ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTAR POLÍTICAS DE SEGURIDAD A NIVEL DE HARDWARE Y APLICADO A UNA EMPRESA PEQUEÑA"

TESIS DE GRADO

Previa la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

- MAZORRA GRANJA MIGUEL ANGEL
- TOAPANTA BERNABÉ HÉCTOR JAVIER
- BRIONES SOLÓRZANO LIVINGTON LEONEL

GUAYAQUIL – ECUADOR

AÑO

2008

AGRADECIMIENTO

❖ **A NUESTROS PADRES**

Por el apoyo incondicional durante toda nuestra carrera.

❖ **A LA ESCUELA SUPERIOR POLITECNICA DEL LITORAL**
Por acogernos durante estos años.

❖ **A TODOS LOS PROFESORES**

Por sus enseñanzas y aportes a nuestra formación.

❖ **AL ING. JOSÉ ESCALANTE**

Director del Tópico de Graduación.

Por su ayuda y colaboración.

TRIBUNAL DE GRADO

Ing. Holger Cevallos

Presidente del Tribunal

Ing. José Escalante

Director del Tópico

Ing. Gómer Rubio

Miembro del Tribunal

Ing. Edgar Leyton

Miembro del Tribunal

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestos en esta tesis, nos corresponden exclusivamente; y la propiedad intelectual de la misma a la Escuela Superior Politécnica del Litoral". (Reglamento de Exámenes y Títulos profesionales de la ESPOL)

Miguel Angel Mazorra Granja

Héctor Javier Toapanta Bernabé

Livington Leonel Briones Solórzano

RESUMEN

Este proyecto tiene como objetivo general implementar una red de datos y aplicar todas las políticas de seguridad a nivel de hardware para evitar el acceso de usuarios no deseados a la red y que además sea un modelo de políticas de seguridad que se apliquen a empresas pequeñas.

En el primer capítulo se detallan las principales características del protocolo TCP/IP. Se describen algunas de las amenazas más comunes para las redes de datos y se exponen las tecnologías de seguridad para contrarrestar éstas. Además se mencionan herramientas para el monitoreo de las redes de datos tanto a nivel de hardware como software.

El segundo capitulo propone una forma de realizar el análisis para establecer las políticas de seguridad y luego se redactan dichas políticas a nivel de hardware que permitirán llegar al nivel de seguridad deseado.

El tercer capítulo es el caso de estudio realizado a una empresa pequeña. Se procede a evaluar de forma completa la posición de seguridad de la red mediante un análisis minucioso de sus dispositivos. Se resuelve qué políticas de seguridad implementar para lograr una protección superior contra las amenazas. Además se gestiona la seguridad a través de revisiones y

simulaciones periódicas para corroborar si los controles siguen siendo eficaces y apropiados.

En el cuarto capítulo se estiman los costos de la Implementación de las Políticas de Seguridad del Caso de Estudio y finalmente se hace un Análisis Costos / Beneficios.

Finalmente se incluyen las conclusiones, recomendaciones y anexos del proyecto.

ÍNDICE DE CAPÍTULOS

ÍNDICE GENERAL

ABREVIATURAS

1RU	One Rack Unit
2RU	Two Rack Unit
3RU	Three Rack Unit
3DES	Triple DES
A	
ACK	Acknowledgement
AES	Advanced Encryption Standard
AH	Cabecera de Autenticación
ARP	Address Resolution Protocol
ASA	Adaptive Security Algorithm
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
AVVID	Architecture for Voice, Video and Integrated Data
B	
BOOTP	Bootstrap Protocol
C	
CoS	Class of Service
D	
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DF	Don't Fragment
DMZ	Zona Desmilitarizada
DNS	Domain Name System
DoS	Denial of Service
Dst	Destino
E	
ESP	Encapsulating Security Payload
EUI	Extended Unique Identifier
F	
FDDI	Fiber Distributed Data Interface
FIN	Finalización
FOS	Finesse Operating System

FTP	File Transfer Protocol

H

HLEN	Header Length
HMAC	Hash Message Authentication Codes
HTTP	Hyper Text Transfer Protocol

I

IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IOS	Internetwork Operating System
IP	Internetwork Protocol
IPCOMP	IP Payload Compression Protocol
IPng	Internet Protocol Next Generation
IPsec	Internet Protocol Security
IPv4	Protocolo Internet versión 4
IPv6	Protocolo Internet versión 6
ISN	Números de Secuencia Iniciales
ISS	Internet Security Scanner

L

L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network

M

MAC	Media Access Control
MD5	Message Digest Algorithm 5
MTU	Maximum Transfer Unit

N

NAPT	Network Address Port Translation
NAT	Network Address Translation
NFS	Network File System

O

OOB	Out Of Band

P

PABX	Private Automatic Brach Exchange
PCI-X	Peripheral Component Interconnect Extended
PIN	Número de Identificación Personal

PIX	Private Internet eXchange
PMTUD	Path MTU Discovery
PPTP	Point to Point Tunneling Protocol
PSH	Push

Q

QoS	Calidad de Servicio

R

RARP	Reverse Address Resolution Protocol
RC	Recuperación de Claves
RFC	Request For Comments
RIP	Routing Information Protocol
RMON	Remote MONitoring
RSA	Rivest Shamir Adleman
RST	Reset

S

SA	Security Associations
SAD	Security Asocciation Databases
SC	Siguiente Cabecera
SEP	Procesamiento de cifrado Escalable
SHA	Secure Hash Algorithm
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SO	Sistema Operativo
SPI	Security Parameter Index
Src	Source
SSH	Secure SHell
SSL	Secure Socket Layer
SYN	Sincronización

T

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TNI	Translation Networks Inc
TOS	Type Of Service
TTL	Time To Live
TU	TCP – UDP ports

U

UDP	User Datagram Protocol
UPS	Suministro de Energía Ininterrumpible

URG	Urgente
URL	Uniform Resource Locator

V

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VPN SSL	Virtual Private Network SSL

W

WAN	Wide Area Network
WLAN	Wireless Local Area Network
WWW	World Wide Web

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: TECNOLOGÍAS

1.1 Arquitectura TCP/IP

1.1.1 Descripción

TCP son las siglas de "Transmission Control Protocol", mientras que IP significa "Internetwork Protocol". Esta es una arquitectura de red cuya operación, esta basada por supuesto en la conmutación de paquetes, pero no está compuesta por sólo dos protocolos, se trata de todo un conjunto "suite" de protocolos que están ligados y que constituyen la base del funcionamiento de Internet. Concretamente, IP es un estándar que subyace en todas las comunicaciones de la red. Incluye todas las especificaciones necesarias para hacer inteligible a cualquier máquina la información contenida en cada datagrama (paquete) transmitido. Entre otras, el tamaño normalizado de las cabeceras, remitente, códigos de control de integridad, etc. Uno de sus elementos más destacados, lo constituye un sistema universal y unificado para establecer las "Direcciones" de las computadoras de la red. A esto se le denomina Dirección IP ("Internet Protocol Address") [1].

En principio IP es el encargado de que la transmisión de los datos sea posible de una computadora a otra, mientras que TCP es el encargado de juntar los paquetes, pedir los que faltan (en su caso) y finalmente ordenarlos,

puesto que la Red no garantiza la llegada de todos los paquetes ni tampoco que su llegada sea en orden. En realidad, TCP se encarga de "negociar" con el equipo remoto determinados parámetros que determinan algunos detalles del modo en que se realizará la transmisión (por ejemplo el tamaño de los paquetes). Una comunicación en Internet es siempre un activo diálogo entre máquinas, incluso cuando aparentemente sólo se está "recibiendo" información, por ejemplo al descargar un archivo. En términos generales, el software TCP/IP está organizado en cuatro capas conceptuales.

La Figura 1.1 muestra el Esquema de las capas conceptuales de la Arquitectura TCP/IP.

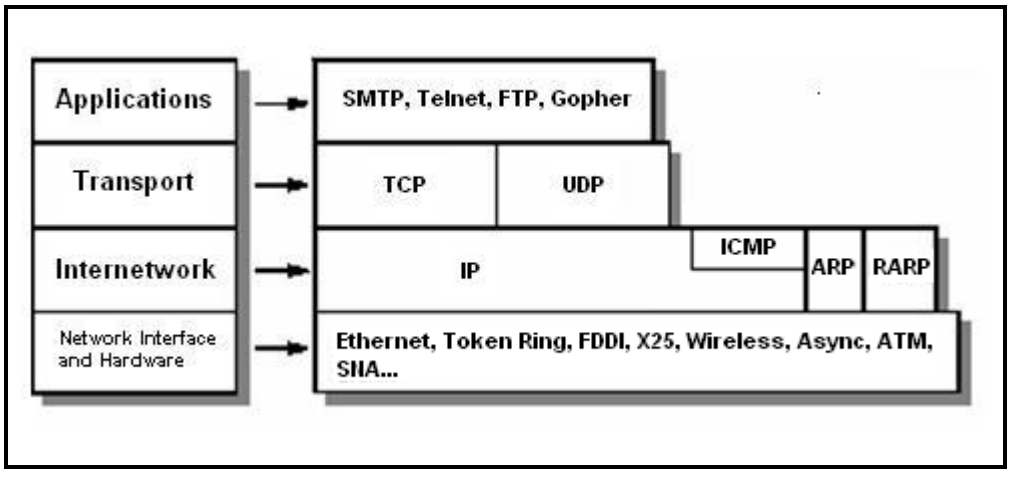


Figura 1.1 Esquema de la Arquitectura TCP/IP

Capa de Aplicación

Es el nivel más alto, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes TCP/IP. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continúo de octetos. El programa de aplicación pasa los datos en la forma requerida hacia el nivel de transporte para su entrega.

Capa de Transporte

La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el software de protocolo de transporte tiene el lado de recepción enviando acuses de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos. El software de transporte divide el flujo de datos que se está enviando en pequeños fragmentos (por lo general conocidos como paquetes) y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión. Aun cuando en el esquema anterior se utiliza un solo bloque para representar la capa de aplicación, una computadora de

propósito general puede tener varios programas de aplicación accesando a la red de redes al mismo tiempo. La capa de transporte debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel.

Para hacer esto, se añade información adicional a cada paquete, incluyendo códigos que identifican qué programa de aplicación envía y qué programa debe recibir, así como una suma de verificación para verificar que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar.

Capa Internet

La capa Internet maneja la comunicación de una máquina a otra. Esta contiene al protocolo IP y se encarga de aceptar una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. La capa Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo para decidir si el datagrama debe procesarse de manera local o debe ser transmitido. Para el caso de los datagramas diseccionados hacia la máquina local, el software de la capa de red de redes borra el encabezado del datagrama y selecciona, de entre varios protocolos de transporte, un protocolo con el que manejará el paquete. Por último, la capa Internet envía

los mensajes ICMP de error y control necesarios y maneja todos los mensajes ICMP entrantes.

Capa de Interfaz de Red

Es la capa inferior de la jerarquía de protocolos de TCP/IP y es equivalente a la capa 1 y 2 del modelo OSI (con algunas funciones de la capa 3). Hay muchos protocolos de acceso a la red (uno por cada estándar físico de red) y su función principal es encapsular Datagramas en Frames y mapear direcciones IP a direcciones físicas.

1.1.2 Protocolo IP

1.1.2.1 Protocolo Internet versión 4: IPv4

El protocolo IP (Internet Protocol) es la pieza fundamental en la que se sustenta el sistema TCP/IP [2], por tanto todo el funcionamiento de Internet.

La unidad de datos del protocolo IP es el datagrama, cuyo tamaño máximo es de 65535 bytes (64K).

El protocolo IP facilita un sistema ***sin conexión*** (connectionless) y ***no fiable*** (unreliable) de entrega de datagramas entre dos ordenadores cualesquiera conectados a Internet.

IP da un servicio de entrega basado en el ***mejor intento*** (best effort). Esto implica que cuando hay algún funcionamiento anómalo de Internet, como podría ser un router colapsado, se contempla un sistema muy simple de tratamiento de errores. Este mecanismo de control de errores viene regulado por el protocolo ICMP (Internet Control Message Protocol).

En nuestro caso, el router colapsado descartaría el datagrama y enviaría un mensaje de error ICMP al ordenador de origen sin encargarse de la retransmisión del datagrama [3], lo que ***no implica fiabilidad***.

Además, no mantiene ningún tipo de información referente al estado de las conexiones. Cada datagrama es encaminado de forma independiente, lo que le convierte en un ***protocolo sin conexión***.

Debido a estas particulares características, puede pasar que se pierdan datagramas y/o que estos no lleguen en orden. De esta manera, cualquier fiabilidad que se necesite, deberá ser realizada por las capas superiores (TCP...).

La estructura de un datagrama IP está dividida en bloques de 32 bits (4 bytes). El datagrama IP se transmite enviando primero el bit 0, luego el bit 1, 2, 3... y así sucesivamente hasta finalizar el datagrama. Este orden se denomina ***network byte order***. Es muy importante conocer este orden de transmisión de la información, puesto que los diferentes ordenadores tienen diferentes sistemas de almacenamiento de bits en memoria.

El formato little endian, consiste en almacenar los bits en orden inverso al network byte order (usando por ejemplo en los procesadores Intel), mientras que la otra posibilidad se denomina byte endian (usado por ejemplo en los procesadores Motorola). La Figura 1.2 muestra la Estructura del datagrama IP versión 4.

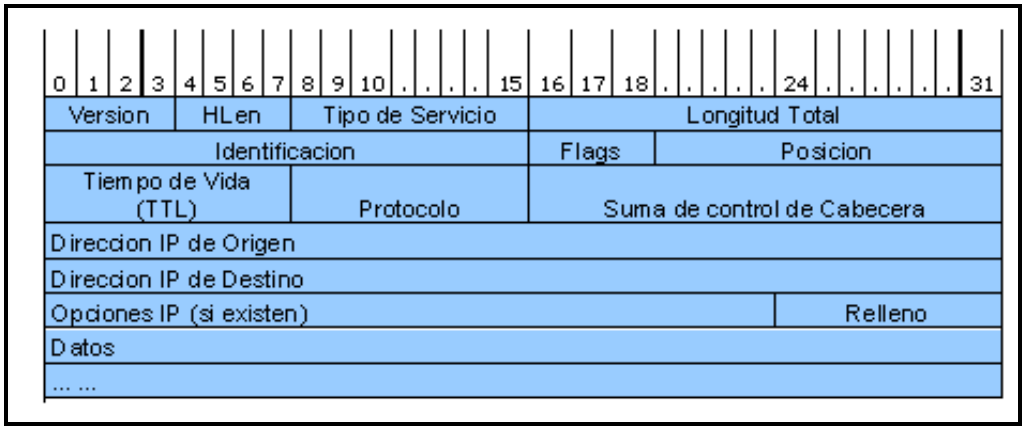


Figura 1.2 Estructura del datagrama IPv4

Versión

La versión (4 bits), sirve para identificar a que versión específica (RFC) hace referencia el formato del datagrama. Esta información sólo es utilizada por los routers [4] y capa IP de origen y final del datagrama. Esto permite la coexistencia de diferentes versiones del protocolo IP de una forma transparente al usuario. La versión actual es la 4 (conocida también cómo Ipv4).

Tamaño de la cabecera (Header Length)

El tamaño de la cabecera son 4 bits (2^4 = 16 posiciones, 0...15) que indican el número de palabras de 32 bits que ocupa la cabecera. Estos 4 bits de tamaño máximo nos limitan a un tamaño de cabecera máximo de 60 bytes (15 * 32 bits = 60 bytes). No obstante, el valor usual de este campo es 5 (5 * 32 bits = 20 bytes).

Tipo de servicio (TOS)

Este campo está formado por 8 bits y especifica el nivel de importancia que se le ha sido asignado a un paquete por un protocolo de capa superior en particular, la gran mayoría de los Host y Routers ignoran este campo.

La Figura 1.3 muestra la Estructura del campo de Tipo de Servicio.

Figura 1.3 Estructura del campo de Tipo de Servicio

La prioridad (0 = Normal, 7 = Control de red) permite implementar algoritmos de control de congestión más eficientes. Los tipos D, T y R solicitan un tipo de transporte dado: D = Procesamiento con retardos cortos, T = Alto Desempeño y R = Alta confiabilidad. Nótese que estos bits son solo "sugerencias", no es obligatorio para la red cumplirlo.

El tipo de servicio determina la política a seguir en el envío del datagrama por Internet. Las opciones posibles son:

1. minimizar el retraso (minimize delay).
2. maximizar el rendimiento (maximize throughput).
3. maximizar la fiabilidad del transporte (maximize reliability).
4. minimizar el coste económico del transporte (minimize monetary cost).

La Tabla 1.1 muestra los valores típicos de servicio según el tipo de aplicación.

Tabla 1.1 Valores típicos de servicio según la aplicación

Tipo de Aplicación	Minimizar retraso	Maximizar rendimiento	Maximizar fiabilidad	Minimizar costo	Valor en Hexadecimal
TELNET	1	0	0	0	0X10
FTP	0	1	0	0	0X08
SMTP	0	1	0	0	0X08
DNS (UDP)	1	0	0	0	0X10
DNS (TCP)	0	0	0	0	0X00
ICMP	0	0	0	0	0X00
BOOTP	0	0	0	0	0X00

La Tabla 1.2 muestra los Valores de Prioridad.

Tabla 1.2 Valores de Prioridad

Prioridad			
0	0	0	Rutina
0	0	1	Prioridad
0	1	0	Inmediato
0	1	1	Urgente (Flash)
1	0	0	Muy Urgente
1	0	1	CRITICO/ECP
1	1	0	Control entre redes
1	1	1	Control de red

La Tabla 1.3 muestra los diferentes Tipos de Transporte.

Tabla 1.3 Tipo de Transporte

	0	1
D (Retardo)	Normal	Baja
T (Desempeño)	Normal	Alto
R (Confiabilidad)	Normal	Alta

Longitud del datagrama (Total Length)

Es un número de 16 bits (2^16 = 65536, 0...65535) que indica la longitud total de todo el paquete IP en bytes, incluyendo los datos y el encabezado. Este valor es muy importante, ya que nos permite saber que tamaño de memoria debemos reservar para la recepción del datagrama. Para calcular la longitud de la carga de datos reste HLEN a la longitud total. Además, nos indica el número de bytes a leer, lo que nos permite un simple control de error. De esta forma, si el valor es incorrecto, el número de bytes leídos será como máximo de 65535, acotando el error. Además nos limita el número de bytes a enviar en un datagrama (Maximum Transfer Unit, MTU) a 65535 – 20 (tamaño típico de la cabecera) = 65515 bytes.

Si el ***tamaño del datagrama***, es mayor que el tamaño máximo del paquete de red (Ej. Datagrama de 32000 bytes enviado sobre una Ethernet, que tiene un tamaño máximo de paquete de 1500 bytes), éste se fragmenta en N trozos.

Identification Field

El número de identificación del datagrama (Identificartion Field), es un número de 16 bits que en caso de fragmentación de un datagrama nos indica su posición en el datagrama original. Esto nos permite recomponer el

datagrama original en la máquina de destino. Este valor nos indica que un datagrama puede ser fragmentado en un máximo de 65535 fragmentos.

Banderas (Flags)

Las banderas (Flags) son 3 bits. El primero permiten señalar si el datagrama recibido es un fragmento de un datagrama mayor, bit M (More) activado. El segundo especifica si el datagrama no debe fragmentarse, bit DF (Don't fragment) activado y el tercero no se utiliza actualmente, asignándole el valor 0.

Fragmentation Offset

El número de byte en el datagrama (Fragmentation Offset), nos indica la posición en bytes que ocupan los datos en el datagrama original. Sólo tiene sentido si el datagrama forma parte de uno mayor que ha sido fragmentado. Este campo tiene un máximo de 13 bits (2^13 = 8192, como nos indica el desplazamiento en bytes 8192 * 8 bits = 65536).

De esta forma, siempre se puede reconstruir el datagrama original con los fragmentos.

Time To Live

El tiempo de vida (Time To Live), es un campo de 8 bits que indica el tiempo máximo que el datagrama será válido y podrá ser transmitido por la red. Esto permite un mecanismo de control para evitar datagramas que circulen eternamente por la red (por ejemplo en el caso de bucles).

Este campo se inicializa en el host de origen a un valor (máximo 2^8 = 256) y se va decrementando en una unidad cada vez que atraviesa un router. De esta forma, si se produce un bucle y/o no alcanza su destino en un máximo de 255 “saltos”, es descartado. En este caso se envía un datagrama ICMP de error al ordenador de origen para avisar de su pérdida.

Protocol

El tipo de protocolo (Protocol), es un valor que indica a que protocolo pertenece el datagrama (TCP, UDP, ICMP...). Es necesario debido a que todos los servicios de Internet utilizan IP como transporte, lo cual hace necesario un mecanismo de discriminación entre los diferentes protocolos.

Header Checksum

El checksum de la cabecera del datagrama (Header Checksum), es una suma de comprobación que afecta sólo a la cabecera del datagrama IP. El resto de protocolos TCP, UDP, IGMP... tienen su propia cabecera y

checksum. Su función es simplemente la de un mecanismo de control de errores. De esta forma, si se encuentra un error en el checksum de un datagrama IP, este es simplemente descartado y no se genera ningún mensaje de error. Esto implica que es deber de las capas superiores el control del flujo de los datagramas para asegurarse que estos lleguen correctamente al destino, ya sea utilizando un protocolo fiable (TCP) o implementando internamente algún tipo de control.

Tanto la dirección IP de origen como la de destino (IP address), están formadas por dos números de 32 bits.

1.1.2.2 Protocolo Internet versión 6: IPv6

¿Qué es IPv6?

IPv6 (Internet Protocol Versión 6) o IPng (Next Generation Internet Protocol") es una nueva versión del protocolo IP, Ha sido diseñada por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4. En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características [5].

¿Por qué surge?

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidad al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades.

Características principales

Las características principales son las siguientes:

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar más niveles de jerarquías de direccionamiento y más nodos direccionables.
- Simplificación del formato del Header. Algunos campos del header IPv4 se quitan o se hacen opcionales.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.
- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara

de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.

- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad.

Formato de la Cabecera Básica

El tamaño de la cabecera que el protocolo IPv6 añade a los datos es de 320 bit, el doble que en la versión antigua. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior. Algunos campos se han retirado de la misma, mientras que otros se han convertido en opcionales por medio de las extensiones. De esta manera los routers no tienen que procesar parte de la información de la cabecera, lo que permite aumentar de rendimiento en la transmisión.

La Figura 1.4 muestra el Formato de la Cabecera Básica de IP versión 6.

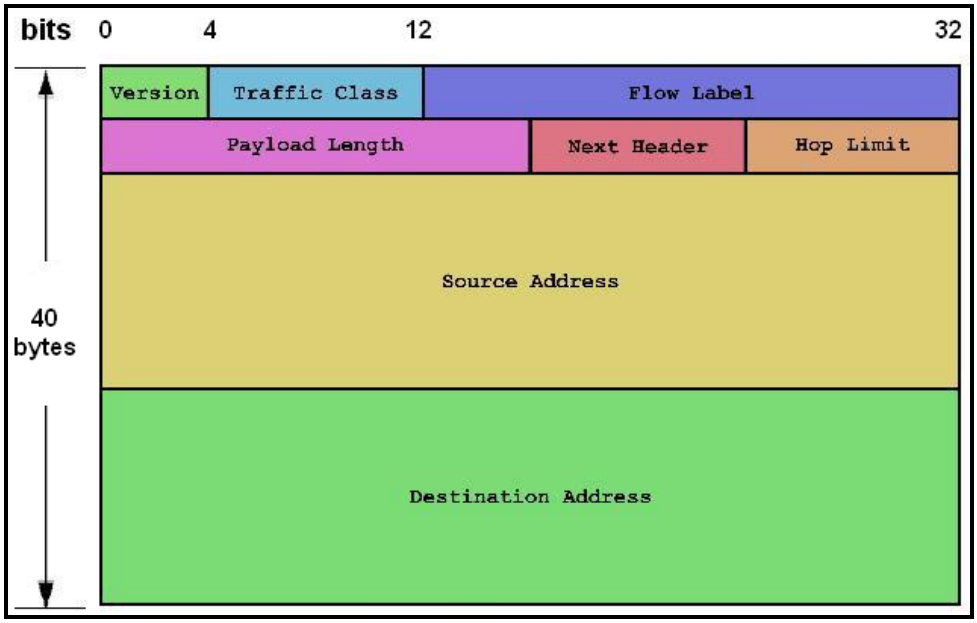


Figura 1.4 Formato de la Cabecera Básica IPv6

El formato completo de la cabecera sin las extensiones es el siguiente:

- **Versión:** Número de versión del protocolo IP, que en este caso contendrá el valor 6. Tamaño: 4 bits.
- **Class of Traffic (Prioridad):** Contiene el valor de la prioridad o importancia del paquete que se está enviando con respecto a otros paquetes provenientes de la misma fuente. Tamaño: 8 bits.
- **Flow Label (Etiqueta de Flujo):** Campo que se utiliza para indicar que el paquete requiere un tratamiento especial por parte de los routers que lo soporten. Tamaño: 20 bits.

- **Payload Length (Longitud de la Carga Útil):** Es la longitud en bytes de los datos que se encuentran a continuación de la cabecera. Tamaño: 16 bits.
- **Next Header (Siguiente Cabecera):** Se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el de protocolo en la versión 4 de IP. Tamaño: 8 bits.
- **Hop Limit (Límite de existencia):** Tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. Tamaño: 8 bits.
- **Source Address (Dirección de origen):** El número de dirección del host que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. Tamaño: 128 bits.
- **Destination Address (Dirección de destino):** Número de dirección de destino, aunque puede no coincidir con la dirección del host final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. Tamaño: 128 bits.

Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo

que supone una mejora en el rendimiento. Otra ventaja adicional es que el tamaño de la cabecera no está limitado a un valor fijo de bytes como ocurría en la versión 4.

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para routing extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

Datagrama IPv6

La Figura 1.5 muestra el Datagrama del Protocolo Internet versión 6 [6].

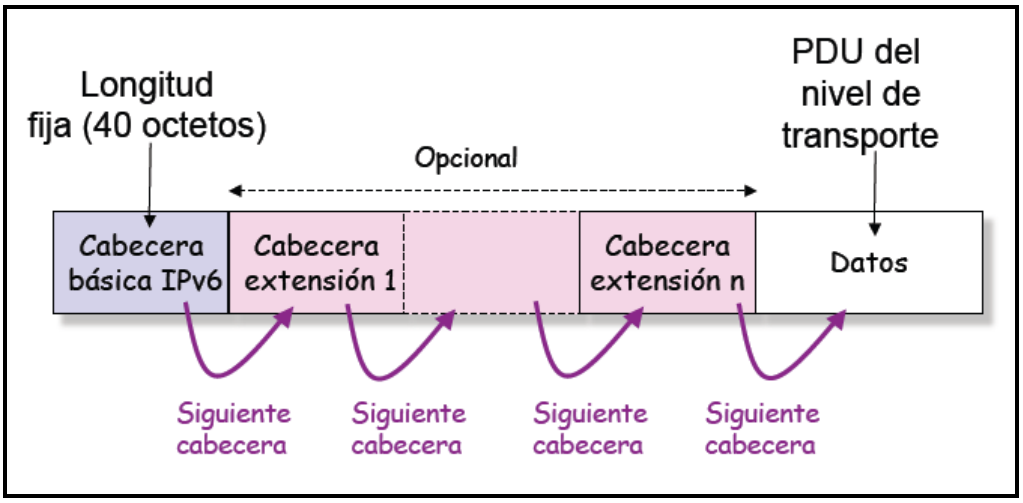


Figura 1.5 Datagrama IPv6

Campo Siguiente Cabecera

La Figura 1.6 muestra el Campo Siguiente Cabecera.

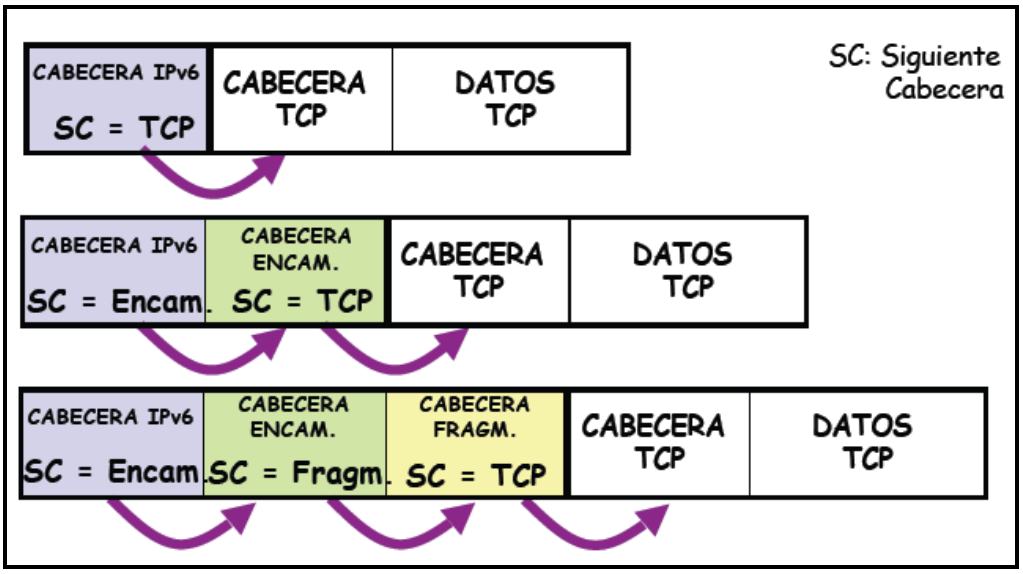


Figura 1.6 Campo Siguiente Cabecera

Direcciones en la versión 6

El sistema de direcciones es uno de los cambios más importantes que afectan a la versión 6 del protocolo IP, donde se han pasado de los 32 a los 128 bits (cuatro veces mayor). Estas nuevas direcciones identifican a un interfaz o conjunto de interfaces y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a éstos a través de su interfaz.

El número de direcciones diferentes que pueden utilizarse con 128 bits es enorme. Teóricamente serían 2^{128} direcciones posibles, siempre que no

apliquemos algún formato u organización a estas direcciones. Este número es extremadamente alto, pudiendo llegar a soportar más de 665.000 trillones de direcciones distintas por cada metro cuadrado de la superficie del planeta Tierra. Según diversas fuentes consultadas, estos números una vez organizados de forma práctica y jerárquica quedarían reducidos en el peor de los casos a 1.564 direcciones por cada metro cuadrado, y siendo optimistas se podrían alcanzar entre los tres y cuatro trillones.

Existen tres tipos básicos de direcciones IPng según se utilicen para identificar a un interfaz en concreto o a un grupo de interfaces. Los bits de mayor peso de los que componen la dirección IPng son los que permiten distinguir el tipo de dirección, empleándose un número variable de bits para cada caso [7].

Estos tres tipos de direcciones son:

- **Direcciones Unicast (Unidifusión):** Son las direcciones dirigidas a un único interfaz de la red. Las direcciones unicast que se encuentran definidas actualmente están divididas en varios grupos. Dentro de este tipo de direcciones se encuentra también un formato especial que facilita la compatibilidad con las direcciones de la versión 4 del protocolo IP. La Figura 1.7 muestra las Direcciones Unicast.

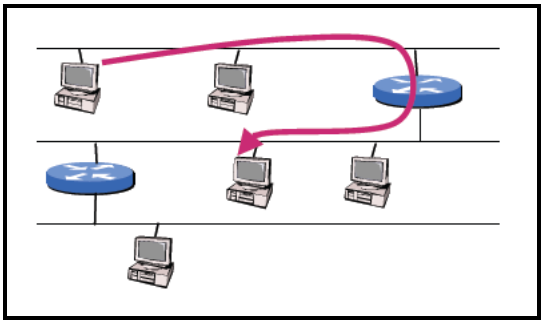


Figura 1.7 Direcciones Unicast

- **Direcciones Anycast (Cualquier difusión):** Identifican a un conjunto de interfaces de la red. El paquete se enviará a un interfaz cualquiera de las que forman parte del conjunto. Estas direcciones son en realidad direcciones unicast que se encuentran asignadas a varios interfaces, los cuales necesitan ser configurados de manera especial. El formato es el mismo que el de las direcciones unicast. La Figura 1.8 muestra las Direcciones Anycast.

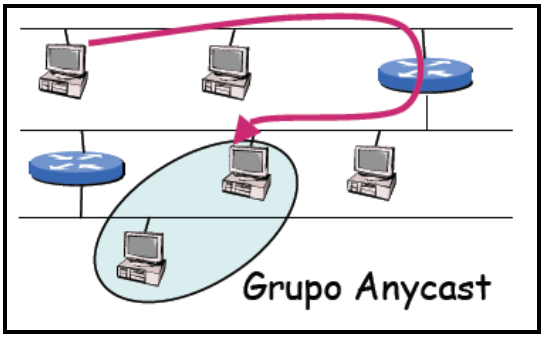


Figura 1.8 Direcciones Anycast

- **Direcciones Multicast (Multidifusión):** Este tipo de direcciones identifica a un conjunto de interfaces de la red, de manera que el paquete es enviado a cada una de ellos individualmente. La Figura 1.9 muestra las Direcciones Multicast.

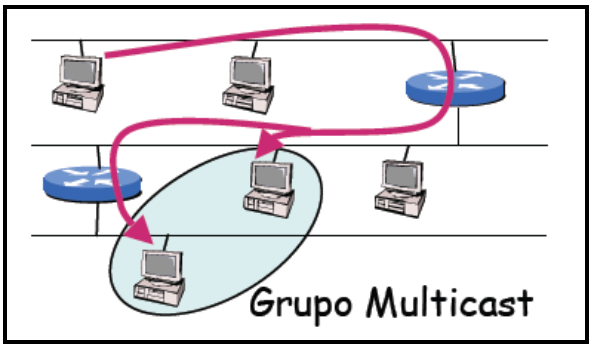


Figura 1.9 Direcciones Multicast

1.2 Tecnologías de Seguridad

1.2.1 Redes de Área Local Virtual: VLANs

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación [8].

Un ejemplo de VLAN se muestra en la figura 1.10.

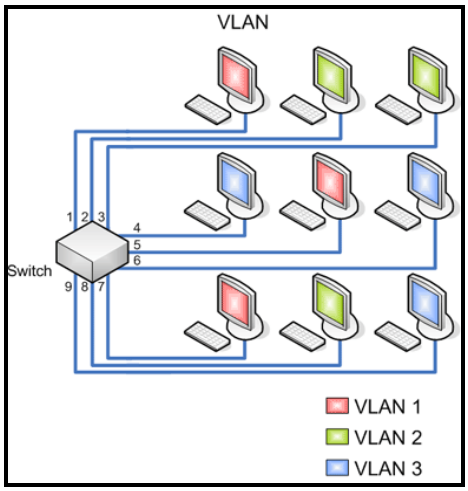


Figura 1.10 Ejemplo de VLAN

La tecnología de las VLANs se basa en el empleo de Switches, en lugar de hubs, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

Una de las ventajas que se pueden notar en las VLAN es la reducción en el trafico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del

ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

La comunicación que se hace entre switches para interconectar VLANs utiliza un proceso llamado Trunking. El protocolo VLAN Trunk Protocol (VTP) es el que se utiliza para esta conexión, el VTP puede ser utilizado en todas las líneas de conexión incluyendo ISL, IEEE 810.10. IEEE 810.1Q y ATM LANE.

Tipos de VLAN

a) VLAN de puerto central

Es en la que todos los nodos de una VLAN se conectan al mismo puerto del switch.

b) VLAN Estáticas

Los puertos del switch están ya preasignados a las estaciones de trabajo.

Por puerto

Se configura por una cantidad “n” de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN.

Por dirección MAC

Los miembros de la VLAN están especificados en la tabla 1.4 por su dirección MAC.

Tabla 1.4 Ejemplo de VLAN por dirección MAC

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1

Por protocolo

Asigna a un protocolo una VLAN. El switch se encarga dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente. Ver la tabla 1.5.

Tabla 1.5 Ejemplo de VLAN por Protocolo

Protocolo	VLAN
IP	1
IPX	2
IPX	2
IPX	2
IP	1

Por direcciones IP

Esta basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

Por nombre de usuario

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

c) VLAN Dinámicas (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también

notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

d) Capa de Red: ELAN o Redes LAN Emuladas

Si bien el concepto de VLAN se creo para las redes LAN, la necesidad llevo a ampliar los horizontes con el crecimiento de las redes ATM. Para los administradores de las VLAN se crearon una serie de estándares para simular en una red ATM una VLAN. Por un lado una tecnología orientada a no conexión, qué es el caso de las LANS y por el otro una orientada a conexión como en el caso de ATM. En el caso de las LANS se trabaja con direcciones MAC, mientras en ATM se usan direcciones ATM y se establecen circuitos virtuales permanentes, por esta razón se requiere hacer cambios de direcciones MAC a ATM.

1.2.2 Filtrado IP

El filtrado de IP es simplemente un mecanismo que decide qué tipos de datagramas de IP serán procesados normalmente y cuáles serán descartados.

Por descartados se entiende que el datagrama se elimina y se ignora completamente, como si nunca se hubiera recibido. Usted puede aplicar

muchos criterios, y en diferentes ordenamientos, para determinar qué datagramas desea filtrar; algunos ejemplos de éstos son [9]:

- Tipo de protocolo: TCP, UDP, ICMP, etc.
- Número de conector (para TCP/UDP).
- Tipo de datagrama: SYN/ACK, datos, petición de eco de ICMP, etc.
- Dirección de origen del datagrama: de donde proviene.
- Dirección de destino del datagrama: a donde se dirige.

Llegado este punto, resulta muy importante comprender que el filtrado de IP es una utilidad en la capa de red. Esto significa que este mecanismo no entiende nada acerca de la aplicación que utiliza las conexiones de red, sólo sabe acerca de las conexiones mismas. Existe un gran número de programas servidores intermediarios. Algunos son software libre y muchos otros son productos comerciales.

El conjunto de reglas de filtrado de IP se construye a partir de muchas combinaciones de los criterios enumerados previamente. Por ejemplo, imagínese que usted quiere que los usuarios del 'World Wide Web' dentro de la red de la Cervecera Virtual no tengan acceso a ningún servicio de Internet excepto a los servidores Web. Entonces configuraría su cortafuego permitiendo el reenvío de:

- Datagramas con una dirección de origen dentro de la red de la Cervecera Virtual, una dirección de destino cualquiera y con un puerto de destino igual a 80 (el de WWW).
- Datagramas con dirección de destino dentro de la red de la Cervecera Virtual y un puerto de origen igual a 80 (WWW) siendo cualquiera la dirección de origen.

1.2.3 Traducción de Direcciones de Red: NAT

¿Qué es NAT?

La "Traducción de Direcciones de Red", Network Address Translation (NAT), es un método mediante el que las direcciones IP son mapeadas desde un dominio de direcciones a otro, proporcionando encaminamiento transparente a las máquinas finales [10]. Existen muchas variantes de traducción de direcciones que se prestan a distintas aplicaciones. Sin embargo todas las variantes de dispositivos NAT debería compartir las siguientes características:

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones (aquí el encaminamiento se refiere al reenvío de paquetes, no al intercambio de información de encaminamiento).
- Traducción de la carga útil de los paquetes de error ICMP.

Aplicación

Como se explicó en el anterior punto, la traducción de la dirección de red, se aplica en redes que fueron implementadas con direcciones IP privadas y necesitan tener un acceso a Internet, se debe solicitar a un proveedor un rango de direcciones válidas para poder asociar dichas direcciones válidas con los hosts que tengan direcciones inválidas y necesiten salida a Internet.

Esta situación ocurre frecuentemente en las empresas que tienen redes internas grandes, también puede darse el caso que el proveedor sólo asigne una dirección válida a la empresa, en esta situación se configura a NAT para que diferentes hosts dentro de la empresa puedan acceder a Internet mediante esta única IP válida asignada por el proveedor, en este caso la configuración del router con NAT asocia además de la dirección IP, un puerto para direccionar correctamente los paquetes a los diferentes hosts. Estos problemas también pueden presentarse en redes caseras más pequeñas y son una solución factible para habilitar una conexión a Internet sin tener que hacer una reconfiguración de la red interna, además que el proceso de traducción de direcciones IP es transparente al usuario final que no se da cuenta de lo que pasa.

Operación Básica

Para que una red privada tenga acceso a Internet, el acceso debe ser por medio de un dispositivo ubicado en la frontera de las dos redes que tenga configurado NAT para la traducción de direcciones, en estos casos lo más conveniente es poner a un router para que los paquetes sean enviados hacia él. Existen dos tipos de asignación de direcciones:

- **Asignación estática de direcciones,** en el caso de asignación estática de direcciones, existe un mapeo uno a uno de direcciones para las máquinas entre una dirección privada de red y una dirección externa de red durante el tiempo en funcionamiento del NAT. La asignación estática de direcciones asegura que NAT no tiene que administrar la gestión de direcciones con los flujos de sesión.

  La Figura 1.11 muestra el NAT estático. Cuando el host 192.168.0.2 envía un paquete al servidor 207.28.194.84 tiene en la cabecera de sus paquetes los datos mostrados en “A”, al pasar estos paquetes por el router NAT, los datos son modificados y llegan al servidor con los datos mostrados en “B”. Las relaciones de direcciones de la tabla del router son puestas estáticamente.

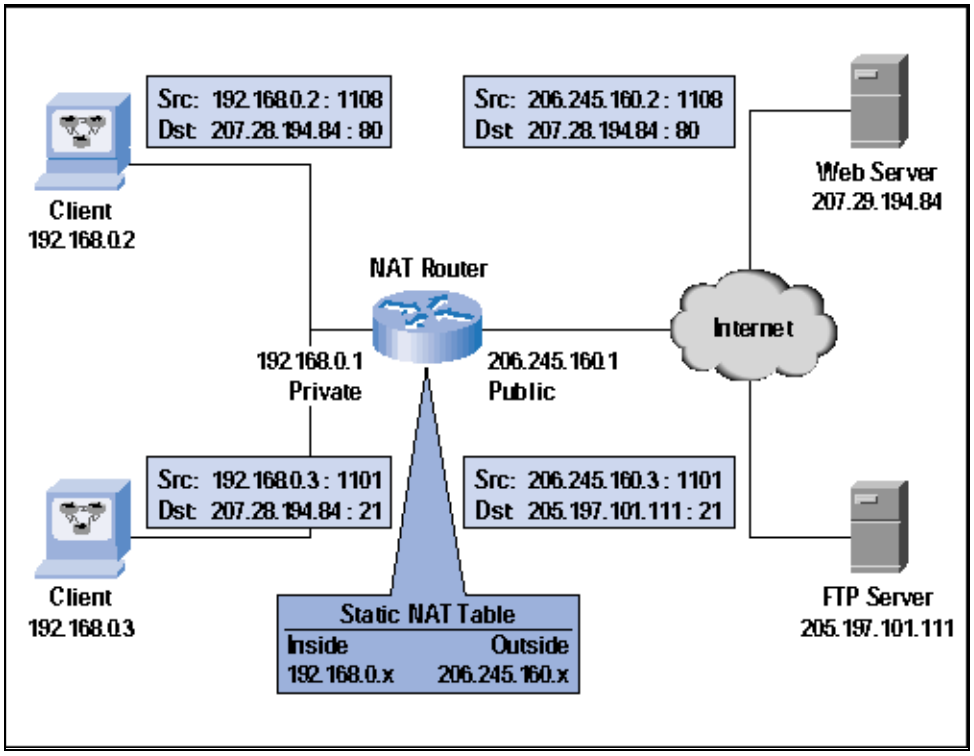


Figura 1.11 NAT Estático

- **Asignación dinámica de direcciones,** en este caso, las direcciones externas son asignadas a las máquinas de la red privada, o viceversa, de manera dinámica, basándose en los requisitos de uso y el flujo de sesión que el NAT determine heurísticamente. Cuando la última de las sesiones que use una dirección asociada termine, NAT liberará la asociación para que la dirección global pueda ser reciclada para su posterior uso. La naturaleza exacta de la asignación de direcciones es específica de cada implementación de NAT.

La Figura 1.12 muestra el NAT dinámico. En este caso sucede lo mismo que en el anterior con las cabeceras de los paquetes que salen de “A”, en este caso la tabla muestra una lista con las direcciones válidas disponibles para ser usadas, estas direcciones son asignadas dinámicamente a los hosts.

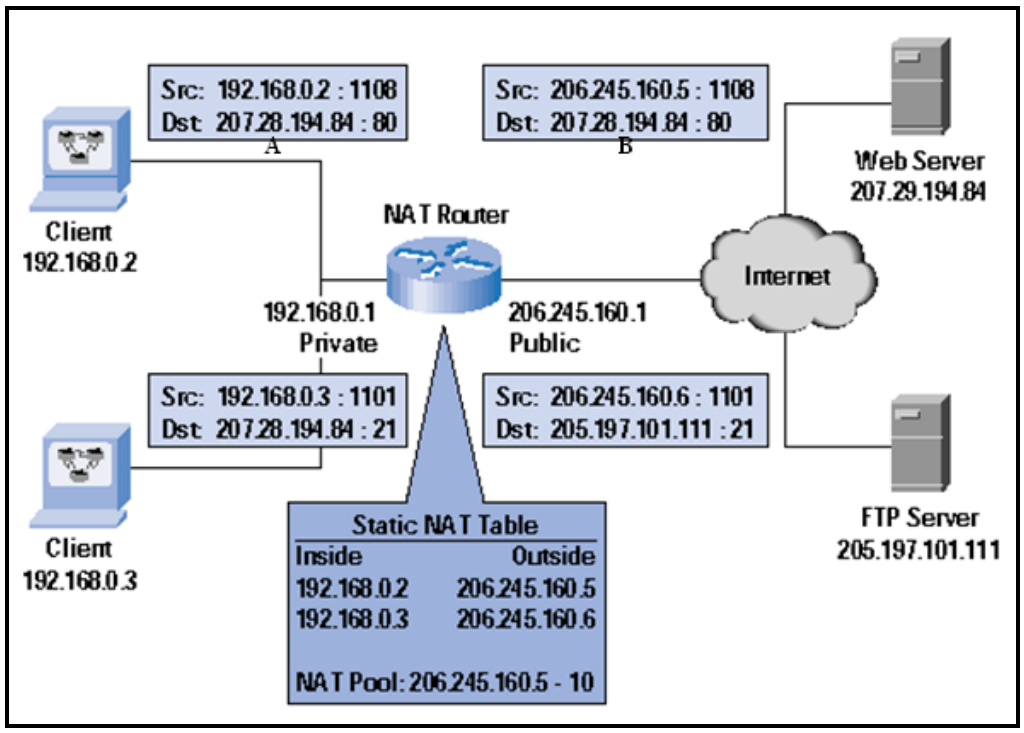


Figura 1.12 NAT Dinámico

NAT Tradicional

La operación de Traducción de Dirección a analizar se denomina “NAT Tradicional”, existen otras variantes de NAT que no serán exploradas. En un NAT tradicional, las sesiones son unidireccionales, salientes de la red

privada. Las sesiones en la dirección opuesta pueden ser permitidas en una base excepcional usando mapeos de dirección estáticos para hosts preseleccionados. Existen dos variantes del NAT Tradicional: NAT Básico y NAPT (Network Address Port Translation).

NAT Básico

La operación de NAT Básico es como se describe a continuación: una zona con un conjunto de direcciones de red privadas puede ser habilitada para comunicarse con una red externa mapeando dinámicamente el conjunto de direcciones privadas a un conjunto de direcciones de red válidas globalmente, cada dirección tiene garantizada una dirección global para ser mapeada a ella. De lo contrario, los nodos habilitados para tener acceso simultáneo a la red externa son limitados por el número de direcciones en el conjunto global.

Direcciones locales individuales pueden ser estáticamente mapeadas a direcciones globales específicas para asegurarse acceso garantizado hacia fuera o para permitir acceso al host local desde hosts externos mediante una dirección pública fija. Sesiones múltiples simultáneas pueden ser iniciadas desde un nodo local, usando el mismo mapeo de dirección.

Las direcciones dentro de la zona son locales para este dominio y no son válidas fuera de él. De este modo, las direcciones dentro de la zona pueden ser reusadas por alguna otra. Por ejemplo, una sola dirección de clase A puede ser usada por muchas zonas. En cada punto de salida entre una zona y el backbone, NAT está instalado. Si hay más de un punto de salida es de gran importancia que cada NAT tenga la misma tabla de traducción.

En el ejemplo de la Figura 1.13 la red de la derecha tiene las direcciones de clases A 10.0.0.0, en 1 una máquina ubicada en una red externa con dirección 130.57.52.13 envía un paquete a la dirección 130.57.199.13, en 2 el paquete llega al router NAT el cuál traduce la dirección de destino 130.57.199.13 por la dirección 10.0.0.1 que es la dirección verdadera del host destino, esto se ve en 3, en 4 la máquina envía una respuesta con dirección fuente 10.0.0.1, al pasar por el router NAT la dirección de fuente de la respuesta es modificada por la dirección 130.57.199.13 que es una dirección global única, esto se ve en 5.

Se puede ver la tabla de traducción que tiene el router, en la cuál se observa la asociación de direcciones locales con las direcciones que usarán en Internet.

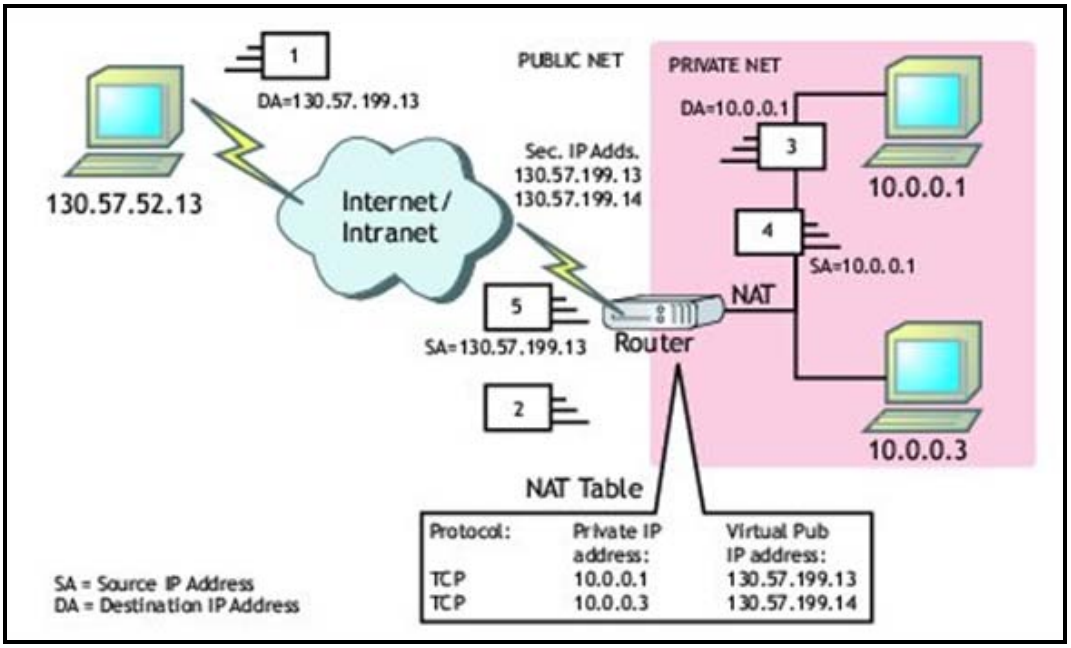


Figura 1.13 NAT Básico

Todo este proceso no requiere cambios en el host o en el router, las traducciones de dirección son transparentes para los hosts finales.

Traducción de Dirección de Red y Puerto: NAPT

Digamos, una organización tiene una red IP privada y una conexión WAN a un proveedor de servicio. El router de zona de la red privada es asignado a una dirección válida globalmente en la conexión WAN y los demás nodos en la organización usan direcciones IP que tienen sólo significado local. En este caso, a los nodos en la red privada se les puede permitir acceder simultáneamente a la red externa, usando la única dirección IP registrada con la ayuda de NAPT. NAPT permitiría mapeos de tuplas del tipo

(direcciones IP local, número de puerto TU local) a tipos del tipo (dirección IP registrada, número de puerto TU asignado).

Este modelo es adecuado para muchos grupos de redes pequeñas para acceder a redes externas usando una sola dirección IP asignada del proveedor de servicio. Este modelo debe ser extendido para permitir acceso entrante mapeando estáticamente un nodo local por cada puerto de servicio TU de la dirección IP registrada.

En el ejemplo de la Figura 1.14 la red interna maneja el rango de direcciones 192.168.0.0 de clase C, la interfase del router que se comunica con Internet tiene asignada la dirección 206.245.160.1. Cuando el host con dirección 192.168.0.2 envía un paquete http (puerto destino 80) al servidor 207.28.194.84, en la cabecera de los paquetes se envía la información mostrada en “A” donde se indica la dirección fuente como Src y la dirección destino como Dst estos paquetes son enviados al router NAT ubicado al centro del gráfico.

El router tiene configurado NAPT y lo que sucede es que se traduce la tupla de dirección de origen 192.168.0.2 y puerto origen 1108 en los encabezados IP y TCP por la tupla 206.245.160.1 que es una dirección globalmente única

y al puerto 61001 antes de reenviar al paquete, es decir los paquetes salen del router con los datos mostrados en “B”.

Los paquetes de regreso que sean enviados por el servidor Web, pasan por una traducción de dirección y puerto similar por la dirección IP de destino y puerto TCP de destino. Se observa que esto no requiere de cambios en los hosts o en los routers. La traducción es completamente transparente para los usuarios.

En el gráfico se muestra la tabla de asignación de los hosts con las direcciones de los hosts de la red interna con sus respectivos puertos y la asociación de puertos con los que será enviada la información afuera.

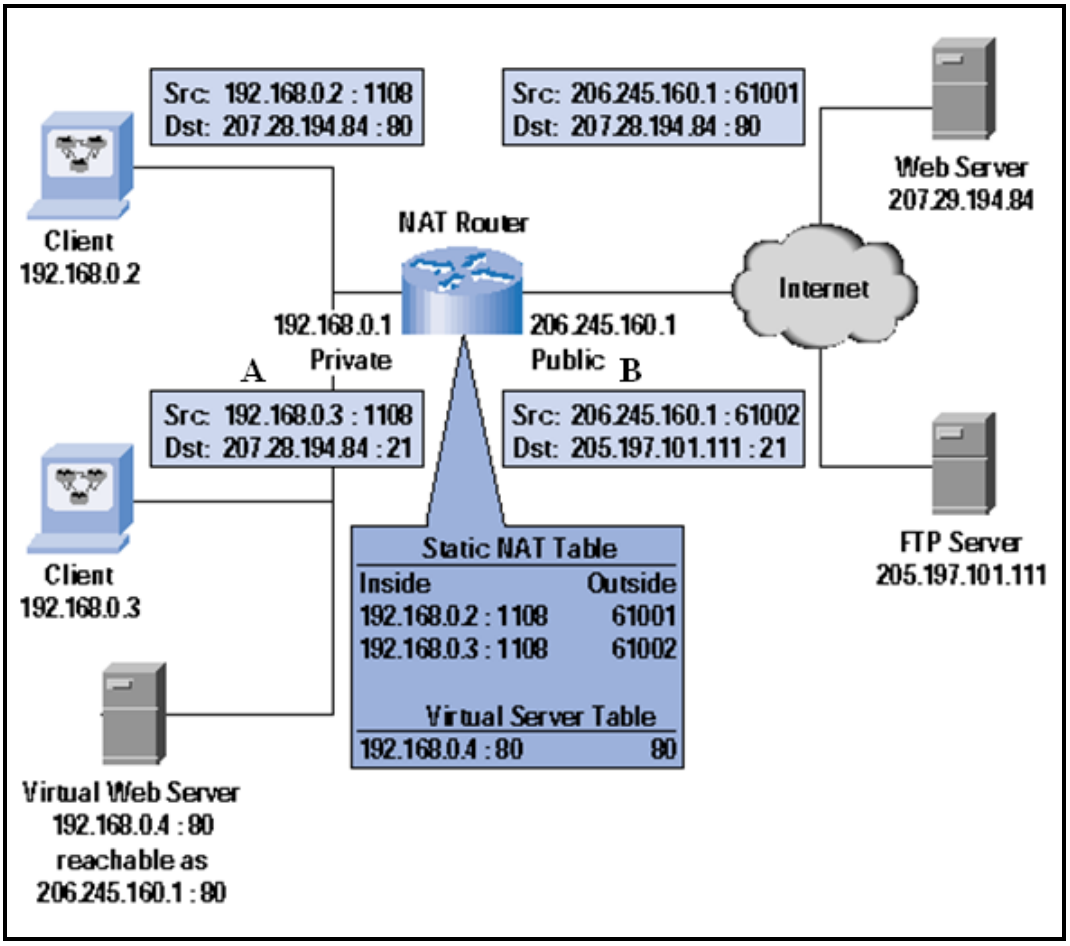


Figura 1.14 NAPT

1.2.4 Cortafuegos

Un cortafuegos, es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento

y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna [11].

También es frecuente conectar al cortafuego una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

La Figura 1.15 muestra como son usados los Firewalls en una Red de Datos.

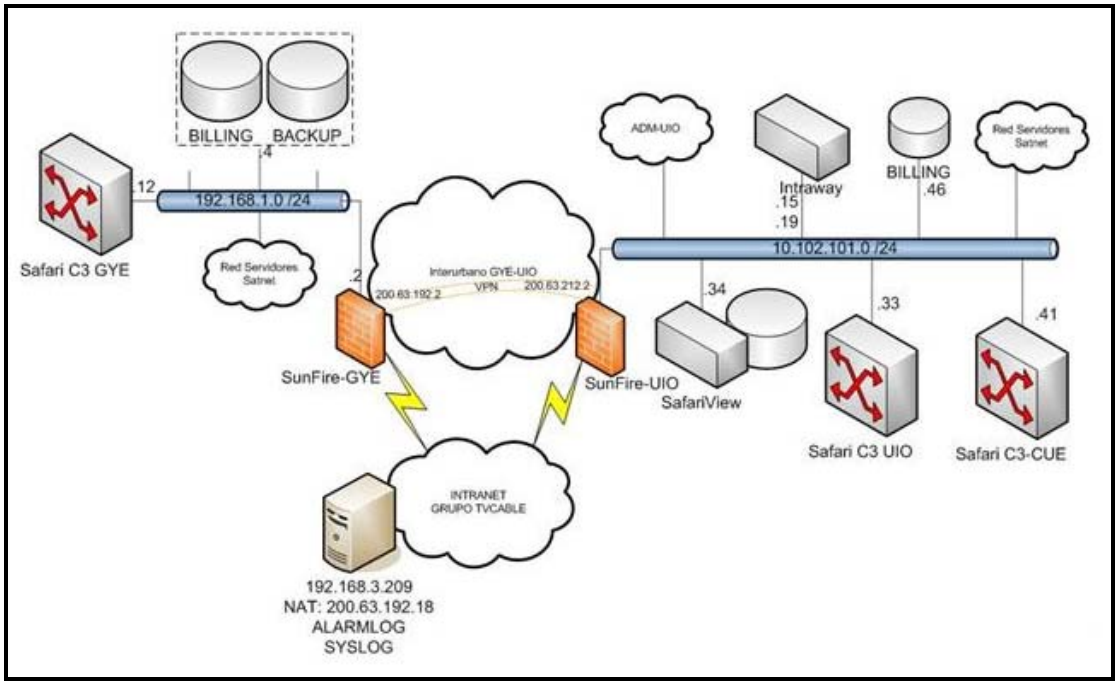


Figura 1.15 Cortafuegos en una Red de Datos

Tipos de cortafuegos:

- **Cortafuegos de capa de red o de filtrado de paquetes.** Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC.
- **Cortafuegos de capa de aplicación.** Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si

se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuego a nivel 7 de tráfico HTTP es normalmente denominado Proxy y permite que los computadores de una organización entren a Internet de una forma controlada.

- **Cortafuegos personal.** Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

Actualmente los cortafuegos también incorporan la opción de bloquear virus y correos spam.

1.2.5 Redes Privadas Virtuales: VPNs

La VPN es una red IP privada y segura que pasa sobre otra red IP no segura normalmente Internet. Una VPN garantiza las siguientes condiciones: Confidencialidad, Autenticidad e Integridad [12].

Para cumplir estas condiciones los paquetes IP que se desean transmitir: Se cifran para garantizar la confidencialidad y se firman para garantizar la autenticidad e integridad. El paquete resultante se encapsula en un nuevo paquete IP y se envía a través de la red insegura al otro extremo de la VPN.

Existen dos escenarios típicos de VPNs: Interconexión de redes privadas a través de Internet y Road Warriors (trabajadores remotos).

Un ejemplo de interconexión de redes privadas es la conexión de dos oficinas de una empresa. Se establece un VPN entre dos gateways, cada uno de una red privada. Las máquinas de las redes utilizan esos gateways como routers. Cuando un gateway recibe un paquete dirigido a la red privada del otro extremo lo envía a través de la VPN de modo seguro. El tráfico solo es protegido por la VPN en el recorrido entre los dos gateways. La Figura 1.16 muestra una Red Privada Virtual.

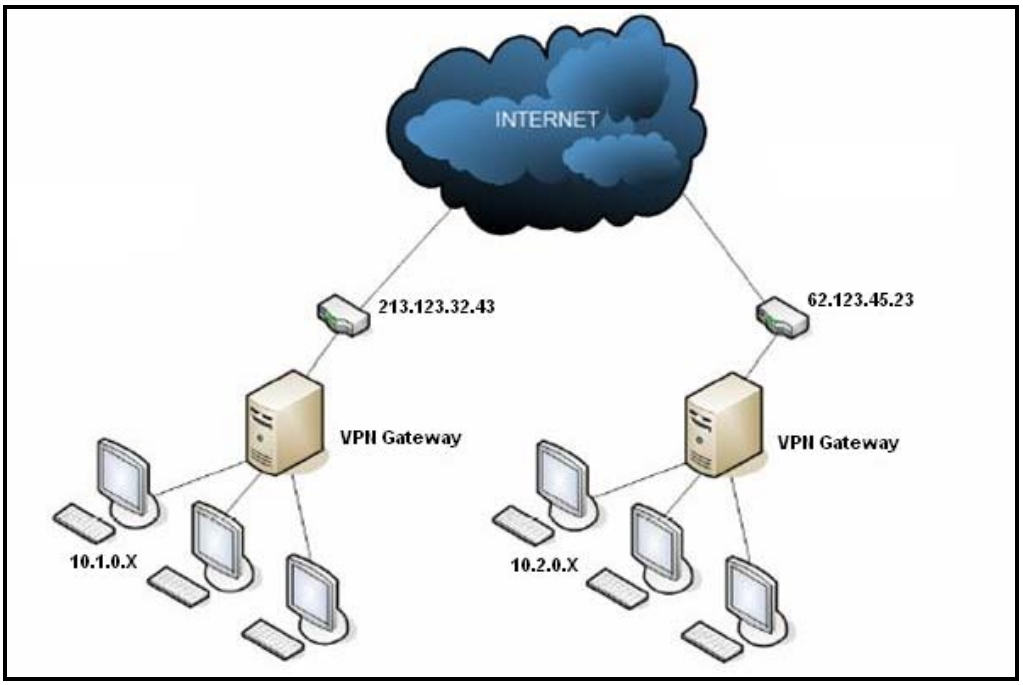


Figura 1.16 Redes Privadas Virtuales

Existen varias tecnologías VPN: IPSec, PPTP, L2TP, VPNs SSL.

1.2.5.1 Seguridad IP: IPSec

¿Qué es IPSec?

IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. Los siguientes párrafos dan una pequeña introducción a IPsec [13].

IPsec emplea dos protocolos diferentes - AH y ESP - para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores.

Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.

La Figura 1.17 muestra los modos Túnel y Transporte de IP Security.

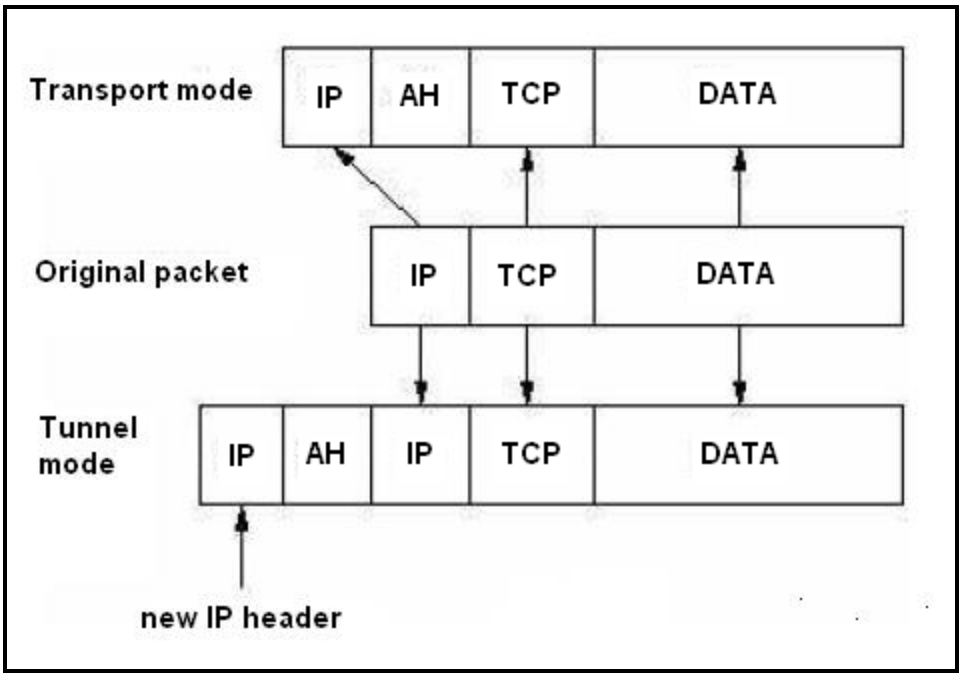


Figura 1.17 IPSec: Modos Túnel y Transporte

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de lo datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la

implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish. Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA – Security Associations). Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Association Databases).

Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.

- Protocolo IPsec (AH o ESP). A veces, se permite compresión (IPCOMP).
- El algoritmo y clave secreta empleados por el protocolo IPsec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.

Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros:

- Modo IPsec (túnel o transporte).
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.
- Tiempo de vida de una asociación de seguridad.

1.2.5.1.1 Cabecera de Autenticación: AH

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete. La Figura 1.18 muestra la cabecera AH.

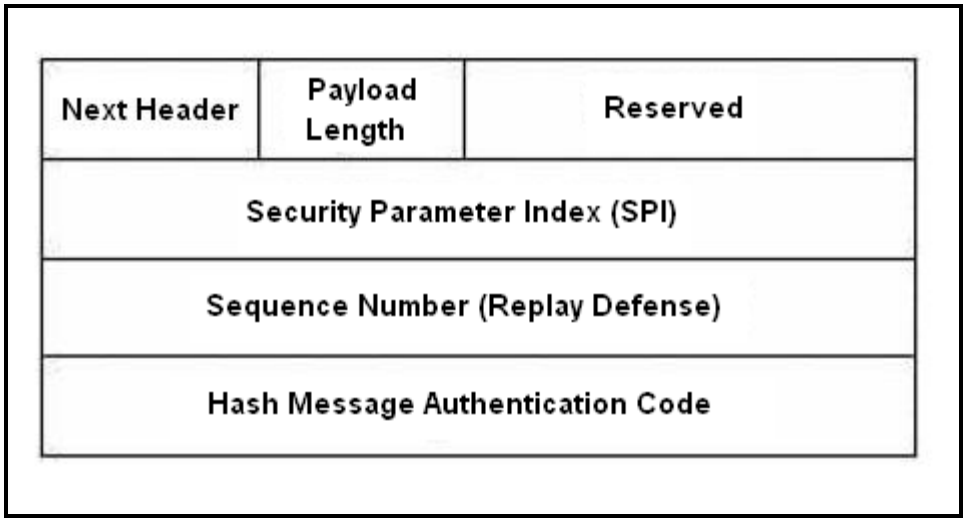


Figura 1.18 Cabecera AH

La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados.

Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bits protege frente a ataques por repetición. Finalmente, los últimos 96 bits almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la

comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network Address Translation - Traducción de direcciones de red, también conocido como Enmascaramiento de direcciones) reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción.

1.2.5.1.2 Encapsulación Segura del Campo de Carga: ESP

El protocolo ESP esta definido en el RFC 2406, ESP proporciona uno o ambos servicios [14], autenticación y encriptación. Puede ser utilizado con o sin AH (cabecera d autenticación). Los RFC describen el soporte para únicamente dos algoritmos de encriptación (DES y encriptación nula) y para dos algoritmos de autenticación (MD5 y SHA).

Formato de la cabecera ESP

La Figura 1.19 muestra los campos de la cabecera ESP, los cuales son:

- **Initialization Vector**.- campo de 64 bits, contiene un valor inicial necesario para preparar el estado inicial de los algoritmos.
- **Security Parameter Index** *(SPI)*.- campo de 32 bits con un numero aleatorio que identifica a la asociación de seguridad (SA).
- **Payload Data.**- Campo de datos encriptados (carga útil) con el algoritmo criptográfico seleccionado.
- **Padding**.- La mayoría de los algoritmos encriptación utilizados requiere que los datos de entrada formen un determinado numero de bloques completos y por esto se incluye un campo de longitud variable.
- **Pad Lenght**.- campo de 8 bits con el número de bytes de padding que le presiden.
- **Next Header**.- Campo de 8 bits con el código del siguiente protocolo de datos en el Playload Data.

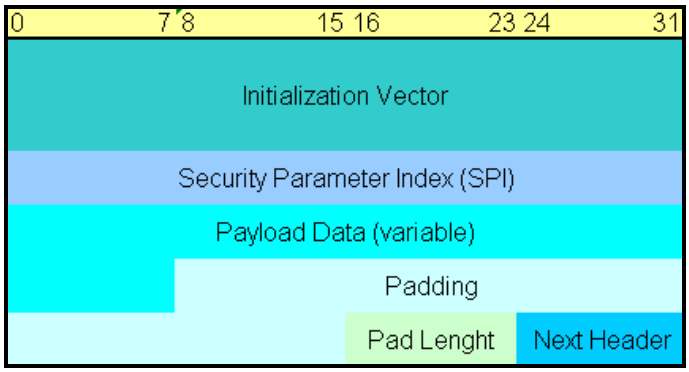


Figura 1.19 Formato de la cabecera ESP

1.2.6 Métodos de Autenticación

Autenticación es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, es decir que reclama hecho por, o sobre la cosa son verdadero. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que el de una persona es autenticar que esa persona es quien dice ser realmente [15].

Los métodos de autenticación se suelen dividir en tres grandes categorías en función de lo que utilizan para la verificación de identidad: algo que el usuario sabe, algo que éste posee, y una característica física del usuario o un acto involuntario del mismo.

1.2.6.1 Sistemas basados en algo conocido: Contraseñas

El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser simplemente basándonos en una prueba de conocimiento, esa prueba de conocimiento no es más que una contraseña que en principio es secreta. En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, clave que han de mantener en secreto si desean que la autenticación sea fiable. Cuando una de las partes

desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común, y si ésta es correcta se otorga el acceso a un recurso. Lo habitual es que existan unos roles preestablecidos, con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior.

Este esquema es muy frágil: basta con que una de las partes no mantenga la contraseña en secreto para que toda la seguridad del modelo se pierda; por ejemplo, si el usuario de una máquina Windows comparte su clave con un tercero, o si ese tercero consigue leerla y rompe su cifrado automáticamente esa persona puede autenticarse ante el sistema con éxito con la identidad de un usuario que no le corresponde.

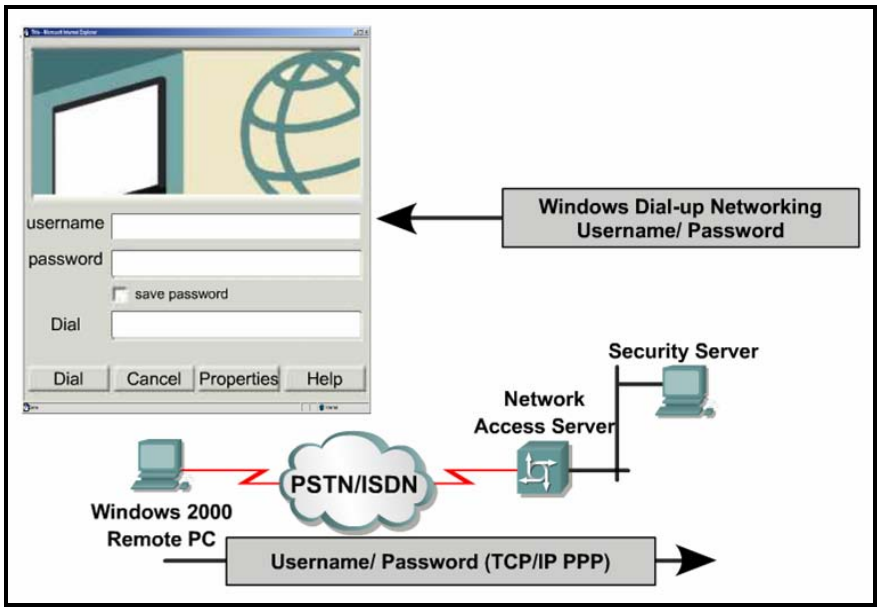


Figura 1.20 Esquema basado en Contraseñas

1.2.6.2 Sistemas basados en algo poseído: Tarjetas Inteligentes

Desde un punto de vista formal una tarjeta inteligente (o smartcard) es un dispositivo de seguridad del tamaño de una tarjeta de crédito, resistente a la adulteración, que ofrece funciones para un almacenamiento seguro de información y también para el procesamiento de la misma en base a tecnología VLSI. En la práctica, las tarjetas inteligentes poseen un chip empotrado en la propia tarjeta que puede implementar un sistema de ficheros cifrado y funciones criptográficas, y además puede detectar activamente intentos no válidos de acceso a la información almacenada; este chip inteligente es el que las diferencia de las simples tarjetas de crédito, que solamente incorporan una banda magnética donde va almacenada cierta información del propietario de la tarjeta.

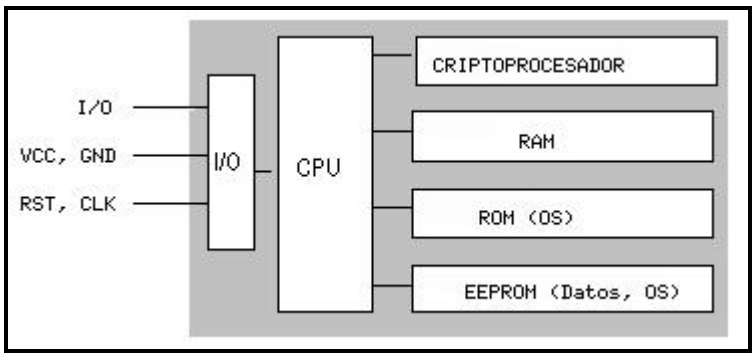


Figura 1.21 Esquema basado en Tarjetas Inteligentes

En la figura se muestra la estructura en general de una tarjeta inteligente; en ella podemos observar que el acceso a las áreas de memoria solamente es posible a través de la unidad de entrada/salida y de una CPU (típicamente de 8 bits), lo que evidentemente aumenta la seguridad del dispositivo. Existe también un sistema operativo empotrado en la tarjeta - generalmente en ROM, aunque también se puede extender con funciones en la EEPROM - cuya función es realizar tareas criptográficas (algoritmos de cifrado como RSA o Triple DES, funciones resumen...); el criptoprocesador apoya estas tareas ofreciendo operaciones RSA con claves de 512 a 1024 bits.

Las ventajas de utilizar tarjetas inteligentes como medio para autenticar usuarios son muchas frente a las desventajas; se trata de un modelo ampliamente aceptado entre los usuarios, rápido, y que incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado. Además, su uso es factible tanto para controles de acceso físico como para controles de acceso lógico a los hosts, y se integra fácilmente con otros mecanismos de autenticación como las contraseñas; y en caso de desear bloquear el acceso de un usuario, no tenemos más que retener su tarjeta cuando la introduzca en el lector o marcarla como inválida en una base de datos (por ejemplo, si se equivoca varias veces al teclear su PIN, igual que sucede con una tarjeta de crédito normal). Como principal inconveniente de las smartcards podemos citar el coste adicional que supone

para una organización el comprar y configurar la infraestructura de dispositivos lectores y las propias tarjetas; aparte, que un usuario pierda su tarjeta es bastante fácil, y durante el tiempo que no disponga de ella o no puede acceder al sistema, o hemos de establecer reglas especiales que pueden comprometer nuestra seguridad (y por supuesto se ha de marcar como tarjeta inválida en una base de datos central, para que un potencial atacante no pueda utilizarla).

1.2.6.3 Sistemas de Autenticación Biométrica

Son sistemas basados en características físicas del usuario a identificar. El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos. La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Obviamente aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado recurso.

Los dispositivos biométricos tienen tres partes principales; por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar. Además disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos (que son considerados válidos), y también ofrecen una interfaz para las aplicaciones que los utilizan. El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: captura o lectura de los datos que el usuario a validar presenta, extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar), comparación de tales características con las guardadas en una base de datos, y decisión de si el usuario es válido o no. Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo (False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechaze a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un

grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Actualmente cualquier sistema biométrico, con excepción de algunos modelos basados en voz, son altamente inmunes a estos ataques.

1.2.7 Criptografía

La criptografía es una ciencia cuyo uso original era el proteger la confidencialidad de informaciones militares y políticas [16], pero en la actualidad se usa en cualquiera sistema que esté interesado en la confidencialidad de unos determinados datos: actualmente existe multitud de software y hardware destinado a analizar y monitorizar el tráfico de datos en redes de computadoras; si bien estas herramientas constituyen un avance en técnicas de seguridad y protección, su uso indebido es al mismo tiempo un grave problema y una enorme fuente de ataques a la intimidad de los usuarios y a la integridad de los propios sistemas. La criptografía proporciona seguridad en el intercambio de mensajes entre un emisor y un receptor a través de un canal de comunicaciones.

1.2.7.1 Métodos Criptográficos

Criptografía de Clave Simétrica

La criptografía simétrica es el método criptográfico que usa una misma clave para cifrar y descifrar mensajes [17]. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Hasta la década de los setenta, la invulnerabilidad de todos los sistemas dependía de este mantenimiento en secreto de la clave de cifrado. Este hecho presentaba una gran desventaja: había que enviar, aparte del criptograma, la clave de cifrado del emisor al receptor, para que éste fuera capaz de descifrar el mensaje. Por tanto, se incurría en los mismos peligros al enviar la clave, por un sistema que había de ser supuestamente seguro, que al enviar el texto plano. De todos los sistemas de clave secreta, el único que se utiliza en la actualidad es DES (Data Encryption Standard) y con seguridad es el algoritmo de cifra más utilizado en la actualidad.

Los sistemas de cifrado de clave única se dividen a su vez en dos grandes grupos de criptosistemas: por una parte tenemos los cifradores de flujo, que son aquellos que pueden cifrar un sólo bit de texto claro al mismo tiempo, y

por tanto su cifrado se produce bit a bit, y por otro lado tenemos los cifradores de bloque, que cifran un bloque de bits (habitualmente, cada bloque es de 64 bits) como una única unidad.

Algunos ejemplos de algoritmos simétricos son 3DES, AES, Blowfish e IDEA.

Criptografía Asimétrica

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes [18]. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee

comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe probar hasta 281-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con un clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos. La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.

- El mensaje cifrado ocupa más espacio que el original.

Algunos algoritmos de técnicas de clave asimétrica son: Diffie-Hellman, RSA, DSA, ElGamal, Criptografía de curva elíptica, Otros algoritmos de clave asimétrica pero inseguros: Merkle-Hellman, algoritmos "Knapsack".

Criptografía de Curva Elíptica

Es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas [19]. Sus autores argumentan que la CCE puede ser más rápida y usar claves más cortas que los métodos antiguos como RSA, al tiempo que proporcionan un nivel de seguridad equivalente.

La Criptografía Híbrida

Usa tanto un cifrado simétrico como uno asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión [20].

1.3 Amenazas

1.3.1 Escaneo de Puertos

¿Qué es un Escaneo de Puertos?

Un escaneo de puertos (portscan) es una técnica de exploración que pretende hallar qué servicios están siendo ofrecidos por una red o servidor, consiste en realizar conexiones o intentos de conexión a diferentes puertos (TCP o UDP) en la víctima esperando obtener respuesta de alguno o algunos de ellos e inferir qué aplicación o servicio está escuchando en dicho puerto. Así por ejemplo, si recibe una respuesta del puerto 22 supondrá que se trata del servicio de SSH, aunque probablemente sea un servidor Web el que esté escuchando peticiones en aquel puerto si el administrador del host así lo ha configurado [21].

Esta actividad es comúnmente el preludio para un ataque de mayores proporciones, pero no es penalizada por la ley de Colombia ni de Estados Unidos ya que se asocia con el caso análogo en el que un ladrón golpea la puerta de una casa para ver si está abierta o no, pero permanece afuera de ella; sin embargo, en el ambiente de la seguridad informática es considerada como un ataque.

La Figura 1.22 muestra la clasificación de las distintas técnicas de Escaneo de Puertos:

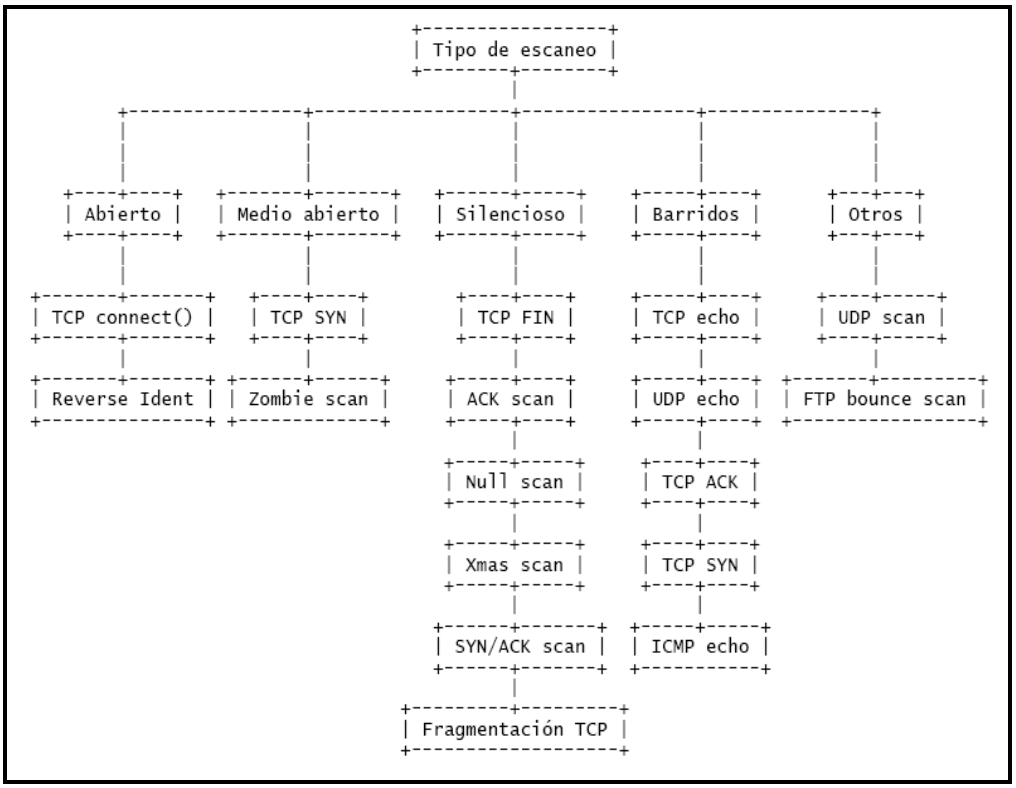


Figura 1.22 Tipos de Escaneos de Puertos

TCP connect()

Esta técnica es quizá la más común en cualquier software de escaneo de puertos. La técnica consiste en usar la llamada connect() de TCP para intentar establecer una conexión con cada uno de los puertos del host a escanear. Si la conexión se establece, el puerto está abierto (escuchando conexiones); en caso de recibir un aviso de cierre de conexión (RST), el

puerto estará cerrado; y en caso de no recibir respuesta, se deduce que el puerto está silencioso.

Este tipo de escaneo es extremadamente rápido, pues puede realizarse de forma paralela para distintos puertos mediante el uso de varios sockets.

Además, es un escaneo fácil de implementar. Su principal desventaja es que es llamativo en exceso, pues resulta a todas luces llamativo establecer cientos o miles de conexiones en un margen de pocos segundos. Además, al realizarse intentos completos de conexión, cualquier sistema guardará registros.

TCP SYN

Esta técnica, también conocida como Half-open scan (es el escaneo medio abierto por excelencia), es parecida a la anterior con la importante salvedad de no establecer completamente las conexiones. En primer lugar, se envía un paquete SYN que finge intentar establecer una conexión y se espera la respuesta. Si llega un paquete SYN/ACK significa que el puerto está abierto; si llega un paquete RST, el puerto está cerrado; y si no se recibe respuesta se asume que está silencioso. En el caso de que el puerto esté abierto y se reciba el paquete SYN/ACK (es decir, están completos dos de los tres pasos del saludo en tres tiempos), no se responde con un paquete ACK como sería

lo esperado, sino que se manda un paquete RST. ¿Para qué? Pues precisamente para evitar que se complete el inicio de conexión y, por tanto, evitar que el sistema registre el suceso como un intento de conexión. En sistemas sin protección específica de cortafuegos o IDS, este escaneo suele pasar desapercibido. Una característica importante de este escaneo es que requiere elevados privilegios en el sistema para poder lanzarlo, debido a que este tipo de paquetes usan sockets TCP raw. Por tanto, solo el root puede lanzar escaneos TCP SYN.

La principal ventaja de este tipo de escaneo es que suele ser bastante discreto y ofrece unos resultados bastante buenos. Entre sus desventajas encontramos el que es algo lento de realizar, y que un sistema con un firewall o un IDS (aunque algunos muy básicos no) lo detectará e identificará como escaneo de puertos sin ninguna duda.

TCP FIN

El escaneo TCP FIN, también conocido como Stealth scan (se trata del escaneo silencioso más conocido), es uno de los más discretos que se puede encontrar dentro de las técnicas convencionales. Se apoya en una particularidad de los estándares internacionales de TCP/IP. A la hora de realizar el escaneo, se envía un paquete FIN al puerto del host destino que queremos escanear. Los estándares de TCP/IP dicen que al recibir un

paquete FIN en un puerto cerrado, se ha de responder con un paquete RST. Así pues, si recibimos RST por respuesta, el puerto está cerrado, y en caso de no recibir respuesta (se ignora el paquete FIN) el puerto puede encontrarse abierto o silencioso.

Esto supone uno de los principales inconvenientes del escaneo TCP FIN, y es que los puertos que nos figuran como abiertos, pueden estar en realidad en estado silencioso (puesto que un puerto silencioso por definición ignora cualquier paquete recibido). Así pues, este tipo de escaneos no obtienen unos resultados fiables, y ese es su talón de Aquiles.

Otra gran desventaja de este sistema de escaneo es que viene de la compañía de Software Microsoft, ya que tiene por costumbre usar cualquier estándar informático. En los sistemas Windows, un puerto cerrado ignora los paquetes FIN, por lo que escanear un sistema de este tipo con SYN FIN nos generará una enorme lista de puertos abiertos, aunque realmente estén cerrados o silenciosos.

Como ventaja, tenemos el que estos escaneos pasan desapercibidos en la gran mayoría de los firewalls, al no intentar establecer ninguna conexión. Un IDS bien configurado, lo detectará.

UDP scan

Esta técnica, frente a las demás técnicas orientadas a TCP, está orientada al protocolo UDP y sus puertos. Aunque a priori parezca que los puertos UDP no son muy interesantes, servicios como el rpcbind de Solaris, TFTP, SNMP, NFS usan todos ellos UDP como protocolo de transferencia. El sistema de escaneo consiste en mandar un paquete UDP vacío (0 bytes de datos) al puerto que deseamos escanear. Si el puerto está cerrado, el sistema responderá con un paquete ICMP de tipo 3 (destino inalcanzable). En caso de no responder, el puerto puede estar abierto o silencioso.

Este sistema puede presentar un grave problema de carencia de velocidad por lo que se recomienda limitar la capacidad de generación de mensajes ICMP de error. En sistemas Linux (consultar el fichero /ipv4/icmp.h de las fuentes del kernel) esta limitación está fijada en unos 20 mensajes por segundo. Sistemas como Solaris son más estrictos y tiene la limitación fijada en 2 por segundo. Pero hay un sistema que, para variar, no hace mucho caso a los estándares, por lo que no tiene ninguna limitación prefijada: Windows. Un escaneo UDP a un sistema Windows resulta extremadamente rápido como consecuencia de ello.

ACK scan

La mayoría de las técnicas de escaneo nos permiten identificar con exactitud los puertos abiertos o cerrados, pero generalmente los puertos silenciosos no se pueden identificar con claridad. El escaneo ACK está destinado a identificar de forma precisa cuándo un puerto se encuentra en estado silencioso. Esta técnica es usada también para poder escanear hosts que estén detrás de un firewall que bloquee los intentos de conexión (paquetes SYN).

Su funcionamiento se basa en el envío de paquetes ACK con números de secuencia y confirmación aleatorios. Cuando reciba el paquete, si el puerto se encuentra abierto, responderá con un paquete RST, pues no identificará la conexión como suya; si el puerto está cerrado responderá con un paquete RST, pero si no se obtiene respuesta (obviamente primero se debe asegurar que el host está en línea) se puede identificar claramente el puerto como filtrado (puerto silencioso).

Normalmente el escaneo ACK se realiza como apoyo a un escaneo anterior, para determinar los puertos silenciosos y poder identificar mediante una combinación de técnicas el estado real de todos ellos. Por ejemplo, ante un host con un firewall que bloquee intentos de conexión (SYN), se puede

realizar un FIN scan para determinar los puertos cerrados, y después un ACK scan para determinar qué puertos están abiertos y cuáles silenciosos.

Esta técnica también es usada como variante del ping (ICMP echo) de toda la vida, para saber si un host está activo (recibiremos respuesta RST) o no (cuando no hay respuesta o la respuesta es destino inalcanzable).

Null scan

Este escaneo tiene muchos puntos en común con el escaneo FIN. Su funcionamiento base es el mismo: Se envía un paquete malformado (en este caso se trata de un paquete TCP con todos los flags desactivados) y se espera la respuesta. En caso de que el puerto destino esté cerrado, responderá con un paquete RST; y en caso de no recibir nada (el paquete es ignorado), se trata de un puerto abierto o silencioso.

La ventaja frente al escaneo FIN radica en que ciertos firewalls vigilan los paquetes de finalización de conexión además de los de establecimiento, de forma que el escaneo nulo podrá realizarse allí dónde el FIN no sería posible.

El resto de ventajas y desventajas son las mismas que en el escaneo FIN.

Xmas scan

El escaneo Xmas se basa también en el principio de la respuesta RST por parte de un puerto cerrado al recibir un paquete incorrecto (como el escaneo FIN). En el caso del escaneo Xmas, se trata de un paquete con los flags FIN, URG y PSH activados (aunque ciertas implementaciones activan FIN, URG, PSH, ACK y SYN e incluso algunas activan todos los flags). Podría decirse que es lo contrario del escaneo Null, pero logrando el mismo efecto.

Al igual que el escaneo Null, se usa bajo ciertas circunstancias en las que el escaneo FIN no es posible; y también comparte con éstos sus particularidades.

SYN / ACK scan

Este tipo de escaneo tiene una base parecida a los anteriormente citados FIN, Null y Xmas, pero con la sustancial diferencia de que en este caso los paquetes malformados fingen ser un error en la transacción de una conexión legítima. Mediante esta técnica, se envía un paquete SYN/ACK al puerto que se desea escanear en el host remoto. Si el puerto se encuentra cerrado, nos responderá con un paquete RST. En caso de estar abierto o silencioso, simplemente ignorará el paquete y no obtendremos respuesta.

Como ventaja, este tipo de escaneo evade la mayoría de firewalls e IDS sencillos, pero comparte con los escaneos anteriormente citados sus problemas, principalmente la falta de fiabilidad a la hora de determinar los puertos abiertos o silenciosos [22].

1.3.2 Suplantación de IP (IP Spoofing)

La clave de este ataque es usurpar la dirección IP de una máquina. Esto permite al cracker ocultar el origen de su ataque (usado en ataques de Denegación de Servicio) o para beneficiarse de una relación de confianza entre dos máquinas [23].

El principio básico de este ataque consiste, para el cracker, en crear sus propios paquetes IP (con programas como hping2 o nemesis) en los cuales se puede cambiar, entre otras cosas, la dirección IP de origen.

IP Spoofing es llamado frecuentemente Blind Spoofing. Las respuestas a los falsos paquetes no pueden ir a la máquina del cracker, ya que el origen ha sido alterado, van hacia la máquina "burlada". Sin embargo hay dos métodos para hacer que las respuestas regresen:

- **Source Routing:** el protocolo IP tiene una opción llamada Source Routing (ruteo de origen) que permite definir la ruta que los paquetes

IP deben tomar. Esta ruta es una serie de rutas de dirección IP que los paquetes deben seguir. Suficiente para que el cracker provea una ruta para los paquetes hacia un router que él controle. Actualmente la mayor parte de las pilas TCP/IP rechazan los paquetes que usen esta opción.

- **Re-routing:** tablas de enrutado usando el protocolo RIP, pueden ser cambiadas enviándoles paquetes RIP con nueva información de enrutado. Se hace esto para enrutar los paquetes hacia un router que controle el cracker.

Estas técnicas son muy usadas: el ataque es llevado a cabo sin saber qué paquetes son los que vienen del servidor objetivo. Blind Spoofing se usa contra servicios como rlogin o rsh. Su mecanismo de autentificación solo recae en la dirección IP de origen de la máquina cliente. Este ataque relativamente conocido (Kevin Mitnick lo usó contra la máquina de Tsutomu Shimomura's en 1994) requiere varios pasos:

- Encontrar la dirección IP que está utilizando la "máquina de confianza", por ejemplo showmount -e que indica a dónde se exporta el sistema de archivos, o rpcinfo que da más información.
- Dejar al host de confianza fuera de servicio usando, por ejemplo, un SYN Flooding. Esto es primordial para evitar que la máquina responda

a los paquetes enviados por el servidor objetivo/víctima. De otro modo, enviaría paquetes TCP RST que pararían/cortarían la conexión.

- Predicción de los números de secuencia TCP: todo paquete TCP está asociado a un número de secuencia inicial. La pila TCP/IP del Sistema Operativo lo genera de forma lineal, dependiendo del tiempo, aleatorio o seudo-aleatorio, según el sistema. El cracker sólo puede atacar a sistemas generando números de secuencia predecibles (generados linealmente o dependientes del tiempo).
- El ataque consiste en abrir una conexión TCP en el puerto deseado (rsh, por ejemplo).

Durante el ataque, el cracker no recibe el SYN-ACK enviado por la víctima. Para establecer la conexión, predecirá el número de secuencia y para poder enviar un paquete con el número ACK correcto (Y+1). La conexión es entonces estabilizada a través de la autentificación por dirección IP. El cracker puede ahora enviar un comando al servicio rsh, como un echo ++ >> /.rhosts para mayores permisos de acceso. Para hacer esto ha de crear un paquete con el flag TCP PSH (Push): los datos recibidos son inmediatamente enviados a la capa superior (aquí el servicio rsh). Puede conectar a la máquina a través de un servicio como rlogin o rsh sin IP Spoofing.

La Figura 1.23 muestra los diferentes pasos de IP Spoofing.

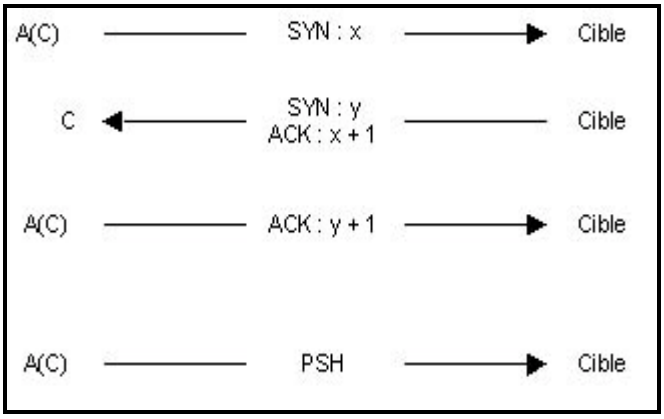


Figura 1.23 Pasos de IP Spoofing

El cracker usa la máquina A, mientras que C representa la máquina de confianza. A(C) significa que el paquete se envía desde A con la dirección IP de C burlada.

Nota: Existe un programa llamado mendax que implementa estos mecanismos de IP Spoofing.

1.3.3 Denegación de Servicio (DoS)

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea

inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no de abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

El llamado DDoS (siglas en inglés de Distributed Denial of Service, denegación de servicio distribuida) es una ampliación del ataque DoS, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos. El invasor consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del flood o saturación de información, pudiendo darse casos de un ataque de cientos o millares de computadoras dirigidas a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido sofisticándose hasta el punto de otorgar poder de causar daños serios a personas con escaso conocimiento técnico.

En ocasiones, esta herramienta ha sido utilizada como un notable método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y perjudicar los servicios que desempeña. Un administrador de redes puede así conocer la capacidad real de cada máquina [24].

1.3.4 Saturación de Red (Net Flood)

El objetivo de éste ataque es degradar la capacidad de conexión a la red de un sistema, saturando sus enlaces de comunicaciones. Por ejemplo, si el enlace de una organización dispone de un ancho de banda de 34 Mb, y un atacante dispone de un enlace de 155 Mb, prácticamente la totalidad del tráfico cursado por la organización pertenecerá al atacante, por lo que no podrá enviarse tráfico útil.

Para disponer de altos anchos de bandas puede recurrirse a la obtención de múltiples sistemas desde los que pueden efectuarse el ataque o apoderarse de sistemas mal administrado y protegidos que posean redes de gran capacidad, como por ejemplo, los existentes en las universidades.

Las dos técnicas aplicadas en este tipo de ataques se basan en los protocolos ICMP y UDP, al tratarse de protocolos no orientados a conexión y que permiten el envío de paquetes sin requisitos previos: ICMP Flood y UDP Flood [25].

1.3.5 Falsificación de IPs (Smurf)

El protocolo ICMP es el encargado de realizar el control de flujo de los datagramas IP que circulan por Internet. Este protocolo consta de diversas funcionalidades que permiten desde la comunicación de situaciones anómalas (no se ha podido realizar la entrega del paquete IP) hasta la comprobación del estado de una máquina en Internet (ping - pong o ECHO - ECHO REPLY).

Este tipo de ataque se basa en falsear las direcciones de origen y destino de una petición ICMP de ECHO (ping).

Como dirección de origen colocamos la dirección IP de la máquina que va a ser atacada. En el campo de la dirección de destino situamos la dirección broadcast de la red local o red que utilizaremos como “lanzadera” para colapsar al sistema elegido [26].

La Figura 1.24 muestra el Ataque Smurf en una Red de Datos.

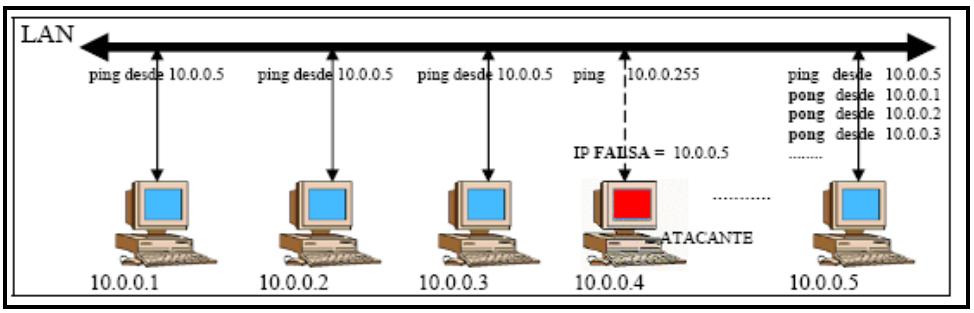


Figura 1.24 Ataque Smurf

Con esta petición fraudulenta, se consigue que todas las máquinas de la red contesten a la vez a una misma máquina, consumiendo el ancho de banda disponible y saturando al ordenador elegido.

1.3.6 Llamada de la Muerte (Ping of death)

El PING de la muerte (*Ping of death*) ha sido probablemente el ataque de denegación de servicio mas conocido y que más artículos de prensa ha conseguido.

Este ataque utiliza una vez más las definiciones de la longitud máxima de paquetes de los protocolos IP/UDP/TCP/ICMP así como la capacidad de fragmentación de los datagramas IP [27].

La longitud máxima de un datagrama IP es de 64K (65535 Bytes) incluyendo la cabecera del paquete (20 Bytes) y asumiendo que no hay opciones especiales especificadas.

El protocolo ICMP es el que se utiliza para la comunicación de mensajes de control de flujo en las comunicaciones (si la red está congestionada, si la dirección de destino no existe o es inalcanzable...) y tiene una cabecera de 8 bytes.

De esta forma tenemos que para enviar un mensaje ICMP tenemos disponibles 65535 - 20 - 8 = **65507 Bytes**.

En el caso de enviar más de 65535 bytes el paquete se fragmenta y se reconstruye en el destino utilizando un mecanismo de posición y desplazamiento relativo.

No obstante, si enviamos ordenes al sistema operativo para que envíe un datagrama con una longitud de 65510 bytes (correcto, puesto que es inferior a 65507 bytes):

ping -l 65510 direcion_ip [Windows]

ping -s 65510 direccion_ip [Unix]

Obtenemos que el tamaño es inferior a los 65535 con lo que los datos a enviar cogen en un único paquete IP (fragmentado en N trozos, pero pertenecientes al mismo datagrama IP).

Sumando el tamaño de las cabeceras obtenemos:
20 bytes cabecera IP + 8 bytes cabecera ICMP + 65510 bytes de datos = **65538**!!!!!

Sin embargo debido a la cabecera ICMP el espacio disponible tan sólo era de 65507 bytes!!. En consecuencia al reensamblar el paquete en el destino se suelen producir errores de *overflow/coredump* que causan la parada del servicio o del sistema atacado.

1.3.7 Canales Encubiertos (Loki)

Este ataque fue inicialmente el nombre de un proyecto, pasando posteriormente a convertirse en una herramienta cuyo objetivo es demostrar la posibilidad de encubrir tráfico en túneles ICMP y UDP, bajo lo que se ha dado en denominar canales encubiertos. En el caso de que este tráfico este permitido a través de los firewalls, el ataque es posible. Debe tenerse en cuenta que en la mayoría de ocasiones es necesario habilitar al menos ciertos tipos de paquetes ICMP, como los de la familia unreachable, para que

funcionalidades de la pila TCP/IP se desarrollen, por ejemplo, el algoritmo PMTUD, Path MTU Discovery.

El objetivo del ataque es introducir tráfico encubierto, típicamente IP, en paquetes ICMP (o UDP) que son permitidos. La herramienta consta de un cliente, loki, y un servidor, loki, que se encargan de encapsular y desencapsular el tráfico en ambos extremos.

1.3.8 Lazo IP (Land)

Este tipo de ataque se basa en falsear la dirección y puerto origen para que sean las mismas que la del destino. De esta forma, se envían al ordenador atacado peticiones de conexión desde él mismo hasta él mismo.

La Figura 1.25 muestra el Ataque LAND.

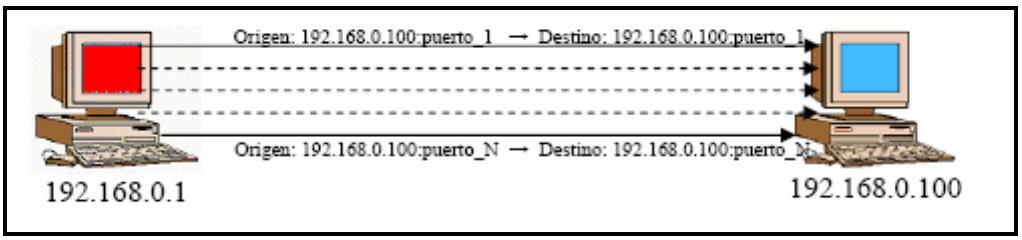


Figura 1.25 Ataque LAND

La mala calidad del software encargado de gestionar las comunicaciones en los sistemas operativos hace que muchas veces este sencillo ataque consiga colapsar el sistema atacado.

Usualmente este tipo de peticiones suelen ir acompañadas de violaciones expresas de los campos de opciones de los protocolos con el objetivo de confundir al ordenador atacado.

1.3.9 Secuestro de Sesión

Considerando la importancia de la información trasmitida a través de las redes de datos, y las medidas de seguridad que deben desarrollarse, esta técnica pretende mostrar la posibilidad de apoderarse de una sesión ya establecida. Este avance podría suponer el obviar todo el proceso de autenticación previo.

El TCP hijaking puede realizarse en entornos de red de difusión, basado en introducir paquetes en medio de una transmisión como si provinieran del dispositivo original (IP spoofing). Este tipo de ataques también se conoce como “Man in the middle attack”, ya que el atacante debe situarse entre el equipo que estableció la conexión original y la víctima.

Para poder tomar el control de una conexión previamente es necesario obtener la información asociada a como transcurre ésta a lo largo del tiempo, concretamente en TCP, deben conocerse los números de secuencia actuales, ya sea directamente o a través de los ISNs y del número de bytes trasmitidos. Una vez conseguido el control, el objetivo será ejecutar algún comando, típicamente se pretende apoderarse de sesiones de terminal, que permita acceder al sistema remoto de forma directa.

Habitualmente el control de la sesión se realiza empleando técnicas como source-routing, de forma que los paquetes de vuelta lleguen al atacante y no al destino real. En caso de no disponer de esta facilidad la técnica se conoce como blind-hijacking y se basa en adivinar o intuir las respuestas de los sistemas que intervienen en la comunicación. Para obtener la información de la conexión existente debe emplearse un sniffer, situándose entre los sistemas que se están comunicando, ataque conocido como "man-in-the-middle attack".

Existen dos herramientas principales para llevarlo a cabo, aunque numerosos sniffers también incluyen esta funcionalidad, por ejemplo Ethereal.

Asimismo, existen métodos para apoderarse de las conexiones encriptadas, por ejemplo de SSH v.1 o SSL. Existen herramientas como “dsniff” o “ettercap” que facilitan aplicar la técnica de hijacking en estos entornos [28].

1.3.10 Fragmentación pequeña (Tiny Fragment)

Para comprender este ataque debe considerarse como tiene lugar la fragmentación de paquetes TCP sobre IP. Cuando un paquete IP supera el tamaño máximo de transmisión, MTU, debe dividirse en paquetes menores.

El primero de ellos incluirá la cabecera TCP asociada al paquete original, mientras que el resto de fragmentos simplemente contendrán la cabecera IP y los datos, pero no información de TCP (cabecera TCP). A través del campo de fragment offset de la cabecera IP se determina si existen más fragmentos y la relación entre éstos.

Cuando se gestiona un sistema de filtrado de paquetes, lo habitual es permitir que los fragmentos de un paquete IP pasen el filtro, ya que no se dispone de información TCP para tomar una decisión de filtrado en función, por ejemplo, de los puertos origen y destino.

La técnica presentada pretende enviar un paquete TCP inicial con la siguiente información: SYN=0, ACK=1, FO=”more packets follow”. De esta forma, el paquete puede atravesar un filtro concreto (stateless), al no disponer del flag SYN activo.

Este paquete no sería peligroso de no ser porque el tamaño de offset (20 bytes) es lo suficientemente pequeño como para sobrescribir ciertos campos de la cabecera TCP mediante el paquete que representa el supuesto fragmento esperado a continuación. Este segundo paquete en el proceso de fragmentación cambiará los valores de TCP a SYN=1, ACK=0, por tanto, se tendrá un paquete de establecimiento de conexión reconstruido en la máquina destino, aunque los filtros explícitamente no permiten el establecimiento de conexión desde ese sistema IP origen.

Por ejemplo, al enviar un paquete de 8 bytes, suficiente para contener los puertos fuente y destino (además del número de secuencia), se obligará a recibir los flags TCP en el siguiente paquete. Este segundo paquete o fragmento no posee cabecera TCP, por lo que el filtro no se podrá aplicar sobre él, ni tampoco en el resto de fragmentos. Realmente, el campo de datos del segundo fragmento, contiene el resto de la cabecera TCP tras los 8 bytes, es decir, los flags TCP.

1.3.11 Ataque al puerto 139 (Winnuke)

Este ataque afecta a los sistemas que utilizan el protocolo NetBIOS sobre TCP/IP, típicamente en el sistema operativo Windows. Este protocolo emplea los puertos UDP 137, 138 y 139. El envío de un paquete urgente (bit URG=1), conocido como paquete “Out of Band” (OOB) da lugar al envío de datagramas UDP a estos puertos, que al intentar ser enviados a las capas superiores, pueden provocar que el sistema destino se “cuelgue” o que disminuya su rendimiento de forma notable (ésta referencia contiene menciones a otros ataques de los protocolos TCP/IP).

Existe una página Web que permite probar la eficacia de este ataque contra un sistema concreto. Asimismo, existen exploits similares, como supernuke.

El termino Nuking (nuke.c) no debe ser confundido con Winnuke. Es una técnica antigua, por lo que no funciona en los sistemas modernos, y para ser ejecutado debe tenerse privilegio de root. El ataque se basa en enviar fragmentos o paquetes ICMP no válidos, con el objetivo de ralentizar al objetivo o incluso bloquearlo. Posteriormente surgió una variante de éste denominada Smurfing.

1.3.12 Envío de paquetes fragmentados (Teardrop)

El ataque teardrop se basa en el envío de fragmentos de paquetes en lugar de paquetes completos. Se comprobó que algunas implementaciones de la pila TCP/IP no eran capaces de reconstruir paquetes con fragmentos cuyos bytes se superponen. El resultado es de nuevo que el sistema destino puede llegar a bloquearse; apareció en Linux inicialmente. Para llevarlo a cabo bastaría con 2 paquetes, A y B, dónde el offset del paquete B indica que comienza dentro del paquete A

Existen dos versiones de este ataque: teardrop y teardrop2. La variación de la segunda respecto a la primera se basa en la inclusión del flag de urgencia (URG) en la cabecera TCP de los fragmentos. Por ejemplo, Windows NT 4 SP3 se parcheó frente a la primera versión, pero era vulnerable a la segunda.

Existen variantes de teardrop en las que el paquete enviado tiene el flag SYN activo, como “syndrop.c”, así como otras orientadas a sistemas Windows, ”bonk.c”.

1.3.13 Del Entorno

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir las amenazas del entorno.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma.

Así, la Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

1.4 Herramientas de Seguridad y Monitoreo de Red

1.4.1 Nivel Hardware

1.4.1.1 PIX 500

El Equipo de seguridad Serie Cisco PIX 500 (Figura 1.29) es el firewall más importante del mundo, que proporciona una confiabilidad, escalabilidad y conjunto de capacidades sin igual en la industria.

Ofrecidos como una serie de equipos especializados y como un módulo integrado para los switches Catalyst de Cisco, los equipos de seguridad PIX de Cisco presentan una arquitectura de seguridad híbrida innovadora que incluye inspección de paquetes que conserva su información de estado y funciones VPN con IPSec integrada.

Los equipos de seguridad PIX de Cisco ofrecen los niveles más elevados de seguridad y rendimiento, y admiten más conexiones simultáneas que cualquier otro firewall, a una velocidad inigualable [29].

PIX "Private Internet eXchange" es el firewall de Cisco Systems para su línea de productos de seguridad "Cisco Secure". Originalmente el PIX fue construido por una empresa llamada TNI "Translation Networks Inc.", hasta que fue adquirida por Cisco, y en 1994 salio al mercado como el primer producto comercial para hacer NAT.

Al contrario de la creencia popular, el sistema operativo del PIX no es un IOS con las Access lists mejoradas, sino que fue especialmente diseñado y bautizado con el nombre de FOS "Finesse Operating System". La última versión del FOS es la 6.3.

Dentro de las muchas cualidades del PIX, podemos nombrar su SO embebido que evita los bugs de SO's para propósitos generales; el ASA "Adaptive Security Algorithm" que realiza la inspección, y mantiene el estado de las conexiones y las traslaciones de red; el Cut-through Proxy que permite autenticar a los usuarios con el PIX utilizando ftp, telnet o http; la opción de filtrado de URL's en el PIX utilizando un software externo; su gran

performance para armar VPN's; y la muy reciente posibilidad de manejar VLAN's, entre otras cosas.

Actualmente podemos encontrar la serie 500 de PIX con cinco modelos, el 501, 506E, 515E, 525 y 535. El 501 para uso hogareño, los 515E, 525 y 535 para empresas medianas y grandes, y el 506 es un intermedio entre estas dos gamas.

Todos estos modelos conservan el gran poder del PIX y su mayor diferencia se encuentra en la memoria, trafico, cantidad de interfaces y licencias [30].

CISCO PIX 501

El dispositivo CISCO PIX 501 entrega seguridad a empresas, para los ambientes pequeños de la oficina y del teleworker. Es confiable. Su diseño compacto de alto rendimiento incorpora un 10/100 switch Fast Ethernet de cuatro puertos haciéndola ideal para asegurar conexiones de banda ancha de alta velocidad del Internet.

El dispositivo de seguridad Cisco PIX 501 proporciona una amplia gama de los servicios integrados de seguridad y avanzados servicios de redes [31]. La Figura 1.26 muestra el dispositivo CISCO PIX 501.

Figura 1.26 PIX 501

CISCO PIX 506E

El dispositivo CISCO PIX 506E entrega seguridad a oficinas alejadas, sucursales y redes de pequeños a medianos negocios. Es de alto rendimiento. Su diseño de escritorio único incorpora 2 interfaces 10/100 de Fast Ethernet y dos 802.1 basados en interfaces virtuales, haciéndola una opción excepcional para los negocios que requieran una solución rentable de la seguridad con la ayuda de DMZ.

El dispositivo de seguridad Cisco PIX 506E proporciona una amplia gama de los servicios integrados de seguridad y avanzados servicios de redes [32]. La Figura 1.27 muestra el dispositivo CISCO PIX 506E.

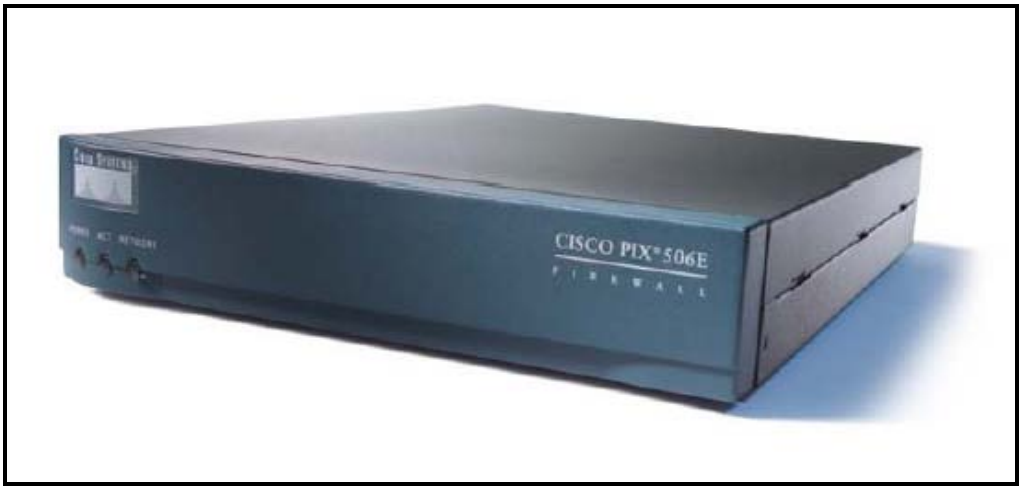


Figura 1.27 PIX 506E

CISCO PIX 515E

El dispositivo CISCO PIX 515E entrega una abundancia de servicios avanzados de seguridad y servicios de redes a pequeños y medianos negocios. Su diseño versátil one rack unit (1RU) incorpora 6 interfaces 10/100 de Fast Ethernet haciéndote una opción excelente para los negocios que requieren una solución rentable [33]. La figura 1.28 muestra el dispositivo CISCO PIX 515E.

Figura 1.28 PIX 515E

CISCO PIX 525

El dispositivo CISCO PIX 525 entrega una abundancia de servicios avanzados de seguridad y servicios de redes para medianas y grandes empresas. Su diseño modular two rack unit (2RU) incorpora 2 interfaces 10/100 de Fast Ethernet y una combinación de hasta 8 interfaces 10/100 de Fast Ethernet, o 3 interfaces adicionales de Gigabit Ethernet haciéndote una opción ideal para los negocios que requieren un alto rendimiento [34]. La Figura 1.29 muestra el dispositivo CISCO PIX 525.

Figura 1.29 PIX 525

CISCO PIX 535

El dispositivo CISCO PIX 535 entrega una abundancia de servicios avanzados de seguridad y servicios de redes para grandes empresas como las proveedoras de servicios de redes. Su diseño altamente modular three rack unit (3RU) incorpora una combinación de hasta 14 interfaces 10/100 de Fast Ethernet o 9 interfaces Gigabit Ethernet haciendo una opción ideal para los negocios que requieren los niveles más altos del funcionamiento, la densidad portuaria, confiabilidad, y protección de la inversión [35]. La Figura 1.30 muestra el dispositivo CISCO PIX 535.

Figura 1.30 PIX 535

1.4.1.2 VPN 3000

Los concentradores de la serie Cisco VPN 3000 son plataformas VPN de acceso remoto que combinan alta disponibilidad, alto rendimiento y escalabilidad con las técnicas de autenticación y cifrado más avanzadas existentes. El uso de la tecnología VPN más avanzada reduce enormemente el costo de las comunicaciones. Los concentradores de la serie Cisco VPN 3000 son las únicas plataformas escalables que ofrecen componentes ampliables por el cliente y que se pueden intercambiar sobre el terreno [36].

Estos componentes, denominados módulos de Procesamiento de cifrado escalable (SEP), permiten a los usuarios agregar capacidad y caudal de procesamiento con facilidad. La flexibilidad de la serie Cisco VPN 3000 permite a la vez la terminación de túneles VPN con IPSec y SSL para lograr

una mayor flexibilidad y reducción del costo de adquisición. La Figura 1.31 muestra el dispositivo VPN 3000.

Figura 1.31 VPN 3000

1.4.1.3 Cisco Catalyst 4507R

La serie Cisco Catalyst 4500, es una gama de conmutadores modulares inteligentes que ofrecen a los clientes redundancia, mejor control de la red, potencia inline integrada, y protección para las inversiones. La serie Catalyst 4500 es un componente clave de la arquitectura Cisco AVVID (Architecture for Voice, Video and Integrated Data). A su vez, la serie Catalyst 4500 permite a las empresas clientes y a los clientes con redes Ethernet metropolitanas desplegar redes convergentes con mayores niveles de rendimiento, flexibilidad, resistencia, seguridad y facilidad de gestión. De esta

forma, los clientes pueden hacer converger y controlar mejor los datos IP (Internet Protocol), el streaming vídeo, la telefonía y las aplicaciones comerciales basadas en Internet, con el fin de mejorar la productividad y rentabilidad de los empleados. La serie Catalyst 4500 permite a los clientes extender el control de la red desde el centro al borde de la red a través de servicios de red inteligentes que ofrecen conmutación de Nivel 2/3/4; rendimiento de routing sostenido a velocidad de línea cualquiera que sea la cantidad de servicios inteligentes activados; Calidad de Servicio (QoS) y gestión de tráfico, que permiten clasificar y priorizar tráfico crítico y sensitivo al mismo tiempo. La flexibilidad y resistencia integradas representan una combinación de redundancia de supervisor integrada, redundancia de potencia y tolerancia a fallos integral [37]. La Figura 1.32 muestra el dispositivo Cisco Catalyst 4500.

Figura 1.32 Cisco Catalyst 4500

1.4.1.4 Sun Fire V65x

Los servidores Sun Fire V60x y V65x son las nuevas opciones que la corporación ofrece a las organizaciones para ser considerados al momento de escoger un servidor que cumpla funciones de firewall y detección de intrusos, informática técnica de alto rendimiento, servicios Web y servidores de bases de datos o de controlador primario de dominios. Con precios muy solidarios, Sun espera que estos equipos revolucionen el mercado [38]. La Figura 1.33 muestra el dispositivo Sun Fire V65x.

Figura 1.33 Sun Fire V65x

Al poder ejecutar el entorno operativo Solaris o las distribuciones Linux estándar, los servidores Sun Fire V60x y V65x ofrecen la flexibilidad que buscan los clientes.

Con la funcionalidad de doble procesador de los servidores, los clientes pueden aprovechar la potencia de dos rápidos chips Intel Xeon. Estos

equipos incluyen, respectivamente, formatos de una y dos unidades en bastidor. Este sólido y compacto diseño es rentable y ayuda a perfeccionar la administración del servidor y en bastidor.

Estos equipos vienen con dos microprocesadores Intel Xeon a 3,06 GHz, hasta 12 GB de memoria RAM, hasta seis ranuras PCI-X a 100 MHz, bus del sistema a 533 MHz y conectividad Gigabit Ethernet dual. El servidor Sun Fire V65x también ofrece fuentes de alimentación con cables independientes, redundantes e intercambiables en funcionamiento.

Los servidores incluyen completas prestaciones de administración integradas, habilitando herramientas como Sun Control Station 2.0, diseñadas para facilitar el trabajo. Asimismo, los clientes pueden utilizar herramientas de administración de terceros, como HP OpenView y CA UniCenter, gracias a la compatibilidad con el protocolo de administración de red simple y a la interfaz de administración de plataforma inteligente.

En materia de sistemas operativos, los servidores pueden correr en Solaris 9 x86 Platform Edition, o en Red Hat Enterprise Linux. El entorno operativo Solaris 9 para x86 ofrece escalabilidad, fiabilidad y seguridad, características necesarias de un entorno de alta disponibilidad. La administración integrada es uno de los distintivos de la plataforma Solaris, por lo que los servidores

Sun Fire V60x y V65x pueden sacar provecho de herramientas de administración como el software Solaris Resource Manager y el software Solaris Volume Manager.

Al utilizar las prestaciones del software Solaris Live Upgrade y la tecnología Solaris Flash del sistema operativo Solaris 9 OS para x86, los servidores Sun Fire V60x y V65x evitan el largo tiempo que se solía perder con los períodos, previstos o imprevistos, de inactividad.

Para quienes no ejecutan una red Solaris, los servidores Sun Fire V60x o V65x con Red Hat Enterprise Linux podrían ser una buena opción. Al ofrecer un sistema operativo de código fuente abierto seguro y estable en su plataforma x86, se pone de manifiesto el compromiso de Sun con la informática de bajo costo. Las aplicaciones personalizadas Linux también se pueden integrar a la perfección con los servidores Sun Fire V60x y V65x. Red Hat Enterprise Linux también ofrece varias características únicas de los servidores Sun Fire V60x y V65x, entre las que se incluye la agrupación en cluster.

1.4.2 Nivel Software

1.4.2.1 Ethereal

Ethereal es un potente analizador libre de protocolos de redes, para máquinas Unix y Windows. Nos permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco (puede leer más de 20 tipos de formato distintos).

Destaca también por su impresionante soporte de más de 300 protocolos, gracias sin duda a la licencia GPL y sus más de 200 colaboradores de todo el mundo [39].

Protocolos Soportados

802.11, 802.11 MGT, 802.11w, AARP, AFP, AFS, AFS (RX), AH, AIM, AODV, AODV ARP/RARP, ARP, ASAP, ASP, ATM, ATM LANE, ATP, AppleTalk, Auto-RP, BACapp, BACnet, BEEP, BGP, BOOTP, BOOTP/DHCP BOOTPARAMS, BROWSER, BVLC, CDP, CGMP, CHDLC, CLNP, CLTP, CONV, COPS, COSEVENTCOMM COSNAMING, COTP, CUPS, DCCP, DCE RPC, DCERPC, DDP, DDTP, DEC spanning tree, DEC_STP, DFS, DHCPv6, DIAMETER, DLSw, DNS, DSI, DSI DVMRP, DVMRP, Data, Diameter, EAP, EAP/ EAPOL, EAPOL, EIGRP, EPM, ESIS, ESP, Ethernet,

FDDI, FR, FTP, FTP-DATA, Frame GIOP, GIOP, GMRP, GNUTELLA, GRE, GTP, GTPv0, GTPv1, GVRP, Gryphon, H.261, H1, HCLNFSD, HMIPv6, HSRP, HTTP, IAPP, IAPP ICAP, ICMP, ICMPv6, ICP, ICQ, IEEE 802.11, IEEE spanning tree, IGMP, IGRP, ILMI, IMAP, IP, IPComp, IPP, IPX, IPX MSG, IPX RIP, IPX SAP, IPv6, IRC, IS-IS, ISAKMP, ISIS, ISL, ISUP, IUA, KLM, KRB5, L2TP, LANMAN, LAPB, LAPBETHER LAPD, LAPD, LDAP, LDP, LLAP, LLC, LMI, LMP, LPD, LSA, Lucent/Ascend, M2PA, M2TP, M2UA, M3UA, MAPI MGCP, MGMT, MIP, MMSE, MOUNT, MPEG1, MPLS, MRDISC, MS Proxy, MSDP, MSNIP, MTP2, MTP3, Mobile IP Modbus/TCP, NBDS, NBIPX, NBNS, NBP, NBSS, NCP, NDMP, NETLOGON, NFS, NFSACL NFSAUTH, NIS+, NIS+ CB, NLM, NMPI, NNTP, NTP, NetBIOS, New dissectors include DHCPv6, Null, ONC RPC, OSPF, OXID, PCNFSD, PFLOG, PGM PIM, PIM, POP, PPP, PPP BACP, PPP BAP, PPP CBCP, PPP CCP, PPP CHAP, PPP Comp, PPP IPCP, PPP LCP, PPP MP PPP PAP, PPP PPPMux, PPP PPPMuxCP, PPP VJ, PPPoED, PPPoES, PPTP, Portmap, Prism, Q.2931, Q.931, QLLC QUAKE, QUAKE2, QUAKE3, QUAKEWORLD, RADIUS, RANAP, RARP, REG, REMACT, RIP, RIPng, RPC, RPC RQUOTA, RSH, RSTAT, RSVP, RTCP, RTMP, RTP, RTSP, RWALL, RX, Raw, Raw IP, Rlogin, SADMIND, SAMR, SAMR SAP, SCCP, SCSI, SCTP, SDB, SDP, SIP, SKINNY, SLARP, SLL, SMB, SMB Mailslot, SMB Pipe, SMB/CIFS, SMPP, SMTP, SMUX SNA, SNA over Ethernet and HiPath HDLC, SNAETH, SNMP, SOCKS, SPOOLSS, SPOOLSS RPC,

SPRAY, SPX, SRVLOC, SRVSVC, SSCOP, SSL, STAT, STAT-CB, STP SUA, Skinny, SliMP3, Socks, Syslog, TACACS, TACACS+, TCP, TELNET, TFTP, TIME, TNS, TPKT, TR MAC, TSP, TSP Token-Ring, UCP, UDP, V.120, VJ, VLAN, VRRP, VTP, Vines, Vines FRP, Vines SPP, WCCP, WCP, WHO WKSSVC, WSP, WTLS, WTP, WebDAV (HTTP), X.25, X11, XDMCP, XOT, YHOO, YP, YPBIND, YPPASSWD, YPSERV, YPXFR , ZEBRA, Zebra, iSCSI, iSCSI/SCSI, ypbind.

En la ventana principal de Ethereal se reconocen tres áreas de despliegue:

- **Resumen de paquetes capturados**, un paquete por línea; uno de ellos ha sido seleccionado como paquete actual (dando clic sobre la línea del paquete). Al desplazarse en la lista y cambiar el paquete actual se actualizan las otras dos ventanas, donde se despliega en dos formatos diferentes el contenido del paquete.
- **Detalles de encabezado de protocolos para el paquete seleccionado**; los encabezados pueden abrirse (clic en +) para ver mayor detalle, o cerrarse (clic en -) para ocupar sólo una línea.
- **Datos crudos del paquete**, representación hexadecimal y ASCII del encabezado del paquete seleccionado en el campo del medio [40].

En la Figura 1.34 se muestra la Ventana principal de Ethereal luego de una captura.

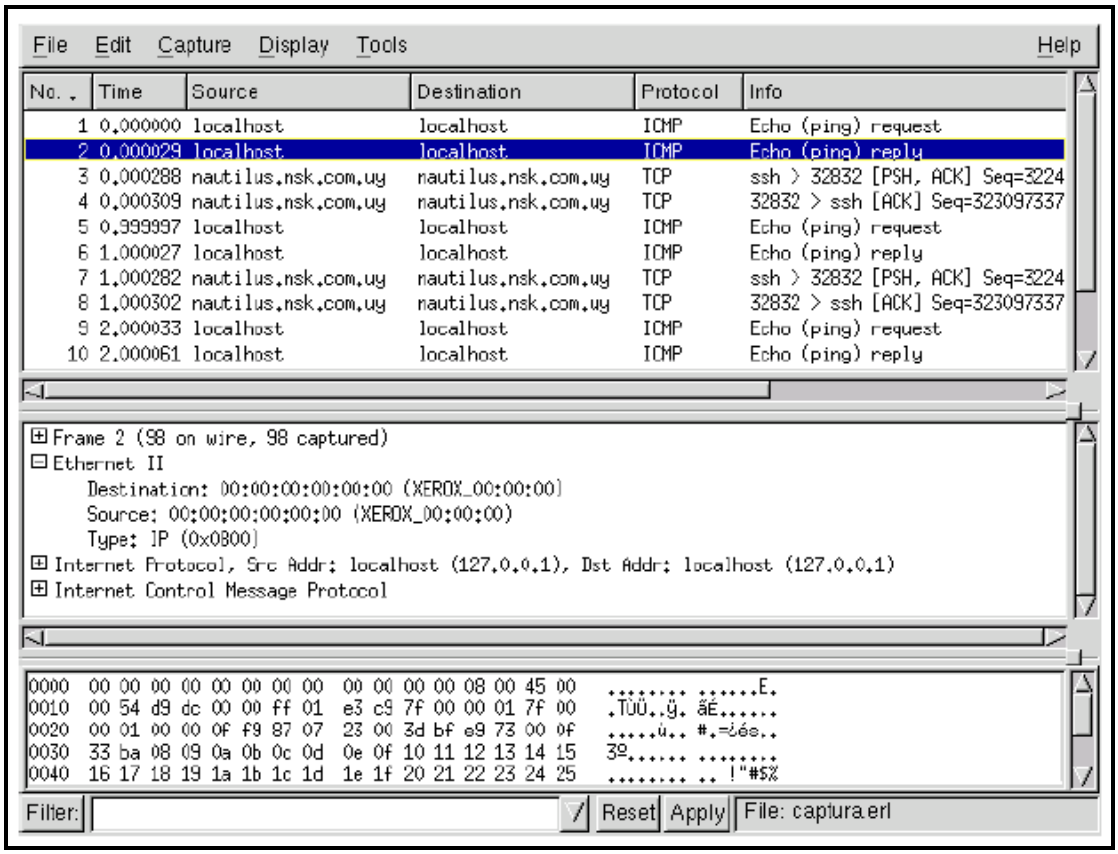


Figura 1.34 Ventana Principal de Ethereal luego de una captura

1.4.2.2 Observer

Observer es un analizador de protocolos, rico en características especiales, flexibles y fáciles de usar. Permite introducirse al nivel de paquetes individuales hasta obtener vistas generales de la actividad de la red, ofreciendo gran diversidad de niveles de revisión. Descubre e identifica los nodos de la red, monitorea los nodos descubriendo su disponibilidad y

rendimiento, decodifica protocolos, produce estadísticas útiles de las actividades que se realizan en la red, ayuda a resolver problemas y reporta el status actual de los dispositivos de la red y sus conexiones [41].

Observer va de lo general a lo particular en varios aspectos de la red, permitiéndole, filtrar el tráfico basado en direcciones de la red, tipos de protocolo y otros criterios de selección. Además acelera el diagnóstico de un problema en la red, revelando la naturaleza del problema, ubicación e impacto. Relacionado la actividad actual con una línea de base de actividad normal previamente capturada, se convierte en parte de la caja de herramientas de planeación informándole de sus tendencias y cambios.

La Figura 1.35 muestra la Pantalla principal de Observer con algunas de sus herramientas.

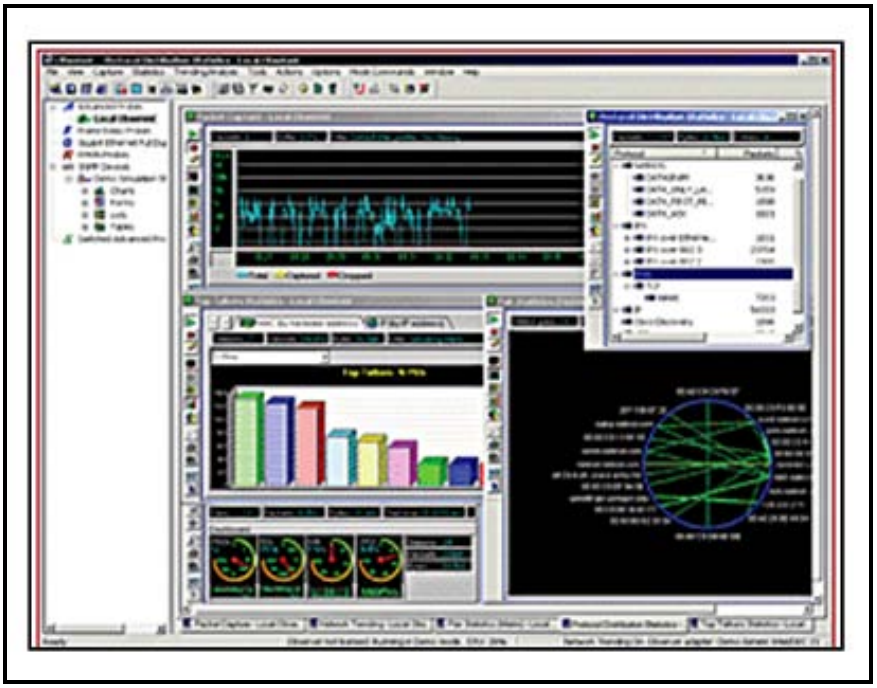


Figura 1.35 Pantalla de Observer

Características particulares de Observer, para el análisis y monitoreo de redes:

- Gran capacidad de interpretación y decodificación de protocolos (>500).
- Útiles comentarios del sistema experto.
- Gran versatilidad y facilidad de manejo de ventanas para determinar problemas.
- La excelente utilidad, facilidad y claridad de sus reportes.

Observer cuenta con los examinadores Advanced y RMON que recolectan la información de un punto remoto para enviársela a la consola de Observer, con éstas, es posible monitorear LANs, WLANs o WANs desde un punto central.

1.4.2.3 Netlog

Es un software de dominio público diseñado por la Universidad de Texas, es una herramienta que [42] genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red (los programas pueden ejecutarse en modo promiscuo) que pudiera ser "sospechoso" y que indicara un posible ataque a una máquina (por la naturaleza de ese tráfico).

El paquete está formado por el siguiente conjunto de programas:

- Tcplogger.
- Udplogger.
- Icmplogger.

1.4.2.3.1 Tcplogger

Este programa escucha todos los servicios sobre TCP, dejando una traza de cada servicio en un archivo de trazas, indicando la hora, la máquina origen y el puerto de esa conexión.

1.4.2.3.2 Udplogger

Es semejante al anterior, pero para los servicios sobre UDP. Los archivos que generan estas dos herramientas pueden ser útiles también para detectar ataques de tipo SATAN o ISS, ya que en los archivos de trazas se aprecian intentos de conexión muy cortos en el tiempo a puertos (tcp o udp) de forma consecutiva.

1.4.2.3.3 Icmplogger

Se encarga de trazar el tráfico de icmp. Estos programas pueden guardar su información en ASCII o en formato binario. En este segundo caso, el programa dispone de una herramienta (extract) que permite consultar los archivos de trazas dándole patrones de búsqueda, como puede ser el tráfico desde una red concreta, los intentos de conexión a puertos específicos, etc.

CAPÍTULO II: ELABORACIÓN DE LAS POLÍTICAS DE SEGURIDAD

2.1 Definición

Una política de seguridad es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de información de una entidad, para proteger sus activos y la reputación de la misma.

Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.

2.2 Cumplimiento Obligatorio

El cumplimiento de las políticas y estándares de seguridad son obligatorio y debe ser considerado como una condición en los contratos del personal.

La empresa puede obviar algunas de las políticas definidas en este documento, únicamente cuando se ha demostrado que el cumplimiento de dichas políticas tendría un impacto significativo e inaceptable para el negocio.

Toda excepción debe ser documentada y aprobada por el área de seguridad informática y el área de auditoria interna, detallando el motivo que justifica el no cumplimiento de la política.

2.3 Parámetros para Establecer las Políticas de Seguridad

Toda empresa para desarrollar políticas de seguridad debe cumplir con ciertas etapas, como: Evaluación de riesgos, identificación de amenazas y asignación de responsabilidades.

Al comenzar el proceso de elaboración de las políticas de seguridad, puede hacerlo basándose en un sistema estandarizado para luego personalizarlo de acuerdo con sus requerimientos específicos, limitaciones de financiación e infraestructura existente.

2.3.1 Identificación de Amenazas

Estas amenazas son externas o internas:

Amenazas Externas: Se originan fuera de la organización y son los virus gusanos, caballos de Troya, intentos de ataques de los hackers, retaliaciones de ex - empleados o espionaje industrial.

Amenazas Internas: Son amenazas que provienen del interior de la empresa y que pueden ser muy costosas porque el infractor tiene mayor acceso y perspicacia para saber las partes mas sensibles e importantes. Las

amenazas internas incluyen: acceso físico y lógico no autorizado a los dispositivos de red de la empresa. Además el uso indebido del acceso a Internet por parte de los empleados, así como los problemas que podrían ocasionar los empleados al enviar y revisar el material ofensivo a través de Internet.

En el **Anexo A** se muestra la matriz de las amenazas, vulnerabilidades con su implicancia y medida de seguridad.

2.3.2 Evaluación de Riesgos

Éste puede ser uno de los componentes más desafiantes en el desarrollo de las políticas de seguridad. Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad.

En la evaluación de riesgos es importante identificar:

- Áreas vulnerables.
- Pérdida potencial.
- Selección de controles y objetivos para mitigar los riesgos, indicando las razones para su inclusión o exclusión.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos. Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse acabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

Con el propósito de evaluar los riesgos, las amenazas y vulnerabilidades en cualquier empresa, se debe llevar a cabo entrevistas con el siguiente personal:

- Gerente Propietario.
- Gerente de división de negocios.
- Gerente de Sistemas.
- Gerente de Departamento Técnico.

En el **Anexo B** está la matriz que muestra los resultados obtenidos de la evaluación. Esta presenta los sistemas involucrados, las implicancias de seguridad asociadas al uso del sistema y los estándares o medidas propuestas para minimizar los riesgos.

2.3.3 Asignación de Responsabilidades

La seguridad de las redes es una responsabilidad de la empresa compartida por todos los empleados. Por consiguiente, debe tenerse en cuenta la creación de un equipo de desarrollo que ayude a identificar las amenazas potenciales en todas las áreas de la empresa. Sería ideal la participación de un representante por cada departamento de la compañía para garantizar que existe una clara dirección y un apoyo manifiesto de la gerencia a las iniciativas de seguridad. Los principales integrantes del equipo serían el administrador de redes, un asesor jurídico, un ejecutivo superior y representantes de los departamentos de Recursos Humanos y Relaciones Públicas.

Este equipo debe promover la seguridad dentro de la organización mediante un adecuado compromiso y una apropiada reasignación de recursos. Un equipo de esta índole comprende las siguientes acciones:

a) Revisar y aprobar la política y las responsabilidades generales en materia de seguridad.
b) Monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes.
c) Revisar y monitorear los incidentes relativos a la seguridad.

2.4 Políticas de Seguridad basadas en la ISO 17799

La ISO ha reservado la serie ISO/IEC 27000 para una gama de normas de gestión de la seguridad de la información. Esta consta de una serie de revisiones, sin embargo la única que hace referencia a buenas prácticas para proteger la información es la 27002 que esta basada en la ISO 17799. Con el objetivo de contar con una guía para la protección del hardware de la empresa se elaborarán las políticas de seguridad tomando en cuenta el estándar de seguridad de información antes mencionado [43].

2.4.1 Inventario de Activos

Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos, y también pueden ser necesarios para otros propósitos de la empresa, como los relacionados con sanidad y seguridad, seguros o finanzas (administración de recursos). El proceso de compilación de un inventario de activos es un aspecto importante de la administración de riesgos. Una organización debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la organización puede entonces asignar niveles de protección proporcionales al valor e importancia de los activos.

Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información. Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo (importante cuando se emprende una recuperación posterior a una pérdida o daño). Ejemplos de activos asociados a sistemas de información son los siguientes:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada.
- Recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales, por ejemplo: calefacción, iluminación, energía eléctrica, aire acondicionado.

2.4.2 Perímetro de Seguridad Física

La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor de las sedes de la organización y de las instalaciones de procesamiento de información. Cada barrera establece un perímetro de seguridad, cada uno de los cuales incrementa la protección total provista.

Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información. Un perímetro de seguridad es algo delimitado por una barrera, por ejemplo: una pared, una puerta de acceso controlado por tarjeta o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos.

Se deben considerar e implementar los siguientes lineamientos y controles, según corresponda:

- El perímetro de seguridad debe estar claramente definido.

- El perímetro de un edificio o área que contenga instalaciones de procesamiento de información debe ser físicamente sólido. Por ejemplo: no deben existir claros (aberturas) en el perímetro o áreas donde pueda producirse fácilmente una irrupción. Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ejemplo: mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal autorizado.
- Las barreras físicas deben, si es necesario, extenderse desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, la ocasionada por incendio e inundación.
- Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.

2.4.3 Controles de Seguridad Física

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:

- Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ejemplo: tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.
- Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.

- Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

2.4.4 Ubicación y Protección de Equipos

El equipamiento debe ser ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado. Se deben tener en cuenta los siguientes puntos:

- El equipamiento debe ser ubicado en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.
- Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso.
- Los ítems que requieren protección especial deben ser aislados para reducir el nivel general de protección requerida.
- Se deben adoptar controles para minimizar el riesgo de amenazas potenciales, por ejemplo: robo, incendio, explosivos, humo, agua (falta de suministro), polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica, radiación electromagnética.
- La organización debe analizar su política respecto de comer, beber y fumar cerca de las instalaciones de procesamiento de información.

- Se deben monitorear las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.
- Se debe tener en cuenta el uso de métodos de protección especial, como las membranas de teclado, para los equipos ubicados en ambientes industriales.
- Se debe considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización, por ejemplo: un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle.

2.4.5 Suministro de Energía

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Se debe contar con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos. Entre las alternativas para asegurar la continuidad del suministro de energía podemos enumerar las siguientes:

- Múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía.

- Suministro de energía ininterrumpible (UPS).
- Generador de respaldo.

Se recomienda una UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la organización. Los planes de contingencia deben contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.

Se debe tener en cuenta el empleo de un generador de respaldo si el procesamiento ha de continuar en caso de una falla prolongada en el suministro de energía. De instalarse, los generadores deben ser probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor.

Se debe disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.

Asimismo, los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación

crítica. Se debe proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se debe implementar protección contra rayos en todos los edificios y se deben adaptar filtros de protección contra rayos en todas las líneas de comunicaciones externas.

2.4.6 Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño. Se deben tener en cuenta los siguientes controles:

- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.
- El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.
- Entre los controles adicionales a considerar para los sistemas sensibles o críticos se encuentran los siguientes:

1. Instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
2. Uso de rutas o medios de transmisión alternativos.
3. Uso de cableado de fibra óptica.
4. Iniciar barridos para eliminar dispositivos no autorizados conectados a los cables.

2.4.7 Mantenimiento de los Equipos

El equipamiento debe mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes. Se deben considerar los siguientes lineamientos:

- El equipamiento debe mantenerse de acuerdo con los intervalos servicio y especificaciones recomendados por el proveedor.
- Sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo.
- Deben implementarse controles cuando se retiran equipos de la sede de la organización para su mantenimiento.
- Se debe cumplir con todos los requisitos impuestos por las pólizas de seguro.

2.4.8 Seguridad del Equipamiento fuera de la Organización

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la organización, deber ser autorizado por la gerencia del área de administración de la seguridad, sin importar quien es el propietario del mismo. La seguridad provista debe ser equivalente a la suministrada dentro de ámbito de la organización, para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma. El equipamiento involucra todo tipo de computadores personales y otros dispositivos necesarios para el trabajo en el domiciliario o que es transportado fuera del lugar habitual de trabajo.

Se deben considerar los siguientes lineamientos:

a) El equipamiento y dispositivos retirados del ámbito de la organización no deben permanecer desatendidos en lugares públicos. Las computadoras personales deben ser transportadas como equipaje de mano y de ser posibles enmascaradas durante el viaje.
b) Se deben respetar permanentemente las instrucciones del fabricante, por ej: protección por exposición a campos electromagnéticos fuertes.
c) Los controles de trabajo en domicilio deben ser determinados a partir de un análisis de riesgo y se aplicarán controles adecuados según corresponda, por ejemplo: gabinetes de archivo con cerradura, políticas de escritorio limpios y control de acceso a computadoras.

d) Una adecuada cobertura de seguro debe estar en orden para proteger el equipamiento fuera del ámbito de la organización.

2.4.9 Reutilización o Eliminación de Equipos

La información puede verse comprometida por una acción descuidada o una reutilización del equipamiento. Los medios de almacenamiento que contienen material sensitivo, deben ser físicamente destruidos o sobrescritos en forma segura en vez de utilizar las funciones de borrado estándar.

Todos los elementos del equipamiento que contengan dispositivos de almacenamiento, por ejemplo discos rígidos no removibles, deben ser controlados para asegurar que todos los datos sensitivos y el software bajo licencia, han sido eliminados o sobrescritos antes de su baja. Puede ser necesario realizar un análisis de riesgo a fin de determinar si medios de almacenamiento dañados, conteniendo datos sensitivos, deben ser destruidos, reparados o desechados.

2.4.10 Ruta Forzosa

Puede resultar necesario controlar el camino desde la terminal de usuario hasta el servicio informático. Las redes están diseñadas para permitir el

máximo alcance de distribución de recursos y flexibilidad de ruteo. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de negocios, o para el uso no autorizado de servicios de información. Estos riesgos pueden reducirse mediante la incorporación de controles, que limiten la ruta entre una terminal de usuario y los servicios del computador, a los cuales sus usuarios están autorizados a acceder, por ejemplo creando un camino forzado.

El objetivo de un camino forzado es evitar que los usuarios seleccionen rutas fuera de la trazada entre la terminal de usuario y los servicios a los cuales el mismo esta autorizado a acceder.

Esto normalmente requiere la implementación de varios controles en diferentes puntos de la ruta. El principio es limitar las opciones de ruteo en cada punto de la red, a través de elecciones predefinidas.

A continuación se enumeran los ejemplos pertinentes:

a) Asignación de números telefónicos o líneas dedicadas.
b) Conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
c) Limitar las opciones de menú y submenú de cada uno de los usuarios.
d) Evitar la navegación ilimitada por la red.

e) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.

f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo, firewalls.

g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro de la organización.

2.4.11 Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la empresa, por ejemplo accesos mediante discado. Por consiguiente, el acceso de usuarios remotos debe estar sujeto a la autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros, por ejemplo los métodos basados en el uso de técnicas criptográficas pueden proveer de una fuerte autenticación. Es importante determinar mediante una evaluación de riesgos el nivel de protección requerido. Esto es necesario para la adecuada selección del método.

La autenticación de usuarios remotos puede llevarse a cabo utilizando, por ejemplo, una técnica basada en criptografía, “tokens” de hardware, o un

protocolo de pregunta/respuesta. También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de rellamada o dail-back, por ejemplo utilizando módems de dial-back, pueden brindar protección contra conexiones no autorizadas y no deseadas a las instalaciones de procesamiento de información de la organización. Este tipo de control autentica a los usuarios que intentan establecer una conexión con una red de la organización desde locaciones remotas. Al aplicar este control, la organización no debe utilizar servicios de red que incluyan desvío de llamadas o, si lo hacen, deben inhabilitar el uso de dichas herramientas para evitar las debilidades asociadas con la misma.

Asimismo, es importante que el proceso de rellamada garantice que se produzca una desconexión real del lado de la organización. De otro modo, el usuario remoto podría mantener la línea abierta fingiendo que se ha llevado a cabo la verificación de rellamada. Los procedimientos y controles de rellamada deben ser probados exhaustivamente respecto de esta posibilidad.

2.4.12 Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la empresa. Por consiguiente, las conexiones a sistemas informativos remotos deben ser autenticadas. Esto es particularmente importante si la conexión utiliza una red que esta fuera de control de la gestión de seguridad de la organización. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

2.4.13 Protección de Puertos de Diagnóstico Remoto

El acceso a los puertos de diagnostico debe ser controlado de manera segura. Muchas computadoras y sistemas de comunicación son instalados con una herramienta de diagnostico remoto por discado, para uso de los ingenieros de mantenimiento. Si no están protegidos, estos puertos de diagnostico proporcionan un medio de acceso no autorizado. Por consiguiente, deben ser protegidos por un mecanismo de seguridad apropiado, por ejemplo una cerradura de seguridad y un procedimiento que garantice que solo son accesibles mediante un acuerdo entre el gerente de

servicios informativos y el personal de soporte de hardware y software que requiere acceso.

2.4.14 Subdivisión de Redes

Las redes se están extendiendo en forma creciente, más allá de los límites tradicionales de la organización, a medida que constituyen sociedades con requerimientos de interconexión, o uso compartido de instalaciones de procesamiento de información y redes. Dichas extensiones pueden incrementar el riesgo de acceso no autorizado a sistemas de información ya existentes que utilizan la red, algunos de los cuales podrían requerir de protección contra otros usuarios de red, debido a su sensibilidad o criticidad. En tales circunstancias, se debe considerar la introducción de controles dentro de la red, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.

Lo que se debe aplicar para controlar la seguridad de redes extensas es dividirlas en dominios lógicos separados, por ejemplo: Dominios de red internos y externos de una organización cada uno protegido por un perímetro de seguridad definido. Dicho perímetro puede ser implementado mediante la instalación de una compuerta (“gateway”) segura entre las dos redes que han de ser interconectadas, para controlar el acceso y flujo de información entre

los dominios. Este “gateway” debe ser configurado para filtrar el tráfico entre los dominios y para boquear el acceso no autorizado. Un ejemplo de este tipo de “gateway” es lo que comúnmente se conoce como firewall.

2.4.15 Control de Conexión a las Redes

Los requerimientos de la política de control de accesos para redes compartidas, especialmente aquellas que se extiendan más allá de los límites de la organización, pueden requerir la incorporación de controles para limitar la capacidad de conexión de los usuarios. Dichos controles pueden implementarse mediante “gateways” de red que filtren el tráfico por medio de reglas o tablas previamente definidas. Las restricciones aplicadas deben basarse en políticas de accesos de las aplicaciones de la empresa, y deben mantenerse y actualizarse de conformidad.

A continuación se enumeran ejemplos de aplicaciones a las cuales deben aplicarse restricciones:

a) Correo electrónico.
b) Transferencia unidireccional de archivos.
c) Transferencia de archivos en ambas direcciones.
d) Acceso interactivo.
e) Acceso de red vinculado a hora y fecha.

2.4.16 Control de Enrutamiento en la Red

Las redes compartidas, especialmente aquellas que se extienden más allá de los límites organizacionales, pueden requerir la incorporación de controles de ruteo para garantizar que las conexiones informáticas y los flujos de información no violen la política de control de acceso de las aplicaciones comerciales. Este control es a menudo esencial para las redes compartidas con usuarios externos.

Los controles de ruteo deben basarse en la verificación positiva de direcciones de origen y destino.

La traducción de direcciones de red también constituye un mecanismo muy útil para aislar redes y evitar que las rutas se propaguen desde una organización a la red de otra. Pueden implementarse en software o hardware. Quienes lleven a cabo la implementación deben estar al corriente de la fortaleza de los mecanismos utilizados.

2.4.17 Autenticación de Mensajes

La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados o una corrupción del contenido de un mensaje transmitido

electrónicamente. Puede implementarse mediante hardware o software soportando un dispositivo físico de autenticación de mensajes o un algoritmo software.

Se debería establecer la autenticación de mensajes para aplicaciones en las que hay un requisito de seguridad para proteger la integridad del contenido del mensaje, por ejemplo, transferencia electrónica de fondos, especificaciones, contratos, propuestas u otros intercambios electrónicos de datos importantes. Se pueden usar técnicas criptográficas y como un medio adecuado para implementar dicha autenticación. Se debería realizar un gravamen de los riesgos de la seguridad para determinar si se requiere la autenticación de mensajes y para identificar la forma más apropiada de la puesta en práctica.

La autenticación de mensajes no protege el contenido de la información frente a su divulgación no autorizada.

2.4.18 Uso de Controles Criptográficos

La decisión sobre la idoneidad de una solución criptográfica debería verse como parte de un proceso más amplio de evaluación de riesgos y selección de medidas de control. Se debería realizar una evaluación de riesgos para

determinar el nivel de protección que debería recibir la información; evaluación que luego puede utilizarse para determinar si las medidas criptográficas son adecuadas, que tipo de medida se debería aplicar, con que propósito y en que proceso del negocio.

La organización debería desarrollar una política sobre el uso de controles criptográficos para la protección de la información. Tal política es necesaria para maximizar los beneficios y minimizar los riesgos del uso de dichas técnicas, evitando su uso incorrecto o inapropiado.

Cifrado

El cifrado es una técnica criptográfica que puede utilizarse para proteger la confidencialidad de la información. Se debería usar para la protección de información sensible o crítica.

El nivel adecuado de protección se debería basar en una evaluación de riesgo, y debería tener en cuenta el tipo y la calidad del algoritmo de cifrado y la longitud de las claves criptográficas que se usarán.

En la implementación de la política criptográfica de la organización se deberían tener en cuenta las regulaciones y restricciones nacionales que se aplican a distintas partes del mundo para el uso de las técnicas criptográficas

y el cifrado de las transmisiones internacionales de datos. Además de los controles que se aplican a la exportación e importación de tecnología criptográfica.

Se debería contemplar el asesoramiento de especialistas para determinar el nivel de apropiado protección, para elegir los productos adecuados que proporcionen la protección requerida y la implementación de un sistema seguro de gestión de claves. Además, se debería contemplar, la opinión de consultores legales sobre las leyes y regulación aplicables al uso previsto del cifrado en la organización.

Firmas Digitales

Las firmas digitales proporcionan un medio de proteger la autenticidad y la integridad de los documentos electrónicos. Por ejemplo, se usan en el comercio electrónico cuando hay necesidad de verificar quien firma un documento electrónico y de verificar si el contenido del documento firmado ha sido cambiado.

Las firmas digitales pueden aplicarse a todo tipo de documento susceptible de procesamiento electrónico, por ejemplo, para firmar pagos electrónicos, transferencia de fondos, contratos o acuerdos. Las firmas digitales pueden implementarse mediante una técnica criptográfica basada en un único par de

claves interrelacionadas, una para crear la firma (clave privada) y otra para comprobarla (clave pública).

Se debería cuidar la protección de la confidencialidad de la clave privada, que ha de mantenerse en secreto ya que todo el que acceda a ella puede firmar documentos como pagos o contratos como si falsificara la firma del propietario de la clave. Así mismo, es importante la protección de la integridad de la clave pública, que se consigue usando un certificado de dicha clave pública.

Se necesitan ciertas consideraciones sobre el tipo y calidad del algoritmo de firma y la longitud de la clave por utilizar. Las claves criptográficas usadas para las firmas deberían ser distintas de las usadas para cifrado.

Al usar firmas digitales se debería tener en cuenta toda legislación relativa que describe las condiciones en las que una firma digital tiene validez legal. Por ejemplo, en el caso del comercio electrónico es importante conocer la situación legal de las firmas digitales. Puede haber necesidad de añadir contratos u otros acuerdos con validez legal para dar soporte al uso de las firmas digitales cuando el marco legal no sea adecuado. Se debería contemplar el asesoramiento legal sobre las leyes y regulación aplicables para el uso previsto de firmas digitales por la Organización.

CAPÍTULO III: CASO DE ESTUDIO

3.1 Análisis de la red de FIBERNET

FIBERNET es una organización que presta el servicio de INTERNET de banda ancha a zonas residenciales, utilizando una infraestructura híbrida de fibra óptica y cobre. Esta inicio operaciones en febrero del año 2007 y actualmente cuenta con dos nodos para cobertura en zonas residenciales ubicadas en Samborondón. Ver mapa de cobertura en **Anexo G**.

Su topología de red es Estrella Extendida y consta de seis subredes:

- Redes de Acceso (2).
- Red de Transporte.
- Core IP.
- Red de Administración o Intranet.
- Red de servidores.

El diseño de la Red de Fibernet se muestra en la figura 3.1.

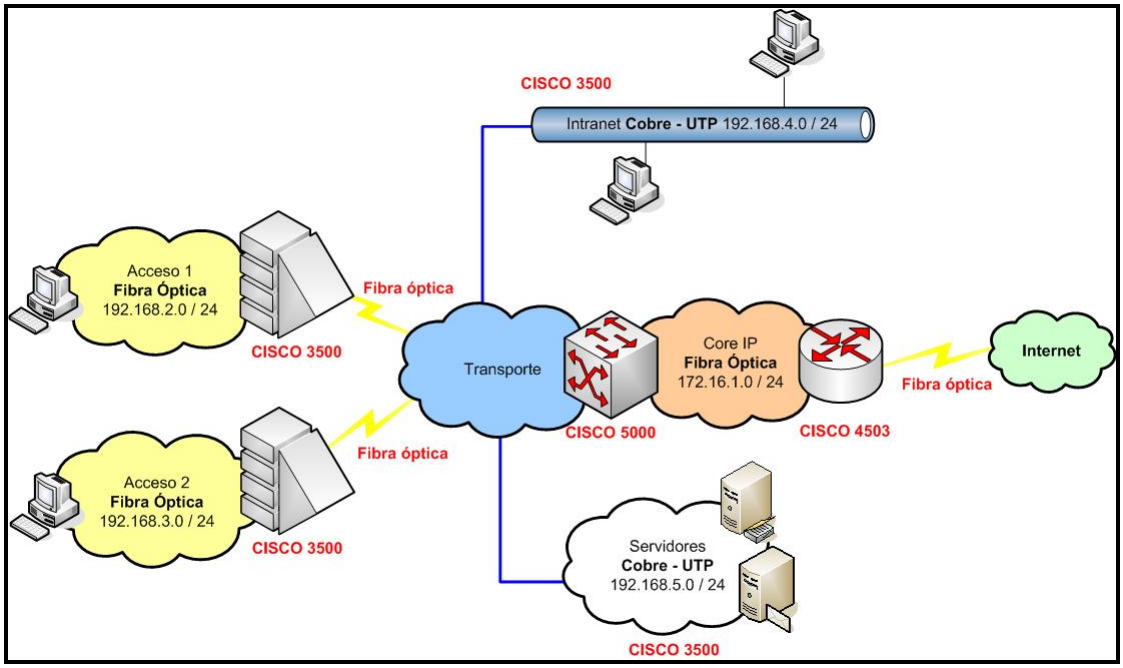


Figura 3.1 Diseño de la Red de FIBERNET

Las redes de acceso constan de un conmutador CISCO 3500 a cada uno llega un enlace de fibra óptica de la red de transporte. Este ofrece interfaces FastEthernet y GigabitEthernet. La velocidad de transmisión que se puede fijar para los cliente es de hasta 1000 Mbps full duplex. La capacidad de estas redes es 102 usuarios, actualmente cuenta con 54. La cobertura máxima de servicio es 2Km. En la figura 3.2 se describe esta red.

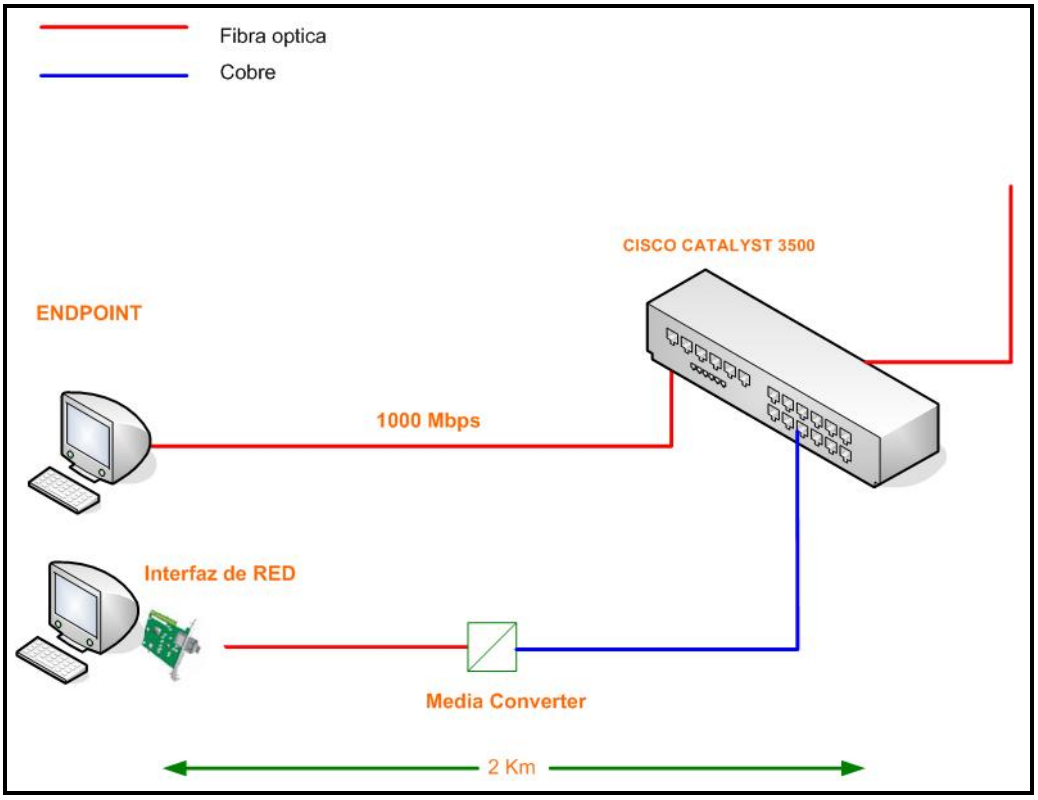


Figura 3.2 Redes de Acceso de FIBERNET

La red de transporte está construida sobre un backbone de fibra óptica y cobre. Esta consta de un nodo CISCO 5000 de capa dos y tres de diseño modular. Ofrece puntos de conexión FastEthernet y GigabitEthernet. La red de transporte se conecta con las redes de acceso, servidores e intranet aplicando VLANs dinámicas y tecnologías trunking de alta velocidad hasta 1000 Mbps. Además se conecta con el Core IP utilizando el protocolo de enrutamiento OSPF. La red de transporte se muestra en la figura 3.3.

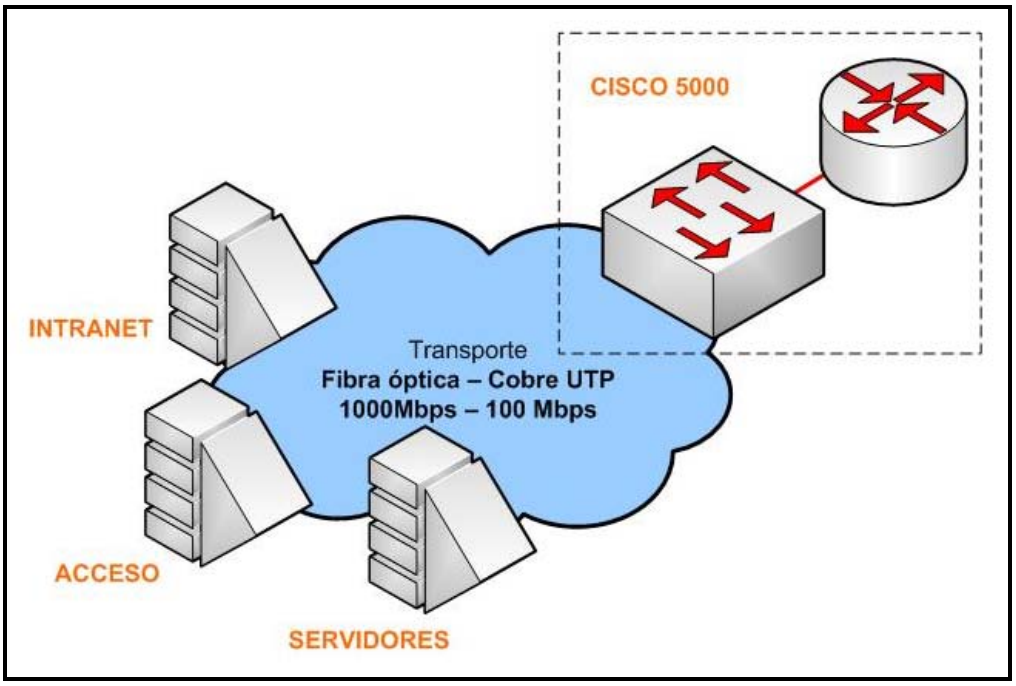


Figura 3.3 Red de Transporte de FIBERNET

La Intranet o red de administración acceso cuentan con el conmutador CISCO 2960, con puntos de conexión Fastethernet y Gigabitethernet para cada una de las estaciones de trabajo de la empresa. La velocidad de transmisión configurada en esta red es 100Mbps full duplex sobre medio de cobre. La red de servidores interna es de igual diseño. Los servidores instalados en esta red son: FTP y servidor multitarea (SysLog, SMNP). En la figura 3.4 se describe estas redes.

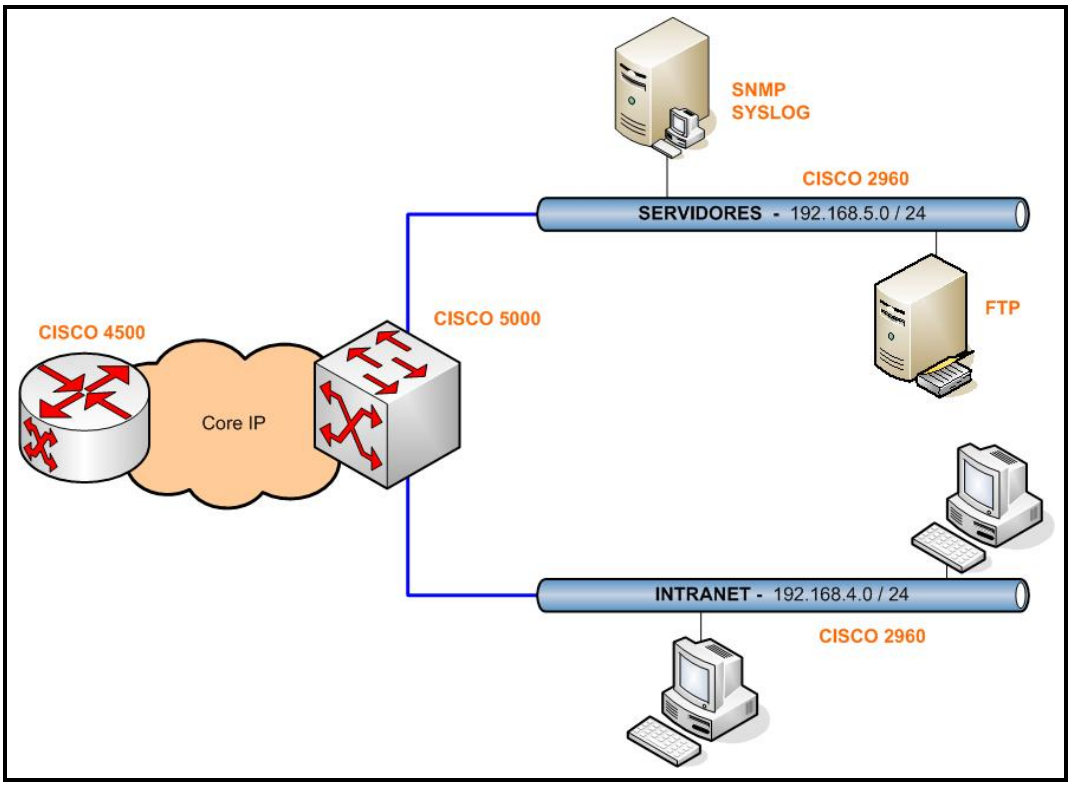


Figura 3.4 Redes de Servidores e Intanet de FIBERNET

El Core IP consta del Cisco Catalyst 4503 de diseño modular, la única tarjeta instalada es la WS-X4448-GB que ofrece 48 puntos de conexión GigabitEthernet. Se enlaza a la red de transporte con fibra óptica y velocidades de 1000Mbps full duplex. La conexión a INTERNET se establece a través de un Carrier con un enlace de fibra óptica. La figura 3.5 describe esta red.

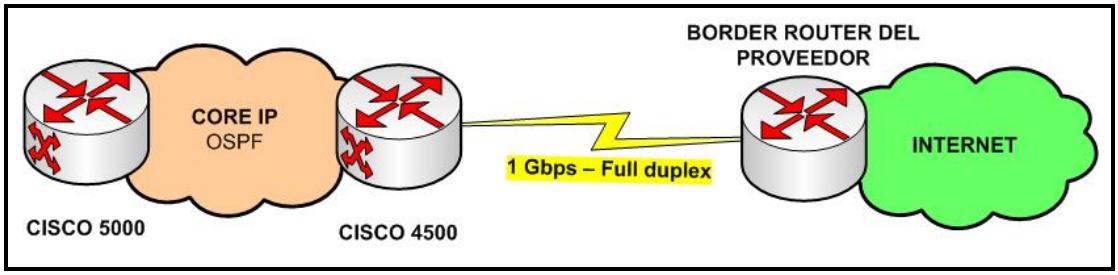


Figura 3.5 Core IP de FIBERNET

3.2 Implementación de las Políticas de Seguridad

Luego de haber identificado las amenazas y llevado a cabo el análisis de riesgo de la red de FIBERNET, se procedió a implementar cada una de las políticas detalladas en el capitulo 2.

El plan de implementación contiene cada una de las actividades realizadas para cumplimiento de las políticas elaboradas y el tiempo estimado de ejecución. El cronograma de implementación de las políticas de seguridad se muestra en el **Anexo I**.

Inventario de Equipos de Comunicaciones

Tiempo: 1 semana

Descripción: Elaboración de un inventario de activos de la red de datos. Los aspectos más importantes a definir son:

- Propietario.

- Nivel de importancia.
- Ubicación.
- Código de identificación.

Observación: Ver el inventario en el **Anexo C**.

Perímetro de Seguridad Física

FIBERNET ya poseía diversas barreras físicas alrededor de las sedes de la organización y de las instalaciones de procesamiento de información.

El perímetro de la Empresa posee cercos eléctricos de 5 líneas. Luego tenemos la Garita donde se encuentran 2 guardias verificando a las personas y carros que ingresan a la sede. Otro perímetro de seguridad física es la puerta principal del Edificio.

Dentro de la empresa están la puerta del área de seguridad informática y la puerta de la sala de telecomunicaciones.

Cabe resaltar que las puertas principales del edificio, la puerta del departamento técnico, la puerta de la sala de CCTV, la puerta del área de seguridad informática y la puerta de la sala de telecomunicaciones poseen cerraduras electromagnéticas y contactos magnéticos.

Tiempo: 3 días

Descripción: Instalación de dos lectores de proximidad (figura 3.6) en la puerta principal del edificio: uno para la entrada y otro para la salida, cuyo ingreso al edificio es validado por la tarjeta de proximidad (figura 3.7).

Figura 3.6 Lectores de Proximidad

Figura 3.7 Tarjeta de Proximidad

Instalación de 2 lectores de proximidad física en la puerta de del área de seguridad informática, uno para la entrada y otro para la salida.

En la sala de telecomunicaciones se instaló 2 lectores: un lector combinado (biométrico de huella digital y teclado) para la entrada, y un lector de proximidad para la salida.

Controles de Seguridad Física

Tiempo: 3 días

Descripción: Instalación de un panel de control de accesos, capacidad para 8 lectores.

Cuando un visitante desea entrar a las instalaciones de FIBERNET, ésta debe pasar por la puerta de la garita, donde el guardia asignado solicita a los visitantes la cédula de identidad y llena el registro en el computador que se muestra en el **Anexo D**.

Si el visitante posee carro, el guardia asignado pedirá de igual manera a cada una de las personas visitantes la cédula de identidad. Luego de esto el mismo guardia asignará un carnet de VISITANTE (tarjeta de proximidad) a cada persona. Esta tarjeta se muestra en la figura 3.8.

Figura 3.8 Tarjeta de Proximidad para Visitantes

Tanto el personal de la empresa como los visitantes podrán validar el ingreso por la puerta principal del edificio con la tarjeta de proximidad. Al ingresar la persona por ésta puerta, el lector de proximidad registra la hora y el código de cada tarjeta. Cuando la persona desee salir por la puerta principal, tiene que validar el lector de proximidad de salida quedando registrado la hora y el código de la tarjeta de proximidad.

La recepcionista verificará que todo el personal de la empresa y los visitantes porten su carnet de identificación (tarjeta de proximidad). Además instruirá a éstos últimos sobre los requerimientos de seguridad y los procedimientos de emergencia.

Al área de seguridad informática sólo podrán ingresar el personal del área de sistemas y el personal del departamento técnico mediante la tarjeta de

proximidad. Cabe mencionar que en el área de seguridad informática trabajan tres personas.

A la sala de telecomunicaciones sólo podrán ingresar el personal del área de seguridad informática, área de sistemas y departamento técnico mediante la tarjeta de proximidad, una clave de 8 dígitos asignada y su huella del dedo pulgar derecho. En caso de que un equipo de ésta sala requiera mantenimiento por parte de empresas externas, el jefe del área de seguridad informática supervisará a la(s) persona(s) en todo momento.

Cada vez que la persona salga de la sala de telecomunicaciones deberá llenar el siguiente registro el cual se encuentra en el buzón plástico de reportes al lado izquierdo de la puerta. Este reporte de servicio técnico se lo detalla en el **Anexo E**.

FIBERNET exige de manera obligatoria que todo el personal exhiba su carnet de identificación (tarjeta de proximidad). Además cuestiona la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.

Los derechos de acceso a las áreas protegidas se revisan y actualizan cada semana.

Ubicación y Protección de Equipos

Actualmente FIBERNET cuenta con los siguientes elementos para protección de sus equipos:

- Una sala para C.C.T.V. que consta de: ocho cámaras de TV. Un Grabador digital DVR, 18 canales, 500 GB, hasta 450 IPS, con capacidad hasta 32 cámaras IP (30 IPS por cámara) modelo DB18C3025R2.
- Un panel de Panel de alarmas, capacidad para 128 puntos, teclado LCD, comunicador para transmisión vía telefónica y vía red, transformador y batería de respaldo. Cinco Detectores de Humo, direccionable, inteligente, fotoeléctrico, dos hilos. Tres Alarmas Manuales de Incendio, direccionable.
- Extintores PQS (Polvo Químico Seco). Las ubicaciones de estos extintores se encuentran en el plano de la empresa. Ver **Anexo H**. Los extintores se encuentran en el cuarto del generador (20 lbs), en la sala de UPS (20 lbs), en la sala de telecomunicaciones (20 lbs) y en la recepción (10 lbs).

Es esencial que el ambiente de la sala de telecomunicaciones pueda mantenerse las 24 horas del día, los 365 días del año, y que sean independientes de los controles del área de trabajo exterior. La sala de telecomunicaciones tiene suficiente calefacción, ventilación y aire

acondicionado (HVAC) para que la temperatura ambiente oscile aproximadamente entre los 17°C y los 21°C (entre los 64°F y los 75°F) mientras todos los equipos de LAN están en pleno funcionamiento.

La humedad relativa oscila entre un 30% y un 50%. El incumplimiento de estas especificaciones particulares podría provocar la corrosión severa de los hilos de cobre que están dentro de los UTP y de los STP. Esta corrosión reduce la eficacia del funcionamiento de la red.

Tiempo: 3 días

Descripción: Instalación de ocho detectores de humo, direccionable, inteligente, fotoeléctrico, dos hilos. La ubicación de estos detectores la podemos observar en el **Anexo H**.

Instalación de un Detector térmico, rapidez de incremento de temperatura en el cuarto para el generador eléctrico.

Se adicionó un extintor de 10 lbs en el pasillo entre la gerencia y la sala de junta, uno de 20 lbs en la sala de C.C.T.V. y uno en el área de seguridad informática.

Suministro de Energía

La empresa posee Suministro de energía ininterrumpible (UPS) que está ubicado al lado de la Sala de Telecomunicaciones. Este puede soportar hasta 8 horas ininterrumpidas.

En caso de una falla prolongada en el suministro de energía se emplea el generador de respaldo. El generador se prueba periódicamente de acuerdo con las instrucciones del fabricante o proveedor. Además se dispone de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.

Los interruptores de emergencia están ubicados en la parte derecha de la Sala de Telecomunicaciones, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.

La empresa provee iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Además posee protección contra rayos en el edificio y tiene adaptados filtros de protección contra rayos en todas las líneas de comunicaciones externas.

Tiempo: 2 días

Descripción: Se revisó la capacidad del UPS, es decir si los KVA son los apropiados con respecto a los equipos que están conectados en él. En el **Anexo F** se detallan los equipos conectados al UPS y se analizan los KVA que estos consumen. Cabe mencionar que se toma como factor de potencia el valor de 0.700 para todos los equipos.

Seguridad del Cableado

Tiempo: 7 días

Descripción: Uso de sistemas de administración de cables especiales denominados conductos internos para cables de fibra óptica (figura 3.9). Estos consisten en una tubería de plástico que protege el cableado de fibra óptica que luego se ata a los bastidores de escalera.

Figura 3.9 Conductos internos para cables de fibra óptica

Uso de ataduras de Nylon (figura 3.10) o de plástico (figura 3.11) o de otros tipos de fijadores disponibles (figura 3.12), como los ganchos J (figura 3.13)

para asegurar los cables y agruparlos. Se los debe posicionar a intervalos que no excedan los 1,5 m.

Figura 3.10 Ataduras de Nylon

Figura 3.11 Ataduras de Plástico

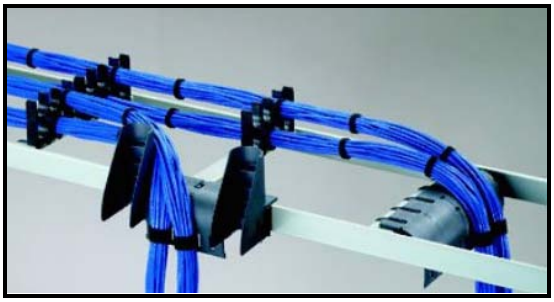


Figura 3.12 Otro tipo de Fijadores

Figura 3.13 Fijador tipo Gancho J

Instalación de soportes verticales y horizontales en los bastidores (figura 3.14) de telecomunicaciones para distribuir los cables de manera prolija y ordenada. Debe haber como mínimo dos soportes verticales y uno horizontal.

Aplicación de rotulación en cada extremo del cable con el origen y destino. Se ubico la etiqueta a 15 cm. del conector o de la chaqueta.

Para el transporte de la fibra fuera de las instalaciones será protegida con una manguera metálica hasta llegar al suelo donde será enterrada a una profundidad de 1.5 metros de profundidad aunque se admite que sea hasta de 3 metros.

Instalación de tres Racks con puerta cada uno de 84" x 44UR x 1m.

Figura 3.14 Bastidores

Mantenimiento de los Equipos

Tiempo: 1 día

Descripción: La empresa respeta y hace cumplir los mantenimientos de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.

Sólo el personal técnico y de sistemas puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento. Se debe utilizar muñequeras antiestática (figura 3.15) siempre que se esté instalando, inspeccionando, actualizando o cambiando módulos en un dispositivo.

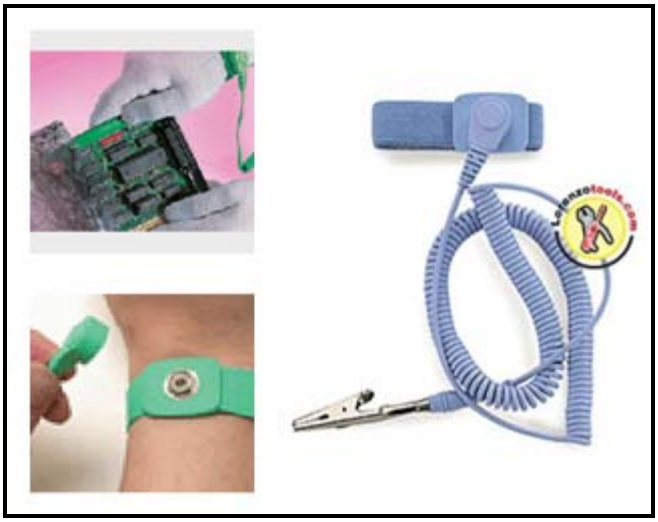


Figura 3.15 Muñequeras Antiestática

Si se necesita los servicios de un técnico externo, éste deberá ser acompañado únicamente por el Jefe del área de seguridad informática de la empresa y deberá llenar el registro ubicado en el buzón plástico al lado izquierdo de la puerta de la sala de telecomunicaciones.

En caso que se retire un equipo de la empresa para su mantenimiento, se deberá solicitar los debidos permisos por escrito indicando el posible tiempo que demandará el mantenimiento o reparación, previa aprobación del área de seguridad informática y la Gerencia.

Los equipos de computación se encuentran en superficies de trabajo protegidas contra la ESD (descarga electrostática) y poseen una alfombra de

protección contra ESD debajo de la silla del usuario de cada computadora. Éstas absorben la ESD.

Seguridad del Equipamiento fuera de la organización

Tiempo: 1 día

Descripción: Cualquier tipo de equipamientos informáticos como portátiles y otros dispositivos utilizados fuera de la organización deben ser protegidos por el responsable del equipo contra accesos no autorizados con el cable de seguridad **DEFCOM Retractable CL,** como se muestra en la figura 3.16.

Figura 3.16 Cable de Seguridad DEFCOM Retractable CL

El equipo deberá ser utilizado solo en lugares seguros.

Reutilización o Eliminación de Equipos

Tiempo: 1 semana

Descripción: A todos los equipos dados de baja se aplicaran controles para determinar si poseen medios de almacenamiento que contengan datos sensitivos. En tal situación estos deberán ser destruidos.

Seguridad de Red y Comunicaciones

Para garantizar mayor seguridad y eficiencia de la red de datos, se requiere que los equipos involucrados se encuentren adecuadamente configurados.

Tiempo: 7 días

Descripción: Para controlar el tráfico desde Internet, y evitar que seleccionen rutas o servicios no autorizados se instaló un Firewall CISCO PIX 535 (figura 3.17) entre la red de la empresa y el proveedor de Internet, definiendo tres zonas de seguridad: inside, outside y DMZ.

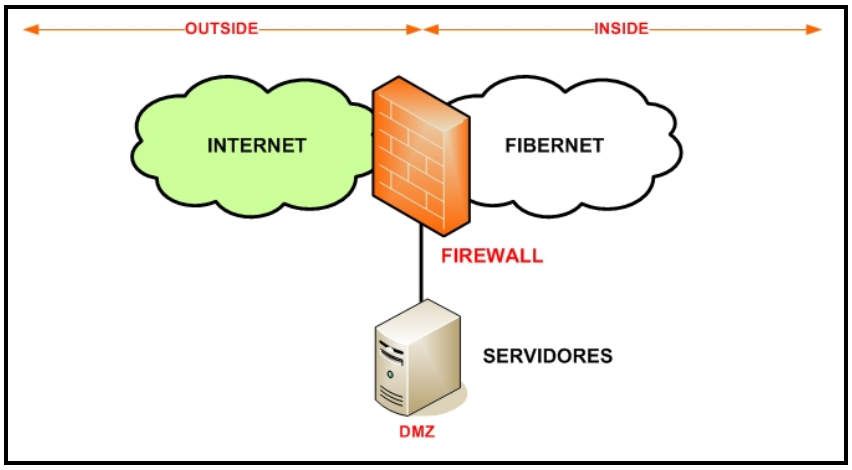


Figura 3.17 Firewall CISCO PIX 535

Con la creación de la zona DMZ la arquitectura de red se ha modificado adaptándose a las políticas de seguridad.

Implementación de NAT estático en el firewall para control y registro de todas las conexiones entrantes y salientes desde outside hacia inside.

Se crearon las siguientes reglas para permitir o rechazar conexiones:

1. Bloqueo de cualquier tipo de servicio orientado a conexión interna, y cuyo acceso externo puede ser innecesario. NFS, FTP, HTTP, DNS, SMTP, TFTP además los puertos 137, 138, 139, entre otros.
2. Bloqueo de servicios con mecanismos de autenticación débiles como TELNET.
3. Bloqueo de todos los puertos que puedan indicar una probabilidad alta de compromiso para un host.

   Back Orifice (puerto 31337)

   NetBus (puerto 12345, 12346, 20034)
4. Bloqueo de puertos de diagnóstico que pueden ser usados para recabar información o amplificar ataques de negación de servicios. ICMP, Traceroute.
5. Permitir los puertos para conexiones remotas VPN.

Creación de la zona DMZ para ubicar los servidores SMTP, DNS y HTTP evitando que las conexiones desde Internet ingresen a la red interna de datos. Además se instaló una máquina de control en la red DMZ con el propósito de monitorear todo el flujo de datos que ingresa y detectar algún tipo intrusión o ataque desde la Internet.

Se crearon las siguientes reglas para permitir o rechazar conexiones desde inside hacia DMZ:

1. El puerto DNS está permitido para todas las subredes internas.
2. El servicio SMTP y POP3 está permitido solo para los usuarios de la intranet y bloqueado para el resto de subredes internas.
3. El servicio HTTP está autorizado para todas las subredes internas, con sus respectivos mecanismos de autenticación.
4. Los puertos de diagnóstico (ICMP), configuración remota (TELNET) y entre otros están permitidos únicamente para los hosts de las áreas de sistemas, administración de seguridad y departamento técnico.

Reglas para permitir o rechazar conexiones desde outside hacia DMZ:

1. Los puertos DNS, ICMP, TELNET así como otros puertos destinados a conexiones internas están denegados.

2. Los puertos de aplicación HTTP, SMTP están permitidos para conexiones externas con los respectivos mecanismos de autenticación.

Instalación del servidor NAS (Network Access Server) en la red interna de servidores (figura 3.18), para conexiones externas. El protocolo VPN utilizado es el IPSec y el mecanismo de implementación es a nivel de software. El cliente al tratar de establecer la comunicación deberá introducir su contraseña (Autenticación) y el servidor deberá revisar en su base de datos y autorizar la conexión externa.

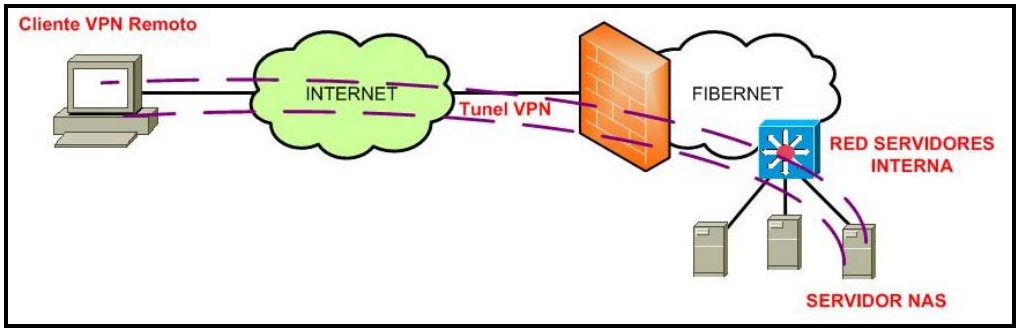


Figura 3.18 Servidor NAS (Network Access Server) en la Red Interna de Servidores

Se habilitó el mecanismo de protección de puertos en todos los conmutadores de las subredes de la empresa.

switchport port-security

Todos los puertos libres en los conmutadores serán bloqueados.

switchport security action shutdown

Subdivisión de la red interna en los siguientes dominios lógicos o VLANs, nombrándolas de acuerdo a la actividad que desempeña el grupo de terminales. Además se asocio los puertos a cada una de las VLANs. Estas son:

Vlan 1 ADMIN

Vlan 2 ACCESO1

Vlan 3 ACCESO2

Vlan 4 INTRANET

Vlan 5 SERVERS

Se estableció el protocolo troncal en el nodo de transporte basado en el estándar 802.1Q para la comunicación entre las VLANs. Siendo este a la vez el perímetro de seguridad o GATEWAY entre los dominios lógicos.

Se limitó la capacidad de conexión entre las subredes internas, aplicando listas de control de acceso en las interfaces del nodo CISCO 5000 estas son:

1. Todo el tráfico de las redes de acceso hacia la Intranet y red de servidores interna será denegado.
2. El tráfico entre redes de acceso debe ser denegado.

3. Todas las conexiones tales como: TFTP, SSH, IPSec entre otras, únicamente desde los hosts de las áreas de sistemas, administración de seguridad y departamento técnico hacia la red de servidores están permitidas. Para el resto de hosts de la Intranet y de las otras subredes están denegados.
4. Todos los puertos de diagnóstico y configuración remota están permitidos para los hosts de las áreas de sistemas, administración de seguridad y departamento técnico. Para el resto de hosts de la Intranet y de las otras subredes están denegados.

Asimismo se instaló una máquina de control en la red de transporte, para monitorear el tráfico y detectar ataques.

Observación: La configuración de cada uno de los equipos de red de datos es información que se reserva la empresa, por eso aquí no se la anexa.

3.3 Organización de la Seguridad

La administración actual de la seguridad de información se encuentra distribuida principalmente entre le área de sistemas y el departamento técnico.

Las labores de seguridad realizadas por el área de sistemas son las siguientes:

- Creación y eliminación de usuarios.
- Verificación y asignación de perfiles en las aplicaciones.
- Administración de accesos a bases de datos.

Las labores de seguridad realizadas por el departamento técnico son las siguientes:

- Monitoreo de red.
- Administración de accesos a la sala de telecomunicaciones.
- Registro de accesos a los equipos de la sala de telecomunicaciones y revisar periódicamente su configuración.

Cabe mencionar que las funciones de desarrollo y mantenimiento de políticas y estándares de seguridad no estaban definidas dentro de los roles de la organización.

3.3.1 Estructura Organizacional

Es necesaria la existencia de un área que administre la seguridad informática. Como requisito indispensable, esta área debe ser independiente del área de sistemas y departamento técnico. Los administradores de la

seguridad tendrán las funciones de controlar el cumplimiento de las políticas definidas, de realizar actualizaciones, así como coordinar esfuerzos entre todos los empleados de la empresa con sus diferentes roles. Asimismo, serán responsables de promover las políticas de seguridad e incluirlas en los objetivos del negocio.

Para este propósito se creó a lo largo de la organización los siguientes roles con sus respectivas responsabilidades:

Área de Seguridad informática

El área organizacional encargada de la administración de la seguridad informática tiene como responsabilidades:

- Establecer y documentar las responsabilidades de la organización en cuanto a la seguridad física.
- Mantener políticas y estándares de seguridad física de la organización.
- Comunicar aspectos básicos de la seguridad física a los empleados de la empresa. Esto incluye un programa de concientización.
- Desarrollar controles para las tecnologías que utiliza la empresa. Esto incluye el monitoreo de las vulnerabilidades descritas por el proveedor.
- Monitorear el cumplimiento de la política.

- Controlar e investigar incidentes de seguridad o violaciones de seguridad física.
- Realizar una evaluación periódica de las vulnerabilidades de los sistemas que conforman la red de datos.
- Evaluar aspectos de seguridad de productos de tecnologías utilizados en la empresa.
- Verificar que cada activo físico haya sido asignado a un propietario el cual debe definir los requerimientos de seguridad como políticas de protección, perfiles de acceso, respuesta ante incidentes, y sea responsable final del mismo.
- Monitorear la aplicación de los controles de seguridad física de los principales activos de la red.
- Elaborar y mantener un registro de los accesos de los usuarios a los equipos de la sala de telecomunicaciones y revisar periódicamente las configuraciones de los mismos.
- Desarrollar y administrar el presupuesto de seguridad.
- Reportar periódicamente a la gerencia de Administración y operaciones.

Área de Sistemas

Es el responsable de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad

en los sistemas que se encuentran bajo su administración. Sus responsabilidades son:

- Administrar accesos a nivel de red (sistema operativo).
- Implementar controles definidos para los sistemas de información, incluyendo investigación e implementación de actualizaciones de seguridad en coordinación con el área de seguridad informática.
- Desarrollar procedimientos de autorización y autenticación.
- Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos físicos que custodia.
- Investigar brechas e incidentes de seguridad.
- Entrenar a los empleados en aspectos de seguridad en nuevas tecnologías o sistemas implantados bajo su custodia.
- Asistir y administrar los procedimientos de backup, recuperación y plan de continuidad de sistemas.

Usuarios

Las responsabilidades de los usuarios finales, es decir, aquellas personas que utilizan los activos físicos de la empresa como parte de su trabajo diario están definidas a continuación:

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
- Reportar supuestas violaciones de la seguridad física.

- Asegurarse de ingresar información adecuada a los sistemas.
- Adecuarse a las políticas de seguridad de la organización.
- Utilizar los activos físicos únicamente para propósitos autorizados.

Propietarios de Equipos

Los propietarios de los equipos son los gerentes y jefes de las unidades de negocio, los cuales, son responsables de los equipos manipulados en las operaciones de su unidad. Las unidades de negocio deben ser conscientes de los riegos de tal forma que sea posible tomar decisiones para disminuir los mismos.

- Entre las responsabilidades de los propietarios de información se tienen:
- Asignar niveles de riesgos de los equipos.
- Revisión periódica de la asignación de niveles de riesgos a los equipos con el propósito de verificar que cumpla con los requerimientos del negocio.
- Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- Determinar los criterios y niveles de acceso a los activos físicos.
- Revisar periódicamente los niveles de acceso a los activos físicos a su cargo.

- Determinar los requerimientos de copias de configuración de los equipos que les pertenece.
- Tomar las acciones adecuadas en caso de violaciones de seguridad.
- Verificar periódicamente la integridad y coherencia de la información producto.

Auditoria Interna

El personal de auditoria interna es responsable de monitorear el cumplimiento de los estándares y guías definidas en las políticas internas. Una estrecha relación del área de auditoria interna con el área de seguridad Informática es crítica para la protección de los activos de la empresa. Por lo tanto dentro del plan anual de evaluación del área de auditoria interna se debe incluir la evaluación periódica de los controles de seguridad definidos por la empresa.

Auditoria interna debe colaborar con el área de seguridad informática en la identificación de amenazas y vulnerabilidades.

Comité de coordinación de la seguridad de la información

Dado el volumen de operaciones y tomando en cuenta las mejores prácticas de la industria se creó el comité de coordinación de seguridad, el mismo que definirá los objetivos de seguridad de la organización, supervisará y planificará todas las actividades que desarrollará el área de seguridad

informática. Además colaborara en el entendimiento de la plataforma tecnológica y de los procesos de negocio de la empresa.

El comité de coordinación de la seguridad de la información será integrado por las siguientes personas:

- Gerente de Administración (Presidente del Comité).
- Gerente de Sistemas.
- Auditor interno.
- Jefe del departamento técnico.

El organigrama del comité de coordinación de la seguridad de la información se muestra en la figura 3.19.

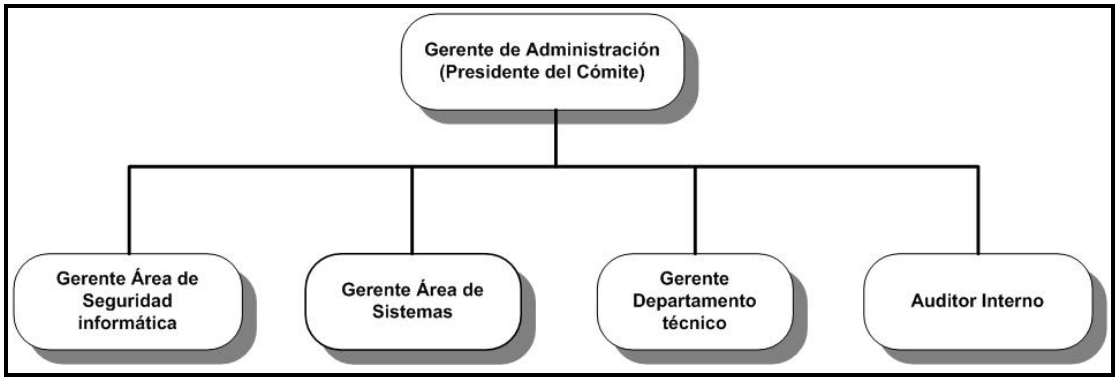


Figura 3.19 Organigrama del Comité de Coordinación de la Seguridad de la Información

3.3.2 Capacitación de Personal

Es responsabilidad del área de seguridad informática promover constantemente la importancia de la seguridad de los sistemas de información a todo el personal. El programa de concientización en seguridad debe contener continuas capacitaciones y charlas, adicionalmente se pueden emplear métodos como afiches, llaveros, mensajes de log-in, etc., los cuales recuerden permanentemente al usuario el papel importante que cumple en el mantenimiento de la seguridad de la información.

Cuando se contrate a un empleado nuevo y/o servicio de algún tercero, se debe entregar la política de seguridad así como las normas y procedimientos para el uso de las aplicaciones y sistemas de información de la empresa. Asimismo se debe entregar un resumen escrito de las medidas básicas de seguridad de la información.

Los usuarios deben ser informados anualmente sobre la importancia de la seguridad de la información. Un resumen escrito de la información básica debe ser entregado nuevamente a cada empleado y una copia firmada debe ser guardada en sus archivos. El personal de terceros debe recibir una copia del acuerdo de no divulgación firmado por la empresa y por el proveedor de servicios de terceros.

La capacitación en seguridad debe incluir principalmente, pero no estar limitado, a los siguientes aspectos:

- Seguridad de claves y contraseñas.
- Seguridad de PC, incluyendo protección de virus.
- Guías de acceso a Internet.
- Guías de uso de correo electrónico.
- Concientización de las técnicas utilizadas por los "hackers".
- Controles de acceso a las instalaciones de cómputo.
- Reglas de manipulación de cada uno de los activos de la empresa.

La capacitación del personal debe llevarse a cabo en las siguientes etapas.

Tiempo: 5 semanas

Etapas:

- Definición del mensaje a transmitir y material a ser empleado para los distintos grupos de usuarios, entre ellos:

  Personal en general: Información general sobre seguridad, políticas y estándares incluyendo protección de virus, contraseñas, seguridad física, sanciones, correo electrónico y uso de Internet.

  Personal de sistemas y técnico: Políticas de seguridad, estándares y controles específicos para la tecnología y aplicaciones utilizadas.

Gerencias y Jefaturas: Monitoreo de seguridad responsabilidades de supervisión, políticas de sanción

- Identificación del personal de cada departamento que se encargará de actualizar a su propio grupo en temas de seguridad.
- Establecimiento de un cronograma de capacitación, el cual debe incluir, empleados nuevos, requerimientos anuales de de capacitación, actualizaciones.
- Realizar la campaña según el cronograma elaborado, asegurándose de mantener un registro actualizado de la capacitación de cada usuario.

Observación: La capacitación del personal varía acorde al tamaño de la empresa.

3.3.3 Prueba de la Seguridad

Con el objetivo de asegurar el cumplimiento de la política de seguridad en los controles ya existentes, se debe verificar el grado de cumplimiento de las políticas de seguridad en los sistemas de información de la empresa y adaptarlos en caso de su incumplimiento.

La prueba de la seguridad comprende las siguientes etapas:

- Elaboración de un inventario de las aplicaciones existentes y de todos los servicios brindados tanto a clientes como personal de la empresa.
- Elaboración de un resumen de los requisitos que deben cumplir las aplicaciones según la política y estándares de seguridad.
- Evaluación del grado de cumplimiento de cada una de las políticas para cada una de las aplicaciones existentes.

La evaluación se llevó a cabo utilizando los formularios de ISO17999 TOOLKIT [44].

3.3.3.1 Puntos de Acceso de Intrusos

Definimos como puntos de acceso de intrusos a toda oportunidad para vulnerar la seguridad de los sistemas de información de la empresa, de parte de personal externo o interno. Un punto de acceso de intruso puede ser: Un puerto físico desconectado de algún equipo de comunicación, un puerto de aplicación orientado a conexión interna no bloqueado o sin control, algún tramo del cableado desprotegido o descuido por parte de los responsables de controlar el acceso a las instalaciones de la empresa.

3.3.3.2 Monitoreo y Detección de Intrusos

Una vez identificados los puntos de acceso para los intrusos. Se procederá a realizar una simulación de ataque a los sistemas informáticos de FIBERNET. El propósito de la simulación es verificar que la configuración de los equipos de comunicaciones esta adaptada a las políticas de seguridad

Para monitorear el tráfico de la red y analizar alguna intrusión se instaló el programa ETHEREAL en las máquinas de inspección de contenido, que están ubicadas en la red DMZ y en la red de servidores interna respectivamente.

En el software se configuró la dirección de red de DMZ para filtrar los paquetes hacia y desde los servidores HTTP, SMTP y DNS.

A continuación se presenta un análisis de intrusión en tiempo real (figura 3.20): El 31 de mayo a las 20:15:00 el equipo de control ha detectado un aumento en el tráfico HTTP con destino al servidor web.

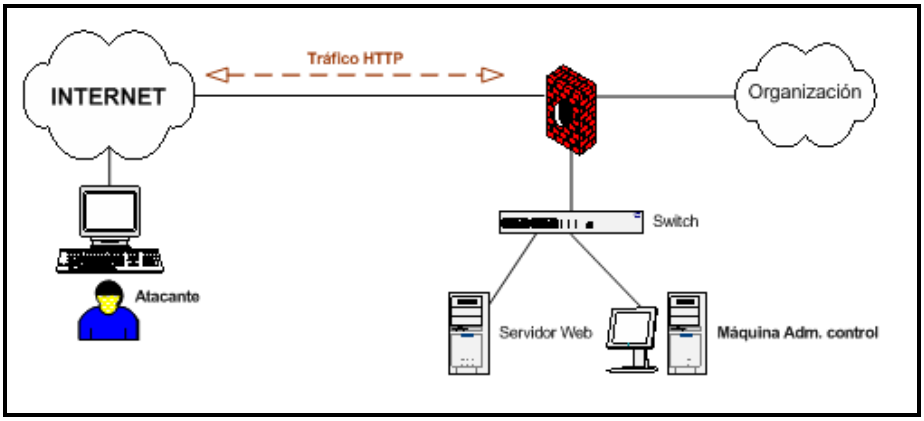


Figura 3.20 Análisis de Intrusión en Tiempo Real

En las conexiones se descubrió la descarga de diversos ficheros binarios. Desde el 3 de Junio hasta 6 de Junio se vuelve a detectar actividad del atacante en el servidor web. Las conversaciones han quedado registradas en la máquina de control y se ha reconstruido con **Ethereal (figuras 3.21.1 y 3.21.2).**

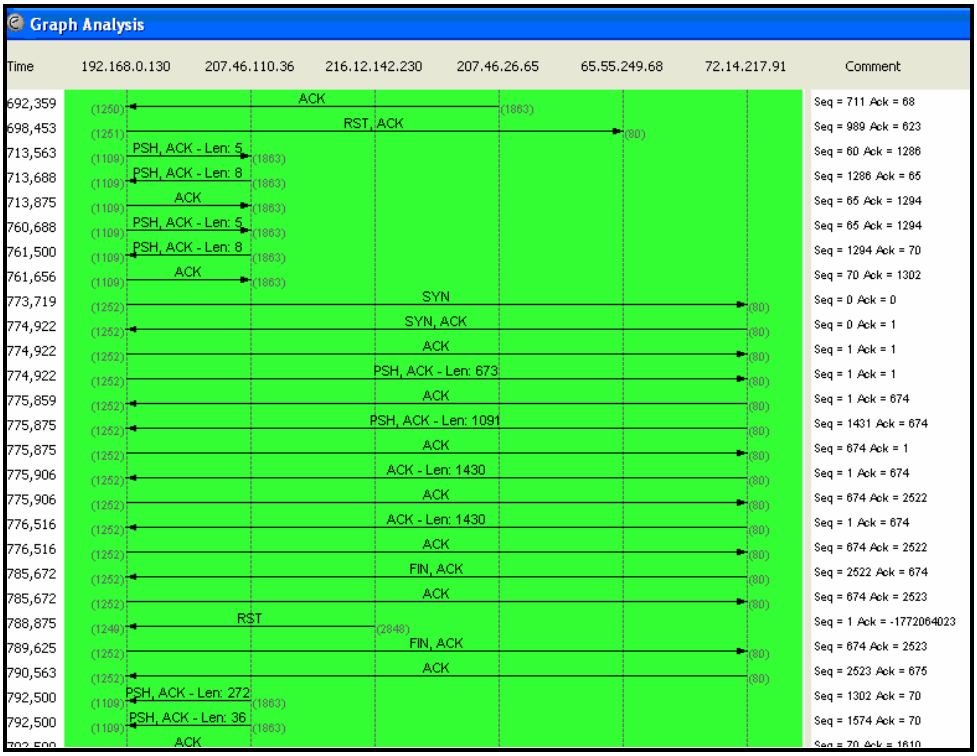


Figura 3.21.1 Análisis de Intrusión en Ethereal

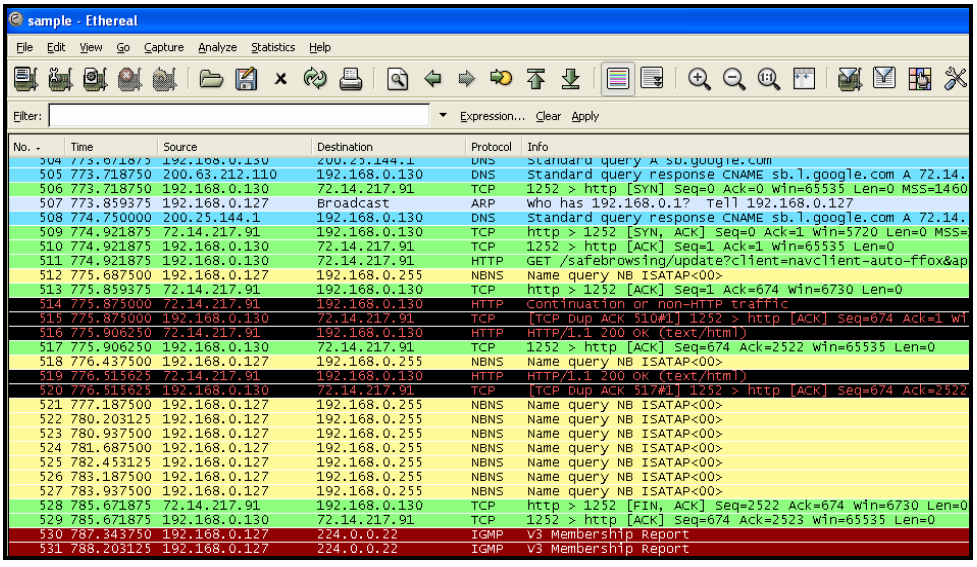


Figura 3.21.2 Análisis de Intrusión en Ethereal

El 10 de junio se decide que ya se ha obtenido suficiente información del atacante. Se aplican el filtrado total a través de la máquina de control. Se apaga la máquina y se desconecta de la red.

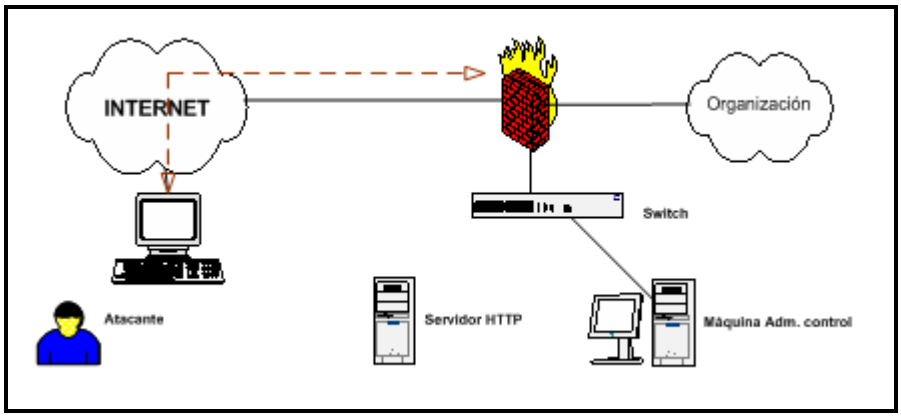


Figura 3.22 Filtrado Total a través de la Máquina de Control

Este procedimiento de análisis de intrusiones se deberá aplicar con toda máquina comprometida. Además se recomienda utilizar otras herramientas como: Analizadores de imágenes del disco duro y de procesos, y que toda esta información sea enviada a la máquina de control. Esto esta fuera del alcance de nuestro tema ya que tiene que ver con la parte de software.

3.3.4 Controles y Vigilancia

En los controles y vigilancia se toman en cuenta dos aspectos: Perfiles de acceso y contrato con los proveedores.

A continuación se detalla las etapas de cada aspecto.

Control Perfiles de Acceso

Con el propósito de obtener un control adecuado sobre el acceso de los usuarios a los sistemas de la empresa, se debe realizar un inventario de todos los accesos que posean ellos sobre cada uno de los sistemas. Este inventario debe ser actualizado al modificar el perfil de acceso a algún usuario y será utilizado para realizar revisiones periódicas de los accesos otorgados en los sistemas.

Etapas

- Elaboración de un inventario de los perfiles de acceso a cada sistema
- Verificación de los perfiles definidos en los sistemas para cada usuario
- Revisión y aprobación de los accesos por parte de las gerencias respectivas.
- Depurar los perfiles de accesos de los usuarios a los sistemas.
- Mantenimiento periódico del inventario.

Control sobre los contratos con proveedores

Con el objetivo de asegurar el cumplimiento de las políticas de seguridad de FIBERNET en el servicio brindado por los proveedores, es necesario realizar una revisión de los mismos y su grado de cumplimiento respecto a las

políticas de seguridad definidas, de ser necesario dichos contratos deben ser modificados para el cumplimiento de la política de seguridad de la empresa.

Etapas

- Elaboración de cláusulas estándar referidas a seguridad se información, para ser incluidas en los contratos con los proveedores.
- Elaboración de un inventario de los contratos existentes con los proveedores. .Revisión de los contratos y analizar el grado de cumplimiento de la política de seguridad.
- Negociar con los proveedores para la inclusión de las cláusulas en los contratos.

3.3.5 Revisiones

Es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de:

a) Reflejar los cambios en los requerimientos y prioridades de la empresa.
b) Considerar nuevas amenazas y vulnerabilidades.
c) Corroborar que los controles siguen siendo eficaces y apropiados.

Las revisiones comprenden las siguientes etapas:

- Revisión y adaptación de controles aplicados a las instalaciones de telecomunicaciones.
- Verificación de los controles aplicados en computadores portátiles, etc.
- Elaboración de procedimientos de monitoreo y reporte sobre la administración de los sistemas y herramientas de seguridad, entre ellas: Antivirus, servidor Firewall, servidor VPN, sistemas de detección de intrusos.
- Revisión de los controles implementados en cada uno de los equipos de red.
- Revisión de los controles para personal externo y interno que realiza labores utilizando activos de la empresa (Soporte técnico, proveedores, etc…)

CAPÍTULO IV: COSTOS

4.1 Costos de Implementación de las Políticas de Seguridad

En esta sección se detallan solamente los costos para implementar cada una de las políticas de seguridad.

- Inventario de Activos

El inventario de activos lo va a realizar 2 personas en un período de 3 días, cuyo costo se detalla en la tabla 4.1:

Tabla 4.1 Costos para implementar la política de Inventario de Activos

Descripción	Cantidad	Valor Unitario	Subtotal
Asesoría técnica	2	$ 400.00	$ 800.00
TOTAL			**$ 800.00**

- Perímetro de Seguridad física

Las instalaciones de los lectores de proximidad, lector biométrico y panel de control para 8 lectores se lo realizarán en un período de 2 días. Los costos se detallan en la tabla 4.2:

Tabla 4.2 Costos para implementar la política de Perímetro de Seguridad Física

Descripción	Marca /Modelo	Cantidad	Valor Unitario	Subtotal
Panel de control, 8 lectores	BOSCH modelo LNL 500	1	$ 847.83	$ 847.83
Lector de proximidad, alcance medio,	HONEYWELL OP-30HON	5	$ 195.84	$ 979.20
Lector combinado Biométrico (Huella Digital) y	HONEYWELL Y-PROX	1	$ 1,160.00	$ 1,160.00
Punto de instalación de lectores		6	$ 30.00	$ 180.00
Punto de instalación del Panel de control		1	$ 250.00	$ 250.00
TOTAL				**$ 3,417.03**

- Controles de Seguridad física

En la tabla 4.3 se detallan los costos de las tarjetas de proximidad, las cuales validan los lectores:

Tabla 4.3 Costos para implementar la política de Controles de Seguridad Física

Descripción	Marca /Modelo	Cantidad	Valor Unitario	Subtotal
Tarjetas de proximidad	PX4H	25	$ 9.50	$ 237.50
TOTAL				**$ 237.50**

- Ubicación y Protección de Equipos

Las instalaciones de las luces estroboscópicas, detectores de humo, detector térmico, extintores se lo realizarán en un período de 2 días. Los costos se detallan en la tabla 4.4:

Tabla 4.4 Costos para implementar la política de Ubicación y Protección de Equipos

Descripción	Marca /Modelo	Cantidad	Valor Unitario	Subtotal
Luz estroboscópica con sirena incluida 17/75 dB para montaje en tumbado y/o pared	NOTIFIER NSA-24MCLU-FR	3	$ 95.60	$ 286.80
Detector de Humo, direccionable, inteligente, fotoeléctrico, dos hilos. Incluye base de montaje.	NOTIFIER FSP-851	8	$ 104.74	$ 837.92
Detector térmico, rapidez de incremento de temperatura y fotoeléctrico, direccionable, inteligente, 2 hilos. Incluye base de montaje.	NOTIFIER FSP-851T	1	$ 110.83	$ 110.83
Extintores PQS de 10 lbs	MTZ-7	1	$ 32.00	$ 32.00
Extintores PQS de 20 lbs	MTZ-7	2	$ 44.00	$ 88.00
Punto de instalación de detectores de humo y térmicos		9	$ 20.00	$ 180.00

Punto de instalación luces estroboscópica con sirena		3	$ 20.00	$ 60.00
TOTAL				**$ 1,595.00**

- Suministro de Energía

El análisis de la correcta capacidad del UPS lo realizarán 2 personas en un período de 1 día. Los costos se detallan en la tabla 4.5:

Tabla 4.5 Costos para implementar la política de Suministro de Energía

Descripción	Cantidad	Valor Unitario	Subtotal
Asesoría técnica	2	$ 400.00	$ 800.00
TOTAL			**$ 800.00**

- Seguridad del Cableado

En esta parte se considera los costos únicamente de los equipos añadidos para mejorar la seguridad del cableado. Ver tabla 4.6.

Tabla 4.6 Costos para implementar la política de Seguridad del Cableado

Descripción	Cantidad	Valor Unitario	Subtotal
Conductos Internos	4	$ 1.81	$ 7.24
Paquete Ataduras Nylon	2	$ 1.74	$ 3.48
Racks	2	$ 845.10	$ 1,690.20
Equipo Rotulador	1	$ 100.00	$ 100.00
Costo de Instalación	2	$ 800.00	$ 1,600.00
TOTAL			**$ 3,400.92**

- Mantenimiento de los Equipos

En el costo de implementación de esta política se considera los siguientes ítems. Ver tabla 4.7.

Tabla 4.7 Costos para implementar la política de Mantenimiento de los Equipos

Descripción	Cantidad	Valor Unitario	Subtotal
Muñequeras electrostáticas	5	$ 17.00	$ 85.00
Alfombras electrostáticas	12	$ 30.00	$ 360.00
TOTAL			**$ 445.00**

- Seguridad del equipamiento fuera de la organización

Ver tabla 4.8.

Tabla 4.8 Costos para implementar la política de Seguridad del equipamiento fuera de la organización

Descripción	Cantidad	Valor Unitario	Subtotal
Cable DEFCOM	3	$ 55.00	$ 165.00
TOTAL			**$ 165.00**

- Seguridad de Red y comunicaciones

Ver tabla 4.9.

Tabla 4.9 Costos para implementar la política de Seguridad de Red y Comunicaciones

Descripción	Cantidad	Valor Unitario	Subtotal
CISCO ASA 5550	1	$ 17,239.99	$ 17,239.99
Servidor NAS	1	$ 866.88	$ 866.88
Servidor Multitarea	1	$ 607.04	$ 607.04
Máquina de Control	2	$ 1,352.96	$ 2,705.92
Costo de configuración de seguridad de los equipos	2	$ 800.00	$ 1,600.00
TOTAL			**$ 23,019.83**

4.2 Análisis Costos / Beneficios

El despliegue de una amplia y compleja infraestructura de sistemas de información y comunicaciones para dar soporte a los procesos de negocio, son fundamentales para la competitividad del mismo. Sin embargo, operar sobre estos sistemas más abiertos e interconectados, aumenta las amenazas que pueden atacar las vulnerabilidades que estos presentan con los consiguientes riesgos operacionales, financieros y legales.

Para realizar procesos o transacciones que de alguna manera se considerarían demasiado arriesgados, la seguridad no debe ser el fin sino el medio para proteger el negocio de amenazas latentes o explicitas.

A continuación se tratará de justificar la implementación de las políticas de seguridad en FIBERNET mediante un análisis Costos/Beneficios.

En la tabla 4.10 se muestra el costo total para implementar las políticas de seguridad de la empresa FIBERNET.

Tabla 4.10 Costo Total para implementar las políticas de Seguridad de FIBERNET

Descripción	Subtotal
Inventario de Activos	$ 800.00
Perímetro de Seguridad Física	$ 3,417.03
Controles de Seguridad Física	$ 237.50
Ubicación y Protección de Equipos	$ 1,595.00
Suministro de Energía	$ 800.00
Seguridad del Cableado	$ 3,400.92
Mantenimiento de los Equipos	$ 445.00
Seguridad del equipamiento fuera de la organización	$ 165.00
Seguridad de Red y Comunicaciones	$ 23,019.83
TOTAL	**$ 33,875.25**

Ya que en el Ecuador no existe la cultura de la Seguridad de la Información, no existen registros de pérdidas de empresas por ataques a sus sistemas de información. Ahora para estimar los beneficios de implementar estas políticas en la empresa, nos basamos en índices de seguridad informática referenciales, que miden las pérdidas anuales que provienen de los ataques hacia los sistemas informáticos. Estos son publicados anualmente por CSI/FBI COMPUTER CRIME AND SECURITY SURVEY. Los datos se han obtenido de los reportes de incidentes presentados por 313 compañías de la rama.

En la tabla 4.11 se muestra la pérdida en dólares de 313 empresas que provienen de las diferentes amenazas y además el promedio de pérdida por empresa de cada tipo de ataque.

Tabla 4.11 Cantidad en dólares de pérdidas por tipos de Ataques

Tipo de Ataque	Suma Pérdidas	Promedio Pérdidas
Contaminación por Virus	$ 15,691,460.00	$ 50,132.46
Acceso no autorizado a la información	$ 10,617,000.00	$ 33,920.13
Robo de Computadora y hardware portátil	$ 6,642,660.00	$ 21,222.56
Robo de información	$ 6,034,000.00	$ 19,277.96
Denegación de Servicio	$ 2,922,010.00	$ 9,335.50
Fraude Financiero	$ 2,556,900.00	$ 8,169.01
Abuso interno de la red o email	$ 1,849,810.00	$ 5,909.94
Fraude de Telecomunicaciones	$ 1,262,410.00	$ 4,033.26
Programas(zombies)dentro de la organización	$ 923,700.00	$ 2,951.12
Penetración al sistema externa	$ 758,000.00	$ 2,421.73
Abuso de mensajería instantánea	$ 647,510.00	$ 2,068.72
Abuso de las aplicaciones Web públicas	$ 291,510.00	$ 931.34
Sabotaje de datos o redes	$ 260,000.00	$ 830.67
Afectar imagen sitio Web	$ 162,500.00	$ 519.17
Robo de contraseñas	$ 161,210.00	$ 515.05
Explotación del Servidor DNS	$ 90,100.00	$ 287.86
Otras	$ 885,000.00	$ 2,827.48
TOTAL	**$ 51,755,780.00**	**$ 165,353.93**

En base a estos resultados se justifica la inversión de FIBERNET en tema de seguridad informática.

CONCLUSIONES Y RECOMENDACIONES

El objetivo principal de todas las políticas de seguridad desarrolladas en este proyecto, para protección del hardware de red de una empresa están destinadas a salvaguardar el mayor de los activos de la misma, la información.

Se deben crear las políticas de seguridad basados en las necesidades de la empresa. Recuerde cada empresa es diferente.

Una política de seguridad de la información debe tener las siguientes características:

- Debe estar escrita en lenguaje simple pero jurídicamente viable.
- Debe basarse en las razones que tiene la empresa para proteger sus activos.
- Debe ser consistente con las demás políticas organizacionales.
- Debe hacerse cumplir se exige y mide el cumplimiento.
- Debe tener en cuenta los aportes hechos por las personas afectadas por la política.
- Debe definir el papel y responsabilidades de las personas, departamentos y organizaciones para los que aplica la política.
- No debe violar las políticas locales, estatales.
- Debe definir las consecuencias en caso de incumplimiento de la política.

- Debe ser aprobada y firmada por el gerente general de la organización. No obtener este compromiso significa que el cumplimiento de la política es opcional situación que hará que fracase las políticas de seguridad.
- Debe estar respaldada por documentos palpables, como los estándares y procedimientos para la seguridad de la información, que se adapten a los cambios en las operaciones de las empresas, las necesidades, los requerimientos jurídicos y los cambios tecnológicos.

Redactar una política para la seguridad de los activos puede ser sencillo comparado con su implementación y viabilidad. La política organizacional y las presiones por lo general aseguran que habrá dificultad y consumo de tiempo para crear y adoptar una política de seguridad, a menos que un líder fuerte dirija el programa de las políticas. Esta persona generalmente será alguien influyente, un facilitador y sobre todo una persona que sepa escuchar, para que pueda articular y aclarar las inquietudes y temores de las personas respecto a la introducción de la nueva política.

Las empresas podrían necesitar más o menos recursos de lo utilizado en este caso estudio, eso dependerá del enfoque adoptado por la organización para el desarrollo de las políticas. Una inversión adicional para protección de

los activos no siempre garantizará el éxito. Pero si es recomendable tener un presupuesto para cumplir con estos fines.

Basados en nuestra experiencia, se elaboró un modelo de seguridad para implementar políticas de seguridad a nivel de hardware en cualquier empresa. Ver **Anexo J**.

Se diseñó varios modelos de prácticas de nivel de seguridad, para que sean realizados por los estudiados de telecomunicaciones (Redes de Datos I o Redes de Datos II) como un complemento de las materias mencionadas. Estos modelos se encuentran en el **Anexo K**.

ANEXOS

Anexo A: Matriz de Amenazas

AMENAZAS	IMPLICANCIA DE SEGURIDAD	MEDIDA DE SEGURIDAD APLICADA
Interés en obtener información estratégica del negocio, por parte de los competidores.	La existencia de información atractiva para competidores de negocio tales como información de clientes, marketing, configuración de equipos entre otras.	Estándares de seguridad para servidores. Control de acceso a las aplicaciones de la empresa. Revisión y depuración periódica de dichos accesos otorgados. Restricciones en el manejo de información enviada por correo electrónico. Verificación de la información impresa en reportes, evitar mostrar información innecesaria.
Acceso no autorizado a los sistemas por hackers o crackers.	La actividad vandálica realizada por hackers o crackers de sistemas, puede afectar la disponibilidad, integridad y confidencialidad de los sistemas informáticos del negocio. Estos actos pueden ser desarrollados por personal interno o externo a la empresa. Adicionalmente si dichas actividades es realizada contra equipos que proveen servicios a los clientes (página web), la reputación de la empresa se podría ver afectada en un grado muy importante.	Estándares de seguridad para servidores. Delimitación de responsabilidades y sanciones en los contratos con proveedores de servicios. Verificación de evaluaciones periódicas de la seguridad de los sistemas involucrados. Concientización y compromiso formal de los usuarios en temas relacionados a la seguridad informática. Políticas de Seguridad.
Interrupción de los Sistemas informáticos producto de infección por virus.	El riesgo de pérdida por virus informático es alto si no se administra adecuadamente el sistema de Antivirus y los usuarios no han sido concientizados en seguridad de información.	Adecuada arquitectura e implementación del sistema antivirus. Verificación periódica de la actualización del antivirus de computadoras personales y servidores. Generación periódica de reportes virus detectados y actualización de antivirus.

Interrupción de los Sistemas informáticos a través del personal que ingresa de manera temporal.	Los accesos otorgados al personal temporal deben ser controlados adecuadamente, asimismo la actividad realizada por los mismos en los sistemas debe ser periódicamente monitoreada. El personal temporal podría realizar actividad no autorizada, la cual podría ser detectada cuando haya finalizado sus labores en la empresa.	Control adecuado de los accesos otorgados. Depuración periódica de accesos otorgados a los sistemas. Adecuada configuración y revisión periódica de los registros (logs) de aplicaciones y sistemas operativos.
No se cuenta con un inventario de perfiles de acceso a los equipos de red.	El control sobre la actividad es llevado en muchos casos, mediante perfiles de usuarios controlando así los privilegios de acceso a los equipos.	Se debe contar con inventarios de los perfiles de acceso a los equipos. Se deben revisar periódicamente los perfiles y acceso.
Exceso de contraseña manejadas por los usuarios.	La necesidad de utilizar contraseña distintas para cada sistema o aplicación de la empresa, puede afectar las seguridad en la medida que el usuario no sea capaz de retener en la memoria, la relación de nombres de usuario y contraseñas utilizadas en todos los sistemas. La necesidad de anotar las contraseñas por parte de los usuarios, expone las mismas a acceso por parte de personal no autorizado.	Uniformizar dentro de lo posible la estructura de las contraseñas empleadas y sus fechas de renovación.
Existencia de usuarios de las áreas de sistemas, departamento técnico y personal temporal en la sala de telecomunicaciones.	El ambiente de producción debe contar con controles de acceso adecuados con respecto a los usuarios de las áreas de sistemas, departamento técnico y personal temporal, esto incluye las aplicaciones y bases de datos de la misma.	Inventario y depuración de perfiles de acceso que poseen los usuarios de las áreas de sistemas, departamento técnico y personal temporal en la sala de telecomunicaciones. Adecuada segregación de funciones del personal del área de sistemas. Procedimientos de pase a las sala de telecomunicaciones.
Falta de conciencia en seguridad por parte del personal interno.	El personal de la empresa es el vínculo entre la política de seguridad y su implementación final para aplicar la política de seguridad, se pueden establecer controles y un monitoreo constante, pero la persona es siempre el punto mas débil de la cadena de seguridad, este riesgo se puede incrementar si el usuario no recibe una adecuada	Programa de capacitación de la empresa relacionado a la seguridad informática.

	capacitación y orientación en seguridad de información. Para una adecuada administración de la seguridad informática se requiere que personal capacitado que pueda cumplir las labores de elaboración de políticas y administración de seguridad en el área de seguridad informática, así como implementación de controles y configuración de sistemas en el área de sistemas.	
Falta de personal con conocimientos técnicos de seguridad informática		Capacitación del personal técnico en temas de seguridad informática o inclusión de nuevo personal con conocimientos de seguridad informática para las áreas de seguridad Informática y sistemas.
Falta de controles adecuados para la información que envían los usuarios hacia Internet.	El acceso hacia Internet por medios como correo electro, ftp (file tranfer protocol) o incluso web puede facilitar el robo de información. No existen controles adecuados sobre el acceso a Internet. No existen herramientas de inspección del tráfico de red.	Implementación de una adecuada arquitectura de red. Mejores práticas para la configuración de firewalls. Implementación y administración de herramientas para inspección del tráfico de la red.
Arquitectura de red inapropiada para controlar accesos desde redes externas	Posibilidad de acceso no autorizado a sistemas por parte de de personal externo a la empresa. Existencia de redes externas que se conectan con la red de FIBERNET sin la protección de un firewall. Los servidores de la red pública nos están aislados de la red interna.	Diseño de arquitectura de seguridad de red. Adecuada configuración de elementos de control de conexiones (Firewall). Implementación y administración de herramientas de seguridad.
Fuga de información estratégica mediante sustracción de computadores portátiles.	Es posible obtener información confidencial de la empresa tales como configuración de equipos, direcciones IP, entre otras, mediante el robo de la misma.	Uso de programas para la encripción de la data en las computadoras. Uso de mecanismos de protección de equipo portátiles como cables de seguridad.
Controles de acceso hacia Internet desde la red interna.	Posibilidad de acceso no autorizado desde la red interna hacia equipos de terceros en Internet. Posibilidad de Fuga de información.	Implementación de una adecuada arquitectura de red. Mejores prácticas para la configuración de Firewalls.

		Implementación y administración de herramientas de inspección de tráfico de red. Monitoreo periódico de la actividad, mediante el análisis de de los registros (logs) de los sistemas.

Anexo B: Matriz de Evaluación de Riesgos

SISTEMA	AMENAZA / VULNERABILIDAD	MEDIDA DE SEGURIDAD
Servidor DNS	Acceso lógico no autorizado al servidor desde Internet, redes internas y externas a la empresa. Además acceso físico no autorizado. La indisponibilidad de este servidor dejaría sin efecto la traducción de nombres de dominios, por lo que significaría un gran impacto para el negocio.	Aplicación de estándares de mejores prácticas de seguridad para servidores DNS. Controles de acceso físico y lógico deben ser lo más restrictivos posibles.
Servidor FTP	Riesgo de acceso físico no autorizado para recabar información del servidor. Posibilidad de interceptación no autorizada a información del servidor de archivos.	Controles de acceso físico. Se debe contar con estándares de encripción. Implementación de un sistema de seguridad del contenido SMTP.
Servidor WEB	Actividad vandálica realizada por hackers o crackers de sistemas. Pueden ser desarrolladas por personal interno o externo a la empresa. Para afectar la imagen y reputación de la empresa.	Asegurar que el equipo cuente con las medidas de seguridad adecuadas tanto físicas como lógicas. Además se debe aplicar estándares de encripción para la transmisión de datos.
Servidor de e-mail Externo	Riesgo de acceso no autorizado desde Internet, redes internas y externas a la empresa. Posibilidad de interceptación no autorizada a información del servidor electrónico.	Controles de acceso físico y lógicos. Se debe contar con estándares de encripción. Implementación de un sistema de seguridad del contenido SMTP.
Servidor Multitarea SMNP –- SysLog	Riesgo de acceso no autorizado físico y lógico por personal de la empresa y/o terceros.	Aplicar controles de acceso físico y lógico.

Nodos de la red de Acceso – Servidores – Intranet	Acceso a la configuración del equipo. Acceso a puertos desconectados.	Aplicación de los estándares de protección de puertos. Controles de acceso a consolas y servicios de administración remota.
Nodo de la red de Transporte	Acceso a la configuración del equipo. Acceso a puertos desconectados.	Aplicación de los estándares de protección de puertos. Controles de acceso a consolas y servicios de administración remota. Monitoreo periódico de la actividad realizada en el Switch. Revisión periódica de los accesos otorgados a los usuarios del sistema.
Router del Core IP	Acceso a la configuración del equipo. Acceso a puertos desconectados. Un acceso no autorizado a este representa un riesgo potencial para el negocio.	Aplicación de los estándares de protección de puertos. Controles de acceso a consolas y servicios de administración remota. Monitoreo periódico de la actividad realizada en el router. Revisión periódica de los accesos otorgados a los usuarios del sistema.
Firewall	Riesgo de acceso no autorizado desde Internet y redes externas. Riesgo de acceso no autorizado por empleados de la empresa. Uso indebido del acceso a Internet por los empleados. Manipulación por personas no autorizadas.	Mejores prácticas de seguridad para la configuración de Firewalls. Utilización de sistemas de detección de intrusos. Controles y filtros para el acceso a Internet. Controles de acceso físico al equipo.

Computadoras Personales	Acceso no autorizado por parte del personal de la empresa y/o terceros. Acceso no autorizado a la información. Uso indebido de las aplicaciones instaladas.	Concientización y entrenamiento del personal en temas de seguridad. Estándares de mejores prácticas de seguridad para estaciones de trabajo. Monitoreo de actividad de los usuarios, sistema de detección de intrusos.

Anexo C: Inventario de Equipos de Comunicaciones de FIBERNET

Imagen	Descripción	Marca / Modelo	Ubicación	Código	Propietario	Nivel Riesgo	Notas
	Dispositivo red Acceso 48 puertos Ethernet 10/100/1000 - PoE. 4 puertos SFP-Gigabit Ethernet.	Catalyst 3560G-48PS	TR - Rack B	**Acceso 1**	FIBERNET	Medio	28 puertos Ethernet disponibles 2 puertos GE disponibles
	Dispositivo red Acceso 48 puertos Ethernet 10/100/1000 - PoE. 4 puertos SFP-Gigabit Ethernet.	Catalyst 3560G-48PS	TR - Rack B	**Acceso 2**	FIBERNET	Medio	18 puertos Ethernet disponibles 2 puertos GE disponibles
	Dispositivo red Servidores 48 puertos Ethernet 10/100/1000 - PoE. 4 puertos SFP-Gigabit Ethernet.	Catalyst 3560G-48PS	TR - Rack A	**Servidores**	FIBERNET	Medio	45 puertos Ethernet disponibles 3 puertos GE disponibles
	Dispositivo Intranet 48 puertos Ethernet 10/100/1000 - PoE. 4 puertos SFP-Gigabit Ethernet.	Catalyst 2950 - 48TC	TR - Rack A	**Intranet**	FIBERNET	Medio	36 puertos Ethernet disponibles 3 puertos GE disponibles

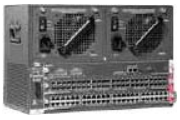
Imagen	Descripción	Marca / Modelo	Ubicación	Código	Propietario	Nivel Riesgo	Notas
	Dispositivo red Transporte	Cisco 5000	TR - Rack A	**NODO 1**	FIBERNET	Alto	
	Dispositivo red Core IP 48 puertos SFP Gigabit Ethernet	Catalyst 4503 - WS-X4448-GB-LX	TR - Rack A	**Core IP**	FIBERNET	Alto	18 puertos Ethernet disponibles 2 puertos GE disponibles
	Firewall 8 puertos Gigabit Ethernet	Cisco ASA 5550	TR - Rack B		FIBERNET	Alto	
	Servidor DNS	SERVER HP ML 110T04 PD925	TR - Rack A	**DNS**	FIBERNET	Medio	3.0 Ghz ,160GB,512MB
	Servidor TFTP	SERVER HP ML115T01	TR - Rack A	**TFTP**	FIBERNET	Bajo	AMD OPTERON 1214
	Servidor Multitarea	SERVER HP ML115T01	TR - Rack B	**MULTITASK**	FIBERNET	Bajo	AMD OPTERON 1214

Imagen	Descripción	Marca / Modelo	Ubicación	Código	Propietario	Nivel Riesgo	Notas
	Servidor NAS	SERVER HP DC5800	TR - Rack B	**NAS**	FIBERNET	Medio	C2D 2.83 GHZ, 160 GB, 2 GB
	Máquina Control	HP DV670b	TR - Rack B	**MAQCON1**	FIBERNET	Bajo	C2D 2.4 GHZ, 160 GB, 4 GB
	Máquina Control	HP DV670b	TR - Rack B	**MAQCON2**	FIBERNET	Bajo	C2D 2.4 GHZ, 160 GB, 2 GB

Anexo D: Registro para Visitantes

Nombres	Apellidos	Cédula de Identidad	Fecha	Hora Ingreso	Hora Egreso

Anexo E: Reporte de Servicio Técnico de FIBERNET

REPORTE DE SERVICIO TÉCNICO Nº 001088

Técnico:

Empresa:

Tipo de Servicio:

□ Improductivo
□ Instalación
□ Mantenimiento
□ Garantía
□ Interno
□ Reparación

Equipo(s):

Mano de Obra:

Fecha			
	Día	Mes	Año
Lunes			
Martes			
Miércoles			
Jueves			
Viernes			
Sábado			
Domingo			

Desde		**Hasta**		**Total**	
H	M	H	M	H	M

Diagnóstico y/o Fallas Reportadas:

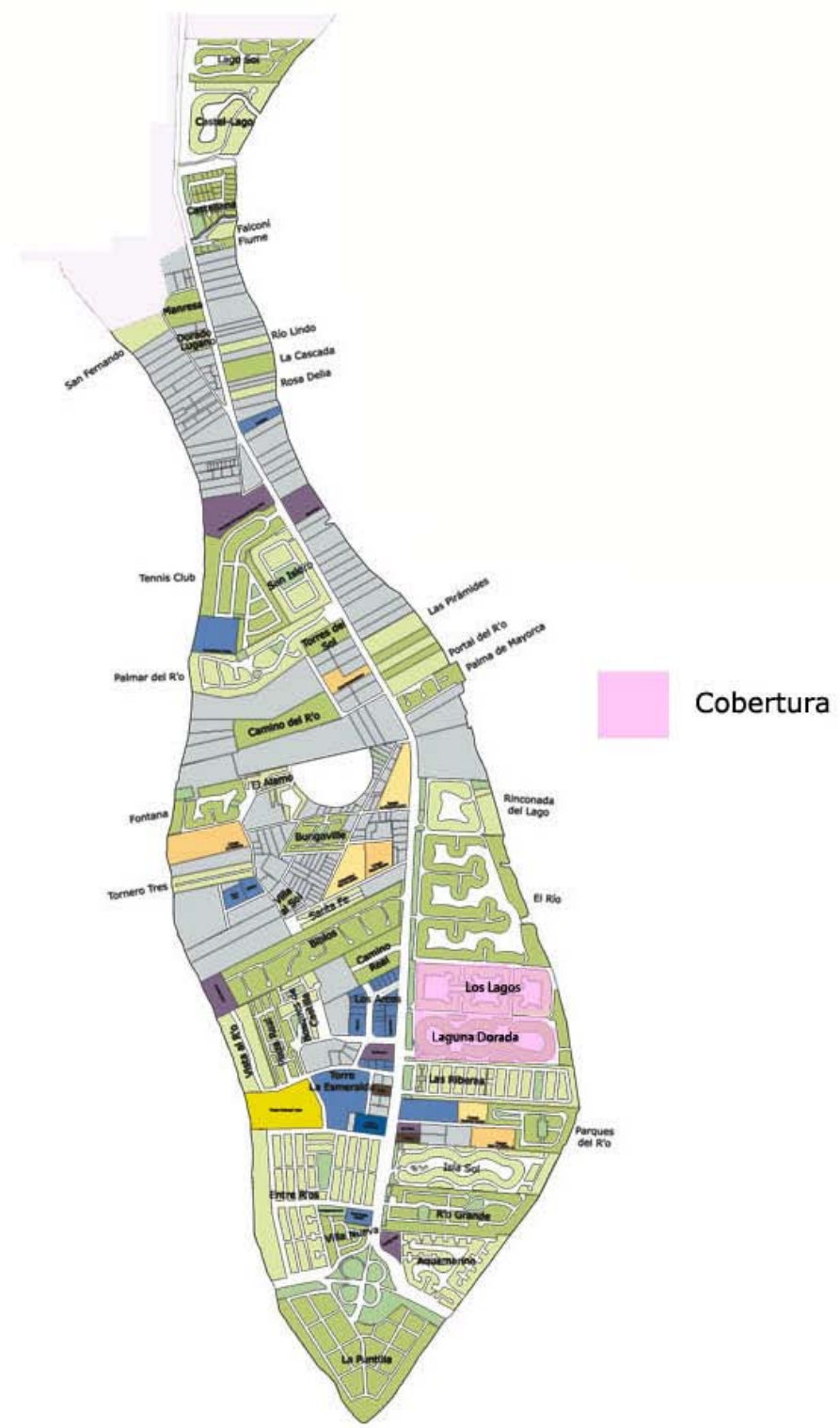
Trabajos Realizados:

Firma

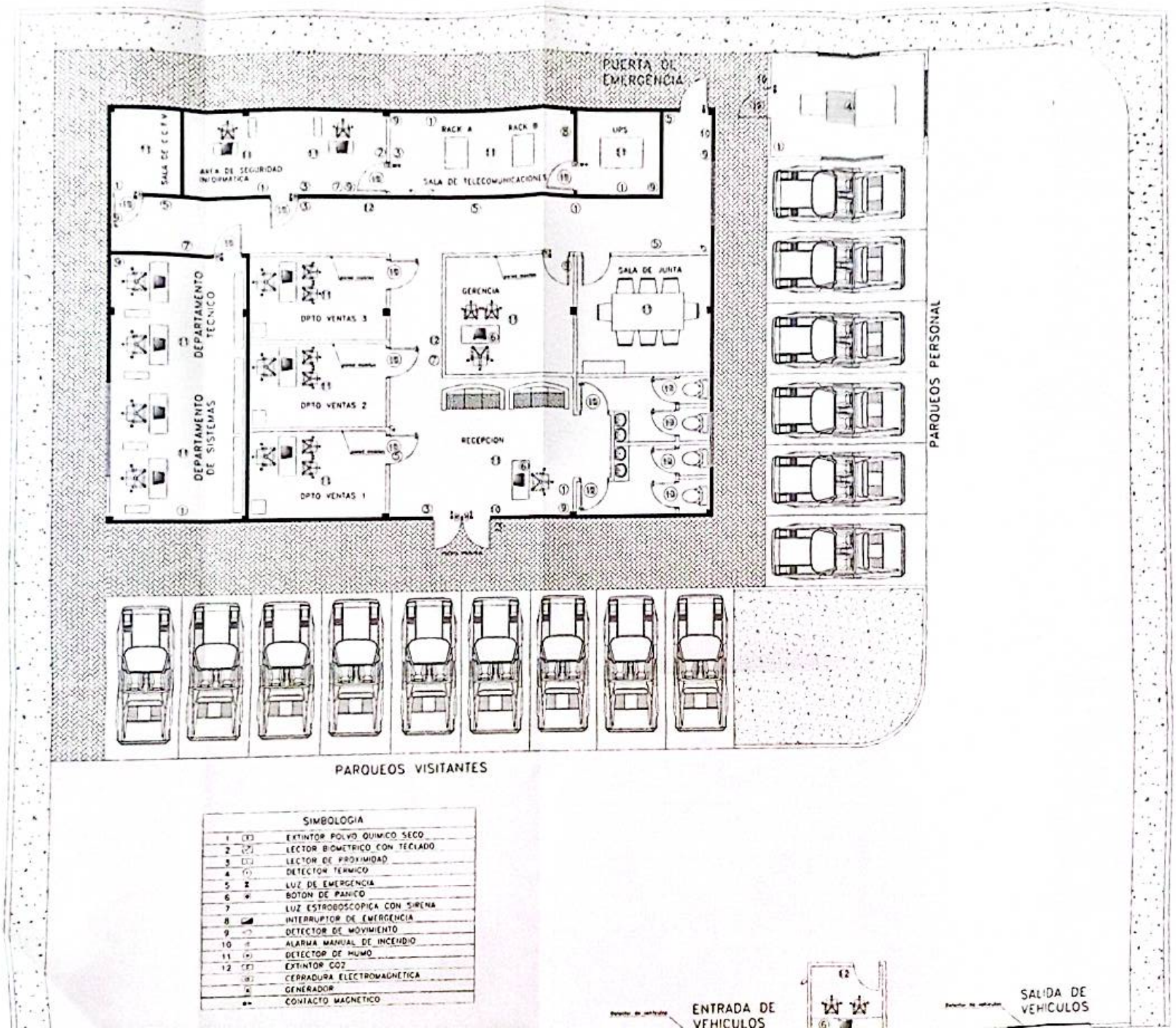
Anexo F: Equipos conectados al UPS

Departamento	Equipo	Cantidad	VA
Garita	PC	1	250
Recepción	PC	1	250
Ventas 1	PC	1	250
Ventas 2	PC	1	250
Ventas 3	PC	1	250
Técnico	PC	4	1,000
Gerencia	PC	1	250
Monitoreo de Red	Portátil	2	500
Sala de C.C.T.V.	Equipo	1	500
Sala de Telecomunicaciones	Router 4503	1	1,160
Sala de Telecomunicaciones	Cisco 5000	1	1,160
Sala de Telecomunicaciones	Swicth 3560	3	1,200
Sala de Telecomunicaciones	Cisco ASA 5550	1	400
Sala de Telecomunicaciones	Servidores	4	1,000
TOTAL			**8,420**

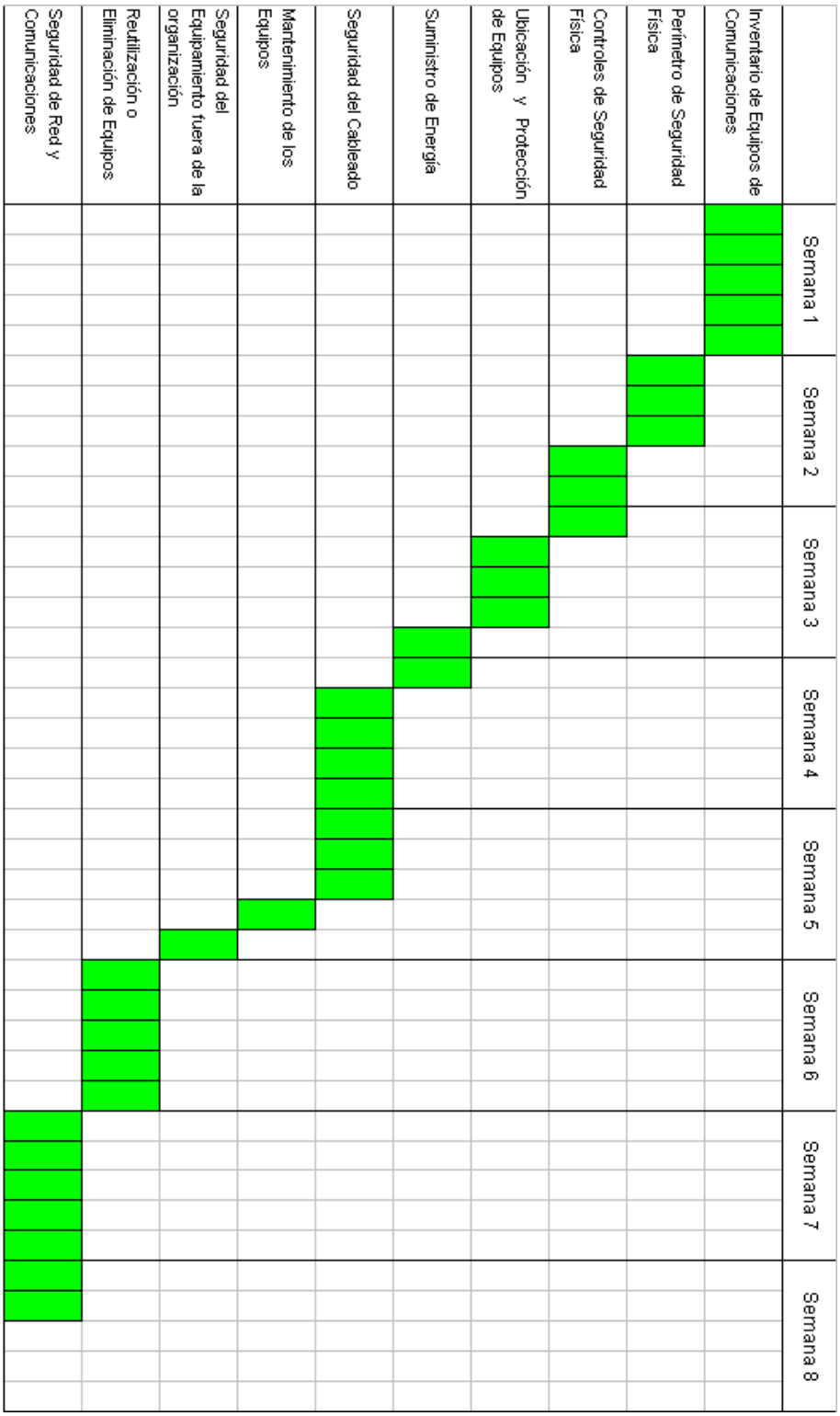
Anexo G: Cobertura de FIBERNET



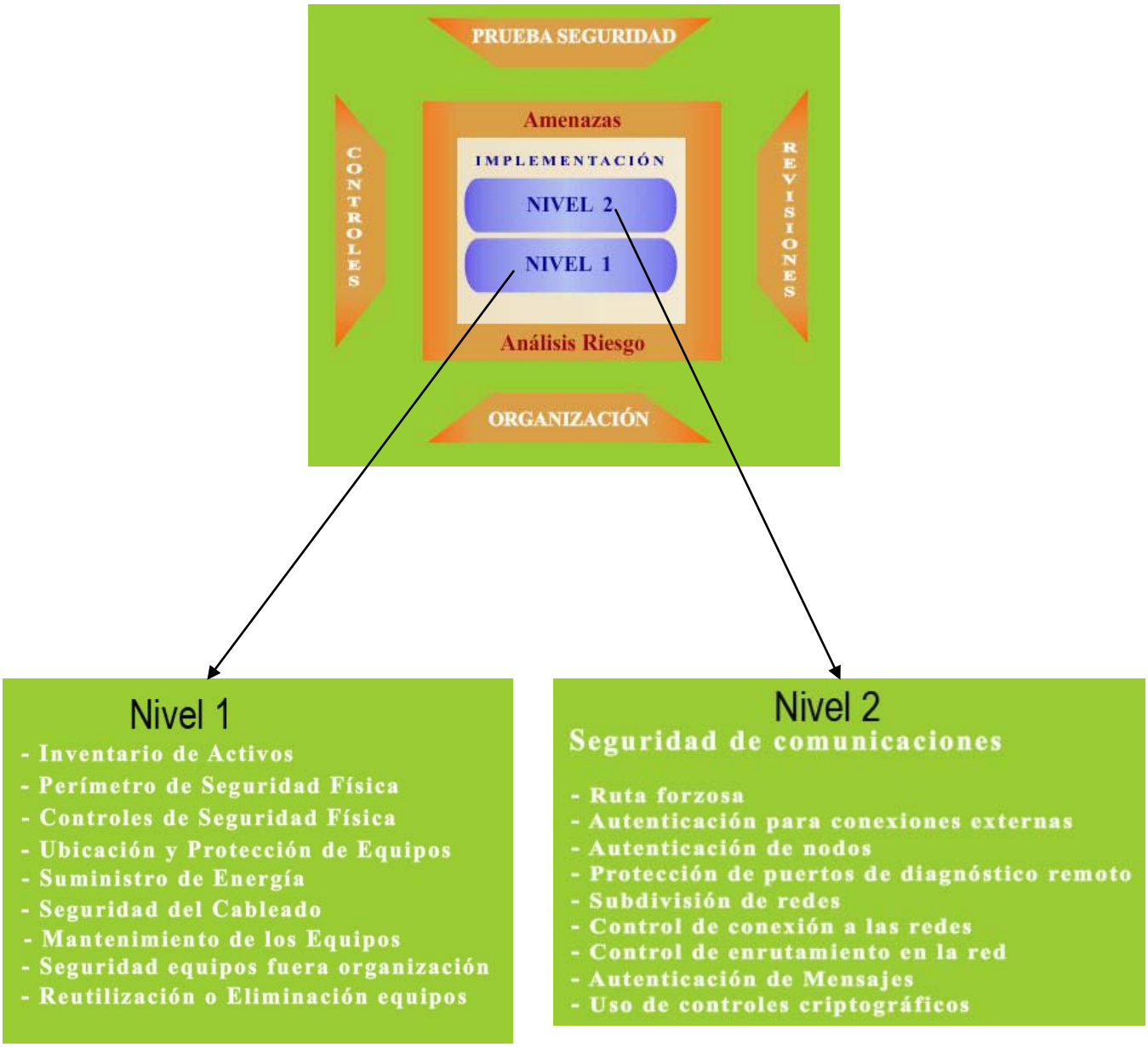
Anexo H: Planos de FIBERNET



Anexo I: Cronograma de Implementación de las Políticas de Seguridad de FIBERNET



Anexo J: Modelo de Seguridad



Anexo K: Modelos de Prácticas de Nivel de Seguridad

PRÁCTICA 1: Control de conexión de la Red

1.- Objetivo

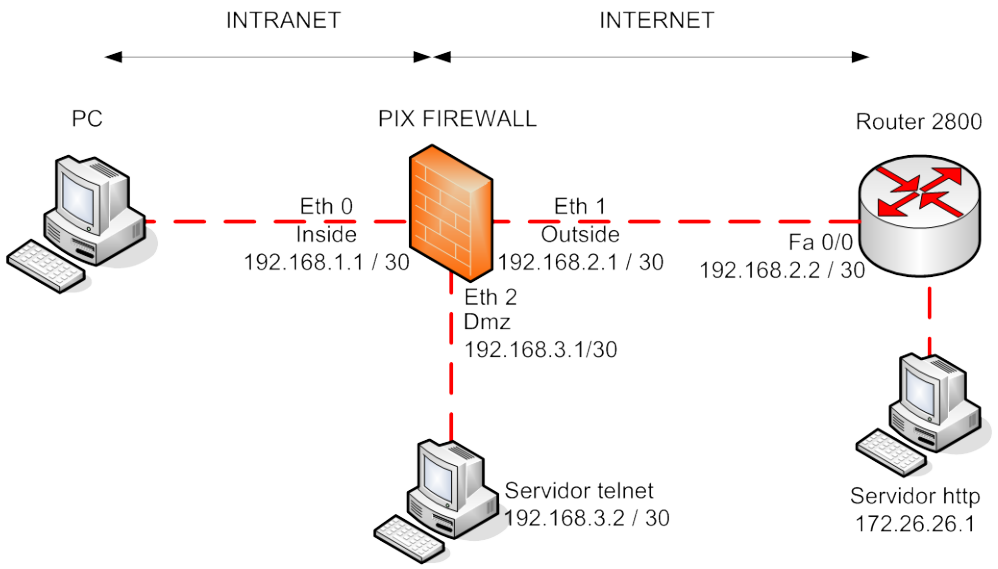
El objetivo de esta práctica es realizar la configuración básica de un Firewall, concretamente de *Cisco Systems*, llamado PIX (*Private Internet eXchange*). Durante el desarrollo de la práctica configuraremos sus interfaces y definiremos niveles de seguridad (*inside, dmz, outside*), habilitando NAT (*Network Address Traslation*) entre ellos. Analizaremos las conexiones permitidas según los niveles de seguridad y realizaremos reglas específicas, mediante listas de acceso para permitir/denegar cierto tráfico.

2.- Introducción

Llevar a cabo el control de conexión de la red es pieza clave de la política de seguridad de una empresa. Es uno de los elementos de seguridad más críticos de una organización cuando se conecta a Internet y por regla general es implementada en cortafuegos o "*firewall*", un dispositivo hardware capaz de analizar todas las conexiones entrantes/salientes simultáneamente. Su configuración debe ser acorde según la política de seguridad definida. Además, dado que sobre este dispositivo se analizan las reglas de seguridad, en ocasiones se puede convertir en el cuello de botella, situación que hay que evitar.

El PIX analiza y registra las conexiones entrantes y salientes implementando NAT. Con esta técnica, al PIX se le permite en todo momento tener control de las conexiones establecidas y rechazar conexiones no permitidas.

El PIX define niveles de seguridad o zonas de seguridad, que en el caso de la presente práctica son tres: *inside,dmz, outside*, las cuales quedan asociadas con niveles 100, 50 y 0 respectivamente. La regla que aplica el PIX por defecto es: "*no se puede pasar de nivel de seguridad menor a uno mayor*". En base a esto, vamos a desarrollar toda la práctica.



Además, los PIX permiten la configuración de listas de acceso, de forma similar a los routers. En el caso de tener configuradas listas de acceso, el PIX ignora los niveles de seguridad preestablecidos entre zonas, para el tráfico comprobado por las listas de acceso.

Además, estas listas de acceso se pueden crear de forma transparente al usuario, es decir los PIX implementan un mecanismo automático de listas de acceso para permitir tráfico de entrada cuando se genera tráfico de salida, acorde con los patrones del tráfico de salida, es decir que si generamos conexiones *http* de salida, no podemos tener tráfico *ftp* de entrada. Por tanto una vez permitido el tráfico de vuelta, puede pasar sin problema de un nivel de menor seguridad a uno de mayor. Este mecanismo se implementa de forma automática en los PIX y se conoce como CBACs "*Context Based Access*". Este mecanismo propietario de Cisco Systems sólo funciona en caso de establecimiento de conexiones y/o pseudoconexiones, como TCP/UDP respectivamente, pero no para ICMP. Por tanto, si generemos tráfico TCP/UDP por ejemplo de "*inside*" a "*outside*", CBACs de forma automática crea y/o genera permisos (como listas de acceso temporales), para permitir tráfico de "*outside*" a "*inside*", respetando que el tráfico sea asociado a la misma conexión.

3.- Realización de la práctica

Los pasos a realizar en esta práctica son:

Paso 0: Cableado del esquema

En primer lugar comprobar la conectividad física del esquema tal como se indica en la figura 1.
Los equipos que la componen son un *router* genérico de *Cisco Systems* y un cortafuegos PIX modelo 515E. Las interfaces del firewall son iguales que la de los *routers*, por tanto conectar directamente el *host* o servidor al PIX por una interfaz *Ethernet u*tilizando cable UTP-5 cruzado.
El servidor web 172.26.26.1 es un servidor virtual que configuraremos en el router.

Paso 1: configuración del Router, host y servidores.

Configuración del Router

Conectar el ordenador al puerto consola del Router y abrir el programa de emulación de terminal (hyperterminal) fijar los siguientes parámetros:

Bits por segundo: 9600 bits/s
Paridad: Ninguno
Bits de datos: 8
Bits de parada: 1
Control de flujo: Ninguno

Encender el R*outer*. Debe aparecer la secuencia de mensajes de arranque. Esto nos confirma que la comunicación por el puerto de consola es correcta.

Una vez que ha arrancado el router debe aparecer el *prompt* 'Router**>**'; teclear el comando **'enable'** para pasar a modo Privilegiado. En caso de que pida una *password* consultar al profesor.

Una vez en modo Privilegiado entraremos en modo Configuración Global para introducir la configuración que corresponde al router:

```
Router>enable
Router#configure terminal
Router(config)#hostname BORDER
BORDER(config)#ip http server

BORDER(config)#interface fastethernet 0
BORDER(config-if)#ip address 192.168.1.2 255.255.255.0
BORDER(config-if)#no shutdown
BORDER(config-if)#exit

BORDER(config)#interface loopback 0
BORDER(config-if)#ip address 172.26.26.1 255.255.255.0
BORDER(config-if)#no shutdown
BORDER(config-if)#exit

BORDER(config)#line vty 0 4
BORDER(config-line)#password cisco
BORDER(config-line)#exit
```

Configuración de HOST/SERVIDOR

Para configurar el host y servidor debemos conectarlos en cada una de las interfaces del firewall y asignar una IP y ruta por defecto. La configuración es:

Insidehost

Dirección IP: 10.0.1.11

Máscara: 255.255.255.0

Puerta de enlace predeterminada: 10.0.1.1

Servidor FTP

Dirección IP: 172.16.1.2

Máscara: 255.255.255.0

Puerta de enlace predeterminada: 172.16.1.1

Paso 2: Configuración del Firewall PIX

Los comandos del PIX guardan mucha relación con los comandos del router y por tanto nos resultarán bastante familiares.

Utilizamos también la conexión de consola mediante el programa de emulación de terminal (hyperterminal) y lo configuramos de la misma forma que para configurar el router.

Introducimos los siguientes comandos:

```
pixfirewall>enable
```

Comprobamos la configuración por defecto cargada en el PIX, los recursos de memoria, la versión del PIX y la utilización del CPU:

pixfirewall# write terminal
pixfirewall# show memory
pixfirewall# show version
pixfirewall# show cpu usage

¿Qué tamaño dispone de memoria?¿Cuántos están libres?

_____

_____

¿Qué versión de PIX se está ejecutando?¿Qué direcciones MAC disponen las interfaces del PIX?¿Qué versiones de VPN dispone en la licencia instalada?

_____

_____

¿Qué utilización tiene la CPU? Una utilización alto puede suponer pérdida de paquetes y además el PIX se puede
convertir en el cuello de botella.

_____

_____

Configuramos las interfaces, fijamos la velocidad y modo de transmisión 100 Mbps full duplex, para que no se presente problemas a nivel físico en la auto negociación:

pixfirewall#configure terminal
PIX(config)# hostname PIX

PIX(config)# interface e0
PIX(config-if)# nameif inside
PIX(config-if)# 100full
PIX(config-if)# ip address inside 10.0.1.1 255.255.255.0
PIX(config-if)# no shutdown

PIX(config)# interface e1
PIX(config-if)# nameif outside
PIX(config-if)# 100full
PIX(config-if)# ip address outside 192.168.1.1 255.255.255.0
PIX(config-if)# no shutdown

PIX(config)# interface e2
PIX(config-if)# nameif dmz
PIX(config-if)# 100full
PIX(config-if)# ip address dmz 172.16.1.1 255.255.255.0
PIX(config-if)# no shutdown

Comprobamos la configuración de las interfaces:
PIX# show interface

Asignamos niveles de seguridad a cada una de las interfaces, con el comando security level:

Inside
PIX(config)# interface e0
PIX(config-if)# security level 100

Outside
PIX(config)# interface e1
PIX(config-if)# security level 0

Dmz
PIX(config)# interface e2
PIX(config-if)# security level 50

PIX# show nameif

Finalmente para que el PIX pueda encaminar dado que también hace funciones de router, configuramos una ruta estática por defecto al router BORDER con coste 1

PIX(config)# route outside 0.0.0.0 0.0.0.0 192.168.1.1 1

Ahora comprobamos la conectividad IP, desde todos los dispositivos hacia todos los dispositivos. Si existe conectividad colocamos 'OK' si no 'NO'.

PING DESDE	INSIDEHOST	SERVIDOR FTP	PIX	BORDER
INSIDEHOST				
SERVIDOR FTP				
PIX				
BORDER				

Comentar los resultados obtenidos y justificar.

_____

_____

_____

_____

Paso 4: configuración de NAT (inside, outside) en el PIX y establecimiento de conexiones

Una vez configuradas las interfaces, vamos a habilitar la comunicación entra las diferentes zonas: *inside, dmz,outside*, según sus niveles de seguridad 100, 50 y 0 respectivamente. La regla que aplica el PIX es: "*no se puede pasar de nivel de seguridad menor a uno mayor*".

Además, para poder establecer la comunicación, el PIX debe poder realizar registro de las conexiones y para ello utiliza NAT. La configuración de NAT conlleva siempre la configuración de 2 comandos, "nat" que se asocia a la interfaz de entrada indicando qué IP interna entra en el NAT y "global" que se asocia a la interfaz de salida donde se especifica la IP (o IPs) externa. Es decir, estos comandos especifican por un lado las direcciones "dentro" (pre-NAT) y por otro lado la dirección o direcciones (en el caso de un conjunto o "pool") "fuera" (post-NAT). Ambos comandos, quedan mutuamente asociados por un identificativo numérico, en nuestro caso como podemos ver abajo con "1".

Configuramos la traducción con identificativo nº 1 de NAT de "incide" a "outside":

```
PIX(config)#nat(inside)1 10.0.1.0 255.255.255.0
PIX(config)#global(outside)1 192.168.1.200-192.168.1.254 netmask
255.255.255.0
```

Para comprobar que la traducción nº 1 de NAT se ha configurado correctamente utilizaremos el comando:

PIX# show global
PIX# show nat

Volvamos a comprobar la conectividad IP utilizando "ping" desde todos los dispositivos a todos los dispositivos.

PING DESDE	INSIDEHOST	SERVIDOR FTP	PIX	BORDER
INSIDEHOST				
SERVIDOR FTP				
PIX				
BORDER				

También podemos comprobar si podemos establecer conexión http desde el "insidehost" con el servidor Web (http://172.26.26.1) y hacer Telnet al "bastionhost".

DESDE	INSIDEHOST	SERVIDOR FTP	PIX	BORDER
Telnet a "bastionhost"				
Http a "Router/Web"				

Comenta los resultados obtenidos y justifícalo.

_____

_____

A simple vista parece extraño que funcionen las conexiones TCP/UDP y no funcione ICMP para el "*ping*". La razón es porque los PIX implementan un mecanismo automático de listas de acceso para permitir tráfico de entrada cuando se genera tráfico de salida, acorde con los patrones del tráfico de salida, es decir que si generamos conexiones *http* de salida, no podemos tener conexiones *ftp* de entrada. Este mecanismo se implementa de forma automática en los PIX y se conoce como CBACs "*Context Based Access*". Este mecanismo propietario de Cisco Systems sólo funciona en caso de establecimiento de conexiones y/o pseudoconexiones, como TCP/UDP respectivamente, pero no para ICMP.

Por tanto, si generemos tráfico TCP/UDP por ejemplo de "*inside*" a "*outside*", CBACs de forma automática crea y/o genera permisos (como listas de acceso temporales), para permitir tráfico de "*outside*" a "*inside*", respetando que el tráfico sea asociada a la misma conexión.

Podemos observar la tabla de traducciones NAT realizada utilizando el siguiente comando:

PIX(config)# show xlate
PIX(config)# show xlate debug

Paso 5: configuración de NAT (de inside a dmz) en el PIX y establecimiento de Conexiones

Como hemos comprobado anteriormente, no podemos acceder a la DMZ porque en ella no se ha asignado ningún proceso de NAT.

Desde "*insidehost*" hacer **telnet 172.16.1.2**.
Desde "*insidehost*" hacer **ping 172.16.1.2**.

Por tanto, a continuación vamos a configurar para que los usuarios de la "*inside*" puedan acceder a la DMZ a

Través de los siguientes comandos:

PIX(config)# global (dmz) **1** 172.16.1.200-172.16.1.254 netmask `255.255.255.0`

Y también podemos comprobar la conexión Telnet a 172.16.1.2, es decir que tenemos permiso para conectarnos al puerto 23 del servidor en la DMZ:

Desde "*insidehost*" hacer **telnet 172.16.1.2**. ¿funciona?

En este caso, el tráfico de vuelta también ha sido permitido por CBACs y por eso, el ping sigue sin funcionar.

Desde "*insidehost*" hacer **ping 172.16.1.2**. ¿funciona?

Para analizar el estado de la conexión, vamos a comprobar con los siguientes comandos "show":

PIX(config)# show arp

PRÁCTICA 2: Subdivisión de Redes

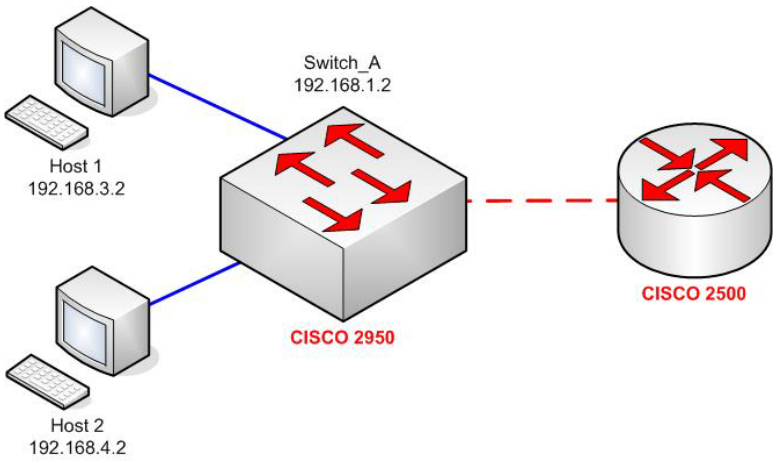
1.- Objetivo

El objetivo de esta práctica es crear VLANs en un conmutador CISCO 2950, realizando la configuración de acuerdo a los mejores procedimientos de seguridad para VLANs.

2.- Introducción

Las redes se están extendiendo en forma creciente, más allá de los límites tradicionales de la organización, a medida que constituyen sociedades con requerimientos de interconexión, o uso compartido de instalaciones de procesamiento de información y redes. Dichas extensiones pueden incrementar el riesgo de acceso no autorizado a sistemas de información ya existentes que utilizan la red, algunos de los cuales podrían requerir de protección contra otros usuarios de red, debido a su sensibilidad o criticidad. En tales circunstancias, se debe considerar la introducción de controles dentro de la red, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.

Lo que se debe aplicar para controlar la seguridad de redes extensas es dividirlas en dominios lógicos separados, por ejemplo: Dominios de red internos y externos de una organización cada uno protegido por un perímetro de seguridad definido. Dicho perímetro puede ser implementado mediante la instalación de una compuerta (“gateway”) segura entre las dos redes que han de ser interconectadas, para controlar el acceso y flujo de información entre los dominios. Este “gateway” debe ser configurado para filtrar el tráfico entre los dominios y para boquear el acceso no autorizado.



3.- Realización de la práctica

Creación de VLANs

En esta parte de la práctica se crearán dos VLANs en el conmutador A y se asignarán los puertos a una u otra. A continuación conectaremos los ordenadores a una y otra VLAN. Por último comunicaremos ambas VLANs entre sí mediante un router.

A las VLANs las llamaremos 'SUBRED1' y 'SUBRED2' y les asignaremos los números 2 y 3 respectivamente (el número 1 está reservado para la VLAN 'default', que es la que viene por defecto configurada en el equipo). Para crear las VLANs entraremos en consola del conmutador y utilizaremos el comando '**vlan database**' según se muestra a continuación:

```
Switch_A#vlan database
Switch_A#vlan 2 name SUBRED1
Switch_A#vlan 3 name SUBRED2
Switch_A#
```

Ahora podemos utilizar el comando 'show vlan' para comprobar que las definiciones se han realizado correctamente. Lo que aparece por pantalla debe ser similar a lo siguiente:

```
VLAN Name Status Ports
---------------------------------
1 default Enabled 1-24, AUI, A, B
2 SUBRED1 Enabled
3 SUBRED2 Enabled
1002 fddi-default Suspended
1003 token-ring-defau Suspended
1004 fddinet-default Suspended
1005 trnet-default Suspended
---------------------------------
VLAN Type SAID MTU Parent RingNo BridgeNo Stp Trans1 Trans2
------------------------------------------------------------------------------
1 Ethernet 100001 1500 0 0 0 Unkn 1002 1003
2 Ethernet 100002 1500 0 1 1 Unkn 0 0
3 Ethernet 100003 1500 0 1 1 Unkn 0 0
1002 FDDI 101002 1500 0 0 0 Unkn 1 1003
1003 Token-Ring 101003 1500 1005 1 0 Unkn 1 1002
1004 FDDI-Net 101004 1500 0 0 1 IEEE 0 0
1005 Token-Ring-Net 101005 1500 0 0 1 IEEE 0 0
------------------------------------------------------------------------------
#
```

Asignación de Puertos a VLANs

Una vez creadas las VLANs podemos asignar los puertos. Si un puerto no lo asignamos a ninguna quedará en la VLAN 'default' (la 1) que es en la que se encuentran todos inicialmente. Únicamente asignaremos los puertos 2, 3, 5, 6, 7 y 8 del Switch A, los pares a la VLAN 'SUBRED1' y los impares a la VLAN 'SUBRED2'.La secuencia de comandos a utilizar es la siguiente:

```
Switch_A #config
Enter configuration commands, one per line. End with CNTL/Z
Switch_A(config)# interface fastethernet 0/2
Switch_A(config-if)# switchport mode access
Switch_A(config-if)# switchport access vlan 2
Switch_A(config-if)# interface fastethernet 0/6
```

```
Switch_A(config-if)# switchport mode access
Switch_A(config-if)# switchport access vlan 2
Switch_A(config-if)# interface fastethernet 0/8
Switch_A(config-if)# switchport mode access
Switch_A(config-if)# switchport access vlan 2
Switch_A(config-if)#end

Switch_A(config)# interface fastethernet 0/3
Switch_A(config-if)# switchport mode access
Switch_A(config-if)# switchport access vlan 3
Switch_A(config-if)# interface fastethernet 0/5
Switch_A(config-if)# switchport mode access
Switch_A(config-if)# switchport access vlan 3
Switch_A(config-if)# interface fastethernet 0/7
Switch_A(config-if)# switchport mode access
Switch_A(config-if)# switchport access vlan 3
Switch_A(config-if)#end
```

Si repetimos ahora el comando ‘show vlan’ obtendremos un resultado como el siguiente:

Switch_A#show vlan

```
VLAN Name Status Ports
-------------------------------------
1 default Enabled 1,4, 9-24, AUI, A, B
2 SUBRED 1 Enabled 2, 6, 8
3 SUBRED 2 Enabled 3, 5, 7
1002 fddi-default Suspended
1003 token-ring-defau Suspended
1004 fddinet-default Suspended
1005 trnet-default Suspended
-------------------------------------
VLAN Type SAID MTU Parent RingNo BridgeNo Stp Trans1 Trans2
------------------------------------------------------------------------------
1 Ethernet 100001 1500 0 0 0 Unkn 1002 1003
2 Ethernet 100002 1500 0 1 1 Unkn 0 0
3 Ethernet 100003 1500 0 1 1 Unkn 0 0
1002 FDDI 101002 1500 0 0 0 Unkn 1 1003
1003 Token-Ring 101003 1500 1005 1 0 Unkn 1 1002
1004 FDDI-Net 101004 1500 0 0 1 IEEE 0 0
1005 Token-Ring-Net 101005 1500 0 0 1 IEEE 0 0
------------------------------------------------------------------------------
#
```

Configuración IP de HOST/SWITCH

Para configurar los ordenadores debemos conectarlos a los puertos del switch respectivamente y asignar una dirección IP y ruta por defecto.

HOST 1
Dirección IP: 192.168.3.2

Máscara: 255.255.255.0

Puerta de enlace predeterminada: 192.168.3.1

HOST 2
Dirección IP: 192.168.4.2

Máscara: 255.255.255.0

Puerta de enlace predeterminada: 192.168.4.1

Para configurar la dirección IP del Switch_A introducimos los siguientes comandos:

Switch_A(config)# interface vlan1
Switch_A(config-if)# ip address 192.168.1.2 255.255.255.0
Switch_A(config-if)# ip default-gateway 192.168.1. 1

Una vez asignadas las interfaces a las VLANs los estudiantes comprobarán con el comando ping que los dos ordenadores conectados al conmutador han perdido la comunicación entre ellos.

¿A que se debe esto?

_____
__

_____
__

Creación del enlace 'trunk'.

Para crear el enlace troncal en el switch A ejecutamos los siguientes comandos:

Switch_A(config)#interface fastethernet 0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#switchport trunk encapsulation dot1q
Switch_A(config-if)#end

Configuración del Router

Para que el router soporte inter-Vlan routing, debe ingresar los siguientes comandos.

Router_A(config)#interface fastethernet 0/0
Router_A(config-if)#no shutdown
Router_A(config-if)#interface fastethernet 0/0.1
Router_A(config-subif)#encapsulation dot1q 1
Router_A(config-subif)#ip address 192.168.1.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/0.2
Router_A(config-subif)#encapsulation dot1q 2
Router_A(config-subif)#ip address 192.168. 3.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/0.3
Router_A(config-subif)#encapsulation dot1q 3

```
Router_A(config-subif)#ip address 192.168.4.1 255.255.255.0
Router_A(config-subif)#end
```

Configuraciones de Seguridad

Bloqueo de paquetes Broadcast, Unicast y Multicast.

Una tormenta de paquetes ocurre cuando se reciben en un puerto gran número de paquetes broadcast, unicast o multicast. Reenviar esos paquetes puede causar una reducción de la performance de la red e incluso la interrupción del servicio.

Storm Control usa umbrales para bloquear y restaurar el reenvío de paquetes broadcast, unicast o multicast.

Usa un método basado en ancho de banda. Los umbrales se expresan como un porcentaje del
total de ancho de banda que puede ser empleado para cada tipo de tráfico.

Deseamos configurar el puerto 2 del switch para que si el tráfico broadcast supere el 45% del ancho de banda disponible envíe una alerta.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface FastEthernet 0/2
Switch(config-if)# storm-control broadcast level 45
Switch(config-if)# storm-control action trap
Switch(config-if)# end
```

Las opciones completas son:
(Dentro del modo configuración de interface del puerto a configurar)

```
storm-control {broadcast | multicast | unicast} level level [level-low]
storm-control action {shutdown | trap}
```

BIBLIOGRAFÍA

[1] **Troubleshooting Windows 2000 TCP/IP**, Debra littlejohn Shinder Thomas W. Shinder.

[2] **Stallings William**, Comunicaciones y Redes de Computadoras, 7ma Edición, Prentice-Hall, http://williamstallings.com/DCC/DCC7e.html, 2004.

[3] **"Principles, Protocols and Architecture, Internetworking with TCP/IP"**, Comer, D.E, 4ta Edición Volumen 1, Prentice-Hall, 2000.

[4] **"Protocolo Internet"**, Traducción al castellano, Pedro J. Ponce de León, www.infosintesis.net/apensintesis/internet/rfc0791-IP-es.pdf, 1999-05.

[5] **"Introducción al IPv6",** RAU, Red Académica Uruguaya, http://www.rau.edu.uy/ipv6/queesipv6.htm, 2005-11.

[6] **"Tipos de Direcciones IPv6",** Grupo de Sistemas y Comunicaciones Universidad Rey Juan Carlos, gsyc.escet.urjc.es/moodle/file.php/26/Transparencias/rom-transpas-3.pdf, 2003-11.

[7] **“La nueva versión de IP”,** Miguel Alejandro Soto, Costa Rica, http://usuarios.lycos.es/janjo/janjo1.html, 2006-12.

[8] **“Redes Virtuales VLANS”,** Textos Científicos, http://www.textoscientificos.com/redes/redes-virtuales.

[9] **“Guía de Administración de Redes con Linux”,** Kirch – Dawson, Editado por O`Reilly&Associates, http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-firewall.filtering.html, 2002-01.

[10] **“Traductor de Dirección de Red”,** Ing. Raúl Antelo Jurado, UMSS – CUJAE Cochabamba – Bolivia, http://www.monografias.com/trabajos20/traductor-nat/traductor-nat.shtml, 2005-02.

[11] **“Cortafuegos”**, Wikimedia Foundation Inc, WIKIPEDIA, http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29, 2007.

[12] **“Redes Privadas Virtuales”**, Warp Networks S.L., Isaac Clerencia, people.warp.es/~isaac/openvpn.pdf, 2005-06.

[13] **“IPsec”,** Ralf Spenneberg, http://www.ipsec-howto.org/spanish/x161.html, 2003.

[14] **“Attacking Predictable IPsec ESP Initialization Vectors”**, Nuopponen, Antti and Vaarala, Sami, Helsinki Univeristy of Technology. www.hut.fi/~svaarala/espiv.pdf, 2002**.**

[15] **“Métodos de Autenticación”**, www.wikilearning.com/metodos_de_ autenticación-wkccp-15516-47.html, 2006-10.

[16] **“Criptografía”**, http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo2.pdf.

[17] **“Criptografía de Clave Simétrica”**, http://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica.

[18] **“Criptografía de Clave Asimétrica”**, http://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica.

[19] **“Criptografía de Curva Elíptica”**, http://es.wikipedia.org/wiki/Criptograf%C3%ADa_de_curva_el%C3%ADptica.

[20] **“Criptografía Híbrida”**, http://es.wikipedia.org/wiki/Criptograf%C3%ADa_h%C3%ADbrida.

[21] **“Utilizando Inteligencia Artificial para la detección de Escaneos de Puertos”,** Amador - Arboleda – Bedón, Universidad del Cauca, http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VI_JornadaSeguridad/ArticuloIAPortScan_VIJNSI.pdf.

[22] **“Sabuesos en la Red: El escaneo de puertos”,** Death Master, akira.azul.googlepages.com/sabuesos.pdf, 2004.

[23] **“Ataques Externos”,** Eric Detoisien, http://www.linuxfocus.org/Castellano/March2003/article282.shtml, 2004-02.

[24] **“Ataque de Denegación de Servicio”,** Licencia de documentación libre de GNU,

http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio, 2007-05.

[25] **“Análisis de Seguridad de la familia de protocolos TCP/IP y sus servicios asociados”,** Raúl Siles Peláez, Edición 1, es.tldp.org/Manuales-LuCAS/doc-seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf, 2002-06.

[26] **“SEGURIDAD EN REDES IP”**, Capítulo 2, Gabriel Verdejo Álvarez. http://tau.uab.es/~gaby, 2003-09.

[27] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000. http://www.kriptopolis.com

[28] **“Soluciones de Seguridad Integrada de Cisco: Una familia de ofertas de Seguridad para la Red”,** Cisco Systems, www.cisco.com/web/LA/soluciones/comercial/SDN_solution_guide.pdf, 2006.

[29] **“Introducción al CISCO PIX”,** Govannom - Seguridad de Sistemas Informáticos,

http://www.govannom.org/modules.php?name=News&file=article&sid=376, 2002.

[30] **“CISCO PIX 501 SECURITY APPLIANCE”,** Cisco Systems, www.cisco.com/web/FR/documents/pdfs/datasheet/vpn_security/cisco_pix_501.pdf, 2004.

[31] **“CISCO PIX 506E SECURITY APPLIANCE”,** Cisco Systems, www.cisco.com/web/FR/documents/pdfs/datasheet/vpn_security/cisco_pix_506.pdf, 2004.

[32] **“CISCO PIX 515E SECURITY APPLIANCE”,** Cisco Systems, www.cisco.com/web/FR/documents/pdfs/datasheet/vpn_security/cisco_pix_515.pdf, 2004.

[33] **“CISCO PIX 525 SECURITY APPLIANCE”,** Cisco Systems, www.cisco.com/web/FR/documents/pdfs/datasheet/vpn_security/cisco_pix_525.pdf, 2004.

[34] **“CISCO PIX 535 SECURITY APPLIANCE”,** Cisco Systems, www.cisco.com/web/FR/documents/pdfs/datasheet/vpn_security/cisco_pix_535.pdf, 2004.

[35] **“Cisco amplía portafolio de switches modulares con el Catalyst 4500”,** Cisco Systems, http://www.ciscoredaccionvirtual.com/redaccion/comunicados/ver_comunicados.asp?Id=480, 2002-09.

[36] **“Dos nuevos servidores de Sun para el mercado de los x86”,** pc-news, www.pc-news.com/detalle.asp?sid=&id=1&Ida=1174, 2003-07.

[37] **“Ethereal: Mucho más que un sniffer”,** Carlos Cortés Cortés, http://bulma.net/body.phtml?nIdNoticia=1498, 2002-09.

[38] **“Ethereal: Depurar las comunicaciones”,** Álvaro del Castillo San Félix - Javier Palanca Cámara, acsblog.es/articulos/trunk/Varios/Ethereal/x27.html, 2002.

[39] **“High Performance Network management Solutions”,** Network Instruments, http://www.ipdsa.com/ni/brochures/Observer_v8.pdf, 2002.

[40] **“Manual de Seguridad en Redes”**, Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina, www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf, 2001-04