sigue en general el siguiente procedimiento para desencriptar los paquetes recibidos:

1. Desencriptar la carga útil de ESP, relleno, longitud del relleno, y siguiente cabecera, utilizando la llave, el algoritmo de criptografía, el modo y en su caso, los datos de sincronización criptográfica, indicados en la SA.
2. Procesar el relleno según haya sido especificado por el algoritmo utilizado.
3. Reconstruir el datagrama IP original:

- Para modo transporte, el encabezado IP original más la información del protocolo de capa superior original en el campo de carga útil de ESP.
- Para modo túnel, el encabezado IP entunelado, más el datagrama IP completo en el campo de carga útil de ESP.

Es importante mencionar que el encriptamiento no debe ser sustituto por la autenticación, la autenticación es el servicio básico de una comunicación segura, reforzada con el encriptamiento de datos.

IP Authentication Header (AH).

AH es el protocolo IPSec utilizado para proveer servicios de integridad de datos, autenticación del origen de los datos, y antireplay para IP. Es un estándar definido en el RFC 2402. La principal diferencia entre la autenticación provista entre ESP y AH tiene que ver con la cobertura, ESP no protege los campos del encabezado IP, a menos que sean encapsulados por ESP (modo túnel). El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado AH contendrá el valor 51 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6).

La figura 1.4.2.13, muestra el encabezado AH, todos los campos son obligatorios, tienen funciones similares a las explicadas en ESP, el campo reservado no se utiliza y su valor debe ser cero.

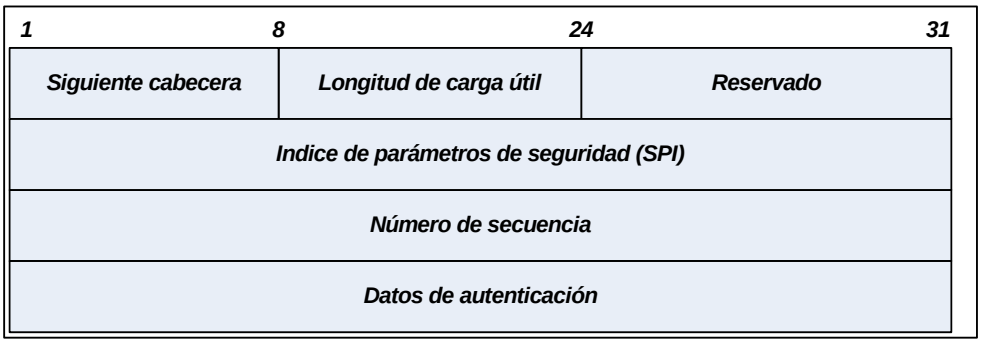


FIGURA 1.4.2.13 ENCABEZADO AH.

Al igual que ESP, AH puede aplicarse tanto en modo túnel como transporte. Las figuras 1.4.2.14 y 1.4.2.15, muestran la ubicación de AH al aplicar IPSec en modo transporte en los paquetes IP.

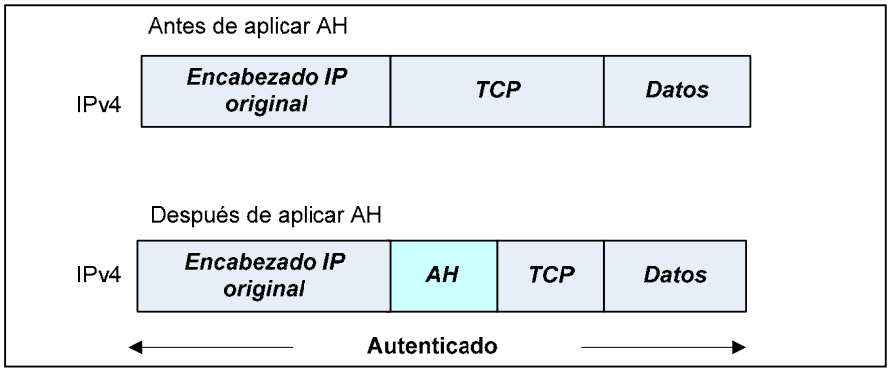


FIGURA 1.4.2.14. TRANSFORMACION DEL PAQUETE IPV4 AL APLICAR AH EN MODO TRANSPORTE.

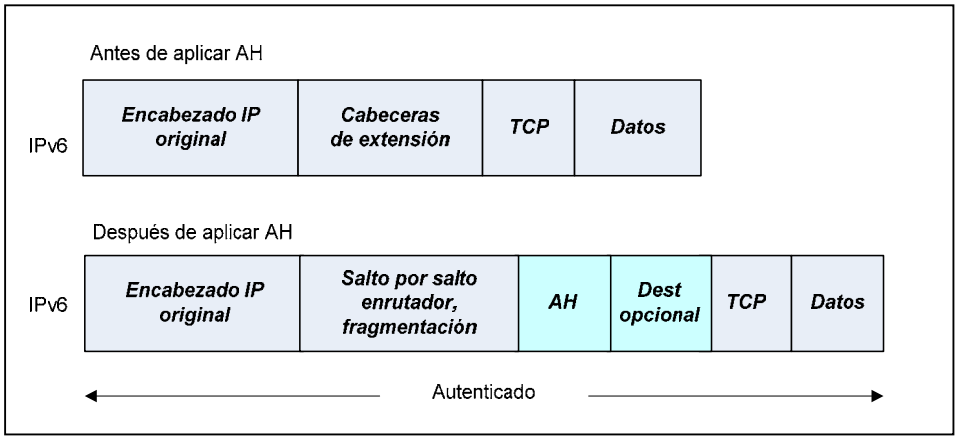


FIGURA 1.4.2.15 TRANSFORMACION DEL PAQUETE IPV6 AL APLICAR AH EN MODO TRANSPORTE.

La aplicación de AH en modo túnel, tiene una ubicación similar a la de ESP, en la figura 1.4.2.16 se muestra la transformación de los paquetes IP al aplicar AH en modo túnel.

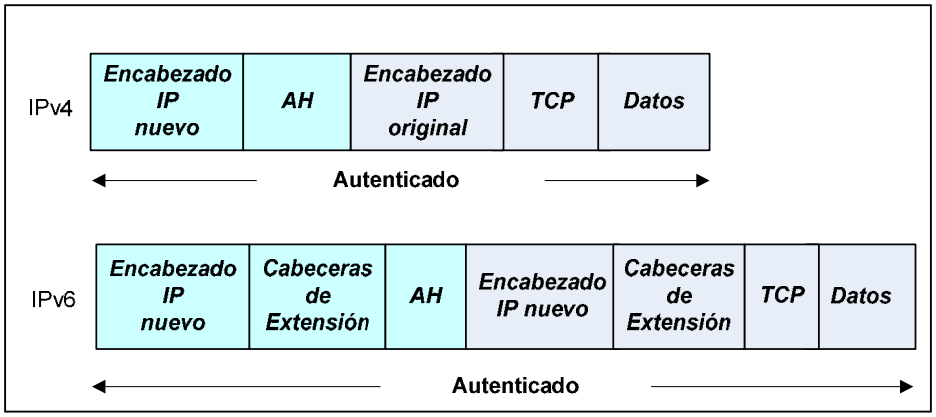


FIGURA 1.4.2.16. TRANSFORMACION DEL PAQUETE IP AL APLICAR AH EN MODO TÚNEL.

El proceso de cálculo del valor de verificación de integridad (Integrity Check Value, ICV) que utiliza AH, llena con ceros los campos vulnerables a cambios en tránsito (TOS, Flags, Fragment, TTL, Header checksum en un encabezado IPv4) y se calcula sobre lo siguiente:

- Los campos del encabezado IP que sean inmunes a cambios en tránsito o pueda predecirse su valor (Versión, longitud de carga útil, longitud total, identificación, dirección de fuente y destino en un encabezado IPv4).
- El encabezado AH (siguiente cabecera, longitud de relleno, reservado, SPI, número de secuencia y datos de autenticación (que es puesta a cero para este cálculo), y bytes de relleno en caso que existan.
- Los datos del protocolo de capa superior, que se asume son inmunes a cambios en tránsito.

1.4.3 SOFTWARE DE MONITOREO DE RED

Las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante.

Las redes, cada vez mas, soportan aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas.

Anteriormente, cuando no existían las herramientas que hoy existen, era necesario contratar a una empresa especializada para esta labor, con un costo muy elevado. Esta herramienta, permitirà, a ud. mismo, realizar esta importante labor, y contar un sistema como aliado, que le ayudarà en la interpretación de los resultados obtenidos.

1.4.3.1 PRTG TRAFFIC GRAPHER

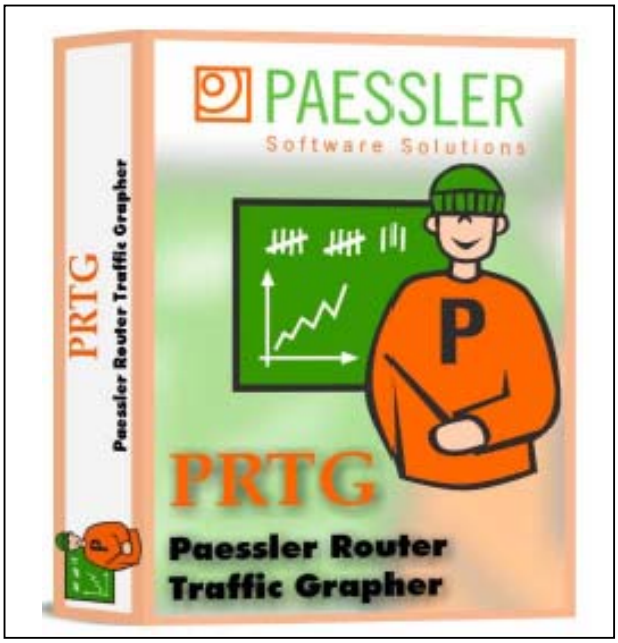


FIGURA 1.4.3.1 SOFTWARE DE MONITOREO DE RED

El PRTG Traffic Grapher figura 1.4.3.1, es un software de Windows fácil de usar que se lo utiliza para monitorear, supervisar y clasificar el ancho de banda. Este le proporciona al administrador lecturas instantáneas de sus dispositivos de red. El uso mas común es el monitoreo del ancho de banda, pero también se lo puede utilizar para monitorear otros aspectos de red como es la memoria y el porcentaje de utilización del CPU.

1.4.3.2 USO DEL MONITOREO DEL ANCHO DE BANDA

PRTG traffic grapher es ejecutado en una máquina con Windows en la red durante las 24 horas y constantemente guardará información de la red.

La figura 1.4.3.2 muestra el uso de una línea arrendada sobre varios periodos de tiempo.

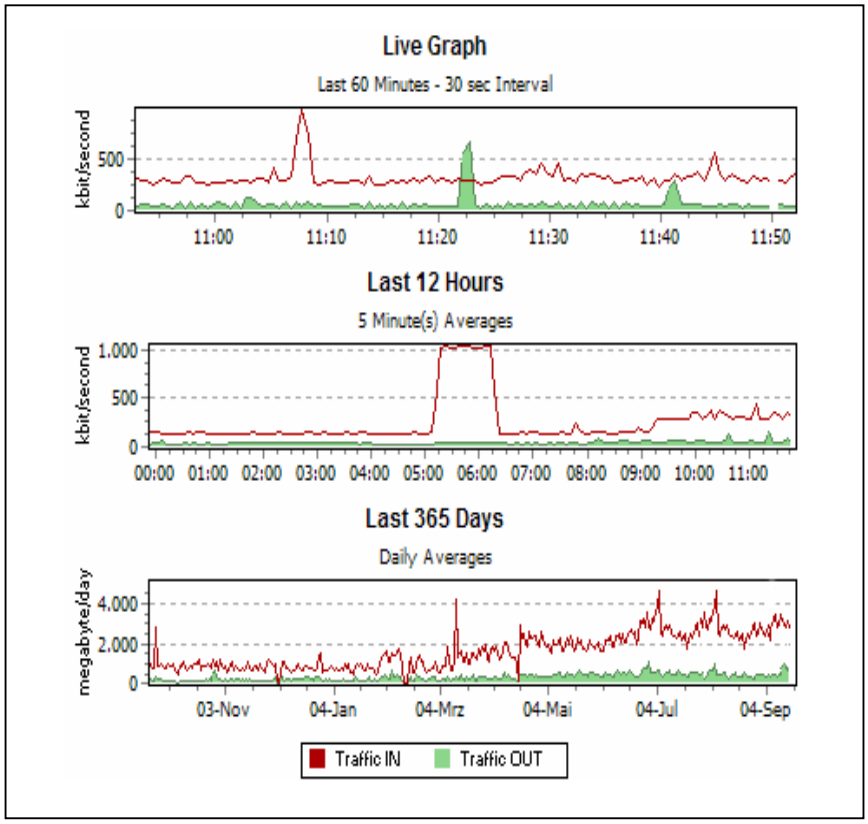


FIGURA 1.4.3.2 UTILIZACION DE UNA LINEA DEDICADA

Usando esta fácil interfase en Windows se puede configurar el monitoreo para realizar informes de utilización. Para el acceso remoto PRTG traffic grapher viene con un Web Server incorporado que provee el acceso a los gráficos y tablas.

Los métodos de red soportados son:

SNMP: Simple Network Management Protocol es el método básico usado para la captura de datos del ancho de banda en la red.

Este puede ser usado para monitorear el ancho de banda usado por los routers y switches puerto por puerto como también leer el porcentaje de carga de la memoria del CPU.

Packet Sniffing: Con el Packet Sniffer PRTG se puede inspeccionar en la red todos los paquetes de datos que estàn pasando por la tejeta de red para calcular el ancho de banda usado.

NetFlow: El protocolo NetFlow es soportado por todos los routers cisco para medir el ancho de banda usado. Aunque es del tipo mas complejo para configurarlo, también el más poderoso método conveniente para redes de alto tráfico

La aplicación corre en todas las versiones de Windows y trabaja con la mayoría los productos de la red de Cisco, HP, 3Com, Linksys, Nortel, etc., y con varios otros dispositivos (ej. Windows PCs o copiadoras de la red).

1.4.3.3 MONITOREANDO EL TRAFICO DE RED

La figura 1.4.3.3 muestra la pantalla de la ventana principal del Traffic Grapher PRTG. A lado izquierdo puede escoger entre las

seis vistas diferentes. En la mitad se puede observar una lista de opciones en verde colorido y a la derecha se observa las gráficas de la opción seleccionada.

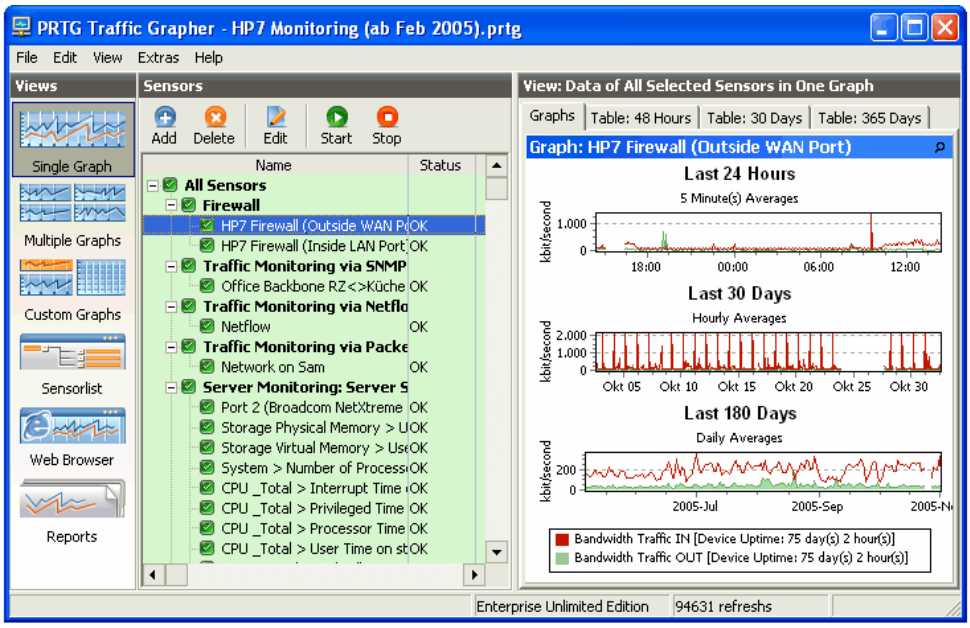


FIGURA 1.4.3.3 VENTANA PRINCIPAL DEL TRAFFIC GRAPHER PRTG

1.4.3.4 ESQUEMA DE LA PANTALLA PERSONALIZABLE

El usuario puede personalizar el esquema de la ventana principal individualmente. Puede crear pantallas individuales con gráficos y tablas.

En la figura 1.4.3.4, se puede ver CPU y ancho de banda monitoreado a dos servidores y una lista de los usuarios con mayor tráfico en la red .

FIGURA 1.4.3.4 PERSONALIZACION DE UNA PANTALLA PRINCIPAL

1.4.3.5 ACCESO AL MONITOREO DE DATOS DE ALGUN LUGAR USANDO EL WEB BROWSER

PRTG Traffic Grapher figura 1.4.3.5, trae su propio web Server interno que permite monitorear los datos mediante un acceso

remoto desde cualquier lugar. Mediante una facil navegación permite mostrar datos de gráficos y tablas. El acceso puede ser opcionalmente protegido por contraseña.

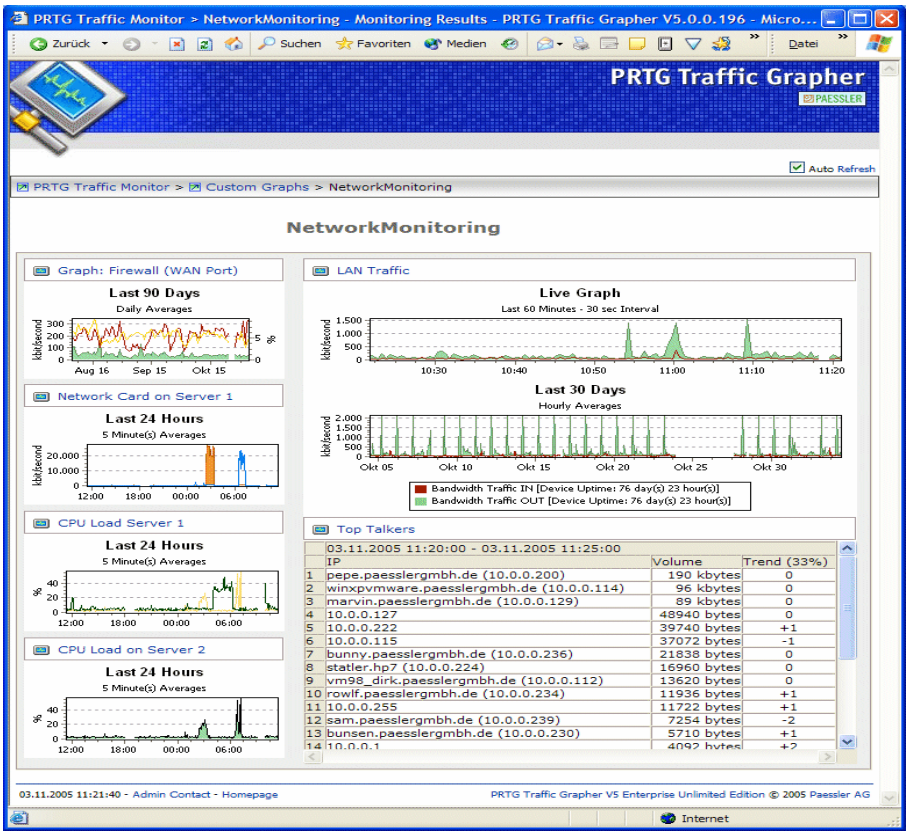


FIGURA 1.4.3.5 ACCESO REMOTO AL PRTG TRAFFIC GRAPHER

1.4.4 ENRUTAMIENTO

Se conoce con el nombre de enrutamiento (routing) el proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.

En su viaje entre ambos host los paquetes han de atravesar un número indefinidos de host o dispositivos de red intermedios, debiendo existir algún mecanismo capaz de direccionar los paquetes correctamente de uno a otro hasta alcanzar el destino final. Este mecanismo de ruteo es responsabilidad del protocolo IP, y lo hace de tal forma que los protocolos de las capas superiores, como TCP y UDP, no tienen constancia alguna del mismo, limitándose a preocuparse de sus respectivas tareas.

Cuando un host debe enviar datos a otro, lo primero que hace es comprobar si la dirección IP de éste se encuentra en su tabla ARP, en cuyo caso los datagramas le son enviados directamente mediante la dirección de su tarjeta de red, conocida como dirección física.

En caso de que no conozca la misma, envía un mensaje de petición ARP, que será respondido por el host destino enviando su dirección física, con la que ya tiene los datos suficientes para la transmisión de las tramas. Este proceso recibe el nombre de routing directo.

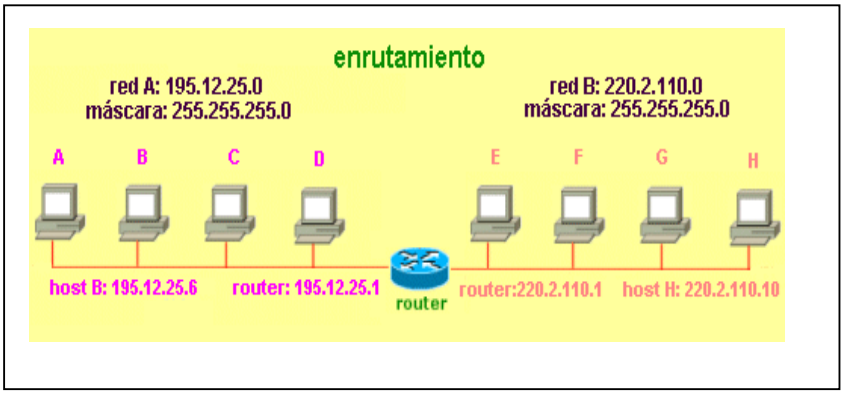


FIGURA 1.4.4.1 REDES UNIDAS POR UN ROUTER

Como ejemplo, supongamos dos redes unidas por un router, figura 1.4.4.1. Si el host B de la red A desea enviar un paquete al host H, lo primero que hará será comprobar si el host de destino aparece en su tabla de resoluciones ARP, y si no es así, realiza la correspondiente petición ARP usando broadcast. Como H no puede responder a la misma, al estar en otra red, B decide enviar los paquetes al router para que éste se encargue de su direccionamiento. Los paquetes que le pasa contienen la dirección IP de H y la dirección física del router.

Los routers poseen unas tablas de enrutamiento en las que almacenan información sobre el mejor camino que pueden seguir los paquetes para llegar a su destino. Cuando le llegan los paquetes, el router debe extraer de ellos la dirección de la red a la que pertenece H, para saber a cuál de las redes que una debe

mandar los paquetes. Para ello, coge la dirección IP de destino y realiza con ella y las máscaras de red de cada una de las redes a las que pertenece una operación AND lógica, con lo que obtendrá la dirección de la red destino. Para realizar la operación AND pasa las direcciones IP a formato binario

Los Routers aprenden acerca de la topología de la red en base a:

- Rutas estáticas
- Protocolos de enrutamiento.

Rutas Estáticas: se administra en forma manual por el administrador de la red figura 1.4.4.2, ya que este es el encargado de actualizar las rutas y las modificaciones se hacen de forma manual.

- Permiten la configuración manual de las tablas de enrutamiento.
- Las tablas no podrán ser modificadas en forma dinámica
- Falta de flexibilidad frente a fallas de los enlaces
- No son necesarios las cargas y procesos asociados a un protocolo de descubrimiento de rutas.
- Es fácil establecer barreras de seguridad bajo este modelo.

- Los Routers no pueden reenrutar ante fallas de enlace

figura 1.4.4.3.

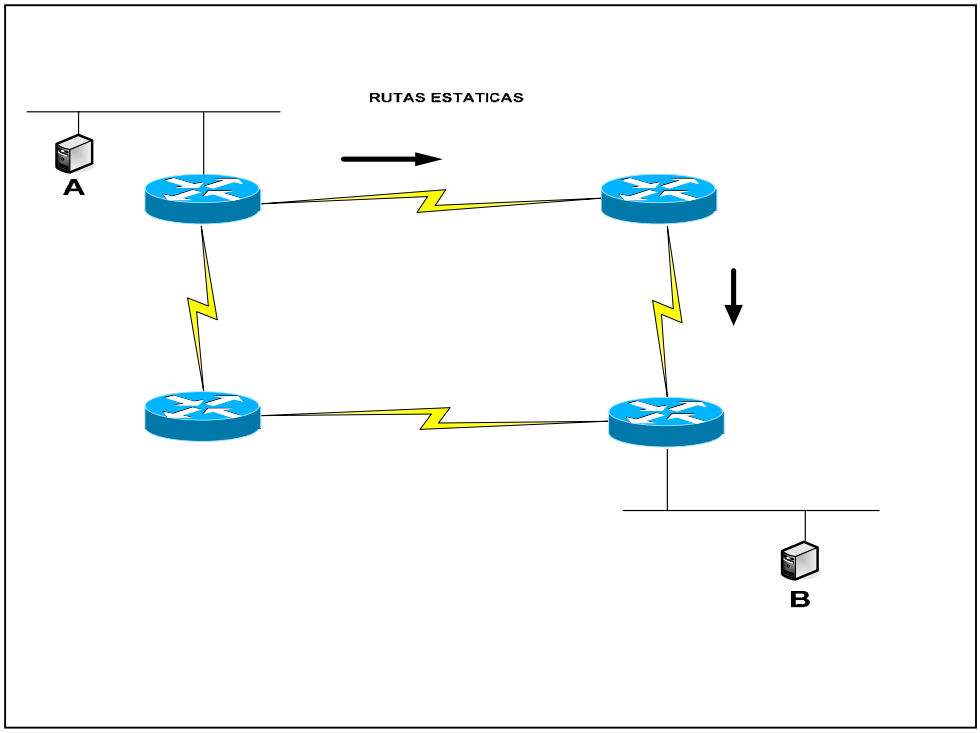


FIGURA 1.4.4.2 RUTAS CONFIGURADAS MANUALMENTE

POR EL ADMINISTRADOR

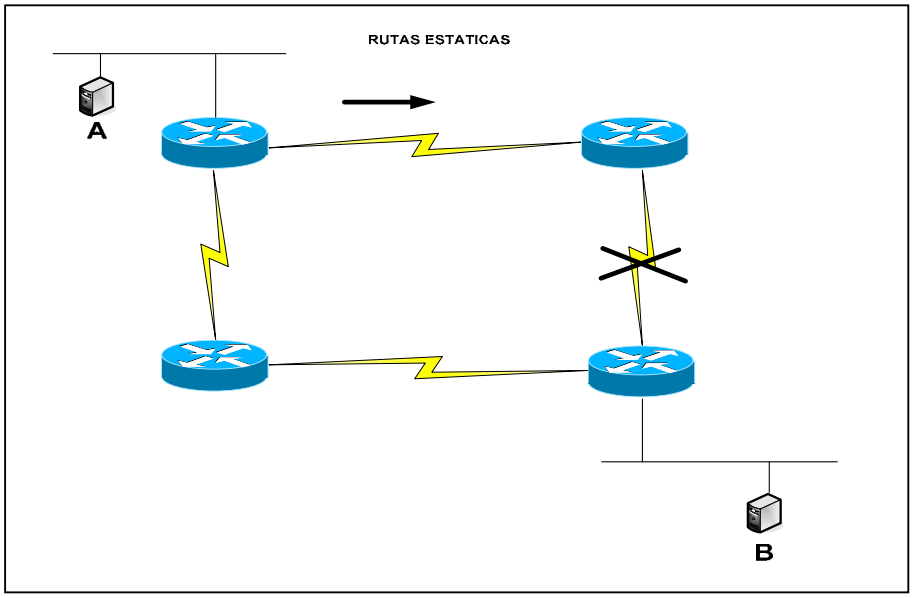


FIGURA 1.4.4.3 FALLA DE ENLACE

Enrutamiento Dinámico: El administrador configura el router, de esta manera el protocolo administra los cambios mediante el envío periódico de información de enrutamiento.

- Se basa en la comunicación, a través de broadcasts, entre los routers.
- Para descubrir las mejores rutas los routers emplean el concepto de métrica.
- No es necesario mantener manualmente las tablas de rutas.

El sistema se vuelve más flexible y autónomo frente a caídas de los enlaces

- Los roturers utilizan un protocolo común

- Se basan en métricas para la selección de rutas

Ruteo por estado de enlace:

- Cada nodo es responsable de aprender todo lo posible acerca de sus vecinos y colocarlo en un LSP (**L**ink **S**tate **P**acket)
- Este LSP es enviado a todos los otros nodos.
- Usando los LSP de los otros nodos se establece un mapa de la topología
- Una vez completo el mapa se utiliza un algoritmo Dijsktra para encontrar la mejor ruta

Ruteo por vector-distancia:

Obtienen información de la red únicamente por la que proporcionan los vecinos figura 1.4.4.4.

- Conocido como algoritmo Bellman - Ford
- Cada nodo mantiene una tabla con las distancias entre el mismo y los routers más cercanos

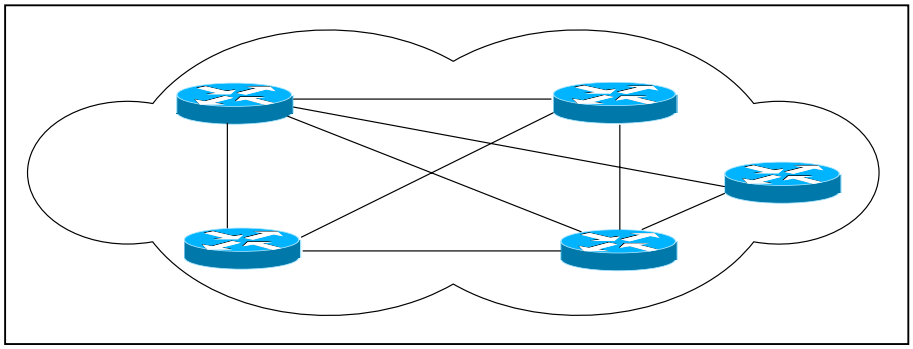


FIGURA 1.4.4.4 RUTEO POR VECTOR DE DISTANCIA

Las distancias son calculadas en base a lo que los otros le cuenten

- Redes bajo administración común.
- Determinan la mejor ruta en forma dinámica

Protocolo de Enrutamiento Interior

- RIP
- IGRP
- OSPF

RIP (Routing Information Protocol)

- Especificado en el RFC 1058
- Se basa en la filosofía de vector - distancia

- Utiliza como métrica el concepto de salto (hop)
- El número máximo de saltos permitidos es 15
- Se actualiza cada 30 segundos

IGRP (Interior Gatway Routing Protocol)

- Desarrollado por CISCO
- Se basa en la filosofía de vector - distancia
- Utiliza una mezcla de criterios para determinar la métrica
- Ancho de banda del canal
- Retardos
- Carga
- Confiabilidad
- Se actualiza cada 90 segundos

OSPF (Open Shortest Path First)

- Especificado en el RFC 1131 y en el RFC 1247
- Se basa en la filosofía de estado del enlace
- Utiliza el concepto de costo para determinar la métrica
- Diseñado para ser usado en un único sistema autónomo

Protocolo de Búsqueda Exteriores

- EGP (Exterior Gateway Protocol)
- BGP (Border Gateway Protocol)

EGP (Exterior Gateway Protocol)

- Especificado en los RFC 827 y RFC 904
- Rutea en base a los routers vecinos
- No utiliza métrica
- Los routers se comunican el estado de los enlaces

BGP (Border Gateway Protocol)

- Especificado en los RFC 1105, RFC 1163 Y RFC 1267
- Utiliza conexiones del tipo TCP
- Realiza medidas periódicas para determinar las mejores rutas

1.4.5 SISTEMAS OPERATIVOS

Un Sistema Operativo es una parte importante de cualquier sistema de computación. Un sistema de computación puede dividirse en cuatro componentes:

- el hardware,
- el Sistema Operativo,
- los programas de aplicación
- los usuarios.

El hardware (Unidad Central de Procesamiento (UCP), memoria y dispositivos de entrada/salida (E/S)) proporciona los recursos de computación básicos.

Concepto y definición de Sistemas Operativos.

Existen diversas definiciones de lo que es un sistema operativo, pero no hay una definición exacta, es decir una que sea estándar; a continuación se presentan algunas:

Gestionar el hardware.- Se refiere al hecho de administrar de una forma más eficiente los recursos de la máquina.

Facilitar el trabajo al usuario.-Permite una comunicación con los dispositivos de la máquina.

El Sistema Operativo se encuentra almacenado en la memoria secundaria. Primero se carga y ejecuta un pedazo de código que se encuentra en el procesador, el cual carga el BIOS, y este a su vez carga el Sistema Operativo que carga todos los programas de aplicación y software variado.

Características de los Sistemas Operativos.

En general, se puede decir que un Sistema Operativo tiene las siguientes características:

- Conveniencia.
- Eficiencia
- Habilidad para evolucionar.
- Manejar las comunicaciones en red.

1.5 SOFTWARE Y HARDWARE DE SEGURIDAD

1.5.1 CHECK POINT

El firewall FireWall-1, desarrollado por la empresa israelí Check Point Software Technologies Ltd. Este firewall se ejecuta sobre diferentes sistemas Unix (Solaris, AIX, Linux y HP-UX), así como sobre Windows NT y también en `cajas negras' como las desarrolladas por Nokia, que poseen un sistema operativo propio (IPSO), basado en FreeBSD.

Quizás la característica más importante de Firewall-1 sea que incorpora una nueva arquitectura dentro del mundo de los firewalls: la inspección con estado (stateful inspection). Firewall-1 inserta un módulo denominado Inspection Modulo en el núcleo del sistema operativo sobre el que se instala, en el nivel software más bajo posible (por debajo incluso del nivel de red), tal y como se muestra en la figura 1.5.1; así, desde ese nivel tan bajo, Firewall-1 puede interceptar y analizar todos los paquetes antes de que lleguen al resto del sistema: se garantiza que ningún paquete es procesado por ninguno de los protocolos superiores hasta que Firewall-1 comprueba que no viola la política de seguridad definida en el cortafuegos.

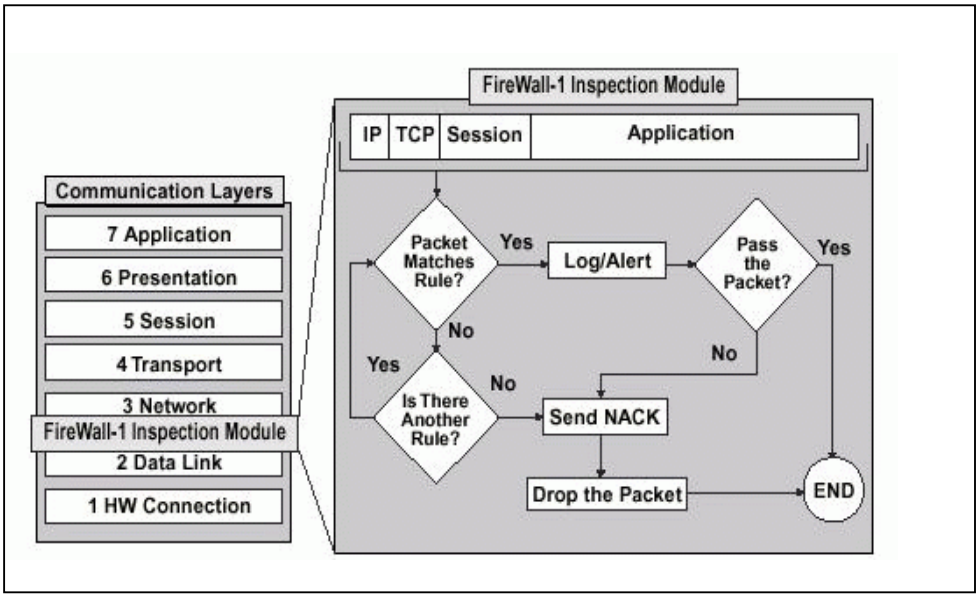


FIGURA 1.5.1 UBICACION DEL MODULO DE INSPECCION DENTRO DE LA PILA DE PROTOCOLOS OSI

Firewall-1 es capaz de analizar la información de una trama en cada uno de los siete niveles OSI y a la vez analizar información de estado registrada de anteriores comunicaciones; el cortafuegos entiende la estructura de los diferentes protocolos TCP/IP, incluso de los ubicados en la capa de aplicación, de forma que el Inspection Module extrae la información relevante de cada paquete para construir tablas dinámicas que se actualizan constantemente, tablas que el firewall utiliza para analizar comunicaciones posteriores. En el módulo de inspección se implantan las políticas de seguridad definidas en cada

organización mediante un sencillo lenguaje denominado INSPECT, también diseñado por Check Point Software Technologies; desde un cómodo interfaz se genera un script en este lenguaje, que se compila y se inserta en el Inspection Module.

CARACTERISTICAS

Intelligent Worm Defender ofrece la protección más potente contra gusanos para redes internas mediante la aplicación de las tecnologías Stateful Inspection y Application Intelligence de Check Point. Estas tecnologías se basan en INSPECT, que proporciona la protección más completa y adaptable del mercado. InterSpect se instala entre zonas protegidas de la red e impide la propagación de gusanos dentro de ésta; para ello inspecciona el tráfico procedente de los dispositivos conectados y bloquea el que identifica como peligroso.

Segmentación de la red en zonas

InterSpect segmenta la red en varias zonas de seguridad definidas por el administrador para impedir el acceso no autorizado de una zona a otra. Con esto se evita el acceso a información y a sistemas no autorizados por parte de usuarios o equipos

infectados conectados a la red. La segmentación de la red en zonas también detiene los ataques que se producen dentro de un subsegmento de la red.

Cuarentena

InterSpect es capaz de identificar en la red los ordenadores sospechosos o infectados y ponerlos en cuarentena, con lo que evita que se ponga en peligro el resto de la red. InterSpect permite también poner ordenadores en cuarentena durante la instalación de parches de seguridad. Esto contribuye a reducir el riesgo de infección mientras los administradores de la red identifican, instalan y prueban los parches. InterSpect también dispone de una función exclusiva de notificación a los usuarios en los casos de cuarentena. Cuando se pone en cuarentena el ordenador de un usuario (normalmente por haberse identificado como infectado), se notifica de ello al usuario por medio de una página web dinámica personalizada. Esta notificación ayuda a minimizar el tiempo invertido en localizar el problema desde el servicio de asistencia técnica y también permite poner al corriente de dicho problema al administrador de la red, reduciendo el tiempo de inactividad del usuario.

Protección de protocolos LAN

InterSpect ofrece la protección más extensa y completa para protocolos de Microsoft, como MS RPC, CIFS, MSSQL y DCOM, así como para otros protocolos LAN como Sun RPC, DCE RPC y HTTP. InterSpect hace uso de la tecnología INSPECT para ofrecer la capacidad de inspección de seguridad más adaptable del sector. Si los usuarios de InterSpect aprovechan las actualizaciones de INSPECT, disponibles mediante suscripción a SmartDefense, pueden mantener actualizada su infraestructura interna de seguridad a medida que surgen nuevos ataques y amenazas.

Protección preventiva contra ataques

InterSpect proporciona protección proactiva y dinámica frente a ataques conocidos y desconocidos, permitiendo a las organizaciones defenderse frente a los efectos de las vulnerabilidades antes de que alguien las aproveche.

InterSpect incluye una versión de SmartDefense, adaptada a la seguridad de las redes internas, que permite a los administradores configurar, imponer y actualizar todas las defensas frente a

ataques a la red y a aplicaciones mediante Stateful Inspection y Application Intelligence, que se basan en INSPECT, la tecnología de inspección de seguridad más inteligente y adaptable del sector. InterSpect incluye SmartDefense para redes internas, proporcionando una protección preventiva frente a ataques conocidos y desconocidos dentro de la red.

1.5.2 GB-1200 (BLACK BOX)

La familia SME firewall socios de tecnología globales, proporciona seguridad poderosa para el nivel de su empresa, con rasgos comprensivos que son fáciles de implementar en la mayoría de los ambientes de red corporativos. El GB-1200 forma parte la fundación de sistema firewall GTA, brinda alto rendimiento , rasgos avanzados de alta disponibilidad y hardware que soporta VPN en gigabit Ethernet. Usando uno de la familia de firewall los robox, pueden realizaarse conecciones VPN con facilidad. Los administradores de red pueden supervisar fácilmente y pueden administrar todos los firewalls GTA que son distribuidos en la red usando el software sistema administrador global GTA. La corporación de la familia de firewall ofrece uno de los mejores precios y proporciona alto rendimiento en la industria firewall.

Los productos firewall GTA combinan un sistema operativo propietario, firewall y hardware en fácil de instalar contenido en un solo equipo. Ofreciendo características Multi-capas, los administradores de red pueden cambiar con un simple plug and play la implementación o personalización.

El Aparato firewall GB-1200 figura 1.5.2, ofrece al usuario licencias ilimitadas, NAT transparente, estado de inspección de paquetes, IPSec VPN, cuatro interfaces 10/100 Ethernet, DCHP server, DNS, server, administración segura remota y filtra volumen en un 1-RU. Opciones disponibles incluye: Acceso a administración la navegación de Internet, disponibilidad alta, GMS administración global, interfaces gigabyte Ethernet e interfaces adicionales.

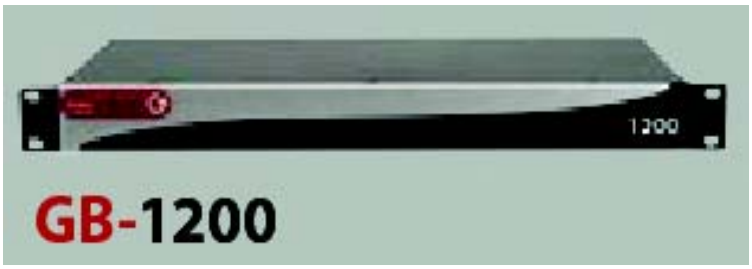


FIGURA 1.5.2 FIREWALL GB-1200

CARACTERISTICAS

NAT.- Estado de inspección de paquetes y aplicaciones de firewall que combina técnicas con un poderoso mecanismo de traslación de direcciones para proveer acceso externo a la red completamente transparente y redes DMZ para aplicaciones basadas en ip.

Alto Rendimiento.- El GB-1200 tiene especificaciones de hardware que provee flexibilidad y alto rendimiento, basado en procesadores Intel que permiten incorporar fácilmente nuevas tecnologías, sin comprometer el rendimiento o la seguridad de sus redes. Con opciones de hardware de aceleración de VPN o interfaces gigabit ethernet.

VPN.- La industria Integró el estandar ipsec red privada virtual para las instalaciones de ambos sitios y usuarios móviles remotos con medio de acceso seguro que puede ser una realidad incluso para la organización mas pequeña.

Detección de intrusos.- La organización es protegida contra los accesos no autorizados e intentos de penetrar el perímetro de

seguridad proporcionado por el firewall, estos son anotados y generan alarmas basadas en reglas establecidas por el administrador del firewall.

También Proporciona

- Autenticación de usuario
- Modo Disimulo
- Hosting Virtual vía IP
- PPPoE
- DHCP client/server
- DMZ
- DNS
- Interfaces de usuario vía administración remota
- Fácil configuración e instalación

CAPITULO II

2. SITUACION ACTUAL DEL CLIENTE Y DEL CARRIER

2.1 SITUACION ACTUAL DEL CLIENTE

El cliente está conformado por dos Oficinas principales, la matriz que está en Gye y la sucursal mayor que está en UIO, una ventanilla de extensión en la Universidad Agraria Gye, cada una con su respectivo cajero automático (ATM), además el cliente tiene enlaces externos con BANRED, SERVIPAGOS, BANCO CENTRAL, SWIFT, VISA OPTAR y MULTISERVICE.

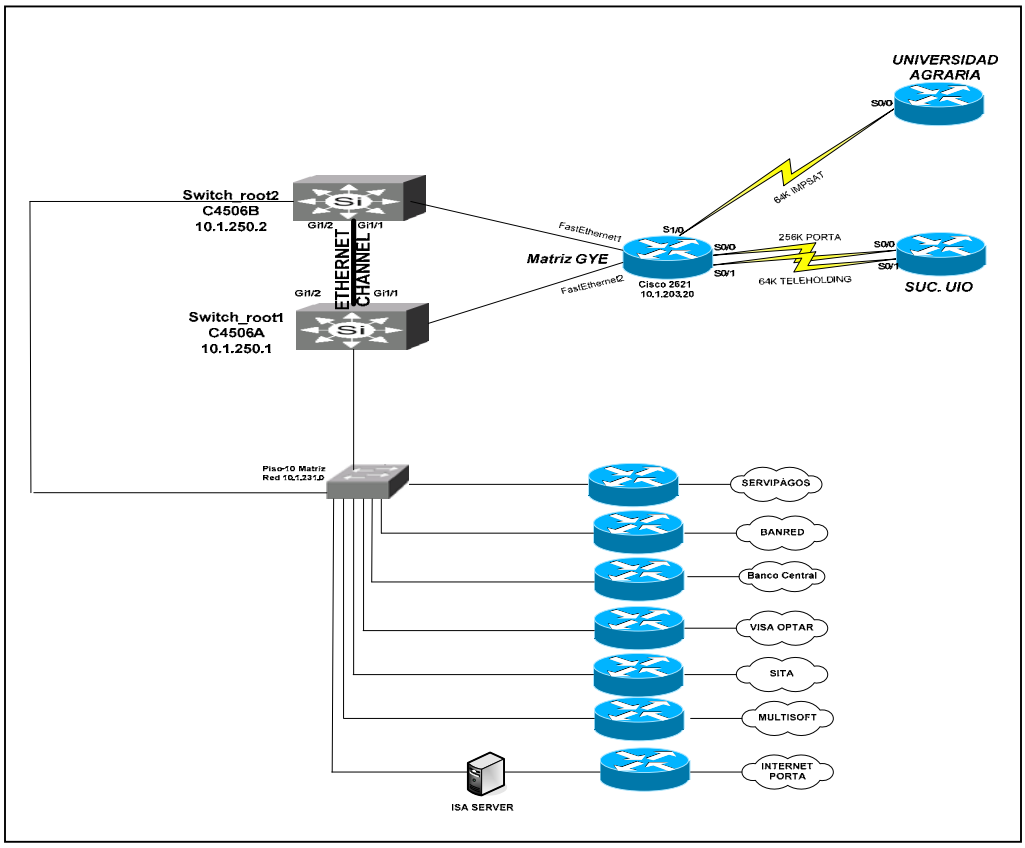


FIGURA 2.1.1 DIAGRAMA DE RED WAN DEL CLIENTE.

FIGURA 2.1.2 RACK DE COMUNICACIONES DEL CLIENTE.

El Backbone del cliente figura 2.1.3, está conformado por dos switchs Cisco Catalyst 4506 como equipos principales figura 2.1.4, 2.1.5 y Switch 2950T por piso que poseen puertos Giga Ethernet, este esquema permite mejorar la eficiencia de la red, ampliando las conexiones entre los switchs de pisos y los switchs principales, sin afectar el funcionamiento de la red y brindarle los recursos necesarios para la implementación de mejoras en la arquitectura física y lógica.

Con el esquema de red basado en VLAN, el cliente cuenta con una mejor administración y funcionamiento

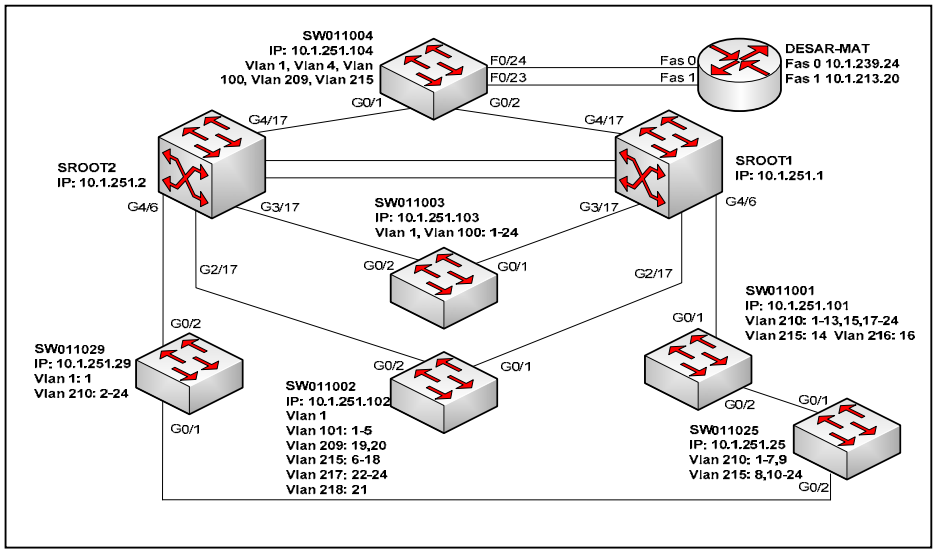


FIGURA 2.1.3 BACKBONE DEL CLIENTE.

FIGURA 2.1.4 RACK DE SWITCH 4506 DEL CLIENTE.

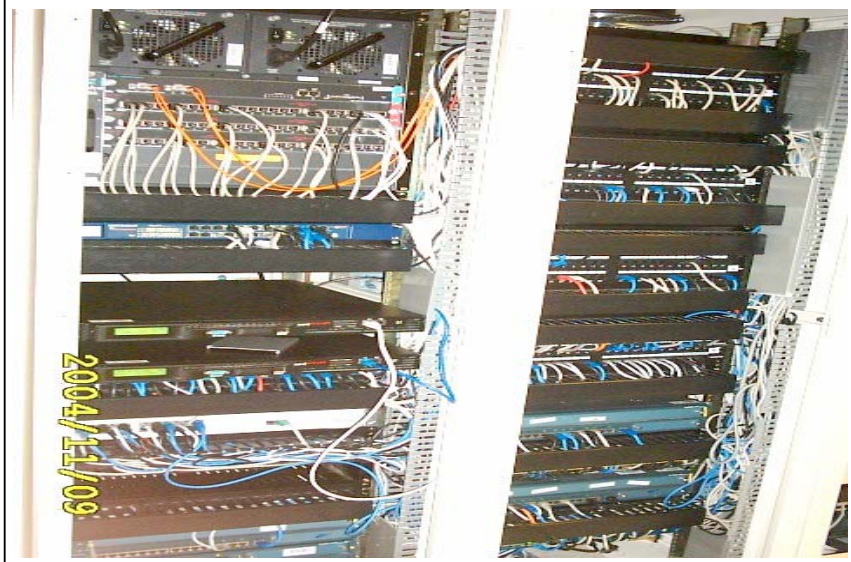


FIGURA 2.1.5 RACK DE SWITCH 4506 DEL CLIENTE

Los pisos tienen instalado 18 Cisco Catalyst 2950T-24 equipo con 24 puertos Fast y 2 Gigabit Ethernet (Figura 2.1.6) que brinda conectividad segura e inteligente, que permite aplicar calidad de servicio (QoS), de acuerdo al esquema implementado, la ubicación física de los switch se describe en la tabla 2.1.1

FIGURA 2.1.6 SWITCH CISCO CATALYST 2950T

Cantidad	Equipo	Ubicación
1	WS-2950T-24	Rack Planta Baja Cuentas Corrientes
1	WS-2950T-24	Rack Planta Baja Giros y Cambios
2	WS-2950T-24	Rack Piso 2
2	WS-2950T-24	Rack Piso 3
2	WS-2950T-24	Rack Piso 4
1	WS-2950T-24	Rack Piso 5
2	WS-2950T-24	Rack Piso 6
2	WS-2950T-24	Rack Piso 7
2	WS-2950T-24	Rack Piso 8
1	WS-2950T-24	Rack Piso 9
2	WS-2950T-24	Rack Cableado Piso 10

TABLA 2.1.1 UBICACION DE SWITCH CISCO CATALYST 2950T

Esquema Técnico

Uno de las maneras de obtener redundancia y mantener uptime es mediante la utilización de HSRP (Hot Standby Router Protocol) que

mediante el uso de IP virtual de manera inmediata y transparente mantiene el trafico a través de la red, adicionalmente del esquema de redundancia que tiene el Cliente estos switchs utilizan Spanning-tree (capa dos) para mantener conexiones redundantes sin que se formen lazos en la arquitectura de la red, la asignación de Vlans por cada uno de los pisos es parte del diseño de red y con ello el PVST (Per-Vlan-Spanning Tree) Tabla 2.1.2. La arquitectura física implementada permite la existencia de enlaces redundantes que mediante el uso del algoritmo Spanning Tree son deshabilitados sin el riesgo de lazos, para el caso de los pisos en el que existen dos switch se conectó ambos switch entre los puertos Gi0/1; y los puerto Gi0/2 con cada uno de los Switch principales, la arquitectura formada por Spanning Tree bloquea la conexión entre los puertos Gi0/1 de los switch de piso, como ejemplo para mostrar este caso tomamos el piso 2, figura 2.1.7.

DIRECCIONAMIENTO DE VLAN

Piso	Vlan	Red	Mascara	C4506A	C4506B	Gateway
PB GC	200	10.1.229.0	255255.255.0	10.1.229.21	10.1.229.22	10.1.229.20
PB CC	211	10.1.230.0	255255.255.0	10.1.230.21	10.1.230.22	10.1.230.20
2	202	10.1.232.0	255255.255.0	10.1.232.21	10.1.232.22	10.1.232.20
3	203	10.1.233.0	255255.255.0	10.1.233.21	10.1.233.22	10.1.233.20
4	204	10.1.234.0	255255.255.0	10.1.234.21	10.1.234.22	10.1.234.20
	212	10.1.206.0	255255.255.0	10.1.206.21	10.1.206.22	10.1.206.20
5	205	10.1.235.0	255255.255.0	10.1.235.21	10.1.235.22	10.1.235.20
6	206	10.1.236.0	255255.255.0	10.1.236.21	10.1.236.22	10.1.236.20
7	207	10.1.237.0	255255.255.0	10.1.237.21	10.1.237.22	10.1.237.20
8	208	10.1.238.0	255255.255.0	10.1.238.21	10.1.238.22	10.1.238.20
9	209	10.1.239.0	255255.255.0	10.1.239.21	10.1.239.22	10.1.239.20
10	210	10.1.240.0	255255.248.0	10.1.240.21	10.1.240.22	10.1.241.20
	215	10.1.231.0	255255.255.0	10.1.231.21	10.1.231.22	10.1.231.20
	216	10.1.208.0	255255.255.0	10.1.208.21	10.1.208.22	10.1.208.20
	217	10.1.203.0	255255.255.0	10.1.203.25	10.1.203.26	10.1.203.20
Servidores	100	10.1.218.0	255255.255.0	10.1.218.21	10.1.218.22	10.1.218.20
	101	10.1.202.0	255255.255.0	10.1.202.21	10.1.202.22	10.1.202.20

TABLA 2.1.2 ASIGNACION DE VLANS POR PISOS

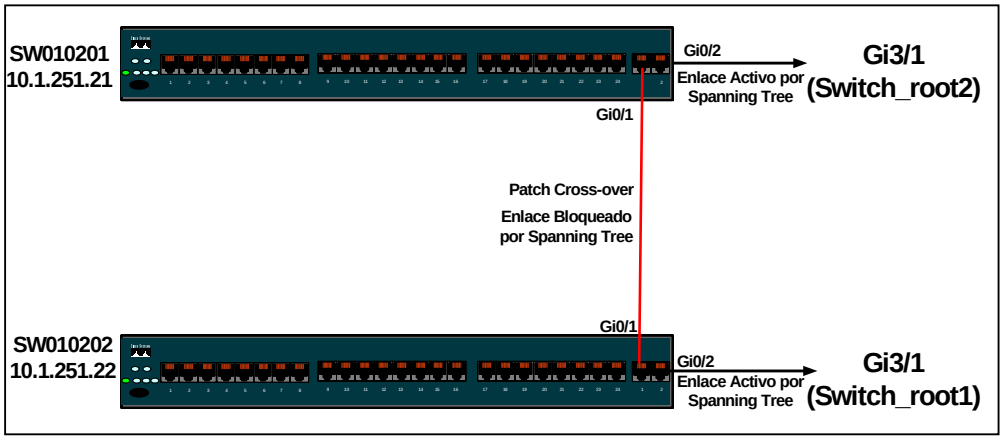


FIGURA 2.1.7 CONEXION DEL PISO 2

Para el caso de los pisos que tienen un solo Switch los puertos Gi0/1 y Gi0/2 fueron conectados a el Switch_root1 y Switch_root2 respectivamente, deshabilitando el Spanning Tree uno de estos enlaces. Figura 2.1.8.

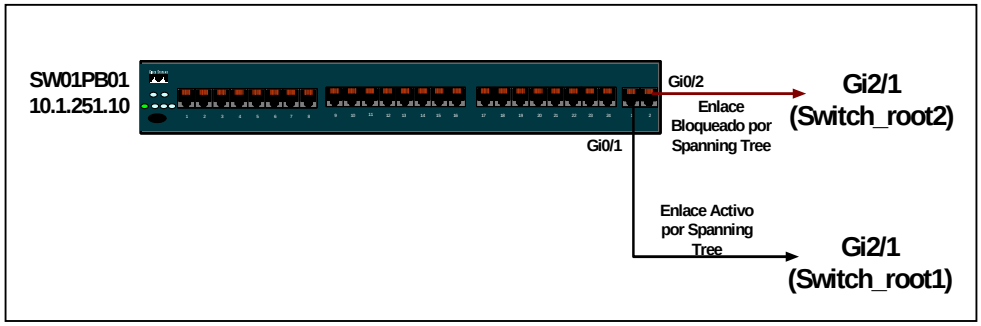


FIGURA 2.1.8 CONEXION DE PLANTA BAJA

La combinación de estas tecnologías tomando los beneficios principales que brindan cada una de ellas fue con la finalidad de obtener un sistema robusto, seguro y confiable que permitan un alto rendimiento, seguridad y posibilidades de crecimiento.

Tecnologías de los equipos

Spanning Tree

El algoritmo Spanning Tree elige el mejor camino, hacia el root poniendo en estado de standby (bloqueo) a las conexiones

redundantes; si un segmento en el Spanning tree falla y existe una conexión redundante el algoritmo Spanning tree recalcula la topología y activa la conexión que esta en standby, pues la función principal del Protocolo de árbol de extensión (STP) es permitir que haya rutas redundantes conmutadas/puenteadas sin sufrir los efectos de los loops en la red.

Los puertos esperan que la información de la nueva topología se propague a través de los switch de la red para empezar a reenviar las tramas.

Cada interfase en capa 2 del switch que usa spanning tree pasa por los siguientes estados:

Bloquear (Blocking): Ninguna trama enviada, se escuchan BPDU.

Escuchar (Listening): No se envían tramas, se escucha para detectar si hay tramas.

Conocer (Learning): No se envían tramas, se aprenden direcciones.

Enviar (Forwarding): Tramas enviadas, se aprenden direcciones.

Desactivado (Disabled): No se envían tramas, no se escucha ninguna BPDU.

De existir dos root se deberá asignar cual de ellos es configurado como primario, asignándole la prioridad de puente mas baja; para todos los switch la prioridad por default es 32768. El Per-Vlan-Spanning Tree (PVST) permite balancear el tráfico de las VLAN de la red entre los enlaces redundantes sin el riesgo que se formen lazos.

Hot Sandby Routing Protocol

Este protocolo permite un uptime cercano al 100% proporcionando redundancia de red a las Ips, compartiendo dirección IP y MAC (Capa 2) en la cual dos o mas routers puedan actuar como un simple router “virtual” esta dirección IP puede ser usada como default gateway de los host de la subnet. De esta manera el router standby asume la responsabilidad de ruteo en caso de que el router activo falle, los host continúan reenviando los paquetes IP a una determinada dirección IP y MAC siendo la transición del equipo que maneja el ruteo transparente para los hosts de la subnet. La característica es activada con el siguiente comando:

Standby [Numero de grupo] **ip** [ip-address(secundaria)]

Con el uso de los comandos priority y preempt uno de los routers es elegido como el router activo y el segundo es designado como backup.

Ethernet Channel

Ethernet Channel convierte enlaces Ethernet en un simple enlace lógico que provee más ancho de banda, pudiéndose obtener hasta 1600 Mbps (Fast EtherChannel full duplex) y 16 Gbps (Gigabit EtherChannel) en la serie Catalyst 4500.

La serie Catalyst 4500 soporta un máximo de 64 Ethernet Channels, usted puede formar un Ethernet Channel hasta con 8 interfaces Ethernet.

Todas las interfaces que forman el Ethernet Channel deberán ser de la misma velocidad y configurados en capa 2 o capa 3. Si una de las interfaces que forman parte del Ethernet Channel falla el tráfico en enviado por las restantes. Las siguientes figuras muestran los esquemas de configuración y los Racks de piso del cliente (figuras 2.1.9, 2.1.10, 2.1.11, 2.112, 2.1.13, 2.1.14, 2.1.15, 2.1.16, 2.1.17, 2.1.18, 2.1.19, 2.1.20, 2.1.21, 2.1.22, 2.1.23, 2.1.24, 2.1.25, 2.1.26)

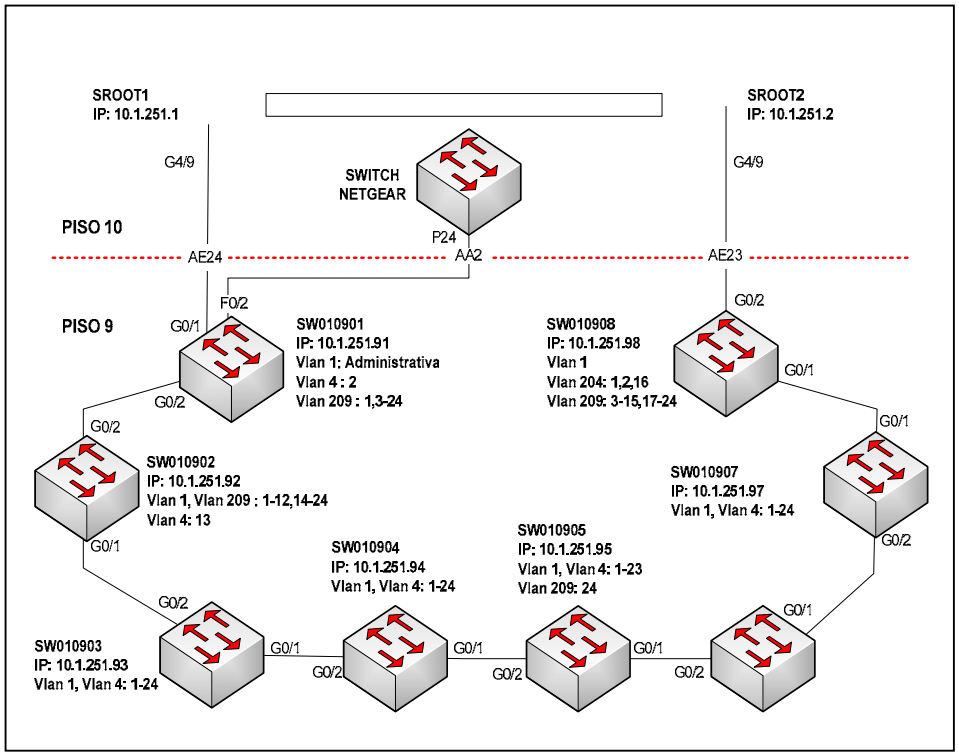


FIGURA 2.1.9 ESQUEMA DE INTERCONEXION DEL PISO 9

FIGURA 2.1.10 WIRING ROOM PISO 9

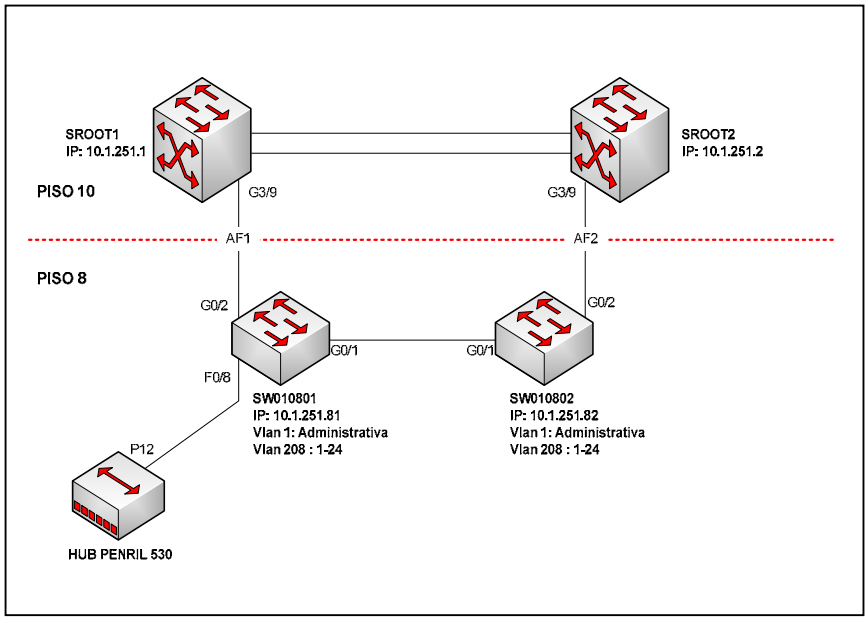


FIGURA 2.1.11 ESQUEMA DE INTERCONEXION DEL PISO 8

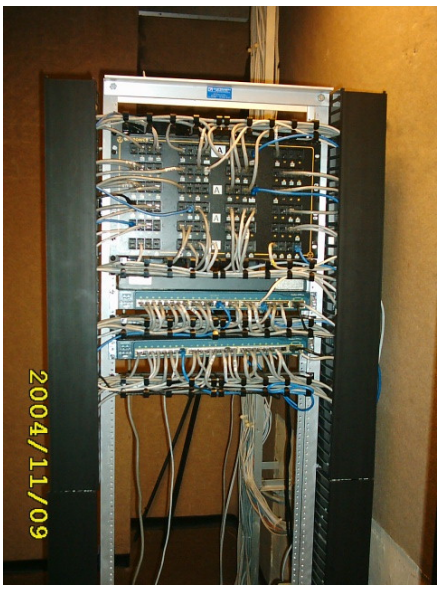


FIGURA 2.1.12 WIRING ROOM PISO 8

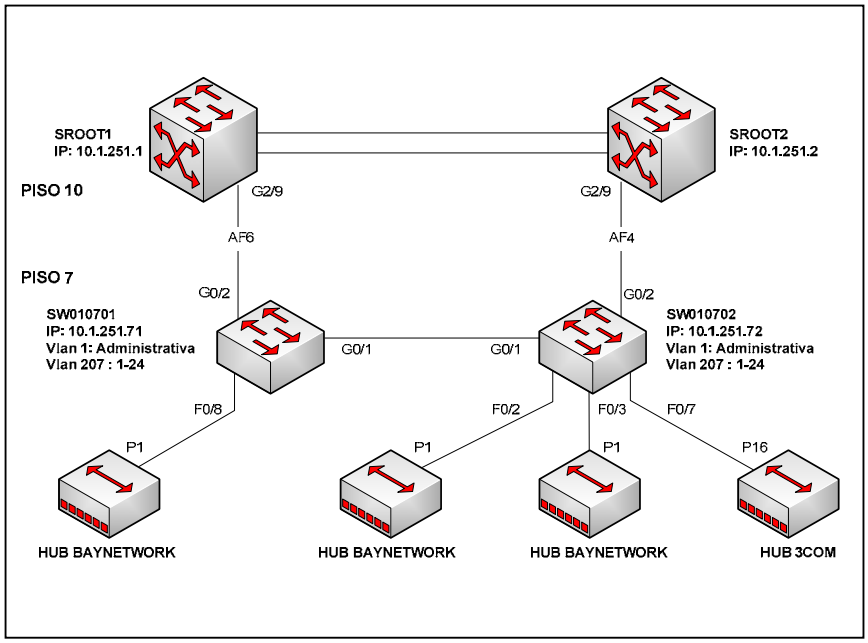


FIGURA 2.1.13 ESQUEMA DE INTERCONEXION DEL PISO 7

FIGURA 2.1.14 WIRING ROOM PISO 7

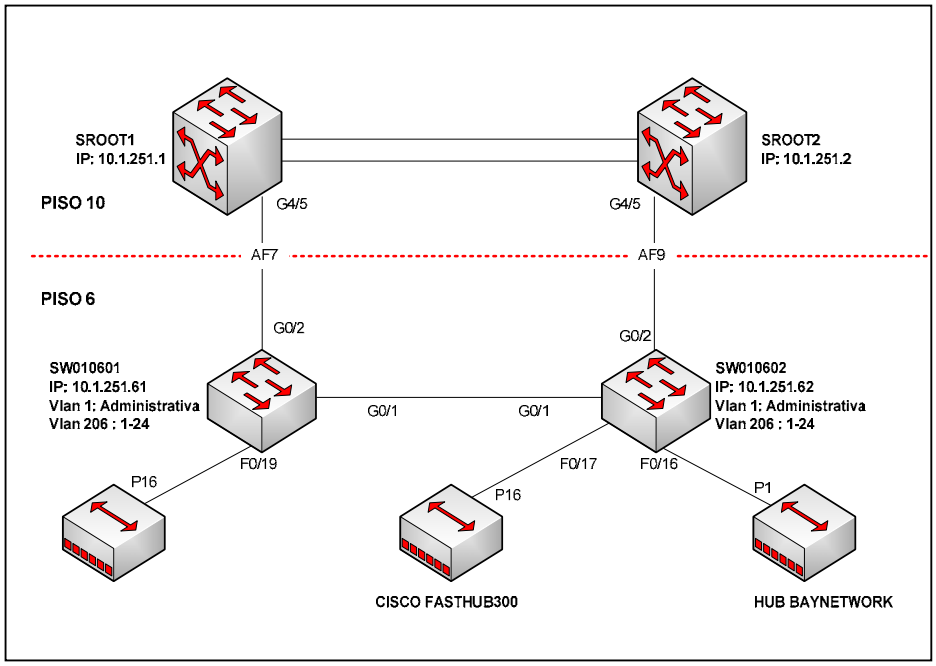


FIGURA 2.1.15 ESQUEMA DE INTERCONEXION DEL PISO 6

FIGURA 2.1.16 WIRING ROOM PISO 6

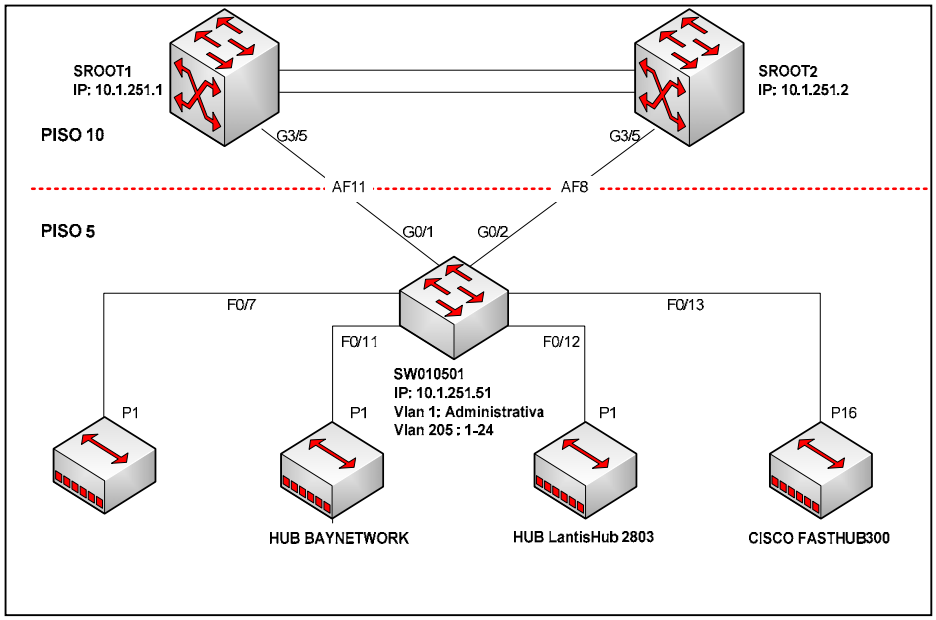


FIGURA 2.1.17 ESQUEMA DE INTERCONEXION DEL PISO 5

FIGURA 2.1.18 WIRING ROOM PISO 5

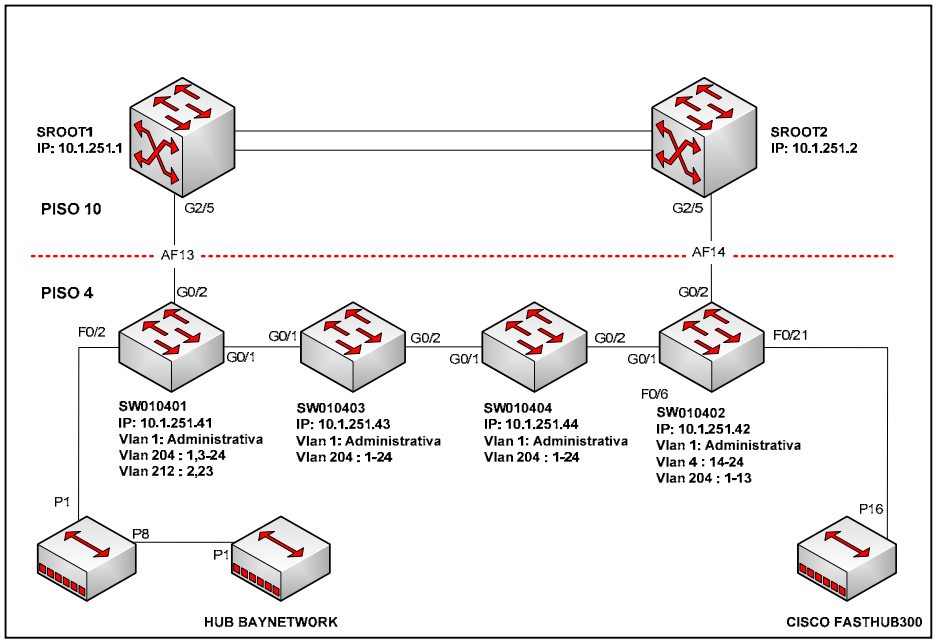


FIGURA 2.1.19 ESQUEMA DE INTERCONEXION DEL PISO 4

FIGURA 2.1.20 WIRING ROOM PISO 4

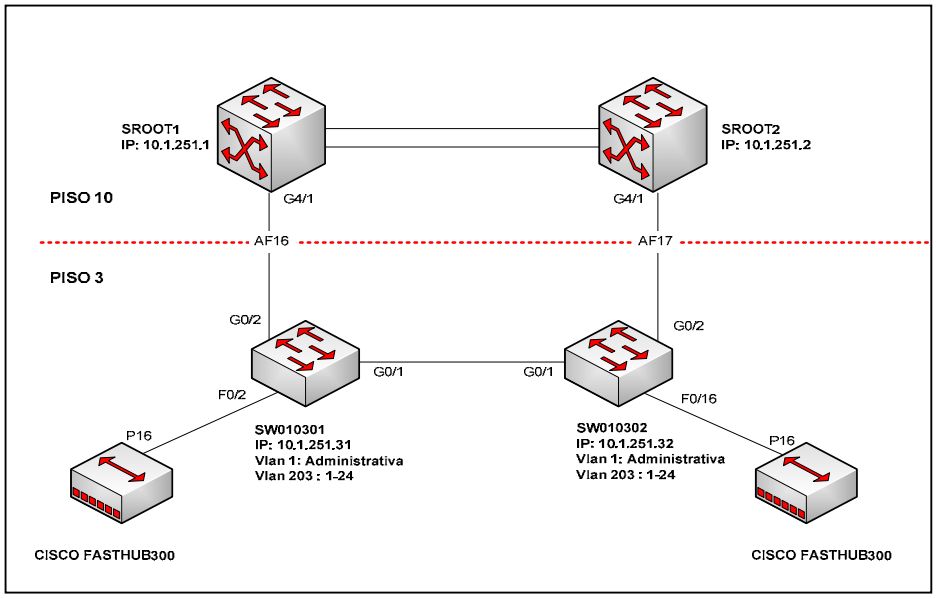


FIGURA 2.1.21 ESQUEMA DE INTERCONEXION DEL PISO 3

FIGURA 2.1.22 WIRING ROOM PISO 3

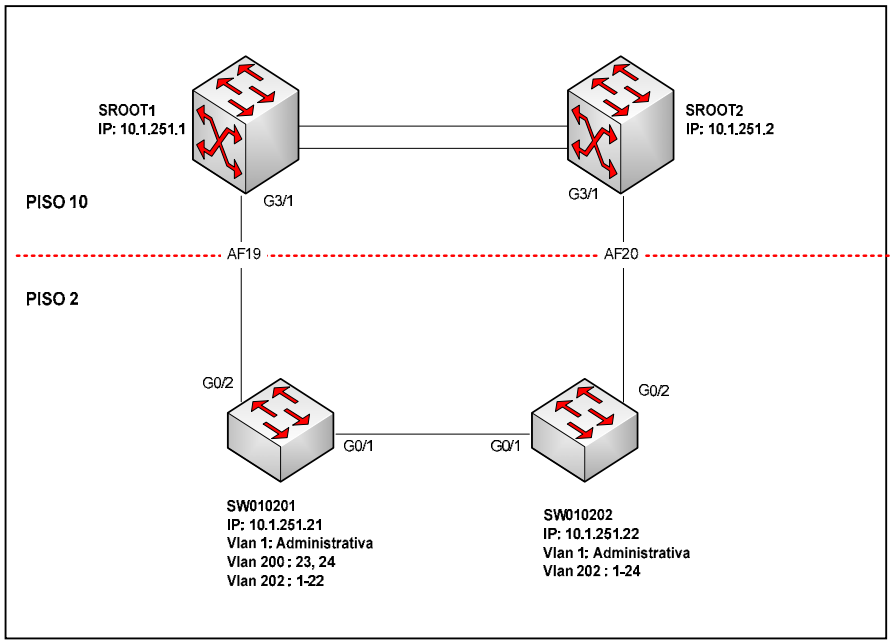


FIGURA 2.1.23 ESQUEMA DE INTERCONEXION DEL PISO 2

FIGURA 2.1.24 WIRING ROOM PISO 2

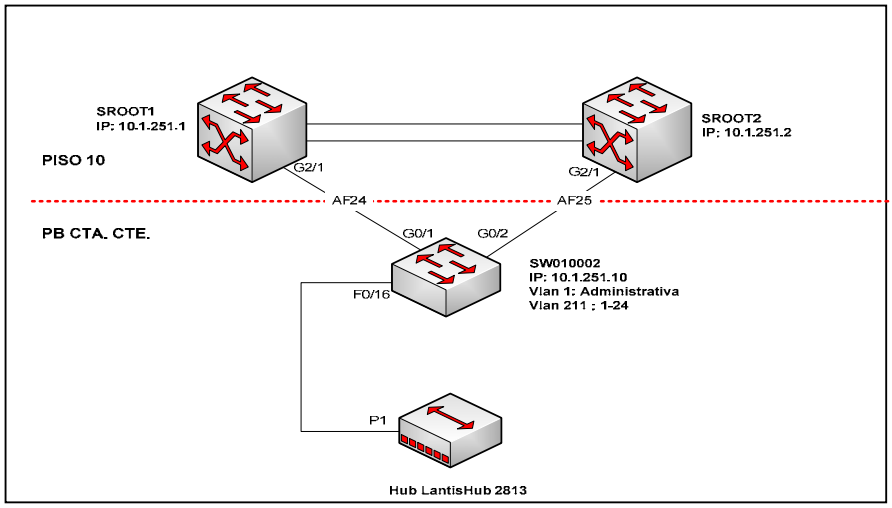


FIGURA 2.1.25 ESQUEMA DE INTERCONEXION DE LA PLANTA BAJA

FIGURA 2.1.26 WIRING ROOM PLANTA BAJA

2.1.1 ENLACE GYE-UIO

El enlace principal (microonda) se lo realiza entre Gye y Uio y está conformado por un canal Frame Relay de 256 Kbps por el cual se trasmite todos los datos figura 2.1.1.1.

Los datos se enrutan entre estas oficinas mediante routers cisco 2621, los cuales se conectan con un puerto WAN Serial S0/0 y S0/1 para el enlace de respaldo, estos equipos ubicados en ambos extremos Gye-Uio son el corazón de las comunicaciones.

FIGURA 2.1.1.1 RACK DE COMUNICACIONES UIO

2.1.2 BANRED

Este enlace está compuesto por un canal digital frame relay de 32 kbps siendo su proveedor Suratel, comunica las oficinas de BANRED con las del cliente a través de dos modem HIGHLINK, el modem que va en Gye se conecta directamente al switch Cisco 2950 que se conecta con el puerto ethernet del router Cisco 2621 Gye.

2.1.3 VISA OPTAR

Este enlace (microonda) está compuesto por un canal frame relay de 32 kbps siendo su proveedor Impsat que comunica las oficinas de VISA OPTAR UIO con el cliente en Gye a través de dos modem Main Street 2603, el modem que va del lado del cliente se conecta con un router cisco 800 y este a su vez se conecta con el switch cisco 2950.

2.1.4 MULTISERVICE

Este es un enlace de cobre que está compuesto por un canal dedicado de 9,6 Kbps y comunican las oficinas de MULTISOFT UIO

con el cliente mediante dos modem, el modem que va del lado del cliente con un router Cisco 805 y este a su vez se comunica con un switch 2950 que va al router Cisco 2621 UIO.

2.1.5 BANCO CENTRAL

Este enlace inalámbrico es un clear channel de 11 Mbps, los equipos de comunicaciones y antenas son del cliente y comunican las oficinas del BANCO CENTRAL Gye con la Matriz del cliente mediante dos modem wireless, el modem que va del lado del cliente se conecta con el switch cisco 2950 y este a su vez se conecta con el router Cisco 2621.

2.1.6 SWIFT

Este es un enlace de cobre dedicado de 19.2 Kbps que lo provee la compañía SITA y comunica las oficinas de Sita con la Matriz del cliente, el modem que va del lado del cliente se comunica con el servidor de swift mediante una tarjeta X.25 y este servidor se conecta con el switch cisco 2950 que está conectado al Cisco 2621, la compañía Sita, permite comunicarse con un centro de cómputo en Bélgica y realizar transacciones internacionales.

2.1.7 UNIVERSIDAD AGRARIA

Este es un enlace clear channel de 64 Kbps que lo provee Impsat y comunica Universidad agraria con la Matriz del cliente, el modem que va a la Matriz del cliente se conecta al router 2621 interface S1/0.

El modem que va a Universidad Agraria se conecta a un router cisco 1750 y este a un hub que da señal al server y ATM.

2.1.8 ENLACE DE RESPALDO

El cliente cuenta con enlace de respaldo Gye Uio el cual comunica Matriz con Sucursal Mayor, este es un enlace clear channel de 64Kbps, la empresa que da este servicio es Teleholding, el modem que va a la matriz se conecta al router cisco 2621 interface s0/1.

2.1.9 INTERNET

El proveedor de Internet del cliente es PORTA quien brinda un enlace frame relay de 128 Kbps, el modem que va del lado del cliente se conecta a un Cisco 1650, este va a un hub que se

conecta con el (ISA-SERVER), este se conecta al switch cisco 2950 y finalmente al Cisco 2621.

2.2 CARRIER TRANSACCIONAL

2.2.1 SERVIPAGOS

Este es un enlace frame relay 128 Kbps, siendo su proveedor Impsat, y comunican las oficinas de SERVIPAGOS UIO con el cliente mediante un enlace microonda, el modem que va del lado del cliente Gye se conecta con un Switch cisco 2950 y este a su vez se conecta con el Router Cisco 2621.

2.3 EVALUACION DE LA RED DEL CLIENTE

El cliente cuenta con una infraestructura que lo hace vulnerable a agentes externos

El cliente no dispone de un equipo de Seguridad Informática (Firewall), solo cuenta con un Servidor ISA-SERVER que sirve de Proxy y ruteo de Direcciones con algunas políticas muy bajas de seguridades.

Una de las vulnerabilidades mas notorias que tiene el cliente es la conexión de enlaces ajenos al cliente directamente conectados al switch 2950 figura 2.3.1, quedando desprotegida de cualquier clase de intrusos.

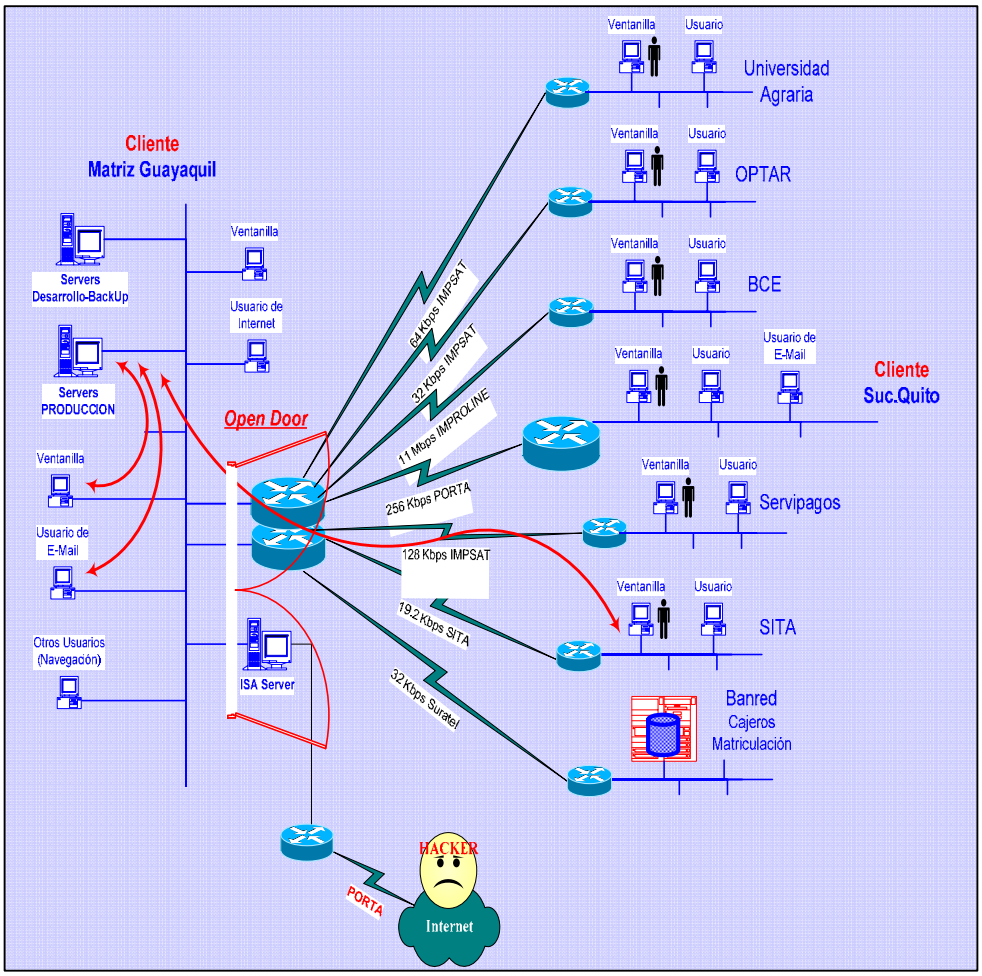


FIGURA 2.3.1 VULNERABILIDAD DE LA RED DEL CLIENTE

Sin embargo las vulnerabilidades siguen siendo elevadas, ya que si bien el ISA-SERVER en algo protege de ataques desde el Internet (seguridad a medias, vulnerabilidad completa), las conexiones con los proveedores o clientes no tienen ninguna restricción. El gráfico 2.3.1 indica claramente que los proveedores pueden ingresar directamente a la red interna del cliente por la extranet sin que se pueda controlar lo que puedan hacer a la información vital del banco. Y recordemos que los proveedores seguramente también tienen conexiones a Internet, y mientras el cliente cree estar cubierto de los ataques desde Internet con el ISA-SERVER, los hackers acceden a través de la redes privadas que en apariencia son seguras, pero como se nota en el gráfico son una **"puerta abierta"** a los ataques del ciberespacio. Por esta puerta pueden llegar códigos maliciosos (virus, gusanos), ataques de denegación de servicios (ping of death) y otras varias vulnerabilidades que en un momento dado pueden detener por completo la operación del banco.

Otro problema detectado es que la red del cliente se ha configurado usando direcciones que están registradas públicamente (ver gráfico 2.3.1), lo que podría generar conflictos en la administración y gestión de los administradores de la red.

Pero la situación más grave es que los servidores están en la misma red que muchos de los usuarios internos, sin ninguna restricción a nivel físico. Esto es un gran **“hueco”** de seguridad, ya que por **“desconocimiento”** (u otras causas) cualquier usuario podría ingresar al directorio de uno de los servidores y borrarlo accidentalmente, ya que las password´s (claves de usuario) no es algo que por si solo garantice seguridad (se filtran, se comparten). Datos estadísticos de varias empresas que se dedican a registrar vulnerabilidades informáticas indican que el 80% de ataques provienen desde la red interna. Esta situación no necesita describirse para imaginarnos lo fatal que seria para la operación del banco perder un directorio completo de información.

Desde esta perspectiva la situación actual no es muy alentadora. Pero empezar por analizar estas vulnerabilidades y tomar la decisión de corregirlas es el paso inicial para llegar a una red más segura y confiable.

2.4.- PROBLEMAS Y SOLUCIONES ENCONTRADAS EN LA RED DEL CLIENTE

Independiente de la marca o del tipo de firewall que se adquiera, el cliente esta en la obligación y necesidad de tener su información segura y confiable.

El cliente debe de tener una sola puerta de entrada para sus proveedores e Internet, controlada por el cliente para así poder verificar y detener los ataques.

El objetivo es llegar a tener una red protegida como la que se muestra en el gráfico 2.5.1.

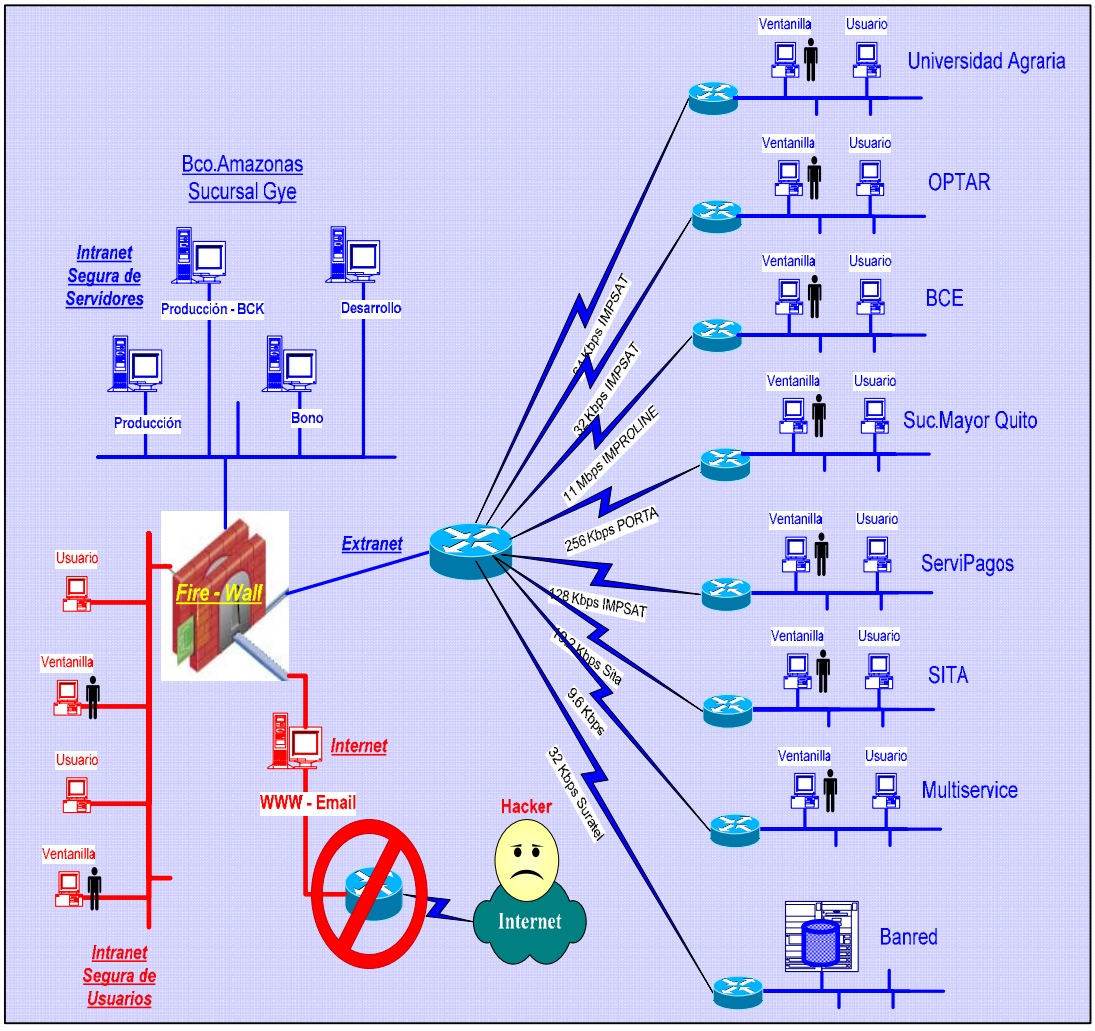


FIGURA 2.5.1 RED PROTEGIDA DEL CLIENTE

CAPITULO III

3. IMPLEMENTACION DE SEGURIDAD APLICADA A UN CARRIER TRANSACCIONAL

3.1 EVALUACIONES TECNOLOGICAS Y ALTERNATIVAS

Empresas líderes a nivel mundial se han dedicado al análisis de las vulnerabilidades informáticas y a corregir dichas falencias en las redes. Estos estudios dieron como resultado inicialmente la creación de los conocidos Proxy´s. Sin embargo estos se han quedado simplemente en un nivel limitado de control de navegación, pero no de detección de códigos maliciosos o ataques de agentes especializados.

Por ello estas mismas empresas han evolucionado y desarrollado un nuevo concepto en detección de intrusiones, más exhaustiva, más detallada que revise los datos y prevenga ataques. Estas nuevas soluciones se llaman firewalls.

Actualmente existen en el mercado dos alternativas de firewalls, los de Software y los de Hardware.

3.1.1 FIREWALL DE SOFTWARE

VENTAJAS

- Una solución de software nos permite modularidad, (crecimiento de acuerdo a requerimientos o necesidades).
- Es portable (compatible con cualquier plataforma).
- Se apropia del Kernell del Hardware lo que lo hace mas seguro.
- Son analizados por certificadores como ICSA.

DESVENTAJAS

- Necesita de un Hardware (máquina) para poder instalarlo.

3.1.2 FIREWALL DE HARDWARE

VENTAJAS

- Es más seguro en su acceso administrativo por ser una caja cerrada (appliances).
- Tiene las mismas virtudes que el Software.
- No necesita de un servidor para implementarlo.

DESVENTAJAS

- No es escalable
- No permite crecimiento

3.1.3 ALTERNATIVAS DE DIFERENTES MARCAS DE FIREWALL

Se evaluaron 2 alternativas de firewall tabla 3.1.4, que existen en el mercado, el CHECK POINT y el GB-1200 BLACK BOX, obteniendo el siguiente cuadro comparativo. La figura 3.1.3 muestra la presencia de firewalls en el mercado y sus rendimientos respectivos.

Comparativo Hardware	CheckPoint (Open Server and Appliances)	GB-1200 (BlackBox)
		
NIC's	4 ó mas 10/100 Ethernet Interfaces	Solo 4 10/100 Ethernet Interfaces
Puertos de Consola	2 ó mas Console Ports	2 DB9 Serial Interfaces Console Ports
Puertos USB	USB Interface	USB Interface
Procesador	3.06 Ghz Proccesor ó mas	1 Ghz Proccesor
Memoria	1 Gb Ram	128Mb Ram
Almacenamiento	40 Gb Hard Disk SCSI ó mas	64 Mb Flash Memory
Comparativo Software		
Software	CheckPoint Express NG with Appliction Inteligence R55 HFA 04	GNAT Box System Software Ver 3.4
Soporte para VPN's	IPSec VPN-1 Pro with 25 Mobile-Remote Client License	IPSec VPN With 1 Mobile Client License
Tecnología de inspección	Stateful Inspection technology. Invented by Check Point (U.S. Patent No. 5,606,668 and 5,835,726)	Stateful Packet Inspection
Network Address Translation	Hide, Static, Transparent and Secure NAT	Secure Transparent NAT
Métodos de Encripción	All Encryptions Methods Supported (Local, Remote, VPN) includes AES (Advanced Encryption Standard)	Encrypted Remote Management
Usuarios permitidos	250 User License	Unrestricted User License
Autenticación de usuarios	User Authentication Enforcement (All methods)	User Authentication
Protección activa/inteligente contra ataques (Robot)	Network and application level attack protection with integrated Smart Defense (IDP: Intrussion Detection Prevention)	Not supported
Plataformas soportadas	Available on a range of platforms for superior perfomance (Unix, Solaris, Windows, Linux, Secure Platform)	Not supported
Opciones (Módulos)		
Monitor de Recursos	Smart View Monitor	Not supported
Generador de Reportes	Smart View Reporter	GTA Reporting Suite
Calidad de Servicio/Manejador de Anchos de Banda	Flood Gate (QOS)	Not supported
Alta disponibilidad	High Availability on Cluster XL	H2A High Availability
Administrador de acceso a Internet	Included on CheckPoint Express	Surf Sentinel Internet Access Management
Licenciamiento	Scalable (client needs adjustment)	N/A

TABLA 3.1.4 COMPARATIVO DE ALTERNATIVAS

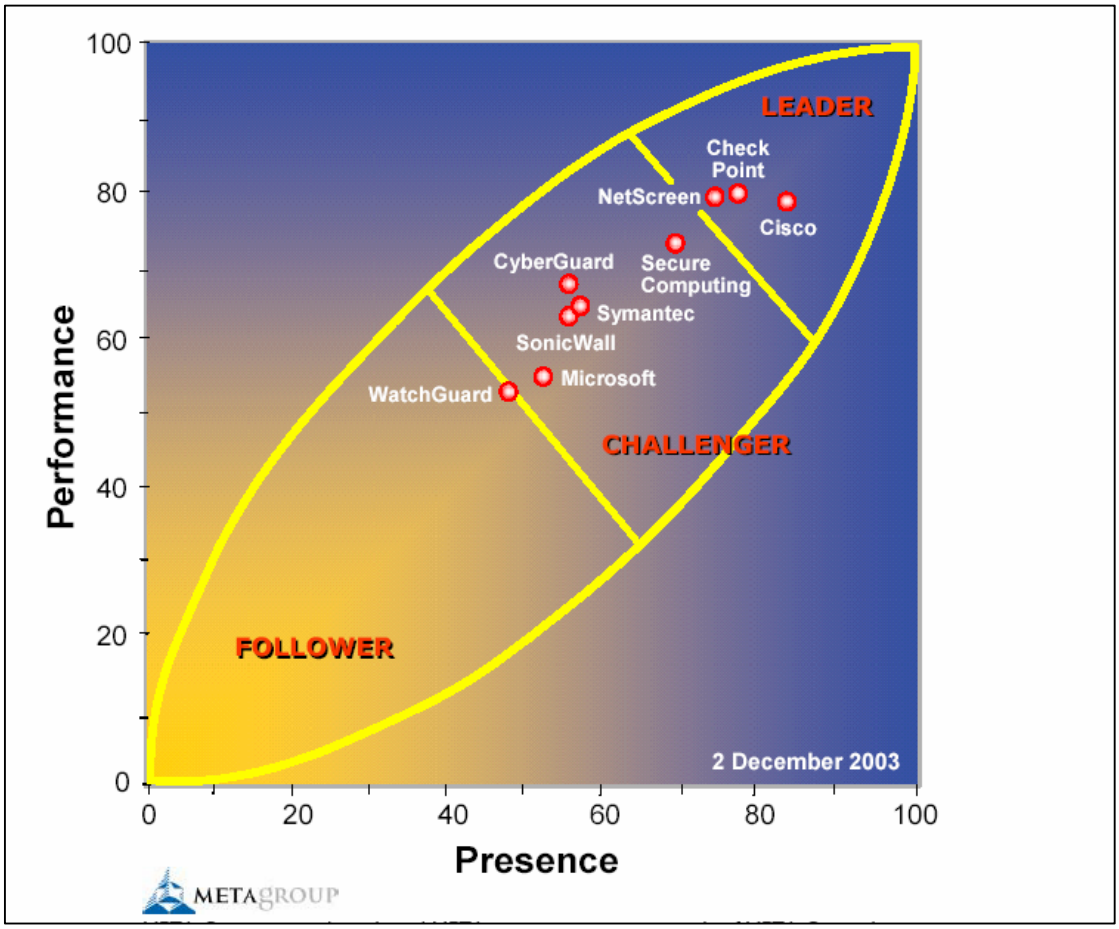


FIGURA 3.1.3 PRESENCIA DE FIREWALLS EN EL MERCADO

3.2 IMPLEMENTACION

3.2.1 EQUIPOS PARA SEGURIDAD

3.2.1.1 HARDWARE

La línea de Cisco utilizada brinda alto performance, funcionabilidad, escalabilidad y flexibilidad que permite el incremento del uptime y la productividad de los empleados, la figura 3.2.1.1 muestra el esquema real de la implementación del firewall y la interconexión de todo el hardware en el cliente.

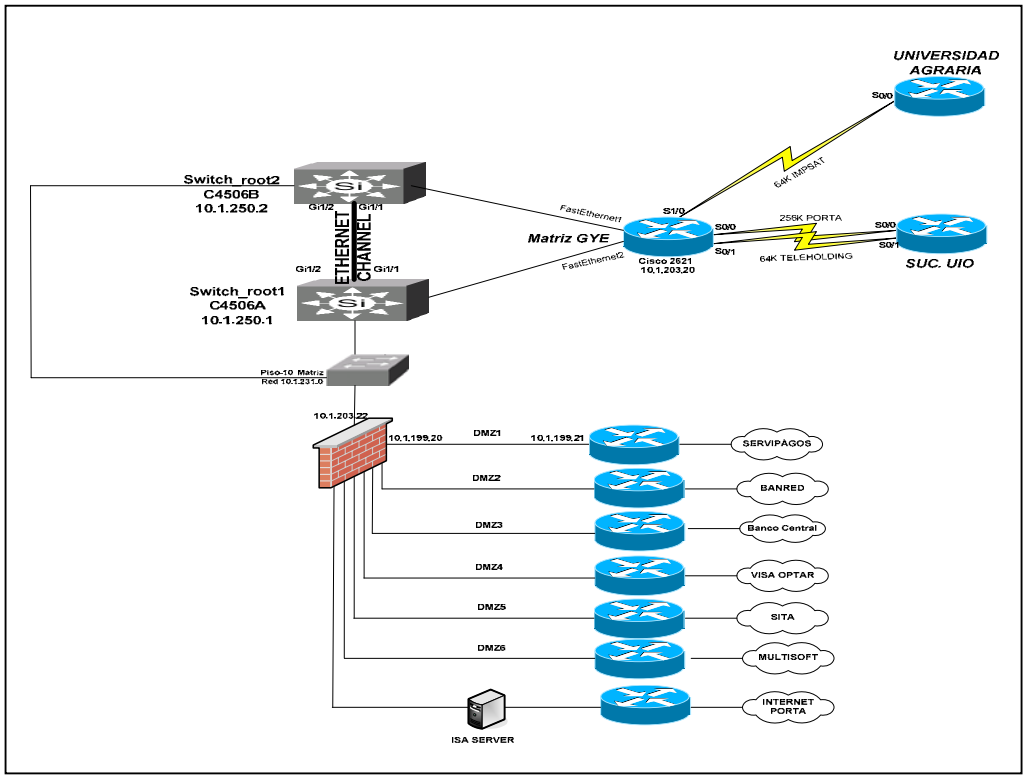


FIGURA 3.2.1.1 ESQUEMA DE IMPLEMENTACION DEL FIREWALL

3.2.1.2 ROUTERS

La serie Cisco 2600 figura 3.2.1.2 comparte las interfaces modulares con las series Cisco 1600 y 3600, ofreciendo una solución rentable para satisfacer las necesidades actuales de las oficinas remotas en aplicaciones tales como:

FIGURA 3.2.1.2 ROUTERS DE ACCESO MODULAR DE LA SERIE CISCO 2600

- Acceso seguro a Internet/intranet con firewall opcional
- Integración multiservicio de voz y datos
- Servicios de acceso analógico y digital por acceso telefónico
- Acceso a redes privadas virtuales (VPN)
- LAN virtuales (VLAN)

La arquitectura modular de la serie Cisco 2600 permite actualizar las interfaces para ajustarlas a la expansión de la red o a los cambios tecnológicos que se producen cuando se instalan nuevos servicios y aplicaciones. Mediante la integración de las funciones de los distintos dispositivos independientes en una sola unidad compacta, la serie Cisco 2600 reduce la complejidad de gestionar la solución para redes remotas. Equipado con un potente procesador RISC, la serie Cisco 2600 ofrece la potencia adicional necesaria para el soporte de avanzadas funciones de calidad de servicio (QoS) y de seguridad indispensables en las oficinas remotas de hoy en día.

La serie Cisco 2600 está disponible en seis configuraciones base:

- Cisco 2610: un puerto Ethernet
- Cisco 2611: dos puertos Ethernet
- Cisco 2612—Un puerto Ethernet, un puerto Token Ring
- Cisco 2613: un puerto Token Ring
- Cisco 2620: un puerto Ethernet 10/100 Mbps con autodetección
- Cisco 2621: dos puertos Ethernet con detección automática de 10/100 Mbps

Todos los modelos también tienen dos ranuras para tarjetas de interfaz WAN (WIC), una ranura para el módulo de red y una ranura

para un módulo de integración avanzada (AIM). Las tarjetas de interfaz WAN disponibles para los routers Cisco 1600, 1720, 2600 y 3600 ofrecen soporte para una amplia gama de opciones serie, ISDN (RDSI) de acceso básico y de unidad de servicio de canal/unidad de servicio de datos (integrated channel service unit/data service unit, CSU/DSU) para conectividad WAN principal y de respaldo.

Los módulos de red disponibles para las series Cisco 2600 y 3600 admiten una amplia gama de aplicaciones, incluyendo la integración multiservicio voz/datos, acceso por acceso telefónico analógico e ISDN (RDSI), y concentración de dispositivos serie. El módulo de integración avanzada para compresión de datos interno de la serie Cisco 2600 descarga del sistema la tarea de realizar compresión de datos a alta velocidad. Desde la CPU principal del 2600, que permite una transferencia de datos comprimidos de un máximo de 8 Mbps a la vez que preserva las ranuras externas de la interfaz para otras aplicaciones.

3.2.1.3 SWITCH

Descripción de Hardware

La infraestructura de hardware instalada en el cliente cuenta con dos equipos principales Switch Cisco Catalyst WS-4506 figura 3.2.1.3, los cuales poseen características tales como: avanzado mecanismo de manejo de Vlan, ruteo y calidad de servicio (QoS) este equipo modular (Figura 3.2.1.3) actualmente tiene una tarjeta WS-X4515 Supervisor engine IV con dos modulos WS-G5484—Cisco 1000BASE-SX Short-Wavelength GBIC (multimode only), 3 módulos WS-X4424-GB-RJ45—Cisco Catalyst 4500 24-Port 10/100/1000 (RJ-45), 2 fuentes redundantes.

Performance y Especificaciones de Supervisor Engine IV

- 64-Gbps nonblocking switch fabric
- 48-Mpps Capa 2 Forwarding (hardware)
- 48-Mpps Capa 3 y Capa 4 forwarding-IP routing, Cisco Express Forwarding-based (hardware)
- Capa 2–4 hardware-based switch engine (application-specific integrated circuit [ASIC]-based)
- Diseño centralizado

- Unicast and multicast routing entries: 131,072
- Capa 2 multicast addresses: 16,384
- MAC addresses: 32,768
- VLANs: 4096 soportadas en el hardware
- PVST
- Uplinks: Dual 1000-Mbps Gigabit Ethernet (Gigabit Interface Converter [GBIC])

La tabla 3.2.1.3 muestra las especificaciones técnicas

Especificaciones Técnicas:

Descripción	Especificación
Temperatura:	
Operando	32 to 104°F (0 to 40°C)
No operando y almacenado	–40 to 167°F (–40 to 75°C)
Humedad, Ambiente(no condensación):	
Operando	10 to 90%
No Operando y almacenado	5 to 95%
Altitud:	
Operando	–500 to 6500 ft (–150 to 2000 m)
No operando	–1000 to 30,000 ft (–300 to 9150 m)
Componentes del Switch:	
Backplane	64 Gbps full duplex
Microprocesador	Supervisor Engine IV: 333 MHz R5000 RISC
Memoria Supervisor engine	Supervisor Engine IV: SDRAM: 512 MB on board, 133 MHz, 64 MB Flash memory, 512 KB NVRAM

Características Físicas	
Dimensiones (HxWxD)	17.38 x 17.31 x 12.50 in. (44.13 x 43.97 x 31.70 cm)
Peso	Peso Mínimo: 56 lb (25.4 kg) Peso Máximo: 100 lb (45.4 kg)
Fuente de Poder	
AC-input tipo	Autoranging input with power factor corrector
AC-input voltage	100 to 240 VAC (10% for full range)
AC-input corriente	12 A @ 100 VAC, 5 A @ 240 VAC
AC-input frequencia	50/60 Hz (nominal) (3 Hz for full range)
Power supply output capacity	1000 W plus 40 W (fan)
Power supply output	12 V @ 83.4 A, 3.3V @12.2 A
Output holdup time	20 ms mínimo

TABLA 3.2.1.3 ESPECIFICACIONES TECNICAS

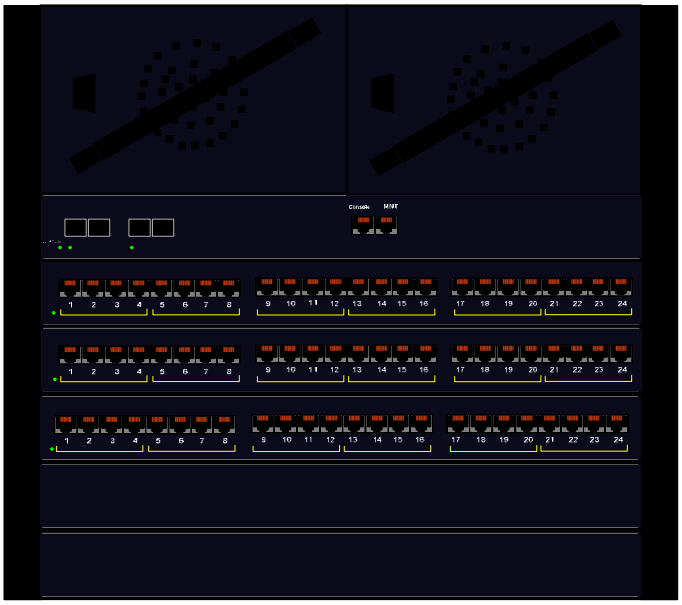


FIGURA 3.2.1.3 SWITCH CISCO CATALYST 4506

3.2.1.4 SERVIDORES

Para realizar la instalación del software Check point y el software de administración se requiere.

- 2 Servidores IBM Xseries modelo 206
- Procesador Pentium IV de 2.8Ghz (800MHz FSB) con
- 1MB de Cache L2. Single Processor. Memoria de
- 512MB expandible a 4GB (PC2700 333MHz ECC DDRSDRAM).
- 16MB Video. Single Channel Ultra320 SCSI
- Controller. Disco de 36.4GB SCSI (10000 rpm).
- Onboard Ethernet 10/100/1000. CD ROM 48X -20X y
- diskettera. 7 Bahías (4 disponibes) y 5 Slots (5
- disponibles).

- 2 módulos de memoria 512MB PC2700 CL2.5 ECC DDR SDRAM UDIMM (Para xSeries 206).

- 2 Monitores IBM 15" standard

3.2.2 SOFTWARE

3.2.2.1 CHECK POINT

Productos de Software Check Point

Check Point Express

SC3-250-NG

Check Point Express, 250 usuarios, Incluye SmartCenter Express Management, one VPN-1 Express Gateway protecting 250 users, SmartDefense and VPN-1 SecuRemote users

Provee seguridad corporativa completa para organizaciones de hasta 250 usuarios.- Incluye SmartCenter para gestión de la política de seguridad para 3 sitios o puntos de reforzamiento; y un gateway VPN-1 Express. Este último comprende a su vez el módulo de protección Firewall-1.

SS- CPXP-SC3-250

Suscripción de Software1 Check Point Express, 250 usuarios.

Suscripción de Software de Check Point es un programa de soporte que brinda al usuario derecho de obtención en forma gratuita de upgrades de versión, paquetes de servicio (service packs) y mejoras parciales del software adquirido, sujeto a

disponibilidad por parte del fabricante, y durante el período de un año a partir de su fecha de licenciamiento o 90 días luego de su compra, lo que ocurra primero. No están incluidos los servicios de apoyo que eventualmente el cliente pueda requerir para incorporar a su producto las actualizaciones disponibles tipicamente éstos servicios pueden requerirse para migrar a una nueva versión mayor.

VPN-1 CLIENTE

25 **CPVP-VSR-NG**

VPN-1 SecuRemote

3.3 INSTALACION DE FIREWALL EN SERVER CLIENTE Y CARRIER

El proceso para la instalaciòn del software Chek Point es el siguiente:

Todo el software Check point puede ser instalado del CD de Check point.

Antes de instalar el producto software Check point, se verificará si la plataforma de software y hardware son apropiadas para el producto a instalar, como se indica en la tabla 3.3.1.

Requerimientos para una mínima instalación en Windows

Sistema Operativo	Windows NT y Windows 2000
Procesador	Intel Pentium II 300+ MHz o equivalente.
Espacio en Disco	40 Mbytes
Memoria	128 Mbytes
Interfase de Red	Todas las interfaces soportadas por el sistema operativo

TABLA 3.3.1 REQUERIMIENTOS MINIMOS BAJO WINDOWS

Comenzando la instalación bajo Windows

1.-Inserte el CD-ROM VPN-1/Firewall-1. El CD-ROM comienza automáticamente la instalación del programa Check Point. Si por alguna razón este no arranca automáticamente, ejecute el archivo setup.exe que está localizado en la ruta \wrappers\windows.

Se puede instalar VPN-1/Firewall-1 directamente del CD-ROM, o también puede copiar los archivos de instalación del CD –ROM a un directorio en su disco duro e instalar de allí.

2.- La ventana de bienvenida es desplegada, figura 3.3.1.

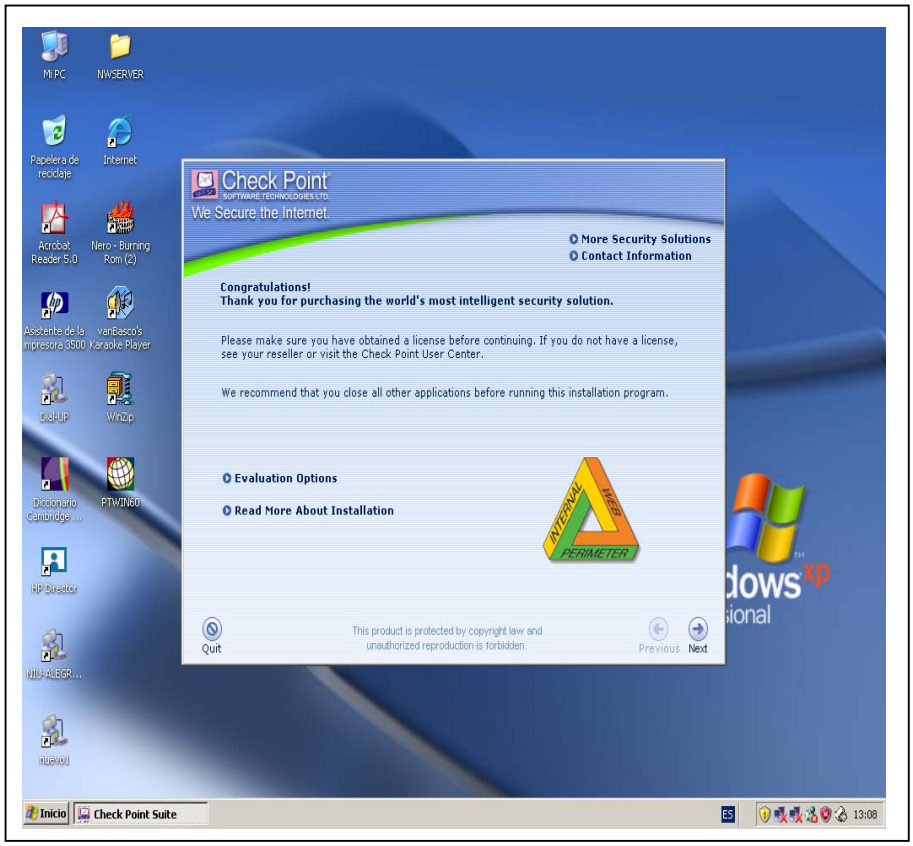


FIGURA 3.3.1 VENTANA DE BIENVENIDA

3.- Dar un Click en :

Next para desplegar la ventana del acuerdo de licencia y aceptar para proceder con la instalación.

4.- La ventana de acuerdo de licencia es desplegada, figura 3.3.2.

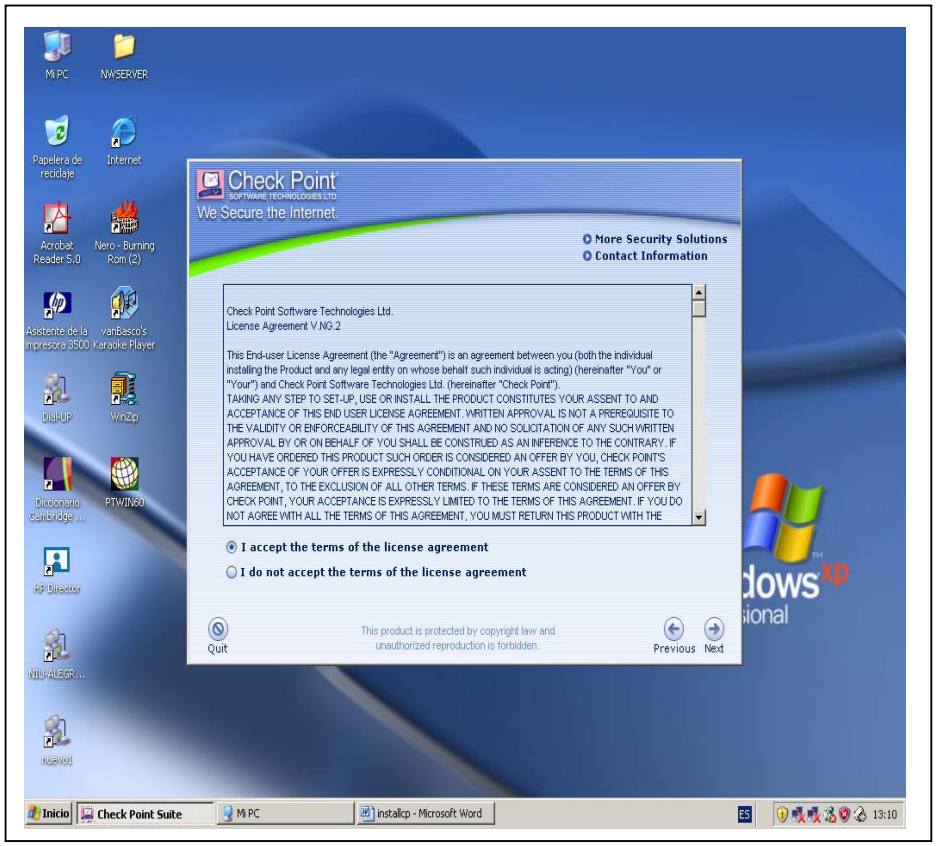


FIGURA 3.3.2 ACUERDO DE LICENCIA

5.-Antes de continuar debe aceptar todos los términos de licencia. Usted puede ver el texto del acuerdo de la licencia. Si usted escoge

no aceptar todos estos términos, pulse el botón NO y el procedimiento de la instalación terminará sin instalar ningún producto de Check Point.

6.- Realizar un click en:

Next para escoger el tipo de instalación, figura 3.3.3

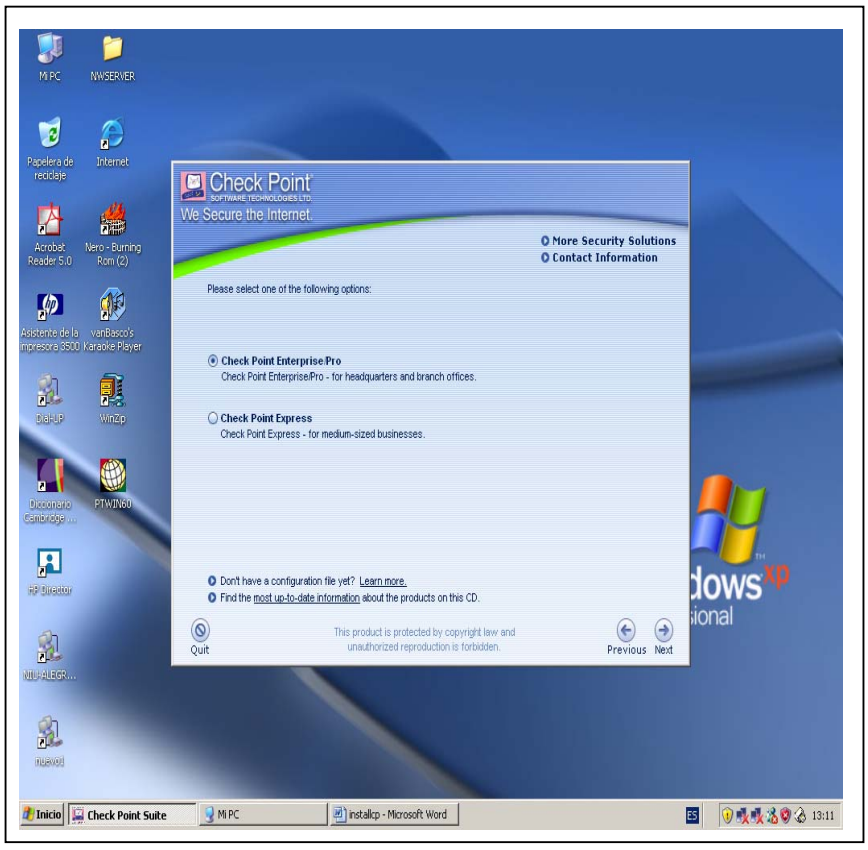


FIGURA 3.3.3 CHECK POINT ENTERPRISE PRO

7.- La ventana para seleccionar el tipo de instalación es desplegada.

Realizar un click en next para escoger el producto, figura 3.3.4.

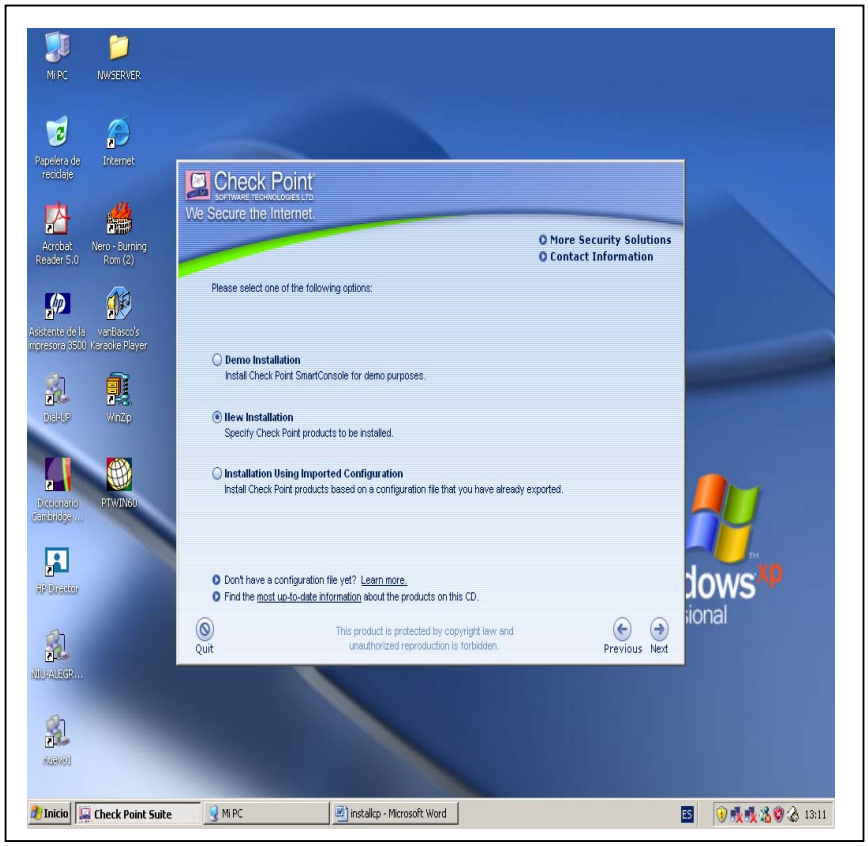


FIGURA 3.3.4 TIPO DE INSTALACION

8.- La ventana del Menú de Productos es desplegada, figura 3.3.5. Seleccione las siguientes opciones VPN-1 Pro, Smart, Center Smart Console y de click en next :

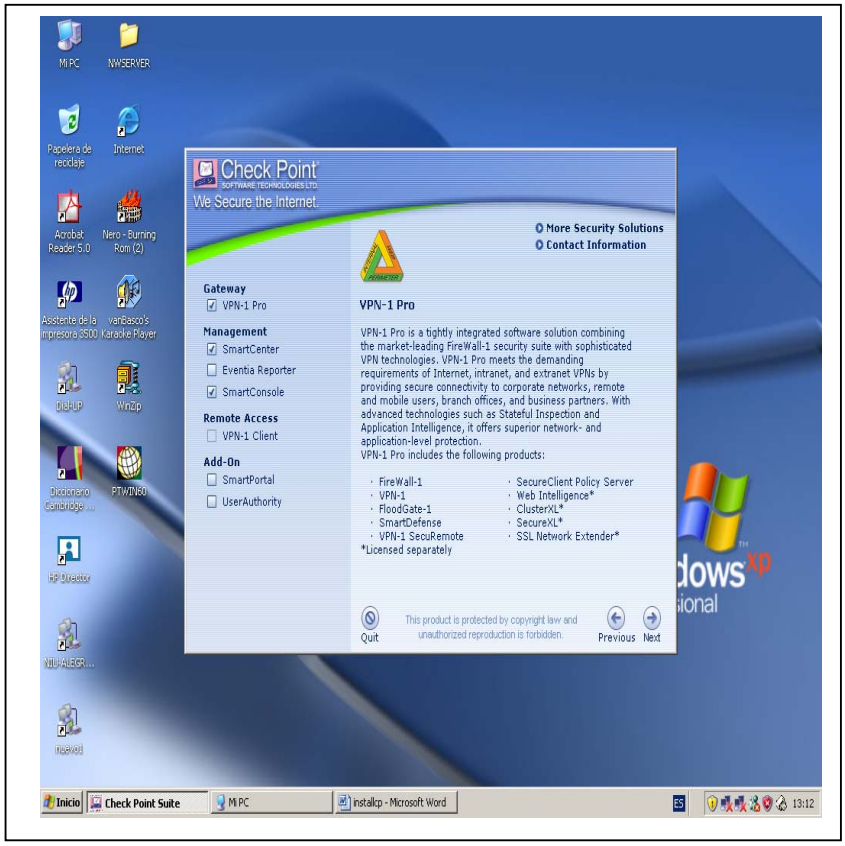


FIGURA 3.3.5 MENU DE PRODUCTOS

9.-Se escoge el tipo de smart center y se da un clic en next, figura 3.3.6.

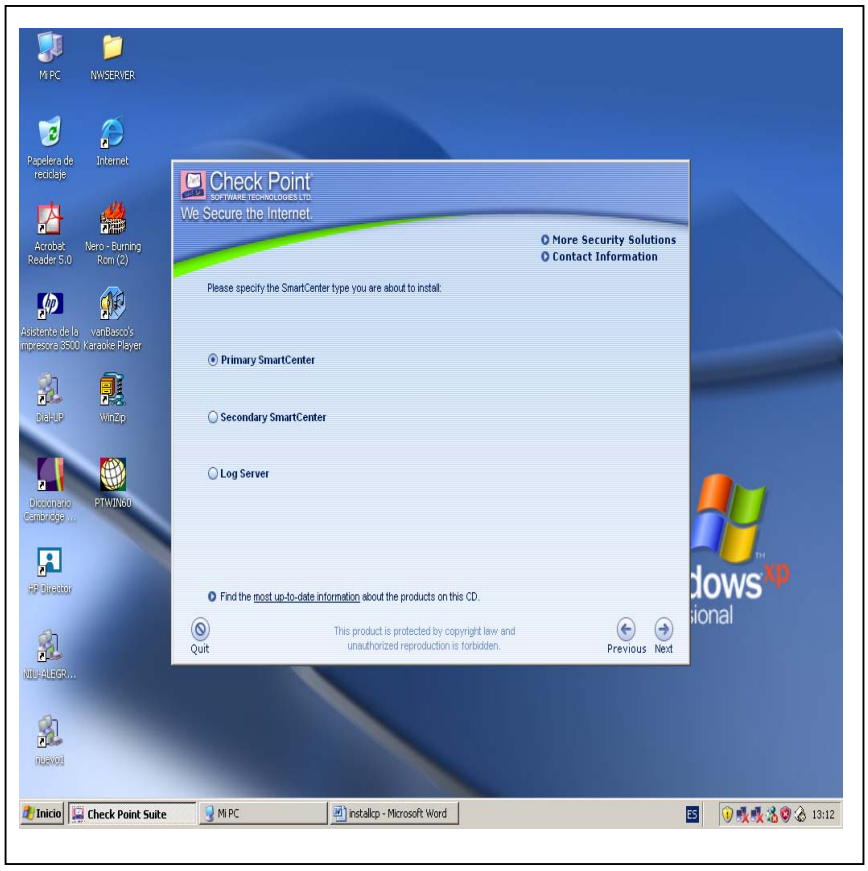


FIGURA 3.3.6 TIPO DE SMART CENTER

10.- La ventana de productos seleccionados es mostrada, figura 3.3.7. Se da click en next para seleccionar las carpetas donde se instalarán los productos.

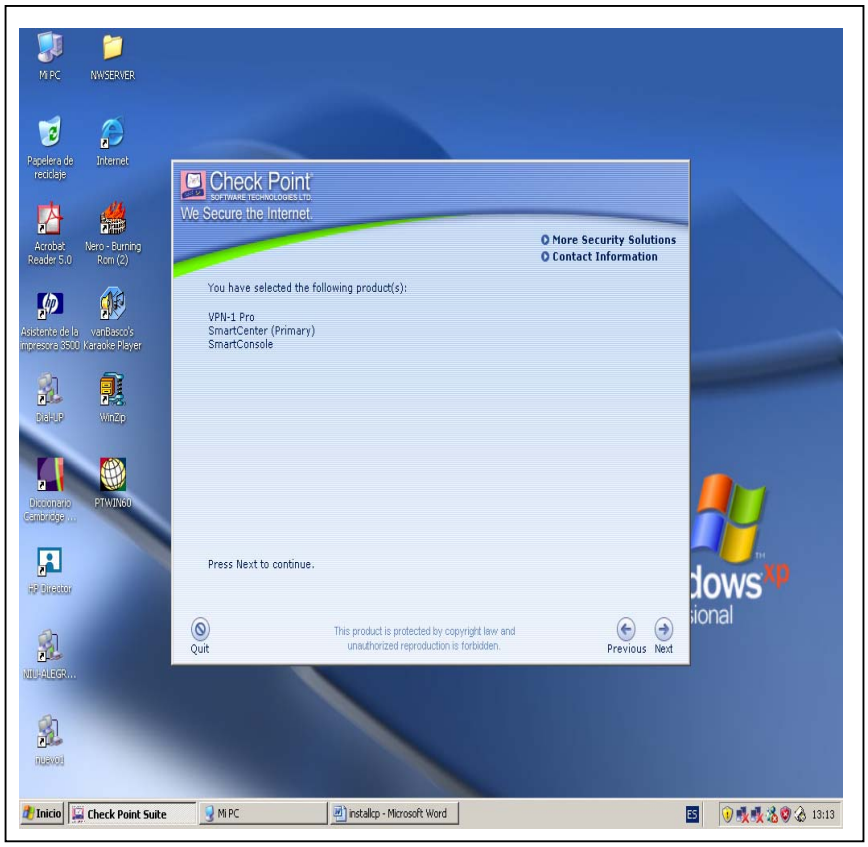


FIGURA 3.3.7 PRODUCTOS SELECCIONADOS

11.- El VPN1-PRO, se instalará en la siguiente carpeta, figura 3.3.8.

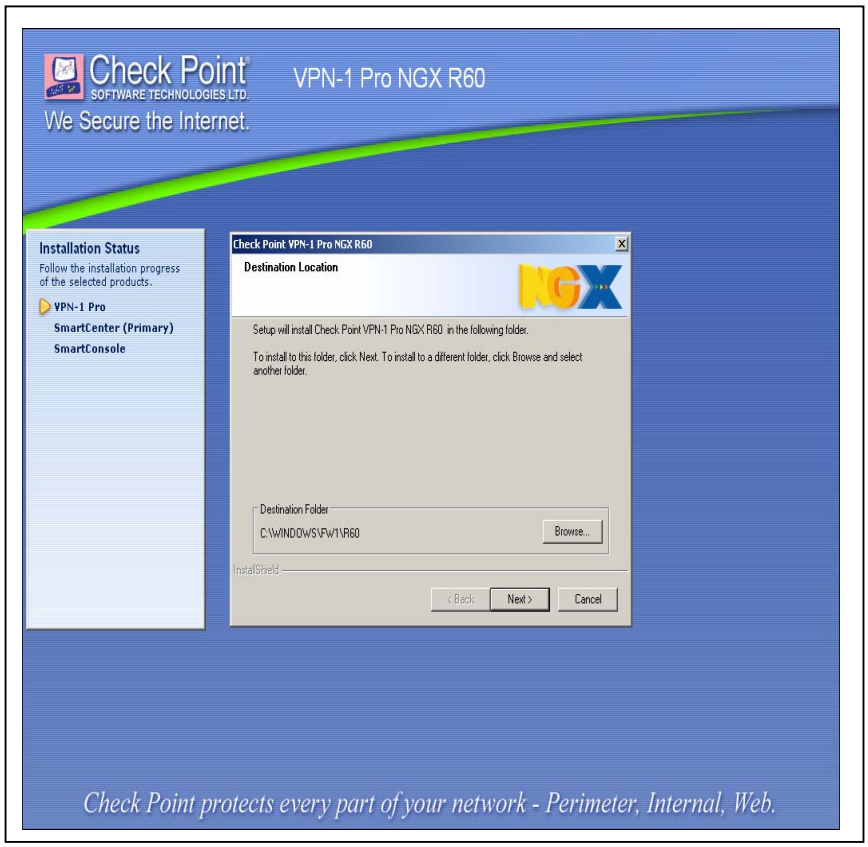


FIGURA 3.3.8 RUTA DE INSTALACION DEL VPN -1 PRO

12.- La figura 3.3.9 muestra la finalización de la instalación del VPN-1 Pro.

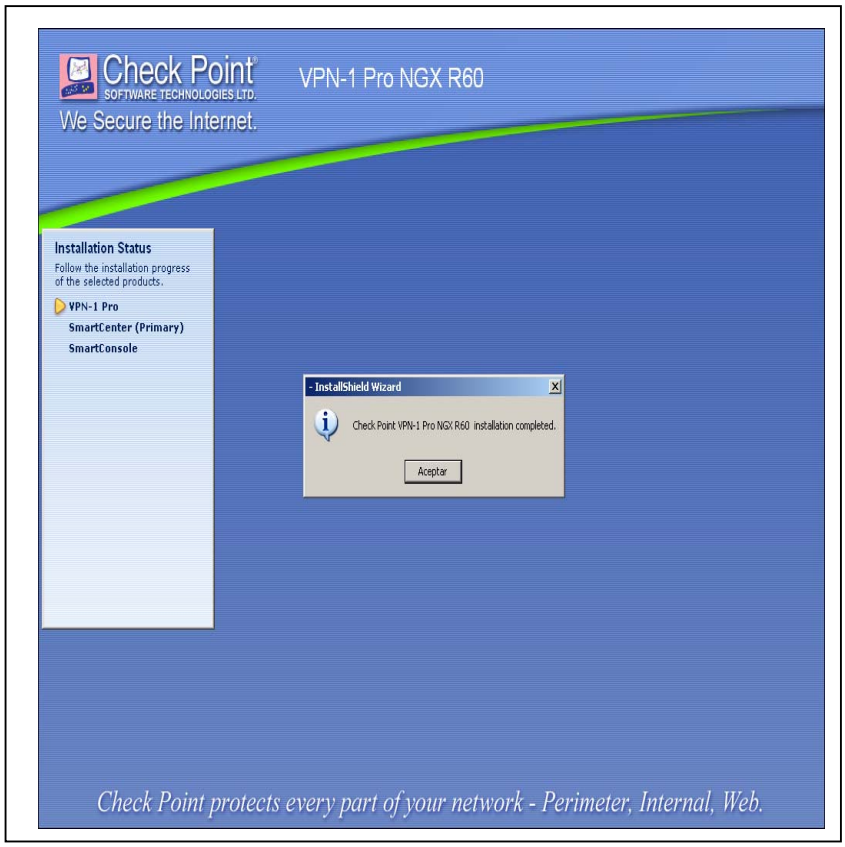


FIGURA 3.3.9 FIN DE INSTALACION DEL VPN -1 PRO

3.4 INSTALACION DE SOFTWARE DE ADMINISTRACION EN CLIENTE Y CARRIER

1.- Una vez finalizada la instalación del VPN-1 Pro, se despliega la ventana que muestra donde será instalado el smart console como se muestra en la figura 3.4.1. Luego se dará un click para continuar con la instalación.

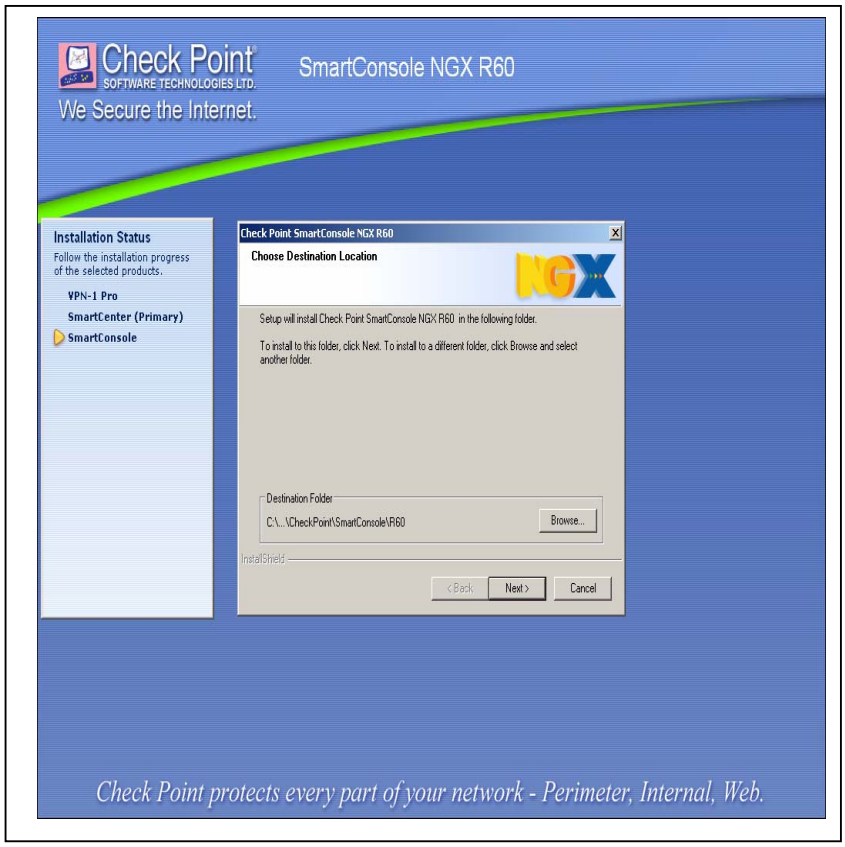


FIGURA 3.4.1 INSTALACION DEL SMART CONSOLE

2.- La figura 3.4.2 muestra los productos que serán instalados en el smart console

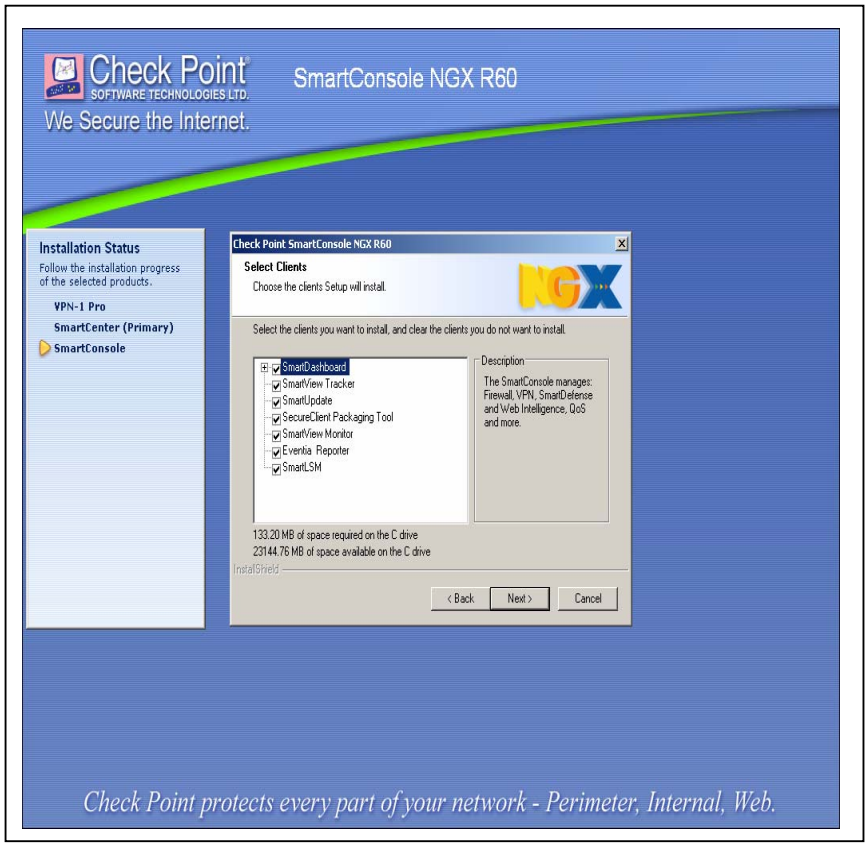


FIGURA 3.4.2 PRODUCTOS DEL SMART CONSOLE

3.- La figura 3.4.3, indica si se desea instalar un acceso directo en el escritorio.

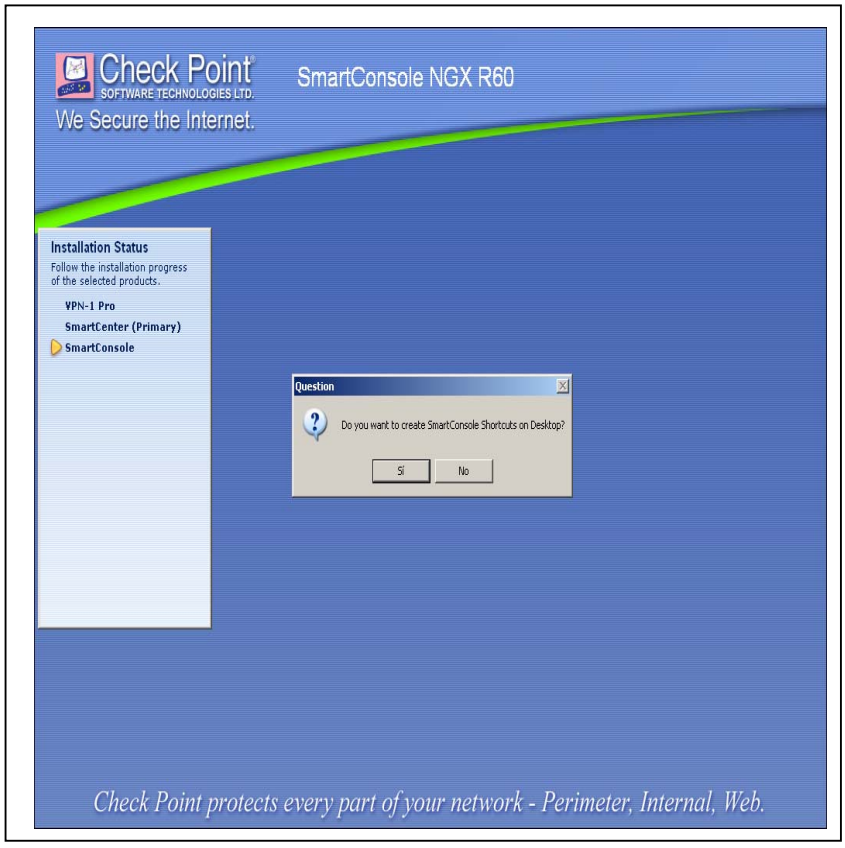


FIGURA 3.4.3 CREACION DE ACCESO DIRECTO DEL SMART CONSOLE

4.- La figura 3.4.4 indica que la instalación es satisfactoria.

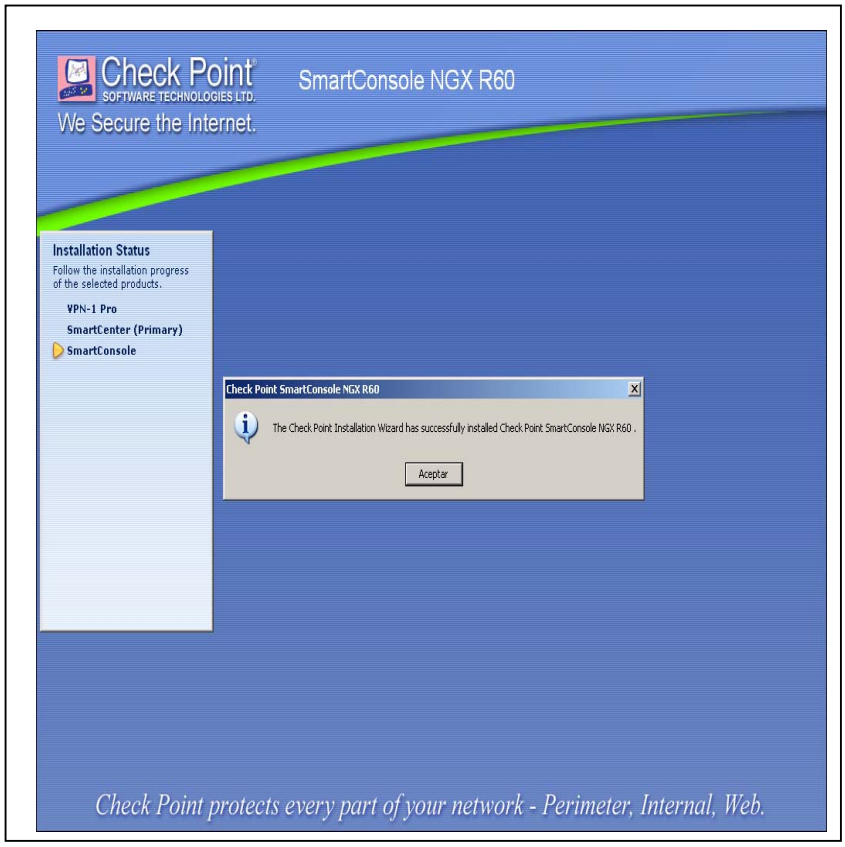


FIGURA 3.4.4 INSTALACION SATISFACTORIA

5.- La figura 3.4.5 muestra que la instalación del smart console ha finalizado.

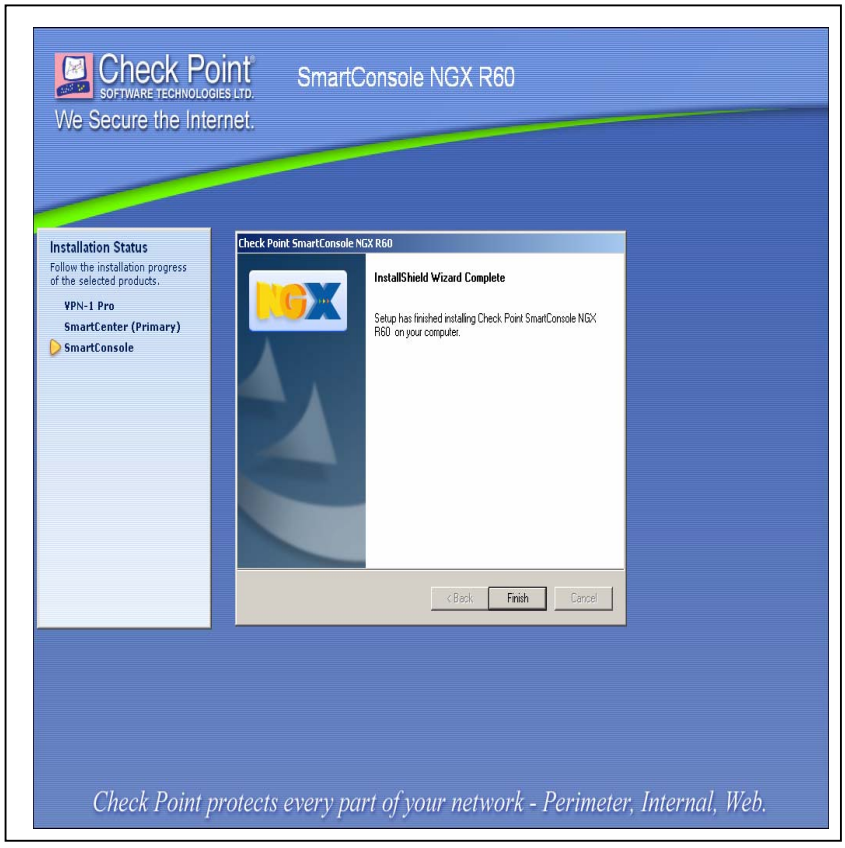


FIGURA 3.4.5 FIN DE LA INSTALACION DEL SMART CONSOLE

6.- La figura 3.4.6 muestra una petición de registro de contraseña de administrador y permisos.

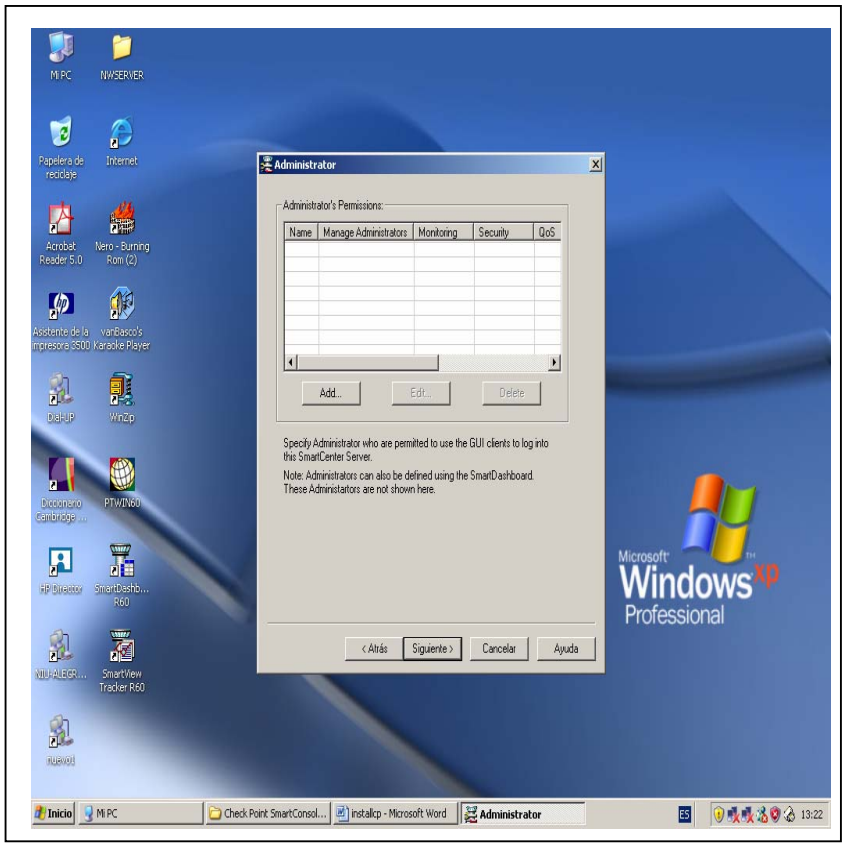


FIGURA 3.4.6 REGISTRO DE CONTRASEÑA DE ADMINISTRADOR

7.- La figura 3.4.7 muestra la ventana de ingreso del usuario y password de administrador.

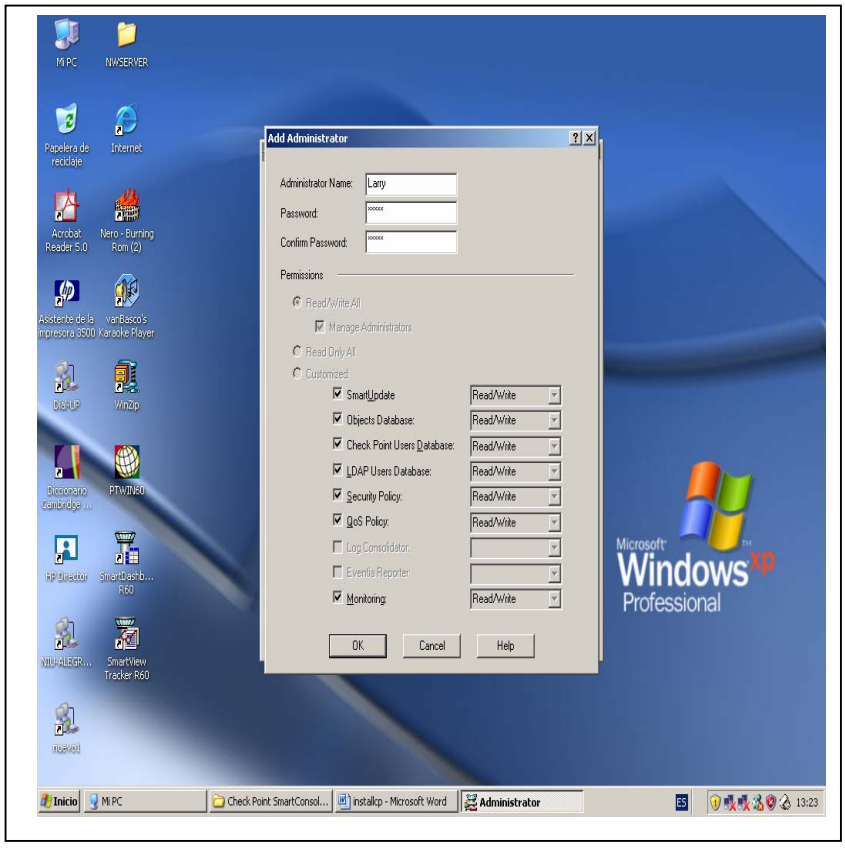


FIGURA 3.4.7 CONTRASEÑA DE ADMINISTRADOR Y PERMISOS

8.- La figura 3.4.8 muestra el ingreso del certificado autorizado para el uso de este software.

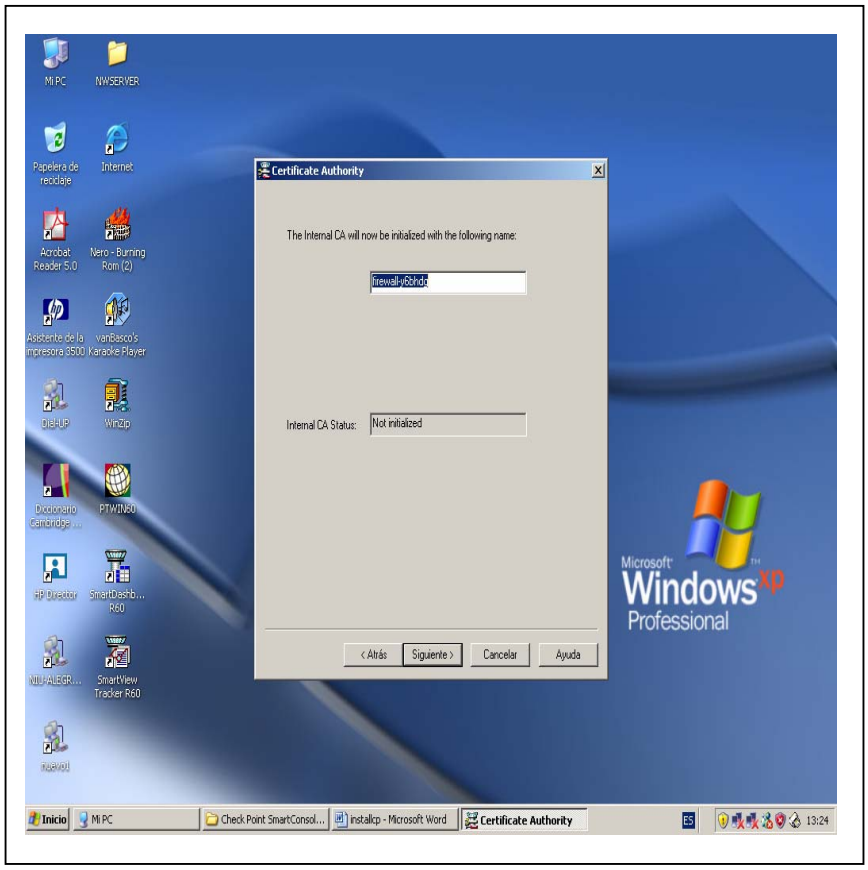


FIGURA 3.4.8 INGRESO DE CERTFICADO DE AUTORIZACION

9- La figura 3.4.9 muestra el final de la instalación del software check point.

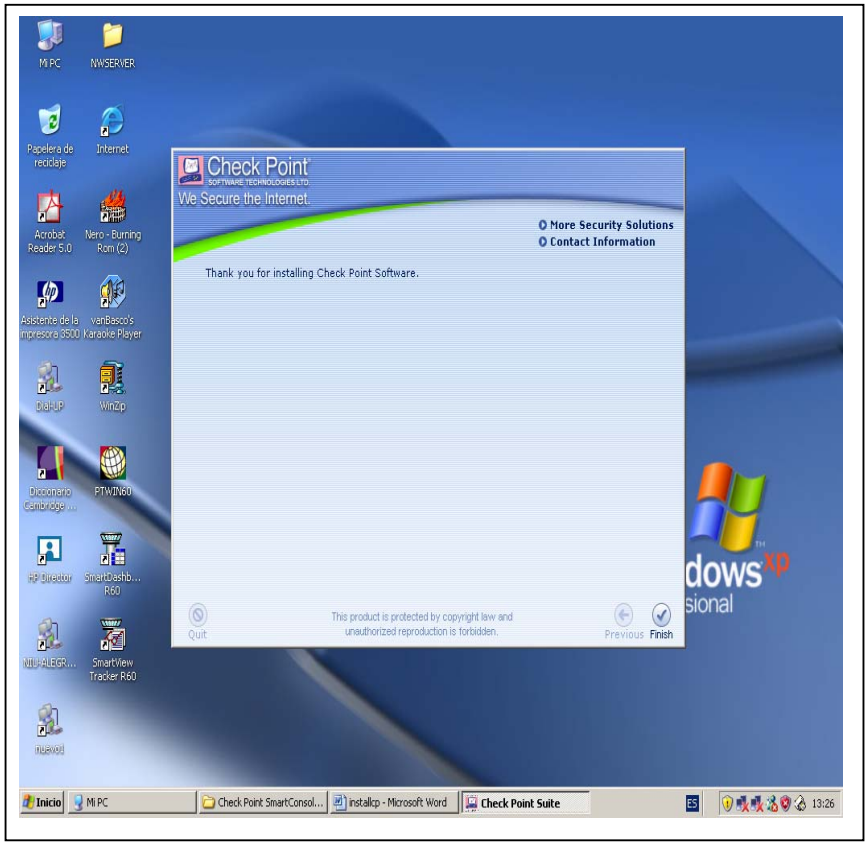


FIGURA 3.4.9 FIN DE LA INSTALACION DEL SOFTWARE CHECK POINT

3.5 CONFIGURACION DE NAT

PASOS GENERALES PARA LA CONFIGURACION DE NAT

Los pasos para la configuración de NAT:

1.- Determine la dirección IP para ser usada en la traslación.

2.- Definir los objetos de red.

3.- Definir las reglas de acceso en el Security Rule Base. Cuando se definen manualmente las reglas NAT, usted debería definir objetos de red con direcciones trasladadas, considerando que estas usando reglas de NAT automáticas, usted necesita definir un solo objeto de red por objeto real. Por ejemplo, si el NAT estático es definido sobre un objeto llamado Alaska_Web, entonces las reglas base de seguridad necesitan solo referirse sobre Alaska_Web (como en la tabla 3.5.1), y allí no es necesario definir una regla para Alaska_Web (Dirección válida).

Source	Destination	Action
Any	Alaska_Web	Accept

TABLA 3.5.1 REGLA BASE DE SEGURIDAD

4.- Definir reglas NAT (Automáticas o Manual)

5.- Instalar políticas de seguridad.

CONFIGURACION BASICA - NODO DE RED CON NAT OCULTO

El siguiente ejemplo muestra como preparar un NAT oculto básico para la configuración como se muestra en la figura 3.5.1. El objetivo es ocultar el IP address de Alaska_Web web Server (10.1.1.10) de conexiones que se originen en el Internet. Alaska_GW tiene tres interfaces, una de ellas conecta al Alaska_Web Server.

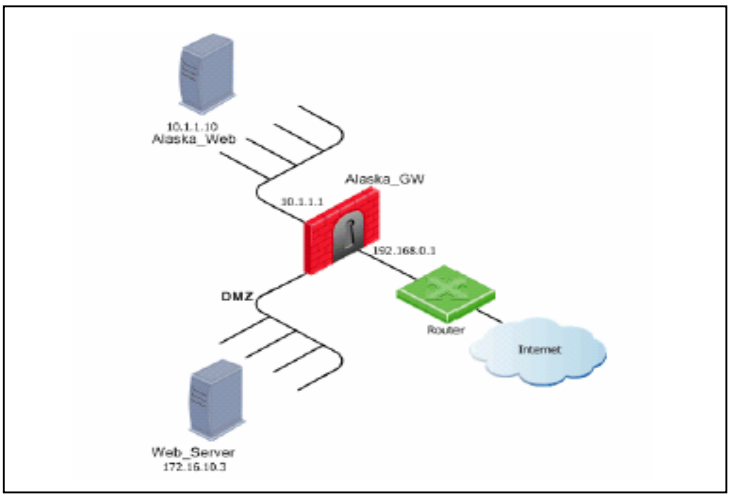


FIGURA 3.5.1 CONFIGURACION BASICA

Edite el nodo objeto para Alaska_Web, y en la página de NAT, seleccione Add Automatic address translation rules (figura 3.5.2).

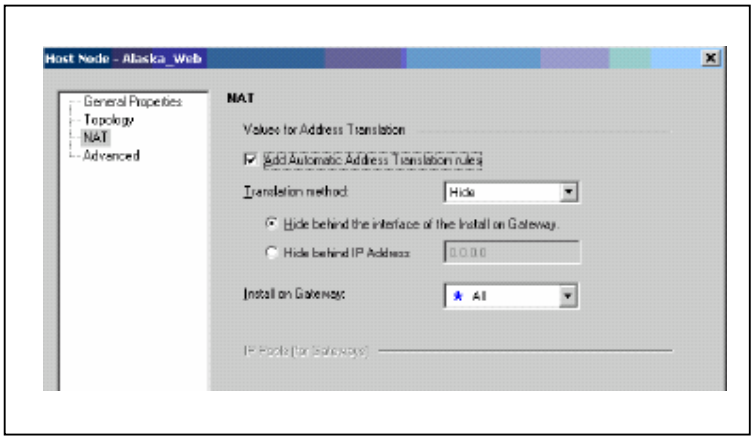


FIGURA 3.5.2 DIRECCION AUTOMATICA DE TRASLACION

Seleccione Translation Method Hide, y la opción **Hide behind the interface of the install on gateway.**

Seleccione el **Install on Gateway**. El NAT gateway en este ejemplo es Alaska_GW, también puede seleccionar cualquiera de los dos **Alaska_GW** or All

Los paquetes que se originan en Alaska_Web con destino la Internet, tendrán la dirección fuente trasladada de 10.1.1.10 a

192.168.0.1. Por ejemplo, los paquetes que se originan en el Web_Server siempre tendrán su dirección fuente cambiada de 172.16.10.3 a 192.168.0.1.

EJEMPLO DE CONFIGURACIÓN - STATIC AND HIDE NAT

La meta es hacer el SMTP Server y el http Server en la red interna disponible para el Internet usando direcciones públicas, y proporcionar acceso a Internet para todos los usuarios en la red interna, como se muestra en la figura 3.5.3.

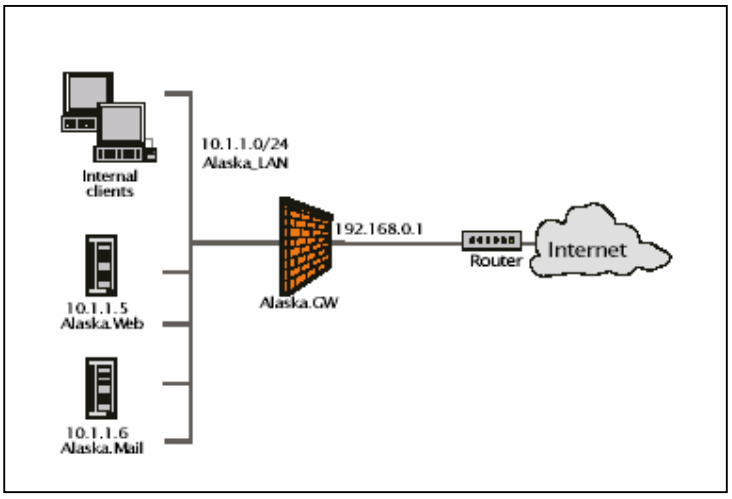


FIGURA 3.5.3 TRASLACION STATICA

El web y mail servers requieren traslación estática porque las conexiones entrantes serán hechas a ellos desde el Internet. Dos

direcciones ruteables están disponibles. La 192.168.0.5 será usada por el Alaska Web HTTPServer

Los clientes interiores requieren hide translation porque ellos iniciarán las conexiones. No se le permiten a ellos conexiones entrantes del internet. Ellos serán ocultos detrás de la interfase externa de los VPN-1 pro Gateway.

Defina objetos de red de Alaska Web (10.1.1.5), Alaska Mail (10.1.1.6), Alaska_LAN (10.1.1.0 con máscara 255.255.255.0), y la VPN-1 Pro Gateway (Alaska.GW).

Edite el objeto Alaska Web, y en la pàgina **NAT** chequee **Add Automatic Address Translation Rules**, seleccione **Translation Method** static, y defina el **Translate to IP Address** como 192.168.0.5

Similarmente para Alaska Mail, Select **Translation Method** static, y defina **Translate to IP Address** como 192.168.0.6

Edite el objeto Alaska_LAN, y en la página del NAT seleccione Translation Method hide, y seleccione **Hide Behind the interface of the install on gateway**. Las direcciones ocultas efectivas para los clients internos en Alaska_LAN son por consiguiente 192.168.0.1

La regla básica resultante de la dirección trasladada se muestra en la figura 3.5.4

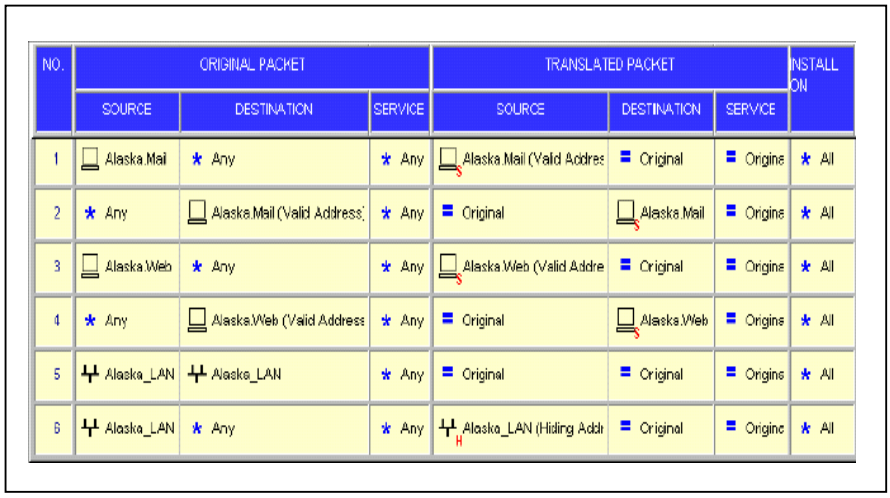


FIGURA 3.5.4 REGLA BASICA DE LA DIRECCION TRASLADADA

Ejemplo de Configuración - Usando reglas manuales de Port Translation

La meta es hacer una red DMZ disponible para web_Server y mail_Server, desde el Internet usando una sola dirección IP como se ilustra figura 3.5.5. El Nat oculto es realizado en todas las direcciones en la DMZ.

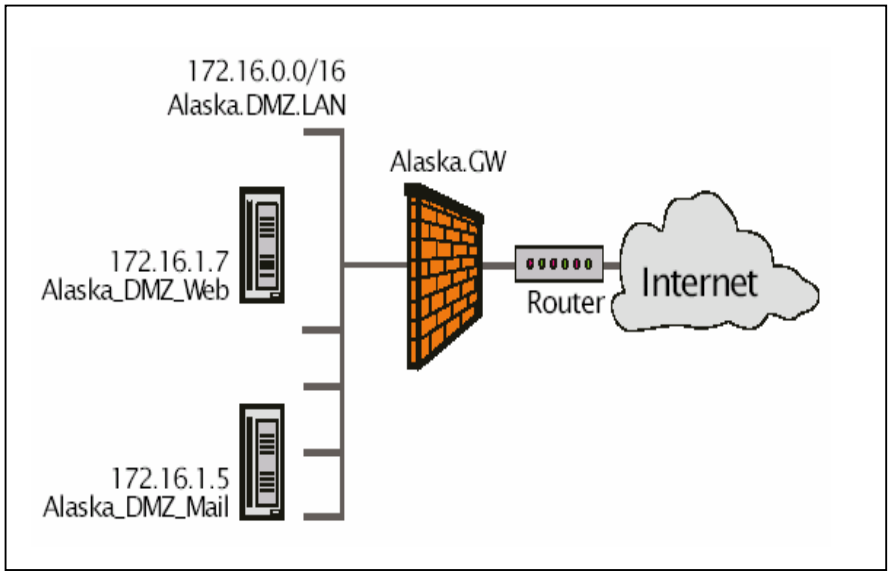


FIGURA 3.5.5 DMZ PARA CADA SERVIDOR

1. Defina un objeto de red para la red Alaska.DMZ.LAN (172.16.0.0 con mascara de red 255.255.0.0). el web Server Alaska_ DMZ_Web (172.16.1..7), y el mail server Alaska_DMZ_Mail (172.16.1.5), y la VPN-1 Pro Gateway (Alaska.GW).

2. En el objeto de red Alaska.DMZ.LAN, en la tabla **NAT**, seleccionar **Add Automatic Address Translation Rules**, y Translation Method Hide, y seleccionar Hide behind the interface of the install on Gateway. Esto agrega dos reglas automáticas a la dirección de la regla base de translación (Reglas 1 y 2 en la figura 3.5.6).

3. En la regla base de la dirección de traslación , defina una regla manual NAT, que traduce las demandas para el HTT Service para el Web Server (Regla 3 en la figura 3.5.6), y una regla manual NAT para trasladar SMTP se solicita al servidor SMTP (Regla 4 en la figura 3.5.6).

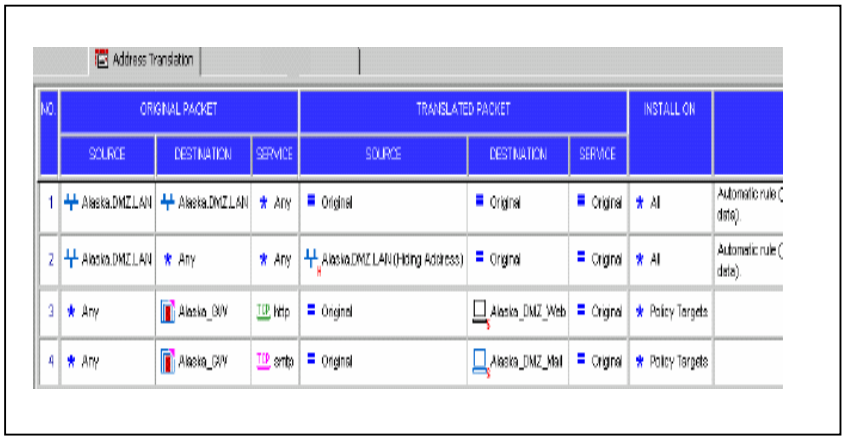


FIGURA 3.5.6 MAPA DE PUERTOS PARA REGLAS BASICAS DE TRASLACION

La figura 3.5.7 muestra la configuración NAT que tiene el cliente.

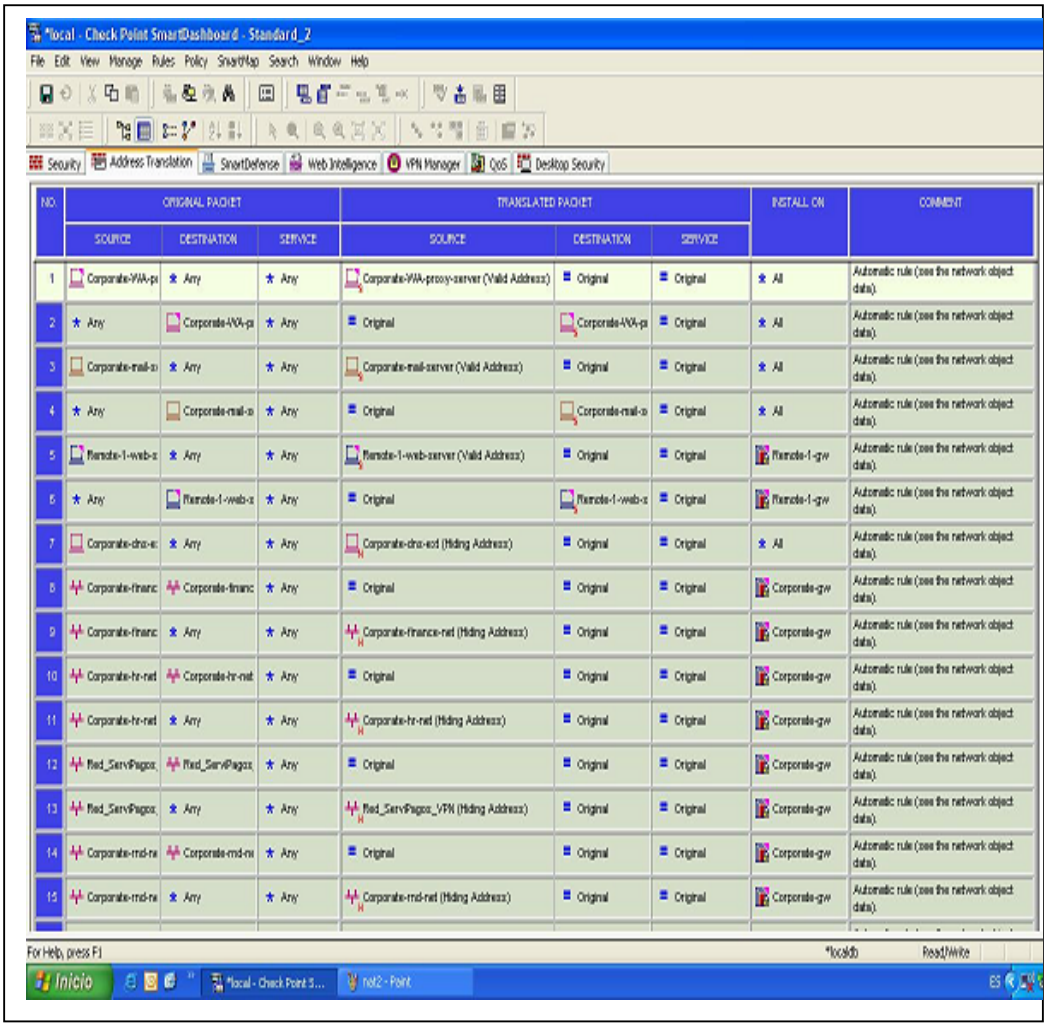


FIGURA 3.5.7 CONFIGURACION NAT DEL CLIENTE

La figura 3.5.8 muestra la configuración de una VPN realizada con un carrier y acceso remoto para los usuarios móviles.

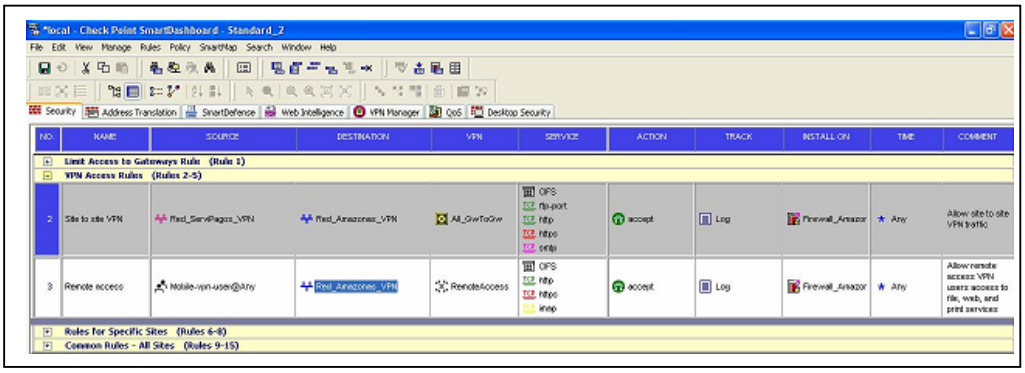


FIGURA 3.5.8 CONFIGURACION DE VPN DEL CLIENTE Y ACCESO REMOTO DE USUARIOS

3.6 CONFIGURACION DE POLITICAS DE SEGURIDAD

La Política de Seguridad es implementada definiendo un juego de reglas en la Security Rule Base. Una Política de Seguridad bien-definida es esencial para la VPN-1 pro para ser una solución efectiva de seguridad.

Los conceptos fundamentales de las Reglas Base de Seguridad son “Eso que no es explícitamente permitido se prohíbe”.

La Regla Base específica de comunicación permitirá pasar y bloqueará. Esta especifica la fuente y destino de la comunicación, qué servicios, pueden ser usados, en qué tiempo, se registró la conexión y en que nivel se registró. Repasando Los registros SmartView Tracker traffic son de aspecto muy importante para el administrador de seguridad y debería dársele una atención cuidadosa.

VPN-1 Pro trabaja inspeccionando paquetes de una manera secuencial. Cuando VPN-1 Pro recibe un paquete que pertenece a una conexión, lo compara contra la primera regla en la Security Rule Base, luego el segundo, luego el tercero, y así sucesivamente. Cuando encuentra un juego de reglas, deja de verificar y aplica esa regla. Si el paquete no encuentra un juego de reglas, entonces ese paquete se niega. Esto es importante para comprender que el primer juego de reglas es aplicado al paquete, no el paquete al mejor juego de reglas.

En la figura 3.6.1 se muestra una típica regla de Control de Acceso. Esta indica que las conexiones de HTTP que se originan de uno de grupo hosts de Alaska_LAN , a cualquier destino, son aceptadas.

FIGURA 3.6.1 REGLA DE CONTROL DE ACCESO

Una regla se compone de varios elementos Básicos como se indica en la tabla 3.6.1. No todos los campos siempre son pertinentes en una regla dada.

Fuente y destino	La fuente y destino es con respecto donde se origina la conexión. Para aplicaciones que trabajan en el modelo cliente servidor , la fuente es el cliente. Una conexión es aceptada, los paquetes en la conexión se permiten en ambas direcciones. Fuente y destino también pueden ser negadas. Usted puede encontrar por ejemplo conveniente especificar que la fuente no esté en una red dada.
Service	La columna de servicio permite especificar las aplicaciones predefinidas. También es posible definir nuevos servicios.

Action	Un paquete también puede ser Accepted, Rejected o Dropped. Otra posible acción se refiere a la autenticación. Si una conexión es Rejected, el firewall envía un paquete RST al origen de la conexión y la conexión es cerrada. Si un paquete es Dropped entonces no hay contestación de envío y la conexión se perderá.
Track	Varias opciones anotadas están disponibles.
Install-one	Especifica los gateways de las VPN que serán instalados en la regla. Allì no necesita una regla en particular para cada VPN. Por ejemplo, una regla puede permitir ciertos servicios de la red para cruzar un gateway en particular. Si estos servicios no son permitidos en las VPN gateways de otras redes, no es necesario instalar la regla en otros gateways.
Time	Especifica el tiempo y los días en que la regla debe ejecutarse.

TABLA 3.6.1 ELEMENTOS DE UNA REGLA

REGLAS IMPLICITAS

Las políticas de seguridad se componen de reglas. Aparte de las reglas definidas por el administrador, VPN-1 Pro también crea reglas implícitas, que son derivadas de las políticas de las propiedades globales. Las reglas implícitas son definidas por la VPN-Pro para permitir ciertas conexiones de los firewall con una variedad de diferentes servicios. Dos ejemplos importantes de estas reglas implìcitas son las que habilitan

- VPN-1 Pro Control Connections
- Paquetes salientes que se originan de las VPN-1 Pro Gateway

Hay también reglas implícitas para otros posibles formas de conexión.

VPN-1 Pro crea un grupo de reglas implícitas de las políticas de las propiedades globales, que es la primera antes de la última regla de seguridad básica definida por el administrador. Las reglas implícitas pueden ser registradas. Las reglas reglas por consiguiente son procesadas en el siguiente orden:

Primero se definen las reglas implícitas. Si es primero una regla implícita, la regla implícita no puede ser modificada o borrada en la regla base de seguridad., porque la primera regla es siempre aplicada al paquete, y ninguna regla puede estar antes que esta. El administrador define una regla explícita, a través de n-1 en la regla base (asumiendo n reglas).

Las reglas implícitas son listadas antes de la última. Configurando una propiedad antes de la última hace esto posible para definir mas detalles de reglas que cumplirá estas propiedades.

La última regla explícita es definida como (regla n).

La regla implícita es la última listada. Si una propiedad es última, esta es ejecutada después de la última regla en el Security Rule Base que normalmente todos los paquetes son desechados, y típicamente este no tendrá efecto.

Las figura 3.6.2 muestra la configuración de reglas implícitas en el cliente

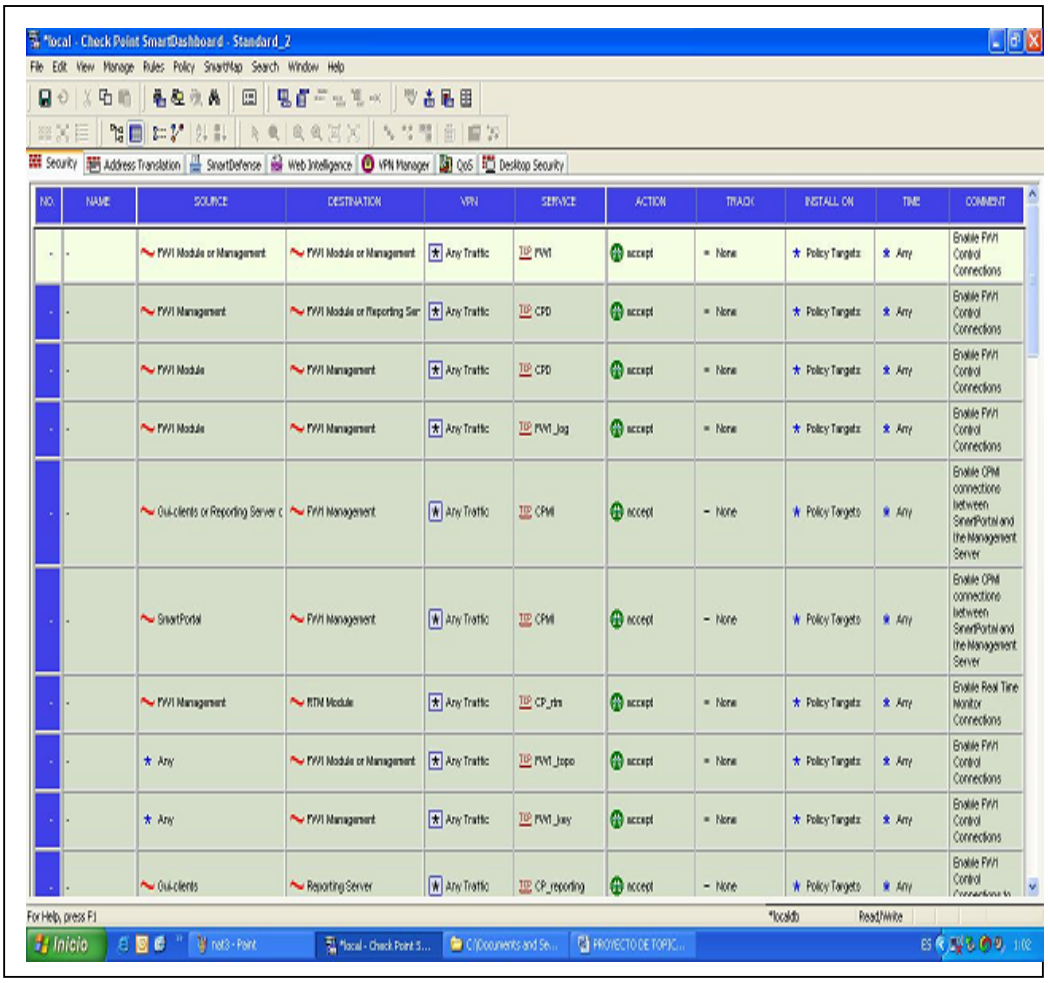


FIGURA 3.6.2 REGLAS IMPLICITAS DEL CLIENTE

CAPITULO IV

4. ANALISIS ECONOMICO

4.1 ANALISIS COSTO BENEFICIO

4.1.1 COSTOS

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

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

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

vez que se difunda mas esta tecnología serán muchas las empresas que la implementarán.

A continuación se detalla la Inversión que demanda la implementación de un Equipo de Seguridad Firewall

4.1.2 INVERSION

La tabla 4.1.1 muestran los costos generados por la inversión de equipos (hardware).

Descripción de Equipos (Hardware)	**CANTIDAD**	**PRECIO Unit Dolls**	**PRECIO Tot. Dolls**
Servidor IBM Xseriesmodelo 206	2	1700,00	3400,00
SERVICIOS:			
Capacitación, instalación y Configuración	2	1500,00	3000,00
TOTAL GASTOS			**6400,00**
IVA			**768,00**
TOTAL INVERSION HARDWARE			**7168,40**

TABLA 4.1.1: COSTOS DE LA INVERSION DE HARDWARE

La tabla 4.1.2 muestra los costos generados por el software e incluye los gastos por servicio que se paga por licencia de uso.

Descripción de Programa de Aplicación	CANTIDAD	PRECIO Unit Dolls	PRECIO Tot. Dolls
CPXP-SC3-250-NG	1	9500,00	9500.00
SS-CPXP-SC3-250	1	1600,00	1600,00
TOTAL GASTOS			**11100,00**
IVA			**1332,00**
TOTAL INVERSION SOFTWARE			**12432,00**

TABLA 4.1.2: COSTOS DE LA INVERSION DE SOFTWARE

La Tabla 4.1.3 muestra el costo total de la inversión para seguridad.

TOTAL INVERSION HARDWARE			**7168,00**
TOTAL INVERSION SOFTWARE			**12432,00**
COSTO TOTAL PARA LA INVERSION			**19600,00**

TABLA 4.1.3: COSTO TOTAL PARA INVERSION DE SEGURIDAD

4.2 Beneficios

Los Beneficios que se obtendrán para la Empresa producto de la implementación de un Sistema de Seguridad la resumimos a continuación:

- La Empresa estará respaldada en la integridad de sus datos por ese sistema implementado, dado que de no tenerlo le acarrearía que esos datos podrían ser intervenidos por usuarios externos.
- La Empresa acortaría o reduciría el tiempo de proceso y se tendría respuesta inmediata en solución de Problemas.

- La Empresa tendría una Ventaja Financiera ya que la Seguridad es imposible intervenir en transacciones que podrían darse de un cliente externo, sin la seguridad un hacker podría distorsionar datos que acarrearían problemas financieros a la empresa (Transacciones fraudulentas) .
- Mejoramiento de la Imagen de la Empresa, y eliminación de reclamos tanto de los clientes Internos como Externos.
- L a Empresa tendría Transacciones reales

CAPITULO V

5. DEMO

5.1 SIMULACION DE FIREWALL EN CLIENTE Y CARRIER

Para simular la seguridad a implementarse en este proyecto se utilizarán tres Pc´s, figura 5.1.1, los cuales van a representar el Firewall, el cliente y el carrier, se realizarán pruebas las cuales ilustrarán el funcionamiento del software de seguridad Check Point.

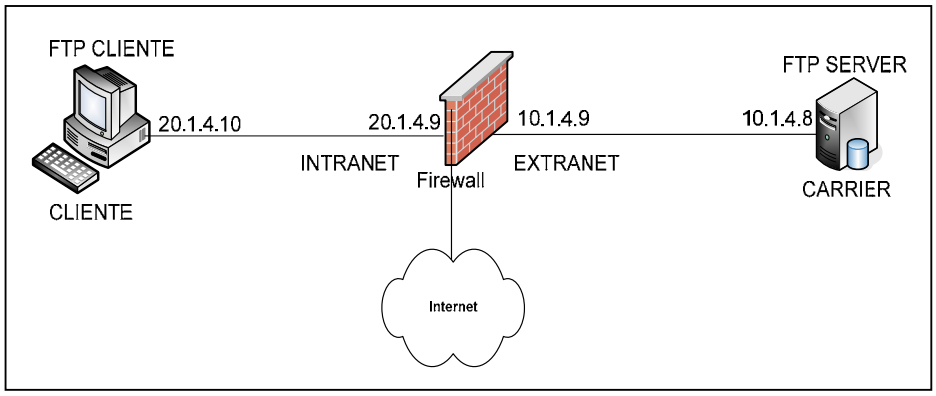


FIGURA 5.1.1 SIMULACION DE FIREWALL

EQUIPAMIENTO A UTILIZAR

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

IMPLEMENTACION DEL LABORATORIO

En el Pc Intel Pentium IV se procederá instalar las 2 tarjetas de red 10/100 Base T con las direcciones 10.1.4.9 - 20.1.4.9 y el software del Firewall Check point con sus componentes:

- VPN-1
- Smart Center
- Event Report
- Smart Console

En el Pc Intel Pentium III se va a instalar el software FTP Servidor, se le configurará a la tarjeta de red la dirección ip 10.1.4.8 con gateway 10.1.4.9 y se conectará mediante el cable cruzado a la tarjeta de red 10.1.4.9 del Firewall.

En el Pc Intel Pentium II se va a instalar el software FTP Cliente, se le configurará a la tarjeta de red la dirección 20.1.4.10 con gateway 20.1.4.9 y se conectará mediante un cable punto a punto al switch y este a su vez a la tarjeta de red 20.1.4.9 del Firewall.

PRUEBAS A REALIZAR

Se definirá en el Firewall reglas que permitan realizar ping y tener acceso del cliente al servidor y viceversa, ya que por omisión no se tiene estos permisos.

Se definirá en el Firewall reglas que activen y bloqueen permisos para realizar una transferencia de archivo desde el cliente.

PRUEBA Nº1

La regla por omisión figura 5.1.2, permitirá realizar un ping desde el Firewall al Cliente y al Servidor.

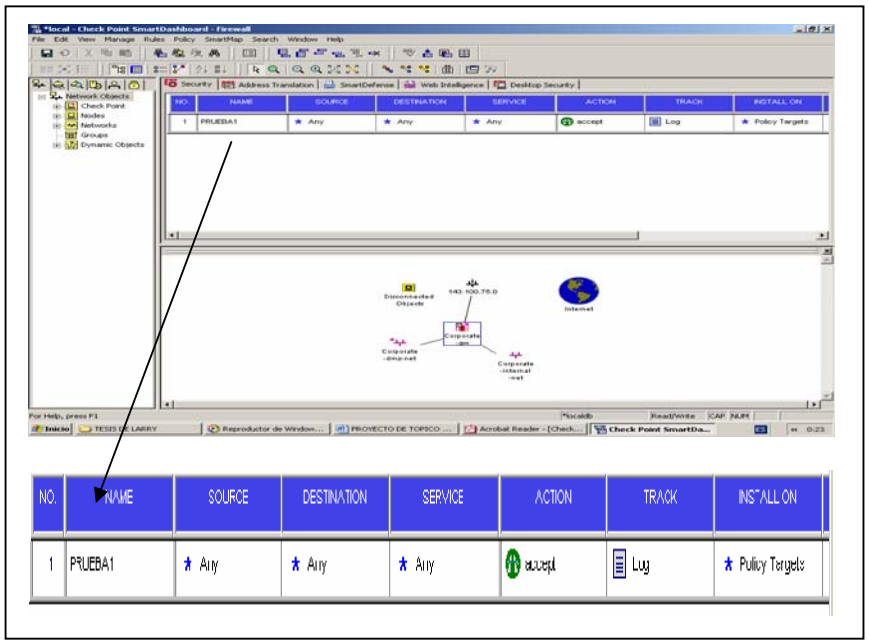


FIGURA 5.1.2 REGLA POR OMISION

PRUEBA Nº 2

Esta regla permitirà hacer un ping del cliente al server, ademàs se podrà tener acceso de la red del cliente a la red del server.

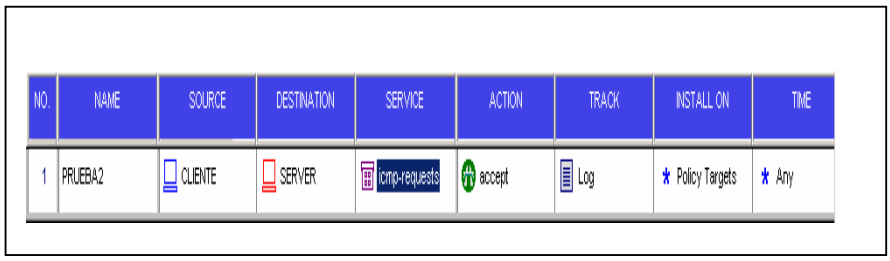


FIGURA 5.1.3 REGLA PING CLIENTE AL SERVER

PRUEBA Nº 3

Esta regla figura 5.1.4, permitirá hacer un ping del server al cliente, además se podrá tener acceso de la red del server a la red del cliente.

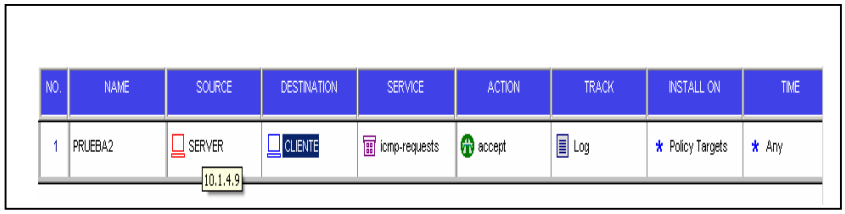


FIGURA 5.1.4 REGLA PING SERVER AL CLIENTE.

PRUEBA Nº 4

Esta regla figura 5.1.5, permitirá dar permisos para realizar una transferencia de archivo FTP del cliente al server, modificando la regla cambiando el servicio a DROP se negarán permisos a la red del cliente para realizar un FTP.

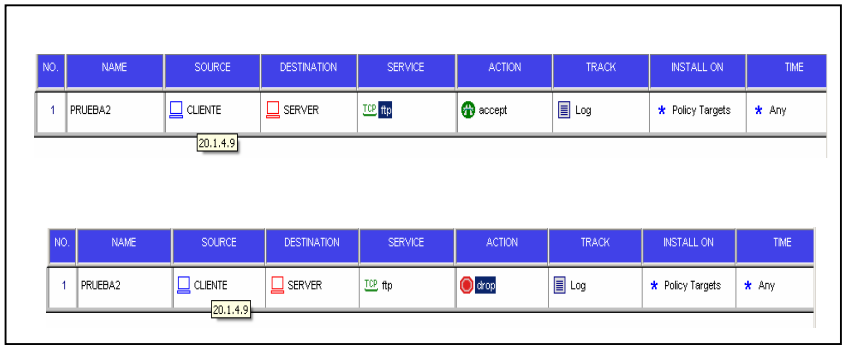


FIGURA 5.1.5 TRANSFERENCIA DE UN ARCHIVO FTP

CONCLUSIONES Y RECOMENDACIONES

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

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

A partir del hecho ya consumado que constituye la interconectividad a través de Internet, es fundamental la utilización de filtros debido a que seguramente nuestra organización estará también accediendo a los servicios que Internet nos ofrece. Qué arquitectura es la más apropiada

tendrá que ver seguramente con la criticidad de nuestros servicios, lo valioso de nuestra información, los servicios que ofreceremos y obtendremos de Internet, y de los recursos con los cuales contemos para llevar adelante este desafío.

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

BIBLIOGRAFIA

1. José Manuel Huidobro, Redes y Servicios de Telecomunicaciones
Paraninfo 2000, pp 272-284

2. William Stalling, Comunicaciones y redes de computadoras
Prentice Hall, 2002, pp 397-419

3. Check Point Software Technologies, Secure Virtual network getting started guide
Check Point Software Technologies, 2002, pp 102-122

4. Karanjit Siyan y Chris Hare, Internet y Seguridad en Redes,
Prentice Hall, 2000 pp 110-125.

ENLACES

1. Internet Routing Architectures. Bassam Halabi
   http://www.cis.ohio-state.edu/hypertext/information/rfc.html

2. Firewalls y seguridad en internet
   http://www.monografias.com

3. CheckPoint_NGX_Firewall_SmartDefense_User_Guide
   http://www.checkpoint.com/support/technical/documents/docs_r60.html