UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

"PROYECTO DE DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE UNA RED CORPORATIVA"

INFORME DE INGENIERÍA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MARLON MACEDO IBERICO

PROMOCIÓN
1997-2
LIMA-PERÚ
2002

A Oscar y Clara Luz,

mis padres.

PROYECTO DE DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE UNA RED CORPORATIVA

SUMARIO

Este informe de ingeniería se propone diseñar e implementar un sistema de seguridad para una red corporativa que abarque los pilares de la seguridad de red, a saber, confidencialidad, integridad, disponibilidad, consistencia, control y auditoría. Se explica primeramente los criterios esenciales topológicos de una red estable, sea ésta corporativa o no. Seguidamente, se presentan y explican suscintamente vulnerabilidades de red y tecnologías de seguridad actuales. Las tecnologías empleadas son estándares y si bien la red se basa en equipos Cisco Systems, toda las secciones de diseño buscan ser lo más general sin importar la plataforma específica. Es en el diseño de seguridad de red justamente donde el criterio y conocimiento ingenieril satisfacerá los seis requerimientos al principio mencionados. Entre las tecnologías aplicadas se tiene Secure Shell, tunelización L2TP y encriptación IPSec. Finalmente la implementación traducirá los requerimientos de diseño en scripts de configuración de los equipos de telecomunicaciones adecuados para las tareas necesitadas. Consideraciones de costo también se agregan, siempre recordando el factor seguridad/costo.

Un agradecimiento especial para el Ing. Luis Alexander Ponce Dioses, por sus consejos permanentes en lo ingenieril, en la elaboración del perfil y durante la tesis entera, y en lo personal. Agradezco también a los compañeros de mi Alma Mater, Milton Alvarez, Ing. Marlon Jimenez, Moisés Zorrilla y Fredy Campos.

INDICE

INDICE

		Página
PROLOGO		1
CAPITULO I		
TOPOLOGÍA DE UNA RED CORPORATIVA		**4**
1.1	Consideraciones Preliminares	4
1.2	Diseño Jerárquico de la Topología	5
1.2.1	El Core	6
1.2.2	La Capa de Acceso	8
1.3	Enrutamiento	9
1.4	Servicios	10
1.5	El Acceso al Internet	10
1.6	El Acceso Remoto	11
1.7	Network Operation Center	12
1.8	Capacity Planning	13

CAPITULO II

VULNERABILIDADES Y TECNOLOGÍAS

DE SEGURIDAD DE RED **14**

2.1 Introducción: Amenazas y Vulnerabilidades 14

2.2 Tipos de amenazas 15

2.3 Vulnerabilidades comunes 16

2.3.1 El Protocolo TCP/IP 16

2.3.2 El Protocolo UDP 23

2.3.3 El Protocolo ICMP 25

2.3.4 El Protocolo NNTP 27

2.3.5. El Protocolo SMTP 27

2.3.6. El Protocolo FTP 28

2.3.7 Los servicios NFS/NIS 29

2.3.8 El Sistema X Windows 30

2.4 Introducción: Tecnologías de Seguridad Actuales 30

2.5. Tecnologías de Identidad 30

2.5.1 Protección de los Passwords 31

2.5.2 Protocolos que Emplean Mecanismos de Autentificación 34

2.6 Seguridad en Capas TCP/IP 40

2.6.1 Protocolos de Seguridad de la Capa de Aplicación 41

2.6.2 Protocolos de Seguridad de la Capa de Transporte 41

2.6.3 Protocolos de Seguridad de la Capa IP 46

2.7 Tecnologías de Seguridad Virtuales Privadas Dial-up 55

CAPITULO III

PROYECTO DE DISEÑO DEL SISTEMA DE SEGURIDAD DEL CAMPUS DE LA RED CORPORATIVA **62**

3.1 Seguridad del NOC 62

3.1.1 Seguridad de las Estaciones del NOC 63

3.1.2 Firewall del NOC 119

3.2 Privilegios de Acceso de los Usuarios sobre los Equipos de Red 120

3.3 Confidencialidad de la Data en el Transporte. Encriptación 122

3.4 Integridad y Control de Conectividad 123

3.5 Disponibilidad de Red. Redundancia 123

3.6 Protección contra Ataques de Red 126

3.7 Bases de Datos Centrales 127

3.8 Logging y Auditoría 128

CAPITULO IV

PROYECTO DE DISEÑO DEL SISTEMA DE SEGURIDAD DEL ACCESO AL INTERNET DE LA RED CORPORATIVA **130**

4.1 Arquitectura del Acceso al Internet 130

4.2 Filtraje de Paquetes y DMZ 131

4.3 Network Address Translation 135

4.4 Redundancia de Firewalls 136

4.5 Auditoría: Monitoreo, Logging y Detección de Intrusos 137

CAPITULO V

PROYECTO DE DISEÑO DEL SISTEMA DE SEGURIDAD DEL ACCESO REMOTO DE LA RED **142**

5.1 Tunelización L2TP 142

5.2 Tunelización IPSec 144

5.3 Acceso Dial Empleando Autentifiación SSH 147

CAPITULO VI

PROYECTO DE IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA RED CORPORATIVA 149

6.1 Implementación del Sistema de Seguridad del Campus De la Red Corporativa 149

6.1.1 Servidores del NOC y Configuración de los Mismos 149

6.1.2 Plan de Direccionamiento y Redundancia de Red 156

6.1.3 Firewall del NOC 163

6.1.4 Switch Principal, Integridad y Control de Conectividad 165

6.1.5 Confidencialidad de la Data en el Transporte 166

6.1.6 Protección contra Ataques de Red 168

6.1.7 Bases de Datos Centrales 169

6.1.8 Control de Acceso sobre los Equipos de Red 170

6.2 Implementación del Sistema de Seguridad del Acceso al Internet 173

6.2.1 Firewall de la Red Corporativa y Router Examinador 173

6.2.2 Failover 175

6.2.3 Auditoría: monitoreo, logging y detección de intrusos 177

6.3 Implementación del Sistema de Seguridad del Acceso Remoto 179

6.3.1 L2TP 179

6.3.2 Tunelización empleando IPSec 185

6.3.3 Acceso Dial empleando Autentificación SSH 188

6.4 Plataformas y Costos 193

6.5 Consideraciones Restantes 200

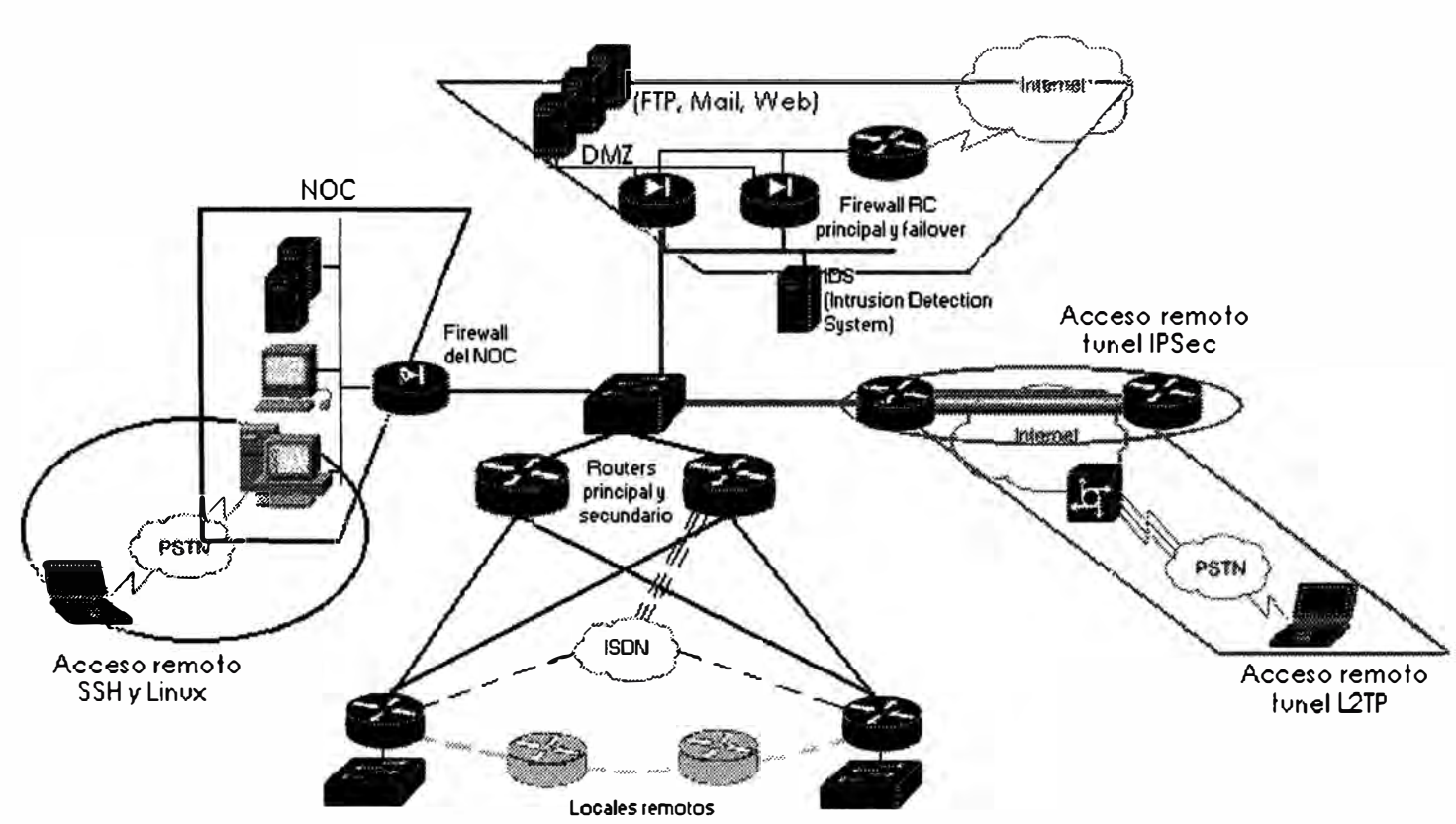
CONCLUSIONES 215

BIBLIOGRAFÍA 218

PROLOGO

En el presente informe de ingeniería se propone un sistema de seguridad para una red corporativa que asegure la confidencialidad de la información, la integridad de la data, la disponibilidad de red, la consistencia del sistema, el control de acceso y la auditoría de red.

En el Capítulo 1 denominado **Topología de una Red Corporativa** se delinean los conceptos básicos necesarios para construir una red escalable, consistente y estable. Se han seguido los preceptos del libro "Advanced IP Network Design" de Alvaro Retana, Don Slice y Russ White de Cisco Systems. El Capítulo 2, **Vulnerabilidades y Tecnologías de Seguridad de Red**, describe y analiza suscintamente vulnerabilidades de red, tecnologías y protocolos de seguridad actuales. Se hace énfasis en las tecnologías empleadas a lo largo del Informe de Ingeniería. El Capítulo 3 denominado **Proyecto de Diseño del Sistema de Seguridad del Campus de la Red Corporativa**, estudia la disposición y seguridad del NOC, Network Operation Center; el plan de direccionamiento y enrutamiento, sobremanera ligados a la redudancia ISDN y HSRP propuestas; el servidor de control de acceso y el control de conectividad, la encriptación, mínima pero presente e importante, y escenarios para la auditoría de red. El Capítulo 4 denominado **Proyecto de Diseño del Sistema de Seguridad del Acceso al Internet de la Red Corporativa** presenta y analiza la arquitectura de red empleando un router examinador y un firewall robusto como el PIX Firewall de Cisco. Hace énfasis este


(FTP, Mail, Web)
Internet
DMZ
NOC
Firewall RC
principal y failover
IDS
(Intrusion Detection
System)
Acceso remoto
tunel IPSec
Firewall
del NOC
Internet
Routers
principal y
secundario
PSTN
PSTN
ISDN
Acceso remoto
SSH y Linux
Acceso remoto
tunel L2TP
Locales remotos

capítulo en la necesidad de elaborar con precisión una política de seguridad de red de acceso al Internet, reflejado posteriormente en la sintaxis del equipo. Se diseña la redundancia del firewall y se expresan las consideraciones para la auditoría de red, específicamente en la detección de intrusos. El Capítulo 5 denominado **Proyecto de Diseño del Sistema de Seguridad del Acceso Remoto de la Red Corporativa** muestra los accesos remotos no tradicionales disponibles a la fecha, a saber, la tunelización IPSec y L2TP. El shell SSH ha sido adecuado dentro de un acceso dial convencional en Linux para ofrecer la seguridad en la autentificación, encriptación y no repudiación.

El Capítulo 6, **Proyecto de Implementación del Sistema de Seguridad de la Red Corporativa**, reuné las consideraciones de los Capítulos 3, 4 y 5 para escoger las plataformas que se adecúan a las necesidades e implimentar los postulados descritos. Fue inevitable escribir algunas configuraciones propietarias a equipos Cisco Systems pero se busco darle una dimensión general al capítulo sin importar la plataforma. Finalmente, las conclusiones de la presente Tésis, con el título del mismo nombre, busca dirigirse a Ingenieros de Telecomunicaciones dedicados a la Seguridad de Red.

CAPITULO I
TOPOLOGÍA DE UNA RED CORPORATIVA

Hablando en general sobre el internetworking, antes de presentar la seguridad de una estructura es importante presentar ante todo lo que hace que dicha estructura sea estable. El presente capítulo expone las consideraciones a tener en cuenta para el diseño topológico de una red corporativa; el detalle técnico será dejado para los capítulos III, IV y V.

La red a analizar es considerada una red "sin protección"; se abarca la jerarquía de redes, los servicios, el acceso al Internet y el acceso dial. Se busca actuar frente a una red estable y que asegure la conectividad total del campus con el Internet y las oficinas remotas.

1.1 Consideraciones Preliminares

La red a diseñar emplea como protocolo de comunicación el TCP/IP (versión 4) debido a su universalidad en LANs, intranets, extranets y el Internet, por antonomasia.

La infraestructura WAN se construye sobre un backbone ATM. La pregunta que surge es si una corporación contará con los recursos para montar este backbone ATM. Lo cómun es asistir a un carrier de telecomunicaciones como Telefonica del Perú o AT&T Latin America. El presente Informe toma el escenario de una corporación que solicita un carrier para su backbone. Supondremos el carrier provee una backbone ATM que se extiende por la provincia de Lima. El grupo de

ingenieros encargados del diseño de la red corporativa deberá indagar sobre la topología del backbone ATM (performance, capacidad) y sus características de seguridad (redundancia fisica y lógica). Lo que se planteará no son consideraciones de diseño ATM (pues al fin y al cabo eso pertenece al carrier) sino que se expondrá las características de red que los ingenieros encargados de montar la red corporativa deberán "exigir" al carrier sobre el backbone ATM. Las consideraciones del backbone ATM serán relatadas en el capítulo VI (la implementación).

El escenario planteado es punto multipunto como se menciona en la sección "Diseño jerárquico de la topología".

1.2 Diseño Jerárquico de la Topología

Se sabe que es más fácil atacar un problema si esté es dividido en pequeñas partes, y las redes de gran escala (como las redes corporativas) no son la excepción. El proceso de la comunicación misma en networking se separa en capas según el modelo OSI para su mejor comprensión.

La jerarquía no sólo hace que los varios elementos del enrutamiento, QoS, accounting y la conmutación de paquetes, sea escalable, sino que presenta la oportunidad para la segmentación operacional de la red, resolución de problemas más sencilla (troubleshooting), configuración individual de routers, switches, firewalls menos complicada y una base lógica para la contabilidad de paquetes (análisis de tráfico).

La red corporativa debe seguir un modelo jerárquico o en capas. Las capas definidas en este modelo se muestran en la Figura 1-1.

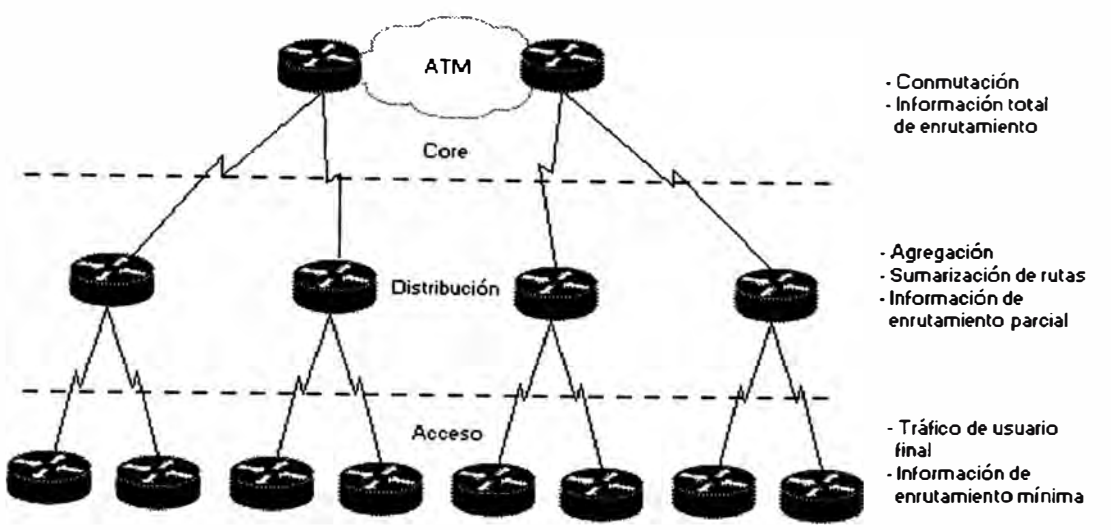


Figura 1.1: Diseño Jerárquico de la Topología

El core desplaza el tráfico a grandes velocidades; la principal misión de un dispositivo del core es conmutar paquetes (packet switching).

- La capa de distribución acumula el tráfico y sumariza (resume) la información de rutas.
- La capa de acceso inyecta tráfico sobre la red, realiza funciones de filtrado de red y provee otros servicios de red.

La mayor debilidad inherente del modelo jerárquico es que crea puntos de fallo único en la capa física. Ciertas medidas de redundancia serán aplicadas para apaliar esta debilidad. De la redundancia se hablará en los capítulo III, IV, V y VI.

La red corporativa se extenderá a lo largo de la provincia de Lima y como tal, el modelo jerárquico de 3 capas presentado, resulta costoso e innecesario. La realidad es que las soluciones que los carriers presentan a las redes corporativas actuales son soluciones punto-multipunto. Por consiguiente, no existirá capa de distribución y mucho menos sumarización.

1.2.1 El Core.- Los dispositivos pertenecientes al core tendrán como misión primordial la conmutación de paquetes, por ello deberán ser cajas de gran

performance y capacidad de procesamiento (características "carrier-class", como múltiples CPUs y fuentes de alimentación).

Para no afectar este objetivo dos estrategias básicas deberán seguirse:

- Ninguna política de red deberá implementarse en el core, por ejemplo el filtraje de paquetes y la política de enrutamiento. En el supuesto de aplicarse en el core, cualquier error al implementar un cambio en la política del core puede causar que la red entera falle.
- Cada dispositivo del core deberá tener alcance total a cada destino en la red. Debido a que no existe sumarización, un router del core conocerá una ruta hacia cada red individual en cada extremo de la red corporativa.

La red punto-multipunto posee un solo router de core (ubicado fisicamente en el campus principal, headquarters). Esto se conoce como un core colapsado.

Este core colapsado es fácil de manejar (al fin y al cabo es un solo router), pero no escala adecuadamente debido a que cada paquete que es llevado a través de la red atravezará el backplane del router central; esto eventualmente sobrecargará incluso el router más grande y veloz. El core colapsado también representa un punto único de fallo.

La redundancia por tanto surge debido a razones de performance y de seguridad (redundancia fisica para la contingencia). La mayoría de redes emplea un grupo de routers interconectados por una red de área local de alta velocidad (por ejemplo, FastEthernet) o una malla de enlaces WAN de alta velocidad para formar una red core.

1.2.2 La capa de acceso.- La capa de acceso es la "interface" hacia las redes de usuarios finales.

Ella debe cumplir tres objetivos:

- Introducir tráfico en la red
- Control de acceso
- Cumplir otras funciones de borde

Es importante que el router de la capa de acceso no sature el enlace hacia el core. Mientras esto es primariamente una cuestión de dimensionamiento (capacity planning), también se relaciona con la ubicación del servidor/servicio y el filtraje de paquetes. El tráfico que no está destinado hacia un host fuera de la red local no deberá ser enviado por el dispositivo de la capa de acceso.

Evitar el emplear los routers de acceso como puntos de traspaso de tráfico, una situación vista en redes altamente redundantes. No olvidar que esa es la misión del core. La redundancia en el acceso es vista en el capítulo VI. La figura 1.2 muestra la redundancia en el acceso.

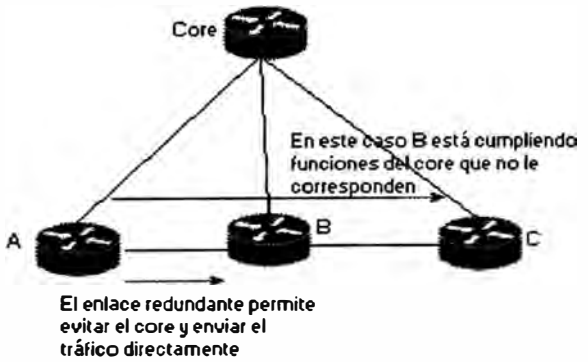


Figura 1.2: Redundancia en el acceso

Desde que la capa de acceso es donde los usuarios se conectan a la red, es también el lugar perfecto para que los intrusos ingresen peligrosamente en ella. El

filtraje de paquetes deberá ser aplicado de modo que el tráfico prohibido hacia el core deberá ser bloqueado, incluyendo paquetes que no se originan en la red localmente conectada. Sobre ello se abordará ampliamente en los capítulos de diseño e implementación.

Los otros servicios de borde abordados son:

- Implementación de Quality of Service (Qos).
- Terminación de túneles, en nuestro caso, para enlaces virtuales privados y encriptación.

1.3 Enrutamiento

El enrutamiento estático es preferido sobre el enrutamiento dinámico en ciertas circunstancias. Como en cualquier proceso, mientras más automático, menos control sobre él. Aún cuando el enrutamiento dinámico automático requiere mucho menos intervención humana, el enrutamiento estático permite más control preciso sobre el comportamiento del enrutamiento sobre un internetwork. El precio a ser pagado por esta precisión es la necesidad de reconfiguración manual cada vez que la topología de la red cambia (por crecimiento, modificación o desastre).

Por otro lado el costo de la automatización es pagado en ancho de banda y quizás espacio de cola, memoria y tiempo de procesamiento.

Como una red corporativa tenderá a crecer geográficamente y a nivel de usuarios, nuevos routers serán agregados y se tornará complejo un esquema de enrutamiento estático. Por consiguiente, lo más recomendable es elegir un protocolo de enrutamiento dinámico como la solución más escalable, a saber, EIGRP (Enhanced Interior Gateway Routing Protocol) u OSPF (Open Shortest Path First).

1.4 Servicios

Los servicios comunes consisten en usuarios accesando regularmente sobre granjas de servidores, conexiones a dominios de enrutamiento externos (partners o el Internet) y mainframes. Existen dos métodos típicos de conectarse a estos tipos de recursos en la red:

- Conexión directa a la red del core
- Conexión a través de una red perimétrica o Zona Desmilitarizada (DMZ, DeMilitarized Zone)

Las granjas de servidores y mainframes se conectan, por lo general, directamente al core (se trata ante todo de servicios para usuarios corporativos internos). En el caso de dominios externos, el tema de seguridad se hace obvio y es necesario proveer una zona de transición entre el dominio externo y el core.

Los servidores más comunes son: FTP, mail, WWW, databases.

1.5 El acceso al Internet

Aún cuando se ha mencionado una red desprotegida es inevitable decir que la corporación accesará al Internet con cierta función de firewall.

Los escenarios comunes para la salida al Internet son:

- Un router examinador con características de firewall (Figura 1.3).
- Un router exterior examinador junto con un firewall robusto (Figura 1.4).
- Un proxy.
- Un bastidor (bastion host).

El acceso al Internet se provee comúnmente desde una LAN conectada directamente al core debido al volumen de tráfico a manejarse y su posición estratégica (el campus principal).

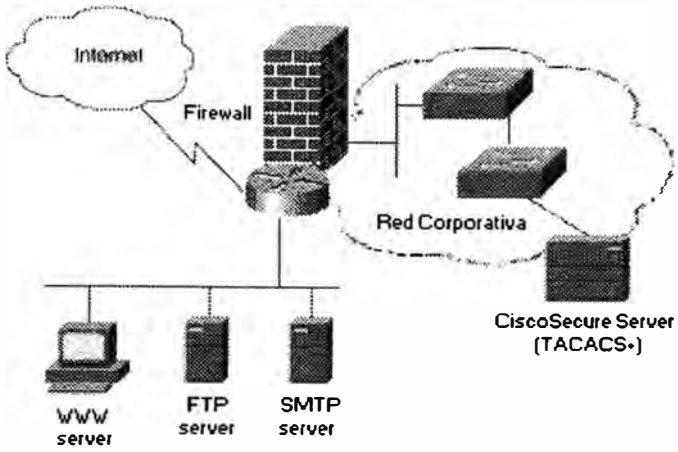


Figura 1.3: Salida al Internet empleando un router examinador con características de firewall

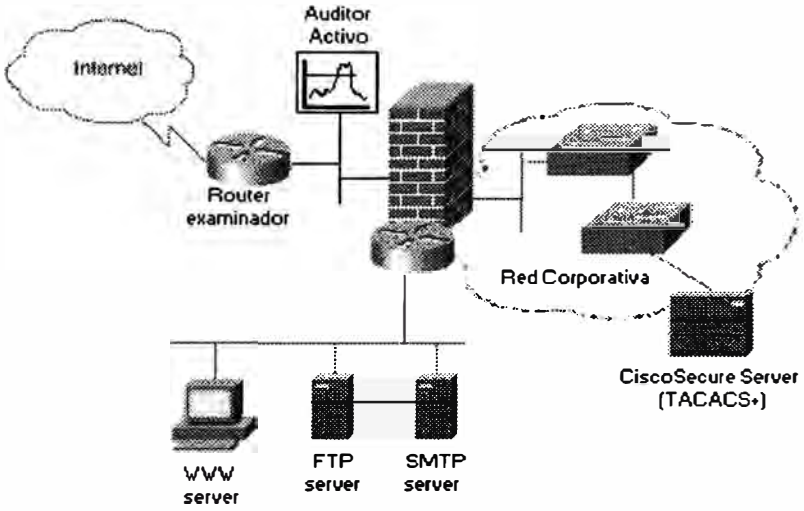


Figura 1.4: Salida al Internet empleando router examinador y firewall

1.6 El acceso remoto

Los accesos remotos disponibles se desenvuelven sobre infraestructuras privadas (direct dial-in) y públicas (virtual dial-in). El acceso dial-in puede ser a través de redes telefónicas publicas conmutadas PSTN (líneas de modem, frame relay, ATM, circuitos T1/T3 o ISDN). El acceso virtual dial-in se realiza empleando la infraestructura pública de un ISP. Para que este modelo opere de manera segura debe implementarse tecnologías de tunelización.

Los accesos dial más comunes son:

- LANs remotas accesando a través de una red PSTN o ISDN (empleando routers Cisco 4500, Cisco 2500 en conjunción con servidores de acceso)
- Nodos remotos accesando a través de una red PSTN o ISDN (empleando pool de modems y servidores de acceso). Por ejemplo, empleando DUN de Microsoft para llamadas analógicas o digitales (empleando un TA, terminal adapter).
- PCs remotas estableciendo llamadas remotas en redes X.25.
- LANs o PCs remotas ingresando a una red privada virtual dial VPDN montada sobre la infraestrucuta de un ISP.

El acceso dial en la parte perteneciente a la corporación puede montarse sobre la LAN del campus principal o sobre aquellas de las oficinas remotas. En el caso del core, será necesario un router dedicado al acceso dial en los casos aplicables mencionados (pues no olvidar la función primordial del core, conmutación de paquetes).

1.7 Network Operation Center

El Centro de Gestión o NOC, Network Operation Center, es aquella sección (staff, equipos) destinada a la gestión de: fallas, configuración, seguridad, registro (accounting) y performance de la red corporativa.

El NOC como centro de operaciones debe tener control total de los equipos, es decir, es necesario que tenga total alcance (a nivel lógico) sobre todos los rincones de la red (routers, switches, modems, firewalls, etc).

Un sistema de gestión de red (NMS, Network Management System) puede arreglarse en arquitecturas centralizada, jerárquica o totalmente distribuida.

Una arquitectura centralizada alivia en costo pero introduce un único punto de falla de dos modos: debido a la falla del NMS o a su pérdida de conectividad. Este modelo no escala adecuadamente pues el polling o traps pueden consumir enorme ancho de banda en las proximidades del NMS (a parte de los problemas en CPU del mismo).

El arreglo jeráquico hace que cada sub-NMS sea responsable de su nivel en la escala. Este diseño alivia el problema de la escalabilidad, pero sufre aún de puntos de fallo únicos según se sube en la jerarquía.

El sistema NMS totalmente distribuído ofrece la arquitectura más escalable y confiable. Los sub-NMS son autónomos e intercambian reportes de sus respectivas áreas de control. Sin embargo la arquitectura NMS distribuída es mucho más complicada que la centralizada.

El arreglo que se propone es el sistema centralizada debido al número de equipos a gestionar (un número menor de 100, ínfimo para un NMS comercial como el CiscoWorks).

Es común costumbre conectar el NOC directamente al core por su posición centralizada.

1.8 Capacity planning

El planeamiento de la capacidad deberá realizar para dimensionar los enlaces y los requerimientos de performance de los equipos. Será necesario generar una matriz de tráfico (desde fuente i, hacia destino j).

La matriz puede construirse tomando en cuenta flujos de tráfico de aplicación o flujos genéricos de paquetes (como los paquetes Ethernet desde una interface LAN)

CAPITULO II
VULNERABILIDADES
Y TECNOLOGIAS DE SEGURIDAD DE RED

El presente capítulo tratatá:

- Las amenazas y vulnerabilidades sobre una red corporativa.
- Las tecnologías de seguridad actuales empleadas en el Informe presente.

2.1 Introducción: amenazas y vulnerabilidades

Hoy en día, existe una dependencia creciente en las redes de computadoras para las transacciones de negocios. Con el flujo libre de información y la alta disponibilidad de muchos recursos, los administradores de redes empresariales deben comprender todas las posibles amenazas a sus redes.

El saber que áreas de la red son más susceptibles a intrusos y quién es el atacante común es de mucha ayuda. La tendencia común es la de confiar en los usuarios internos de la red corporativa y desconfiar de las conexiones que se originan del Internet o modems dial-in y líneas ISDN. Es importante confiar en los empleados internos de la red y en personas autorizadas tratanto de emplear recursos de red internos desde el exterior de la corporación. La confianza también debe ser pesada frente a la realidad. El uso restringido de equipos de infraestructura de red y recursos críticos es necesario. La limitación del acceso a red a aquellos que

requieren acceso es un manera inteligente de detener muchas amenazas que resquebrajan la seguridad de red.

2.2 Tipos de amenazas

Existen diferentes tipos de amenazas, pero se puede realizar una categorización tentativa:

- Acceso no autorizado
- Suplantación
- Anulación de servicio

2.2.1 Acceso no autorizado.- El acceso no autorizado es cuando una entidad no autorizada gana acceso a un recurso y tiene la posibilidad manipular tal recurso. El ganar acceso es usualmente el resultado de interceptar cierta información en tránsito sobre un canal inseguro o explotando una debilidad inherente en un tecnología o producto.

2.2.2 Suplantación.- La suplantación está estrechamente relacionada al acceso no autorizado pero es lo suficientemente significativo como para ser discutido aparte. La suplantación es la habilidad de presentar credenciales como si uno fuese algo u alguien que no es. Estos ataques pueden tomar varias formas: robar una clave privada, ganar acceso al par username/password; o incluso guardar una secuencia de autorización para repetirla en el futuro.

2.2.3 Anulación de servicio.- La Anulación de servicio (DoS, Denial of Service) es una interrupción del servicio bien porque el sistema es destruido, bien porque está temporalmente fuera de disposición. Por ejemplo, la destrucción del disco duro de una PC, afectar la infraestructura fisica, o usar al tope la memoria disponible de un recurso.

Los ataque DoS se aprovechan generalmente de las debilidades y vacíos en protocolos como el IP. La tabla enumera los ataques DoS más comunes.

Ataque DoS	*Vulnerabilidad explotada*
TCP Syn Flooding	Memoria es reservada para conexiones TCP abiertas a medias (half-open connection) de manera que no hay memoria de más para futuras sesiones.
Ping de la muerte (Ping of Death)	Implementación de la fragmentación IP por la cual paquetes largos son reemsamblados y puden causar que las máquinas sucumban.
Ataque Land.c	Establecimiento de conexiones TCP.
Ataque Teardrop.c	Implementación de la fragmentación IP por la cual problemas en el reensamblaje puede ocasionar que las máquinas sucumban.
Ataque Smurf	Inundación de las redes con tráfico broadcast, saturando las mismas.

2.3 Vulnerabilidades comunes

Los ataques explotan las debilidades de los sistemas. Estas debilidades pueden deberse a redes diseñadas pobremente o por un planeamiento descuidado.

2.3.1 El protocolo TCP/IP.- El Protocolo Internet (IP, Internet Protocol) es un protocolo no orientado a conexión, poco fiable (unreliable) de la suite TCP/IP. Tiene dos campos de 32 bits en la cabecera para guardar la información de las direcciones. IP es también el más ocupado de todos los protocolos TCP/IP puesto que prácticamente todo el tráfico TCP/IP es encapsulado en datagramas IP. La función de IP es rutear los paquetes por la red. No provee mecanismos de confiabilidad o registro (accounting), para ella, confia en las capas superiores. IP simplemente despacha los datagrams y espera que transcurran intactos. Si no, IP puede tratar de

enviar un mensaje de error ICMP de regreso a la fuente, sin embargo este paquete puede perderse también. IP no tiene medios de garantizar el despacho. Desde que IP es no orientado a conexión, no mantiene ninguna información sobre el estado de la conexión. Cada datagrama IP es enviado a su suerte sin miramiento respecto al último enviado o al siguiente.

La figura 2.1 muestra la cabecera IP.

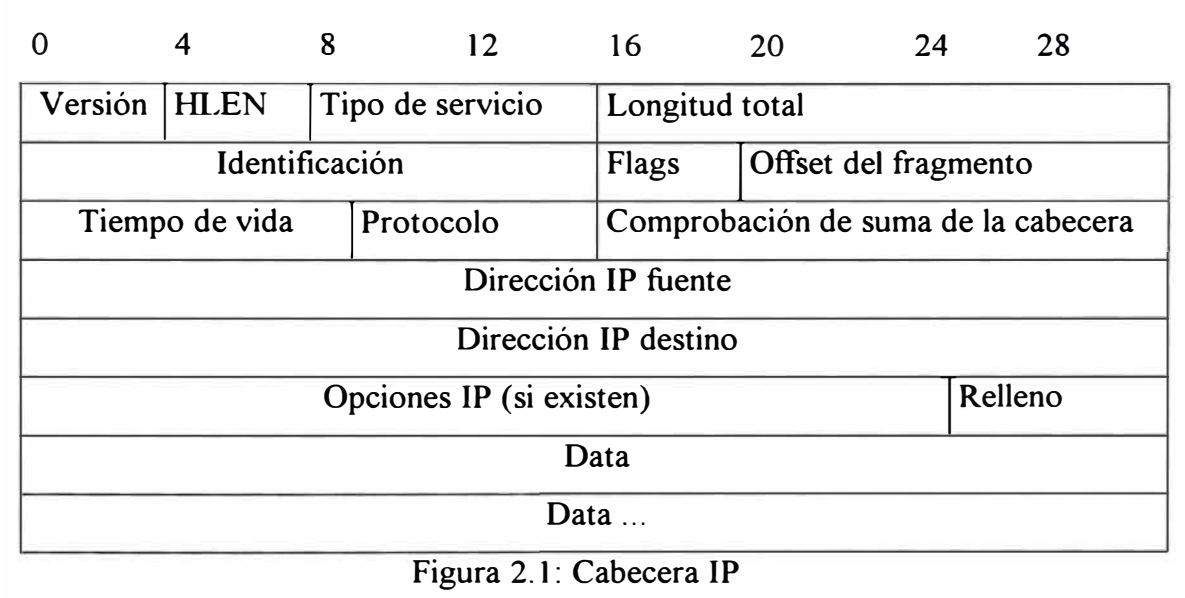


Figura 2.1: Cabecera IP

El protocolo TCP es el protocolo orientado a conexión y el protocolo de transporte confiable de la suite TCP/IP. Que sea orientado a conexión simplemente significa que los dos hosts participantes en una transacción deben primero establecer una conexión antes que la data cambie de manos. La fiabilidad es proveída de diferentes maneras pero las que nos competen son la secuencia de data y el acuse de recibo, reconocimiento o acknoledgment.

TCP permite que múltiples aplicaciones en un sistema se comuniquen concurrentemente debido a que maneja toda la demultiplexación del tráfico de entrada antre los programas de aplicación.

La figura 2.2 muestra la cabecera TCP.

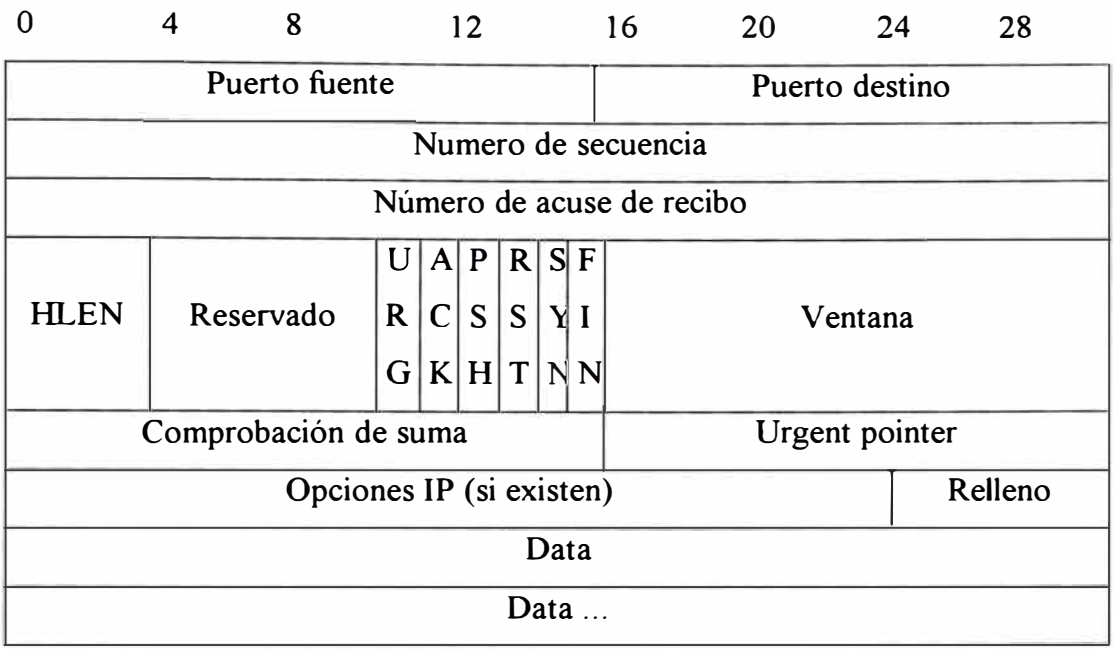


Figura 2.2: Cabecera TCP

2.3.1.1 Establecimiento de una conexión TCP.- Para establecer una conexión TCP, una negociación de tres fases (three-way handshake) debe ocurrir entre las dos estaciones a comunicarse. Cada paquete de esta negociación contiene un número de secuencia; los números de secuencia son únicos para la conexión.

La figura muestra esta negociación de tres fases:

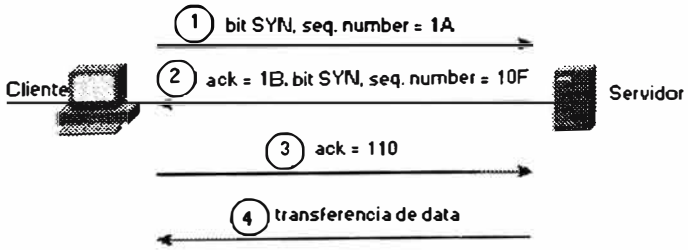


Figura 2.3: Establecimiento de una Conexión TCP/IP

2.3.1.2 Ataque sobre el número de secuencia TCP.- Cuando un atacante conoce el patrón de un número de secuencia, es bastante fácil suplantar otro host. El atacante se conecta a un puerto TCP del objeto (SMTP es una buena elección) justo antes de lanzar el ataque y completa la negociación de tres vías. El proceso es como se

muestra en las líneas de abajo, excepto que el atacante debe grabar el valor del ISN enviado por la estación presa.

A ---- SYN → B

A --- SYN/ACK → B

A --- ACK → B

Muy a menudo, este proceso es repetido varias veces y el ISN final enviado es almacenado. El atacante necesita tener una idea del RTT (round-trip time) desde su estación al objetivo. El proceso puede ser repetido varias veces y un promedio de RTT es calculado). El RTT es necesario para ser capaz de predecir con precisión el siguiente ISN. El atacante tiene la base (el último ISN enviado) y conoce cómo los números de secuencia son incremetados (128 000/segundo y 64 000 por conexión) y ahora tiene una buena idea de cuánto tiempo le toma a un datagrama IP, viajar a través del Internet para alcanzar la presa (aproximadamente la mitad del RTT, la mayoría de las veces las rutas son simétricas). Luego que el atacante tiene esta información, inmediatamente procede a la siguiente fase del ataque (si otra conexión TCP fuese a llegar a algún puerto del objetivo antes de que el atacante sea capaz de continuar el ataque, el ISN predecido por el atacante estará apartado un valor de 64000 de lo que fue predecido).

Cuando el segmento suplantado hace su viaje hacia el objetivo, muchas cosas diferentes pueden ocurrir dependiendo de la precisión de la predicción del atacante:

- Si el número de secuencia está exactamente donde el módulo TCP receptor lo espera, la data entrante será colocada en la siguiente posición disponible del buffer.

- Si el número de secuencia es menor que el valor esperado, la data es considerada una retransmisión y por ende descartada.
- Si el número de secuencia es mayor que el valor esperado pero aún dentro de los límites de la ventana receptora, la data es considerada un byte futuro y es ayudada por TCP, el cual asume la espera de los paquetes restantes. Si un segmento llega con un número de secuencia mayor que el valor esperado y no está fuera de los límites de la ventana de recepción, el segmento es descartado, y TCP enviará de retorno un paquete con el número de secuencia "esperado".

He aquí donde la arremetida final del atacante empieza:

1 Z(b) ---- SYN -→ A

2 B --- SYN/ACK -→ A

3 Z(b) --- ACK -→ A

4 Z(b) --- PSH -→ A

La estación atacante falsea su dirección IP para ser la de una estación confiable (la cual estará aún ejecutando un ataque denial of service) y envía su petición de conexión al puerto 513 del objetivo (1). En (2), el objetivo responde a la petición de conexión falseada con un SYN/ACK, la cual se enrutará hacia la estación confiable (la cual, si pudiese procesar el segmento TCP entrante, lo consideraría un error, e inmediatamente enviaría un RST al objetivo). Si todo marcha de acuerdo al plan, el SYN/ACK será descartado por la estación confiable (pues simplemente no puede contestar). Luego de (1), el atacante debe aguantarse un instante para dar tiempo al envío del SYN/ACK (el atacante, después de todo, no puede ver este segmento). Luego, en (3) el atacante envía un ACK al objetivo con el número de secuencia predecido (más uno, pues debe confirmarlo). Si el atacante está correcto en

su predicción, el objetivo aceptara la conexión. La presa se ve comprometida y la transferencia de data puede comenzar.

Generalmente, luego del compromiso, el atacante insertará una puerta falsa en el sistema que le permitirá un modo más simple de intromisión. A menudo se ejecuta un "cat + + >> ~/.rhosts". Esta es una buena idea por muchas razones: es rápido, permite un ingreso simple y "no es interactivo". Se debe recordar que el atacante no puede ver el tráfico proveniente del objetivo, de modo que cualquier respuesta es enviada a la nada.

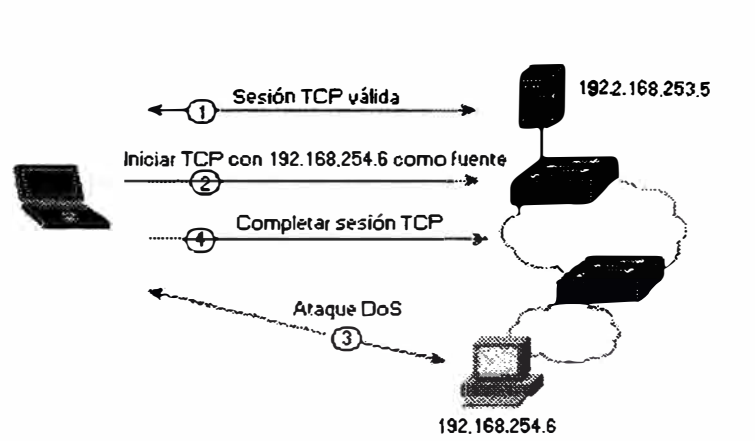


Figura 2.4: Spoofing al Número de Secuencia TCP/IP

2.3.1.3 Sesión Hijacking TCP/IP.- La sesión Hijacking es un caso especial de spoofing IP y es más fácil de ejecutar que el ataque al número de secuencia. Un intruso monitorea una sesión entre dos estaciones comunicándose e injecta tráfico que parece venir de una de estas estaciones, robando efectivamente la sesión del otro. La estación legítima es retirada de la conexión mientras el impostor la continúa con los mismos privilegios que el dueño verdadero.

La sesión Hijacking es muy dificil de detectar. La mejor defensa es la de usar servicios de confidencialidad y encriptar la data.

2.3.1.4 Ataque SYN TCP.- El potencial de abuso nace en el punto donde el sistema del servidor ha enviado una confirmación SYN-ACK de regreso al cliente pero el mensaje (de respuesta) ACK aún no ha sido recibido. Esto es lo que se entiende por "conexiones a medio abrir". El servidor ha elaborado en la memoria del sistema un estructura de data describiendo las conexiones pendientes. Esta estructura de data es de tamaño finito, y puede desbordarse intencionalmente creando demasiadas conexiones parcialmente abiertas (half-open or partially-open conecctions).

En la mayoría de casos, la víctima de tal ataque tendrá dificultades en aceptar la llegada de cualquier nueva conexión. En estos casos, el ataque no afecta las conexiones de entrada existentes ni la habilidad de originar conexiónes de salida. Sin embargo, en algunos casos, el sistema quedará agotado de memoría o sucumbirá, quedando inoperativo.

2.3.1.5 Ataque Land.- El ataque Land emplea spoofing IP en combinación con la apertura de una conexión TCP. Este envía un paquete que solicita abrir una conexión TCP, es decir con el bit SYN activado en la cabecera TCP. Este es un procedimiento legal. Pero lo que es ilegal es cambiar las direcciones IP de la cabecera IP subyacente. En Land, ambas direcciones IP, fuente y destino son modificadas para ser similares, la dirección de la estación víctima.

Cuando la víctima recibe el paquete, ésta responde a la petición SYN. Al responder, el host destino típicamente construye un paquete con la bandera ACK activada, cambia la dirección destino por la dirección fuente y viceversa. Esto resulta en el envío del paquete de regreso a sí mismo, debido a que las direcciones

son las mismas. Como resultado, el kernel ingresa en un remolino de ACKs contra sí mismo. En la máquina de estado TCP esto origina el problema inicial puesto que en el estado SYN RECEIVED la máquina espera recibir un mensaje ACK, no SYN+ACK.

2.3.2 El protocolo UDP.- Al igual que TCP, UDP (User Datagram Protocol) es un protocolo de la capa de transporte. Sin embargo, UDP provee un servicio de despacho no confiable y no orientado a conexión para el transporte de mensajes. No ofrece corección, retransmisión, o protección contra paquetes duplicados o perdidos. UDP fue diseñado para simplicidad y rapidez, y evitar el alto costo en la cabecera asociado con el establecimiento de la conexión y su finalización.

La figura 2.5 muestra el formato de la cabecera UDP.

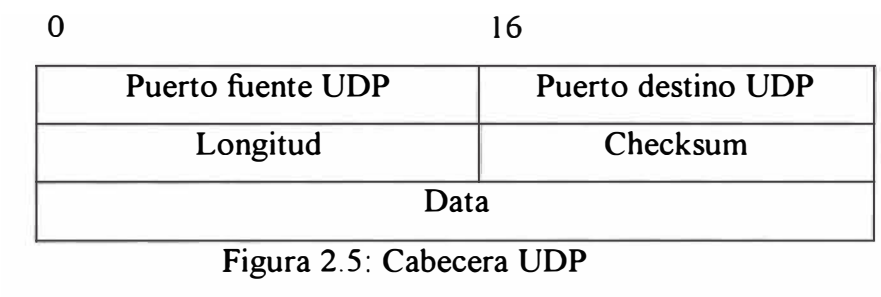


Figura 2.5: Cabecera UDP

Debido a que no existe control sobre que tan rápido son enviados los mensajes UDP, y a que no hay negociación en el establecimiento de la conexión o números de secuencia, los paquetes UDP son más fáciles de falsificar que los paquetes TCP.

2.3.2.1 El ataque Teardrop.- Teardrop es un ataque que explota la vulnerabilidad en el reemsamblaje de paquetes IP. Las tecnologías de redes tienen un máximo tamaño de paquete que pueden manejar. Este tamaño de paquete es llamado el MTU, Maximum Transfer Unit. Si la capa de red subyacente no puede transportar

un paquete dado porque es demasiado largo, el paquete deberá ser fragmentado en piezas más pequeñas. Esto se conoce como fragmentación.

Una vez que los fragmentos del paquete han llegado a su destino final, el paquete es reemsamblado a partir de los fragmentos. Tanto la fragmentación como el reemsamblaje son ejecutados por la capa IP.

Cuando la capa IP recibe un paquete IP realiza típicamente lo siguiente:

1. Verificar que al lo menos el paquete es tan largo como la cabecera IP.
2. Realizar la comprobación de suma de la cabecera, y descartar el paquete en caso de error.
3. Verificar que el paquete es de longitud como lo indica la cabecera, y descartarlo en caso contrario. Recortar cualquier relleno.
4. Procesar las opciones IP.
5. Verificar si el paquete es para el host, en cuyo caso continuar procesar, o de lo contrario, bien reenviarlo o descartarlo.
6. Si el paquete ha sido fragmentado, guardar el fragmento en una cola hasta que el resto de fragmentos arribe.
7. Pasar el paquete a las capas superiores.

Si un paquete es manipulado de manera que sobreviva a las cinco primeros observaciones, se puede aprovechar la deficiencia en el reemsamblaje. Cuando un paquete es procesado, las implementacioens típicamente observan si el paquete dado es demasiado largo, pero no se percatan de si es demasiado corto y si se halla desalineado.

La siguiente figura 2.6 muestra el falso cálculo en el reemsamblaje causado por el ataque Teardrop.

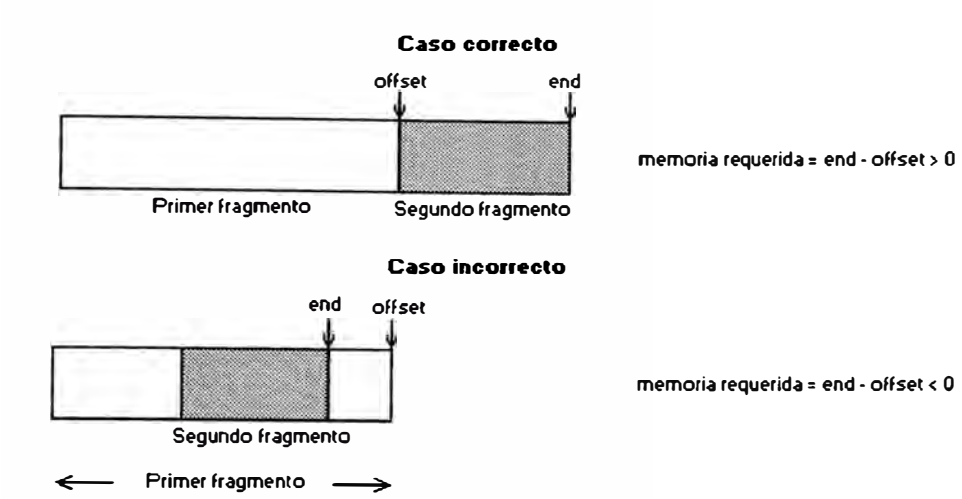


Figura 2.6: Cálculo Errado en el Reemsamblaje debido al Ataque Teardrop

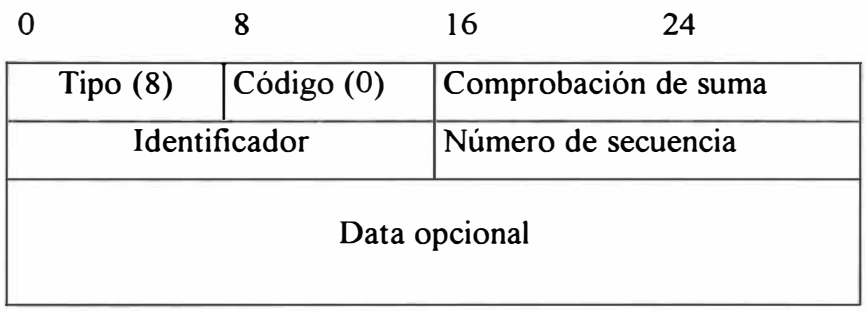
La pila recibe el primer fragmento y separa memoria para él. El offset del siguiente paquete es colocado al final del área de memoria así como el puntero final. La pila espera que el siguiente datagrama empiece en el offset y calcula que el puntero final apunte al final del nuevo paquete, lo cual significa, el tamaño del primer paquete más el tamaño del segundo menos la segunda cabecera IP descartada. El tamaño de memoria necesitada es igual a: end – offset. Pero el offset en el segundo paquete es falseado y apunta dentro de la primera área de memoria. La pila trata de realinar para corregir el error, pero el segundo paquete es lo suficientemente corto como para que el puntero aún apunte dentro del área de memoria inicial. Ahora, el resultado del cálculo necesita de memoria: end - offset, que es negativo. Como siguiente paso en el reemsamblaje es reservar memoria para el nuevo paquete, la rutina de reserva de memoria eventualmente fallará pues un valor negativo le es dado como argumento. La falla en la disposición de memoria ocasiona que el host sucumba.

2.3.3 El protocolo ICMP.- El protocolo ICMP (Internet Control Message Protocol) es empleado por la capa IP para intercambiar mensajes de control. ICMP

es también empleado para herramientas de diagnóstico tan populares como el Ping y el Traceroute.

El mensaje ICMP es encapsulado dentro del paquete IP. Los paquetes IP pueden ser de hasta 65535 octetos de longitud (RFC-791); esta longitud del paquete incluye la longitud de la cabecera (típicamente 20 octetos si no se especifican opciones). Los paquetes más grandes que la Unidad Máxima de Transmisión son fragmentados por el emisor y reemsablados por el receptor.

2.3.3.1 El Ping de la Muerte (The Ping of Death).- El Ping de la Muerte es un ataque que explota la vulnerabilidad de la fragmentación de un paquete ICMP echo largo. La figura muestra la estructura de un paquete ICMP echo (que se encapsula dentro de un paquete IP).



El paquete ICMP echo request consiste de 8 bytes de cabecera seguido del campo de data (opcional). Muchas implementaciones por defecto envían paquetes ICMP de solo 8 octetos pero permiten al usuario especificar un paquete más largo si se desea. El máximo tamaño de paquete permitido es:

(65535 – 20 – 8) = 65507 octetos

El problema es que es posible enviar un paquete ICMP echo ilegal con más de 65507 octetos de data debido a la forma en que la fragmentación es ejecutada. La fragmentación confia en el valor del offfset de cada fragmento para determinar donde

los fragmentos individuales irán cuando ocurra el reemsamblaje. Por consiguiente, en el último fragmento, será posible combinar un offset válido con un tamaño de fragmento adecuado de modo que lo siguiente sea cierto:

(offset + tamaño) > 65535

Debido a que típicamente las máquinas no procesan el paquete hasta que todos los paquetes hayan sido recibidos y hayan tratado de reemsamblarlos, existe la posibilidad de sobredimensionar las variables internas de 16 bits, lo que hace que las máquinas sucumban, se reinicien o cualquier comportamiento inesperado.

2.3.3.2 Ataque SMURF.- El ataque SMURF empieza con un atacante enviando un gran número de petición echo ICMP falseada hacia direcciones broadcast, esperando que estos paquetes sean magnificados y enviadas a las direcciones presa. Si el dispositivo de ruteo envía dicho tráfico a la direcciones broadcast, ejecuta la función de broadcast de capa 3 hacia broadcast de capa 2. La mayoría de la estaciones en tal red IP responderá con un echo reply ICMP a la petición original, amplificando el tráfico por el número de estaciones respondiendo.

2.3.4 El protocolo NNTP.- Toda el tráfico Usenet emplea NNTP, Network News Transfer Protocol, para enviar mensajes entre servidores de noticias y entres servidores y lectores. Debido a que el protocolo de control empleado por NNTP no provee ningún tipo de autentificación, puede ser fácil cancelar mensajes antes de ser remitidos, crear nuevos grupos de noticias no autorizados, o borrar los grupos existentes de servidores.

2.3.5 El protocolo SMTP.- Todo correo electrónico en el Internet está basado en Simple Mail Transfer Protocol. La mayoría de los programas email carecen de servicios de autentificación, integridad y confidencialidad a menos que se empleen

programas especiales como S/MIME o Pretty Good Privacy PGP. Si estos programas no son usados, los servicios de autentificación, integridad y confidencialidad pueden aún ser proveídos empleando IPSec en routers y firewalls y especificando que todo el tráfico de correo sea autentificado y encriptado.

2.3.5.1 Ataque Spam.- Un gran contingente de ataques sobre e-mail están basados en el bombardeo emailo o spamming. E-mail bombing está caracterizado por el envío abusivo repetitivo de un mensaje e-mail idéntido a una dirección en particular. E-mail spamming es una variante del bombing; se refiere a enviar un e-mail a centenas de miles de usuarios o listas. E-mail spamming se torna peor si los recipientes responden a dicho e-mail, causando que todas las direcciones originales reciban la respuesta.

Cuando grandes cantidades de correo son enviadas hacia un solo sitio, el sitio puede sufrir una denegación de servicio debido a pérdida de conectividad, corrupción del sistema, o falla de un servicio debido a: sobrecarga en la conexiones de red, uso de todos los recursos disponibles del sistema, llenado de un disco como resultado de múltiples destinos y las entradas syslog resultantes.

2.3.6 El protocolo FTP.- El File Transfer Protocol es un programa de aplicación basado en TCP empleado a menudo para almacenar y recuperar archivos de data extensos. El protocolo emplea dos tipos de conexiones:

- Una conexión para la conexión de control FTP inicial, el cual es iniciado por el c liente hacia el servidor.
- La otra conexión para conexión de data FTP, la cual es iniciada desde el servidor hacia el cliente.

La mayoría de las implementaciones FTP crea una nueva conexión de data FTP por cada transferencia de archivos y también requiere que un nuevo número de puerto sea usado por cada una de estas nuevas conexiones de data FTP. Estos requerimientos pueden causar problemas para ambientes restringidos que desean bloquear conexiones FTP iniciadas desde el exterior. Los filtros de paquetes bloquearán la conexión de data entrante desde el servidor dado que la transferencia de archivos no trabajará.

Para vencer este problema, se desarrolló FTP en modo pasivo. Con FTP pasivo, el cliente inicia tanto la conexión de control como la conexión de data de modo que un firewall con estructura de filtro de paquetes puede proveer cierta protección y no bloqueará las transferencias de archivos.

2.3.6 Los servicios NFS/NIS.- Los servicios NFS, Network File System, y NIS, Network Information System, son servicios comúnmente empleados en ambientes UNIX. NFS es usado para accesar sistemas de archivos remotos al permitir que los usuarios monten sistemas de archivos remotos de modo que ellos puedan accederlos localmente. NIS es usado para establecer servicios y base de datos centrales en relaciones cliente/servidor (típicamente, estos servicios incluyen passwords e información de contabilidad de usuarios).

Tanto NFS como NIS emplea UDP como su protocolo de transporte subyacente. En configuraciones típicas, existe autentificación limitado en cualquiera de los extremos de la conexión.

Estos servicios son extremadamente inseguros; esta clase de tráfico nunca deberá ser permitido a través de los puntos de ingreso y salida de la red corporativa.

En un firewall o router se deberá filtrar los puertos: TCP 111, UDP 111 (portmapper), TCP 2049, UDP 2049 (nfsd).

2.3.7 El sistema X Windows.- El sistema X Windows es uno de los más comúnmente empleados en sistemas de ventanas. El servidor X ofrece recursos como teclado, mouse y ventanas de la pantalla a clientes X. El servidor accepta peticiones del cliente para la entrada de teclado, salida de pantalla, o movimientos del ratón y retorna los resultados de dichas peticiones. El protocolo X11 ha sido adoptado por muchos de los vendedores de estaciones de trabajo para mostrar gráficas de red y es el elemento común sobre el que se basa cada interface de usuario gráfica del vendedor.

En una infraestructura de red, limitar el tráfico X11 sólo a estaciones internas en una manera de limitar este tipo de ataques.

2.4 Introducción: Tecnologías de seguridad actuales

Existe un amplio rango de tecnologías de seguridad que proveen soluciones para proteger los mecanismos de acceso de red y transporte de data dentro de la infraestructure de la red corporativa. Muchas de las tecnologías se sobreponen en resolver problemas que se relacionan con la protección de la identidad del usuario o dispositivo, la integridad y la confidencialidad de la data.

2.5 Tecnologías de Identidad

Las tecnologías de identidad buscan establecer la identidad de un host, un usuario final, o ambos. El nivel de identidad depende de la importancia del recurso y el costo del método.

Se puede clasificar holgadamente los métodos de autentificación como aquellos que proveen control local y los que proveen verificación de autentificación a través de una tercera parte confiable (trusted third party).

2.5.1 Protección de los passwords.- Aún cuando los passwords son a menudo empleados como prueba para la autentificación de usuarios o dispositivos, los passwords pueden verse fácilmente comprometidos si son fáciles de adivinar, si no son cambiados muy a menudo, y si son transmitidos en texto claro a través de la red. Como medio de autentificación de personal, estos passwords son categorizados como "algo que uno sabe". Esto es una ventaja pues no se requiere equipo especial, y también una desventaja porque lo que se sabe puede ser contado a otro, o adivinado o capturado. Con el fin de hacer los passwords más seguros, métodos más robustos son ofrecidos encriptando los passwords o modificando la encriptación de modo que los valores encriptados cambien cada vez. Este es el caso con la mayoría de esquemas de passwords de un solo uso (one-time passwords); siendo los más comunes el protocolo S/Key y la autentificación de passwords por token.

2.5.1.1 Autenficaciòn por Token.- El sistema de autentificaciòn por token generalmente requiere del uso de una tarjeta especial (llamada tarjeta inteligente, tarjeta token o tarjeta vale; smart card o token card), sin embargo algunas implementaciones emplean software para aliviar el problema de perder la tarjeta token. La mayoría de vendedores emplean DES con claves de 56 bits, haciendo casi imposible que los hackers rompan el código antes que haya cambiado. Estos tipos de mecanismos de autentificaciòn son basados en uno de dos esquemas alternativos: challenge response o time-synchronous authentication.

2.5.1.2 Protocolo de passwords S/Key.- Oficialmente conocido como S/Key One-Time Password System, este protocolo fue elaborado por Bellcore y definido en el RFC 1760. Se basa en la generación de passwords de un solo uso mediante MD4 y MD5. El protocolo S/Key es configurado para contrarrestar un ataque de repetición (replay attack) cuando un usuario intenta ingresar a un sistema.

Hay cuatro programas implicados en el sistema S/Key. El programa key acepta una cuenta de iteración, una semilla, un password secreto, y genera un password de un solo uso. El programa keyinit es empleado para inicializar S/Key, y para cambiar passwords, cuentas de iteración, o semillas. El programa keyinfo examina el archivo /etc/skeykeys e imprime la semilla y cuenta de iteración actuales del usuario que invoca la sesión. Finalmente, los programs login y su contienen la lógica necesaria para aceptar passwords de un solo uso S/Key para autentificación.

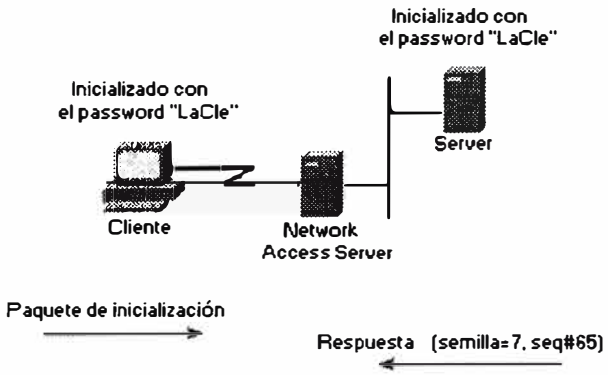


Figura 2.7: El Intercambio Inicial S/Key

El cliente luego computa el password de un solo uso, un proceso que implica tres pasos: un paso preparatorio, un paso de generación, y una función de salida.

- En el paso de inicialización, el cliente ingresa una frase de paso secreta. Esta frase de paso es concatenada con la semilla, el conjunto en texto claro, por ello

debe ser hecho desde la consola de una máquina segura o a través de una sesión telnet encriptada.

- El paso de generación aplica la función de seguridad hash múltiples veces, produciendo una salida final de 64 bits.
- La función de salida toma el password de un solo uso de 64 bits y lo muestra en forma legible.

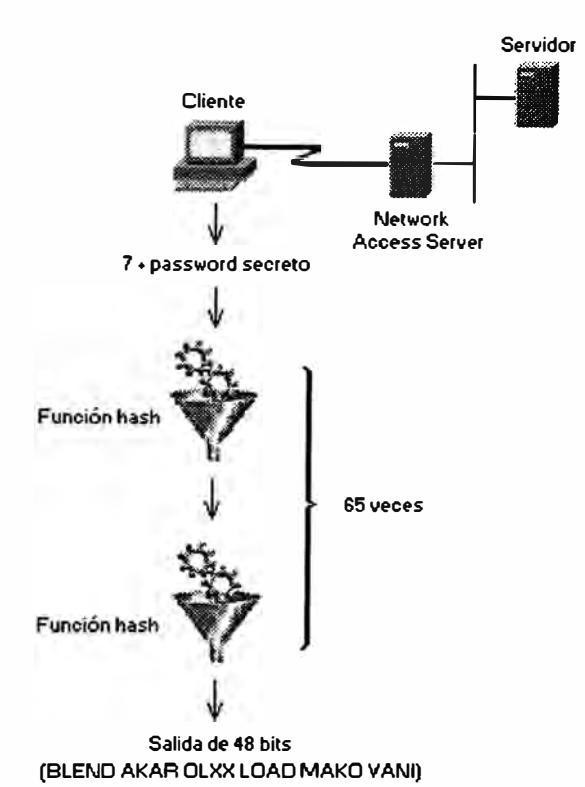


Figura 2.8: Calculando el password de un solo uso S/Key

La última fase consiste en que el cliente pasa el password de un solo uso al servidor donde es verificado.

Debido a que el número de aplicaciones de la función hash ejecutada por el cliente disminuye por uno cada vez, este asegura una única secuencia de passwords generada. Sin embargo, en cierto momento, el usuario debe reinicializar el sistema para evitar el ser incapaz de ingresar nuevamente. Este sistema es reinicializado

empleando el comando keyinit, el cual permite cambiar la frase de paso secreta, la cuenta de iteración y la semilla.

Los passwords son enviados en forma clara; sin embargo, luego que un password ha sido usado, ya no será útil para un intruso.

2.5.2 Protocolos que Emplean Mecanismos de Autentificación.- Muchos protocolos requieren verificación de autentificación antes de proveer autorización y derechos de acceso al usuario o dispositivo. RADIUS, TACACS+ y Kerberos son ejemplos de tales protocolos. TACACS+ y RADIUS son a menudo empleados en ambientes dial-in para proveer una base de datos de autentificación escalable y pueden incorporan una variedad de métodos de autentificación. Kerberos es un protocolo empleado para dos propósitos: autentificación y distribución de clave; esto es, provee a los hosts –o más precisamente, a varios servicios en hosts- credenciales infalsificables para identificar usuarios individuales.

2.5.2.1 El Protocolo TACACS+.- El protocolo TACACS+ es la última generación de TACACS. TACACS es un protocolo de control de acceso simple basado en UDP originalmente desarrollado por BBN para MILNET. Cisco ha mejorado (extendido) TACACS en varias oportunidades, y la implementación de cisco, basada en el TACACS original, es referida como XTACACS.

TACACS+ emplea TCP para su transporte. El demonio servidor usualmente escucha en el puerto 49, el puerto LOGIN asignado para el protocolo TACACS. Este puerto está reservado en el RFC de números asignados tanto para TCP como para UDP.

TACACS+ provee facilidades de autentificación, autorización y contabilidad modulares y separadas. TACACS+ permite un único servidor de control de acceso

(el demonio TACACS+) provea cada servicio independientemente. Cada servicio puede ser ligado a su propia base de datos para sacar provecho de los otros servicios disponibles en tal servidor o en la red, dependiendo de las capacidades del demonio.

TACACS+ permite intercambios de autentificación de contenido y longitud arbitraria, lo cual permite que cualquier mecanismo de autentificación sea empleado con clientes TACACS+ (incluyendo PAP, CHAP, EAP, tarjetas token y Kerberos). La autentificación no es obligatoria; es una opción dependiente del lugar.

La autentificación TACACS+ intercambia tres tipos de paquetes:

- START, enviado siempre por el cliente
- CONTINUE, enviado siempre por el cliente
- REPLY, enviado siempre por el servidor

La autentificación empieza con el cliente enviando un mensaje START al servidor. El mensaje START describe el tipo de autentificación a ser ejecutado (por ejemplo, password sencillo en texto claro, PAP o CHAP), y puede contener el nombre de usuario y alguna data de autentificación. El paquete START es enviado sólo como el primer mensaje en una sesión de autentificación TACACS+, o como el paquete inmediato a una reinicialización. (Una reinicialización puede ser requerida por el servidor en un paquete REPLY). Un paquete START siempre tiene un número de secuencia igual a 1.

En respuesta a un paquete START, el servidor envía un REPLY. El mensaje REPLY indica si la autentificación ha culminado, o si debería continuar. Si el REPLY indica que la autentificación debería continuar, el mensaje también indica que nueva información es solicitada. El cliente obtienee tal información y la retorna

en un mensaje CONTINUE. Este proceso se repite hasta que toda la información de autentificación es recogida, y el proceso de autentificación concluye.

La autorización es la acción de determinar lo que un usuario está permitido a hacer. Generalmente, el proceso de autentificación precede al de autorización, pero, éste no es requerido. Un petición de autorización puede indicar que el usuario no está autentificado. En este caso, depende del agente autorizador el determinar si a un usuario no autentificado se le está permitido ciertos servicios.

Cuando la autentificación está completa, el cliente puede iniciar el proceso de autorización, si ella es requerida. Una sesión de autorización está definida como un simple par de mensajes: un REQUEST seguido por un RESPONSE. El mensaje REQUEST de autorización contiene un juego fijo de campos que describe la autenticidad del usuario o proceso, y un juego variable de argumentos que describe los servicios y opciones para los cuales la autorización es solicitada.

La autorización TACACS+ no provee meramente respuesta de si o no, de hecho adapta el servicio al usuario particular. Por ejemplo, cuando un usuario inicia una sesión PPP y desea emplear IP con una dirección IP en particular, el demonio del servidor TACACS+ podría responder a estas peticiones permitiendo el enlace con ciertas restricciones en el shell, o colocando listas de acceso o una nueva ruta en la tabla del router.

Típicamente accounting es la tercera acción luego de la autentificación y la autorización. La contabilidad o accounting es la acción de registrar lo que un usuario está haciendo o ha hecho. El accounting en TACACS+ puede cumplir dos propósitos:

- Puede ser usado para registrar los servicios utilizados, beneficioso para efectos de facturación.
- Puede ser empleado como una herramienta de auditoría para servicios de seguridad.

Para este fin, TACACS+ soporta tres tipos de registros de contabilidad:

- Los registros de inicio indican que un servicio está a punto de comenzar.
- Los registros de término indican que un servicio ha terminado en el momento.
- Los registros de actualización son notificaciones intermedias que indica que un servicio está aún siendo ejecutado.

Los registros de contabilidad TACACS+ contienen toda la información empleada en los registros de autorización y también contienen información específica de contabilidad tal como tiempos de inicio y término e información de utilización de recursos.

2.5.2.2 El Protocolo RADIUS.- El protocolo RADIUS, Remote Address Dial-IN User Service, fue desarrollado por Livingston Enterprises Inc. como un protocolo de contabilidad y autentificación para servicios de acceso. En junio de 1996, la especificación del protocolo RADIUS fue sometida al IETF. La especificación RADIUS (RFC 2058) y el estándar de contabilidad RADIUS (RFC 2059) son protocolos estándares.

RADIUS emplea UDP como su transporte. Generalmente, el protocolo RADIUS es considerado un servicio no orientado a conexión. Asuntos relacionados a la disponibilidad del servidor, retransmisión, y timeouts son manejados por dispositivos con soporte RADIUS en vez de serlos por el protocolo de transmisión.

RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un NAS; el servidor RADIUS es usualmente un proceso demonio corriendo en una estación UNIX o NT. El cliente es responsable de pasar la informaciónd de usuario hacia servidores RADIUS designados y luego actuar sobre la respuesta retornada. Los servidores RADIUS son responsables de recibir peticiones de conexión de usuarios, autentificar usuarios, y luego regresar toda la información de configuración necesaria para que el cliente ofrezca el servicio al usuario. Un servidor RADIUS puede actuar como un cliente proxy hacia otros servidores RADIUS u otros tipos de servidores de autentificación.

El servidor RADIUS puede soportar una variedad de métodos para autentificar un usuario. Cuando el servidor es proveído del nombre de usuario y el password original dado por el usuario, el servidor puede soportar PAP o CHAP, login UNIX y otros mecanismos de autentificación. Lo que es soportado depende de lo que un vendedor ha implementado.

Típicamente, un ingreso de usuario consiste de una petición (Access-Request) del NAS hacia el servidor RADIUS y una correspondiente respuesta (Access-Accept o Access-Reject) desde el servidor. El paquete Access-Request contiene el nombre de usuario, password encriptado, dirección IP del NAS, y puerto. El formato de la petición también provee información respecto al tipo de sesión que el usuario desea iniciar.

Cuando el servidor RADIUS recibe el paquete Access-Request del NAS, indaga en una base de datos por el nombre de usuario listado. Si el nombre de usuario no existe en la base de datos, bien un perfil por defecto es cargado o bien el servidor RADIUS envía inmediatamente un mensaje Access-Reject. Este mensaje

Access-Reject puede ser acompañado por un mensaje de texto opcional, el cual puede indicar la razón del rechazo.

En RADIUS las funcionalidades de autentificación y autorización están acopladas. Si el nombre de usuario es encontrado y el password es correcto, el servidor RADIUS retorna una respuesta Access-Accept, incluyendo una lista de pares atributo-valor que describe los parámetros a ser usados para la sesión. Los parámetros típicos incluyen tipo de servicio (shell o en cuadros, frames), tipo de protocolo, dirección IP para asignar al usuario (estática o dinámica), lista de acceso a aplicar, o una ruta estática a instalar en la tabla de ruteo del NAS. La información de configuración en el servidor RADIUS define lo que será instalado en el NAS.

El diccionario de atributos contiene una lista de atributos de autentificación, autorización y contabilidad preconfigurados que pueden ser parte de la configuración de un cliente o usuario. Los atributos tienen un nombre asequible a los humanos y un equivalente enumerado en el rango 1 a 255.

Existen 63 atributos estándares, los cuales son definidos en los RFC 2138 y 2139. Existen también atributos específicos de vendedores adicionales que depende del NAS particular que se esté usando.

Algunos atributos incluídos son:

- User-Name.
- User-Password.
- NAS-IP-Address
- NAS-Port
- Framed Protocol, tal como SLIP o PPP

- Framed-IP-Address. La dirección IP del cliente empleada por el usuario para la sesión.
- Filter-ID. Específico del vendedor; identifica un juego de filtros configurados en el NAS.
- Callback-Number.

Las características de contabilidad del protocolo RADIUS pueden ser utilizadas independientemente de la autentificación y autorización RADIUS. Las funciones de contabilidad RADIUS permiten que la data sea enviada al inicio y al final de las sesiones, indicando la cantidad de recursos (tiempo, paquetes, bytes, etc) empleados durante la sesión. Un ISP podría emplear el software de contabilidad y control de acceso RADIUS para abordar necesidades en la facturación y seguridad.

2.6 Seguridad en Capas TCP/IP

El modelo estructural del protocolo TCP/IP se compone de cuatro capas: Aplicación, Transporte, Red, Enlace.

Aplicación	Telnet, FTP, e-mail
Transporte	TCP, UDP
Red	IP, ICMP
Enlace	Driver o tarjeta de red

La capa de Aplicación pertenece a los detalles de una aplicación particular tal como Telnet, FTP o HTTP y no concierne específicamente ella misma a los detalles del movimiento de la data a través de una red. La capa de Transporte provee los detalles del movimiento de la data entre dos estaciones o puntos finales. Tanto la capa de Aplicación como la de Transporte emplean protocolos punto-a-punto (end-to-end), en el cual los sistemas extremos o finales son responsables de proveer

seguridad para el protocolo de aplicación o transporte. La capa de red provee el manejo de paquetes de data entre sistemas intermedios de la red, por ejemplo routers.

2.6.1 Protocolos de Seguridad de la Capa de Aplicación.- No existen muchos protocolos de seguridad específicamente diseñados para aplicaciones individuales. Existen muchas aplicaciones que hacen de tal enfoque escalable. Sin embargo, debido a que la World Wide Web se ha convertido en una de las aplicaciones de mayor rapidez en el Internet, un protocolo de seguridad específico fue diseñado para ser usado en transacciones Web seguras, el SHTTP o Secure HyperText Transport Protocol.

2.6.2 Protocolos de Seguridad de la Capa de Transporte

2.6.2.1 Secure Shell Protocol.- El Secure Shell (SSH) es un protocolo para ingreso remoto seguro y otros servicios de red seguros sobre una red insegura. Provee acceso remoto seguro, transferencia de archivos segura, y servicio de transporte seguro del tráfico TCP/IP y sistemas X Window. Puede automáticamente encriptar, autentificar, y comprimir la data transmitida. El trabajo en progreso que define el protocolo SSH asegura que el protocolo SSH puede proveer seguridad sólida frente a ataques de protocolo y criptoanálisis, puede trabajar razonablemente bien sin infraestructura de manejo de clave global o certificados, y puede usar infraestruturas de certificado existentes (como DNSSEC y X.509) si se hallan disponibles.

Tatu Ylonen de SSH Communications Security escribió este shell cuando era investigador en la Universidad de Tecnología de Helsinki en Julio de 1995. Tatu creó una aplicación de seguridad que reemplaza muchas de las aplicaciones de networking de UNIX inseguras.

El protocolo SSH consiste de tres componentes principales:

- El protocolo de capa de transporte, el cual provee autentificación de servidor, confidencialidad e integridad con PDF (perfect forwar secrecy). Opcionalmente, también provee compresión.
- El protocolo de autentificación de usuario, el cual autentifica el cliente sobre el servidor.
- El protocolo de conexión, el cual multiplexa el tunel encriptado en varios canales lógicos.

El protocolo de transporte SSH es un protocolo de transporte de bajo nivel seguro. Provee encriptación potente, autentificación de host criptográfica, y protección de integridad. La autentificación en SSH es basada en el host; este protocolo no desarrolla ninguna autentificación de usuario. Un protocolo de mayor nivel para autentificación de usuario puede ser designado a la cabeza de SSH.

El protocolo ha sido diseñado para ser lo suficientemente simple y flexible para permitir negociación de parámetros y minimizar el número de idas y vueltas. El método de intercambio de clave, el algoritmo de clave pública, el algoritmo de encriptación simétrico, el algoritmo de autentificación de mensaje, y el algoritmo hash, todos son negociados.

La integridad de la data es asegurada incluyendo en cada paquete un código de autentificación de mensaje MAC calculado a partir de una clave compartida, un número de secuencia de paquete, y el contenido del paquete.

SSH protege contra spoofing de paquetes, spoofing de hosts/IP, sniffing de passwords e intromisión (eavesdropping). SSH no ofrece protección contra montaje NFS, ataques locales, ataques Internet y denegación de servicio.

Los comandos "s" de SSH fueron diseñados para ser reemplazos de los comandos "r". Los escritores de SSH hiciero los comandos idénticos en uso y nomenclatura a los comandos "r" de Berkeley. La mayoría de las características de seguridad proveídas por los comandos "s" son transparentes para el usuario cuando SSH se instala y configura apropiadamente.

A diferencia de los servicios Berkeley, los comandos SSH emplean solamente un demonio, *sshd*, y un puerto TCP único, 22. Con sólo un demonio manejando los servicios, SSH se torna fácil de monitorear y configurar. La tabla siguiente lista los comandos de cliente disponibles con SSH.

Comando	*Función*
Ssh	Shell remoto seguro
Scp	Copia remota segura
Slogin	Login remoto seguro
Sftp	Transferencia de archivos segura

SSH tiene dos partes – un cliente y un servidor. El servidor es un *demonio*, lo cual significa que corre como proceso de fonfo sin ningú tipo de administración constante, y acepta conexiones sobre el sistema desde le cliente. El cliente es la interface del usuario

- El Servidor. El servidor consiste de un archivo, el programa *sshd*. Este es usualmente ubicado en el directorio */usr/local/sbin*. El servidor provee el procesamiento para conexiones remotas, incluyendo autentificación de clave pública e intercambio de clave, encriptación de clave simétrica, y la conexión insegura misma. Para SSH2, el demonio *sftp-server* maneja la conexión de transferencia de archivos segura.

- El Cliente. El cliente consiste de diferentes archivos. Estos archivos incluyen ssh, el cual permite a uno correr programas en una máquina remota sin tener que autentificarse (logging), copia remota (*scp*), y accesos (logon) remotos (*slogin*).

SSH2 posee ahora un cliente de transferencia de archivos seguro (sftp) el cual es usado como reemplado de FTP.

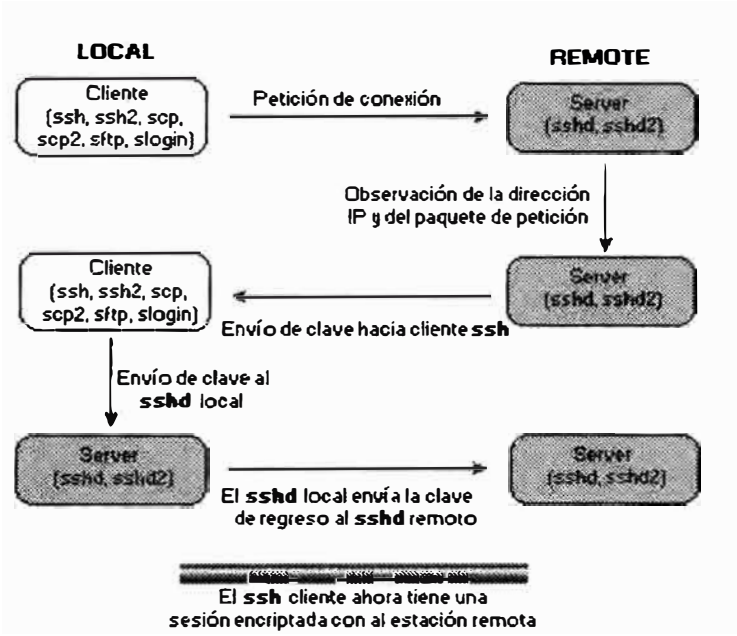


Figura 2.9: Operación de SSH

2.6.2.2 SOCKS Protocol.- Socket Security Protocol es un protocolo proxy para seguridad de networking basado en la capa de Transporte. Está diseñado para proveer un marco para aplicaciones cliente/servidor en dominios TCP y UDP para convenientemente y de manera segura emplear los servicios de un firewall de red.

Un servidor proxy realiza una conexión sobre el servidor de aplicación por el cliente. El servidor proxy reenvía la data entre el cliente y el servidor de aplicaciones. Desde la perspectiva del servidor de aplicación, el servidor proxy es el cliente.

SOCKS fue originalmente desarrollado por David y Michelle Koblas; el código fue entregado libremente al Internet. SOCKS Version 4 previene transacciones por firewall inseguras para aplicaciones TCP cliente/servidor (Telnet, FTP, HTTP, WAIS, Gopher). SOCKS Version 5, desarrollado por NEC y definido en el RFC 1928, extiende el modelo de la versión 4 para incluir UDP, extiende el marco para incluir provisiones para potentes esquemas de autentificación generalizados, y extiende el esquema de direccionamiento para abarcar direcciones Ipv6 y domain-name.

SOCKS trabaja reemplazando las llamadas del sistema de red estándar en una aplicación con versiones especiales. Por esta razón es que SOCKS es a veces referenciado como un proxy de capa de Aplicación. Estas nuevas llamadas de sistema abren conexiones a un servidor proxy SOCKS (configurado en la aplicación por el usuario, o por un archivo de configuración del sistema) on un puerto conocido (well-known port), usualmente el puerto TCP 1080. Si la petición de conexión se logra, el cliente ingresa a una negociación para que el método de autentificación sea empleado, se autentifica con el método escogido, y envía una petición retransmisora. El servidor SOCKS evalúa la petición y bien establece la conexión apropiada o bien la deniega. Luego que la conexión ha sido establecida con el servidor SOCKS, la aplicación del cliente envía al servidor el nombre de la máquina y el número de puerto a la cual el usuario desea conectarse. El servidor SOCKS realmente realiza la conexión con el host remoto y luego transparentemente transporta la data ida y vuelta entre la aplicación y la estación remota. El usuario no tiene conciencia de que el servidor SOCKs está en un ciclo de lazo.

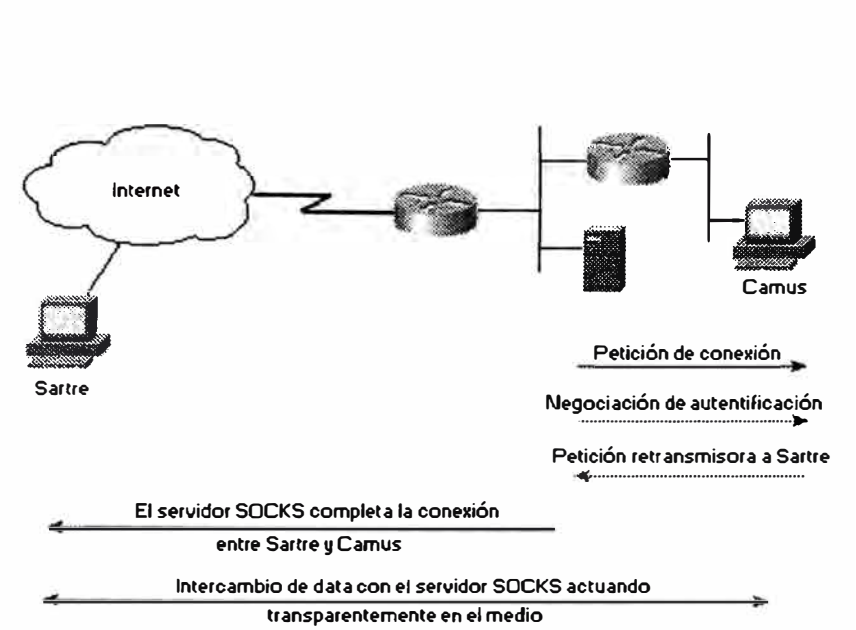


Figura 2.10: Modelo de Seguridad SOCKS

La dificultad al emplear SOCKS es que alguien tiene que reemplazar las llamadas del sistema de red con las versiones SOCKS (este proceso es generamente reconocido como SOCKSificación o SOCKSificando una aplicación). Afortunadamente, la mayoría de aplicaciones de red (tales como Telnet, FTP) ya han sido SOCKSificadas y muchos vendedores lo están incluyendo en aplicaciones comerciales.

2.6.3 Protocolos de Seguridad de la Capa IP

2.6.3.1 IPSec.- Internet Protocol Security (IPSec) es un conjunto de estándares abiertos para garantizar la seguridad de las comunicaciones privadas sobre redes IP. Basado en estándares desarrollados por el IETF (Internet Engineering Task Force), IPSec garantiza la confidencialidad, la integridad y la autenticidad de las comunicaciones de datos sobre una red IP pública.

Una Asociación de Seguridad es una política negociada o manera acordada de manejar la data que será intercambiada entre dos dispositivos pares.

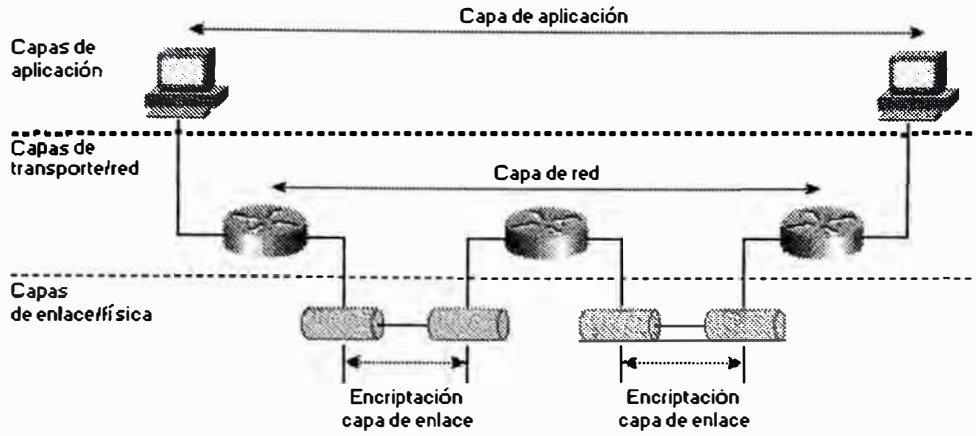


Figura 2.11: Implementaciones de la encriptación

2.6.3.1.1 Tecnologías empleadas por IPSec.- IPSec combina diferentes tecnologías de seguridad que proveen confidencialidad, integridad y autenticidad. He aquí algunas:

- La clave de intercambio Diffie-Hellman para derivar lo referente a claves entre pares en una red pública.
- Criptografia de clave pública para firmar los intercambios Diffie-Hellman y garantizar la identidad de las dos partes y evitar ataques "man-in-the-middle".
- Algoritmos de encriptación, tal como DES, para encriptar la data.
- Algoritmos "keyed hash", tal como HMAC, combinado con algoritmos hash tradicionales tales como MD5 o SHA para proveer la autentificación del paquete.
- Certificados digitales firmados por una autoridad certificada para actuar como tarjetas digitales ID.

2.6.3.1.2 Detalles de IPSec.- Dentro del ambiente TCP/IP, los protocolos IPSec ofrecen servicios de seguridad en la capa IP. Estos servicios de seguridad incluyen control de acceso, integridad no orientada a conexión, autentificación del origen de la

data, protección contra repetición, confidencialidad (cifrado), y confidencialidad limitada en el flujo de tráfico.

Estos servicios de seguridad son proveidos por los protocolos Cabecera de Autentificación (AH, Authentication Header) y Encapsulating Security Payload (ESP). Cada protocolo ofrece ciertos servicios y pueden ser empleados separadamente o en conjunto, sin embargo no es necesariamente usual emplear ambos protocolos juntos.

2.6.3.1.3 Authentification Header AH.- El modo AH provee autentificación para lo más que se pueda de la cabecera IP, así como de todos los protocolos de capa superior de un datagrama IP. Sin embargo, algunos de los campos de cabecera IP pueden cambiar en tránsito y el valor de estos campos, cuando el paquete llega al receptor, puede no ser predecible por el emisor. Los valores de tales campos no pueden ser protegidos por AH.

2.6.3.1.4 Encapsulating Security Payload.- ESP desarrolla encriptación en la capa IP. Soporta una varieda de algoritmos de encriptación simétricos. El algoritmo de encriptación por defecto del IPSec es el DES de 56 bits (Data Encryption Standard) en el modo de encadenamiento de bloque cifrado (DES-CBC, Cipher Block Chaining). Este cifrador debe ser implementado para garantizar interoperabilidad entre productos IPSec.

El estándar actual de IPSec especifica HMAC (un esquema de firma simétrico) con SHA1 (Security Hash Algorithm) y MD5 (Message Digest 5) como implementaciones mandatorias.

2.6.3.1.5 Los modos de AH y ESP.- Existen dos modos de operación que IPSec provee: el modo de transporte y el modo de tunel. El formato cd las cabeceras

AH y ESP, y los valores contenidos en ellos, variarán según el modo en que ellos son aplicados.

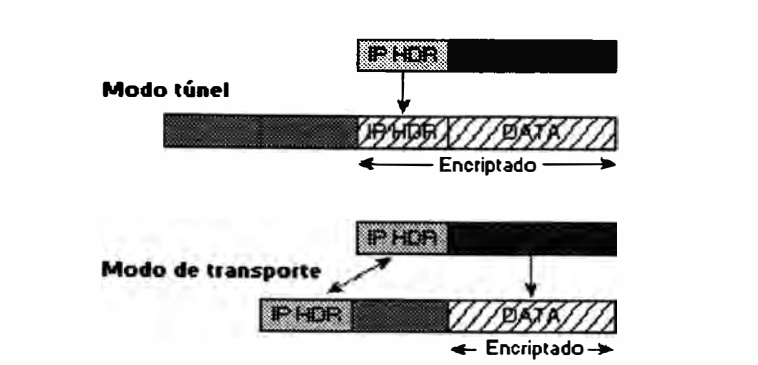


Figura 2.12: Modos IPSec: Túnel y Transporte

2.6.3.1.5.1 Modo de transporte.- El modo de transporte es empleado cuando ambos pares de la comunicación son estaciones (hosts).

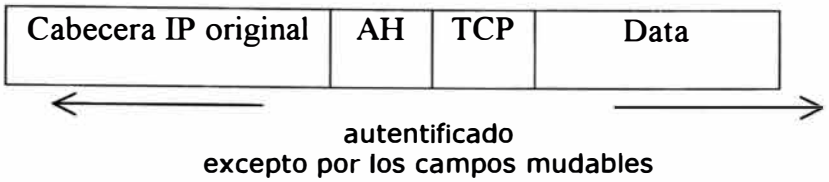
En el modo de transporte, sólo la carga de data IP es encriptada, y las cabeceras IP originales son dejadas intactas (desprotegidas). Este modo tiene la ventaja de añadir sólo unos cuantos bytes a la cabecera de cada paquete. También permite que los dispositivos en la red pública vean la fuente y el destino finales del paquete.

La figura muestra el paquete IP original.

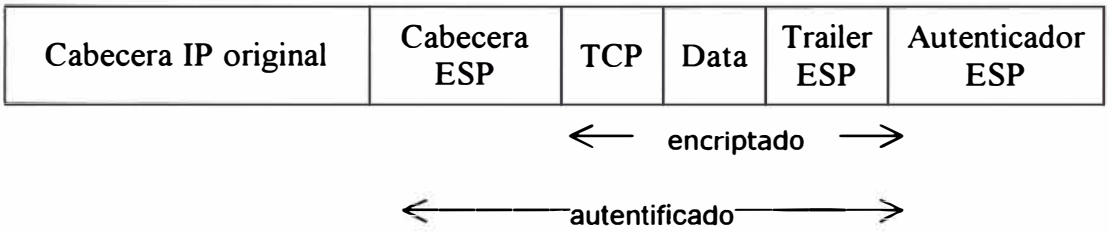
Cabecera IP original	TCP	Data

Los servicios de AH proveen protección a la cabecera IP externa junto con la carga de data útil. Protege todos los campos en la cabecera que no varían en el transporte. La cabecera sigue luego de la cabecera IP y antes de la cabecera ESP, si se emplea, y otros protocolos de capas superiores.

La figura muestra el paquete IP luego de sufrir autentificación AH en el modo de transporte.

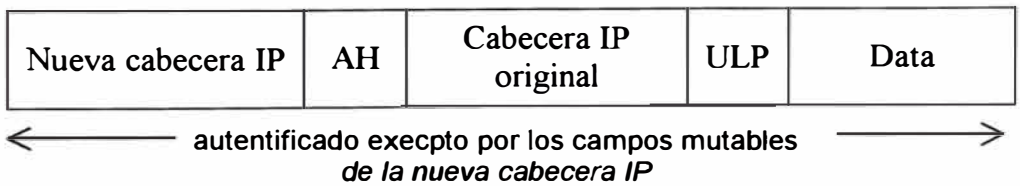


En el modo de transporte, la carga útil IP es encriptada y las cabeceras originales son dejadas intactas. La cabecera ESP es insertada luego de la cabecera IP y antes de la cabecera de los protocolos superiores. Los protocolos superiores son encriptados y autentificados junto con la cabecera ESP.

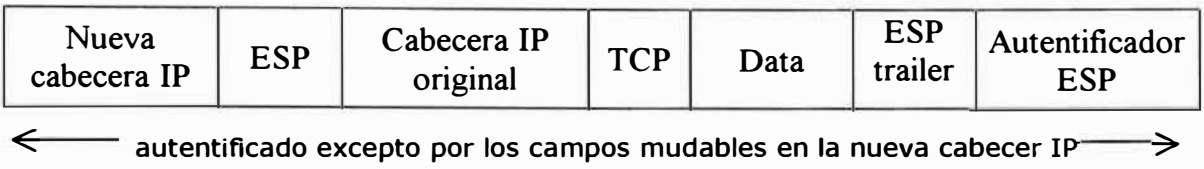


2.6.3.1.5.2 Modo tunel.- En el modo de tunel el paquete original IP es encriptado, y se convierte en la carga de data de un nuevo paquete IP. Esto es, el router ejecuta la encriptación en representación de los hosts. El router del origen encripta los paquetes y los envía a través del tunel IPSec. El router de destino desencripta el datagrama IP original y lo envía al sistema de destino. La mayor ventaja del modo tunel es que los sistemas finales no necesitan ser modificados para gozar de los beneficios de la seguridad IPSec.

Toda la cabecera IP original es autentificada y la nueva cabecera IP es protegido de la misma manera que la cabecera IP en el modo de transporte.



Cuando ESP es usado y la confidencialidad es seleccionada en modo tunel, la cabecera IP original está bien protegida por el datagrama IP original entero es encriptado.



Si se desea mantener la confidencialidad de la data, se debe emplear ESP. ESP encriptará los protocolos de capas superiores en el modo de transporte y el datagrama IP original entero en el modo tunel de modo que en ambos casos no sean entendible en la tránsito. ESP también puede proveer autentificación para los paquetes. Sin embargo, cuando se emplea ESP en el modo de transporte, la cabecera IP original externa no está protegida; en modo tunel, la nueva cabecera IP no se protege.

La siguiente tabla resume los algoritmos requeridos en una implementación IPSec.

Servicio	AH	ESP
Autentificación e integridad	HMAC-MD5 (128-bit hash) HMAC-SHA (160-bit hash) Ambos calculados sobre la carga útil y campos no mutables de la cabecera IP	HMAC-MD5 HMAC-SHA Ambos calculados sobre la carga útil del datagrama IP encriptado y cabecera ESP.
Encriptación y privacidad		56-bit DES-CBC 3 DES con 3 claves únicas

2.6.3.1.6 Asociaciones de Seguridad.- El establecimiento de SAs facilita una conversación entre dos entes basada en IPSec. Cada dispositivo debe acordar respecto a las políticas o reglas de su conversación, negociando estas políticas con su potencial vecino.

IKE provee negociación, autentificación de par, gestión de clave, e intercambio de clave. IKE negocia un contrato entre dos puntos finales IPSec. La SA es usada para seguir el rastro de todos los detalles de esta negociación para una simple sesión IPSec. De hecho, una de las principales funciones de IKE es establecer y mantener las Asociaciones de Seguridad. Los detalles rastreados incluyen:

- El modo del algoritmo de autentificación usadon en AH, y las claves del mismo.
- El modo del algoritmo de encriptación usado en ESP, y las claves del mismo.
- El algoritmo de autentificación, modo usado en ESP, y las claves.
- El tiempo de vida de la Asociación de Seguridad y de las claves correspondientes.
- La dirección destino de la Asociación de Seguridad.
- Las identidades en cuyos nombres esta Asociación de Seguridad es establecida.

Una asociación de seguridad es unidireccional, lo que significa que por cada para de sistemas de comunicación existe al menos dos conecciones de seguridad.

La asociación de seguridad es identificada unívocamente por un único número escogido al azar llamado índice de parámetro de seguridad (SPI, Security Parameter Index), un identificador de protocolo de seguridad (AH o ESP) y la dirección IP del destino.

En resumen, la asociación de seguridad es simplemente una declaración de la política de seguridad negociada entre dos dispositivos dentro de un ambiente IKE/IPSec.

2.6.3.1.7 Gestión de clave

2.6.3.1.7.1 Internet Key Exchange.- IKE es el facilitador y gestor de las conversaciones basadas en IPSec. IKE está basado en ISAKMP/Oakley, Internet Security Association Key Management Protocol/Oakley; es un derivativo de este adecuado para IPSec.

IKE provee tres modos para el intercambio de información de claves y establecimiento de las IKE SAs. Los primeros dos modos son intercambios de fase 1, los cuales son usados para establecer el canal seguro inicial. El otro modo es el intercambio de fase 2, el cual negocia las Asociaciones de Seguridad IPSec. Los dos modos en fase 1 son el modo principal y el modo agresivo (main and agressive modes), y el modo de fase 2 es llamada modo rápido (quick mode). La idea básica es erigir una Asociación de Seguridad IKE para provee el tubo protegido para subsecuentes intercambios IKE protegidos entre pares IKE, y luego emplea el modo rápido de la fase 2 con la IKE SA para negociar las Asociaciones de Seguridad IPSec. IPSec emplea solamente la IPSec SA para proteger el tráfico.

El modo principal tiene tres intercambios de dos vías entre el iniciador y el receptor. En el primer intercambio, los algoritmos y hashes se acuerdon. El segundo intercambio emplea Diffie-Hellman para acordar un secreto compartido y pasarse números claves (nonces, números aleatorios enviados a la otra parte, firmados y retornados para probar su identidad – son firmados sólo si se emplea números claves aleatorios o firmas digitales).

En el modo agresivo, menos intercambios son realizados y con menor número de paquetes. En el primer intercambio, casi todo es logrado introducir – la SA propuesta (algoritmo, hashes, y modo), valor público Diffie-Hellman, un número clave (nonce) que la otra parte firma, un paquete ID, el cual puede ser usado para verificar la identidad via una tercera parte. El receptor envía de retorno todo lo necesario para completar el intercambio. Lo restante es dejado al iniciador para confirmar el intercambio.

Antes que IKE proceda, es un requerimiento que las partes potenciales acuerden una manera de autentificarse entrambos. Este método de autentificación es negociado durante la fase 1 de IKE en el intercambio del modo principal.

2.6.3.1.7.2 Autentificación IKE (Internet Key Management Protocol).- El IETF escogió el IKE (Internet Key Exchange) como el método estándar para configurar las asociaciones de seguridad de IPSec.

IKE crea un tunel seguro y autentificado entre dos entidades y luego negocia la asociación de seguridad para IPSec. Este proceso requiere que las dos entidades se autentifiquen ellas mismas y entrambas y establezcan claves compartidas. El protocolo IKE es muy flexible y soporta múltiples métodos de autentificación como parte del intercambio de fase 1. Los mecanismos siguientes son implementados:

- Claves pre-compartidas. La misma clave es preinstalada en cada host. Los pares IKE se autentifican uno al otro al computar y enviar un fragmento cifrado que incluye la clave pre-compartida. Como con las claves manuales, cada par comparte una clave secreta, la cual ha sido intercambiada fuera de banda (out-of-band) y configurada dentro del router.

- Criptografía de clave pública. Cada parte genera un número pseudo-aleatorio y la encripta en la llave pública de la otra parte. La habilidad para que cada parte compute el fragmento cifrado conteniendo el número inventado por el par, desencriptado con la llave privada local así como otra información disponible pública y privadamente, autentifica las partes una a la otra.
- Firma digital. Cada dispositivo firma digitalmente un juego de data y lo envía a la otra parte. Este método es similar al anterior, excepto que provee no-repudiación (no-rechazo).

2.6.3.1.7.3 Empleo de IKE con IPSec.- Estos dos pasos, autentificación e intercambio de clave, crean la IKE SA, un tunel seguro entre dos dispositivos. Un lado del tunel ofrece una serie de algoritmos, y el otro lado debe luego aceptar uno de los ofrecidos o rechazar la conexión entera. Cuando los dos lados han acordado sobre el algoritmo a emplear, deben derivan el material de claves a usar para IPSec con AH, ESP, o ambos juntos. IPSec emplea un clave compartida diferente a la de IKE. La clave IPSec compartida debe ser derivada empleando nuevamente el protocolo Diffie-Hellman para asegurar el perfecto secreto futuro, o refrescando el secreto compartido derivado del intercambio Diffie-Hellman original que generó la asociación IKE SA mutándolo con números pseudo-aleatorios.

2.7 Tecnologías de Seguridad Virtuales Privadas Dial-Up

VPDN o Virtual Private Dial-Up Network permite a empresas grandes extender sus redes privadas a través de líneas dial-up. En vez de incurrir en grandes costos para asegurar la protección marcando sobre un campus desde cualquier lugar del mundo o aminorando la seguridad marcando localmente y empleando el Internet como transporte para alcanzar el campus de la empresa principal, nuevas tecnologías

permiten a sitios y usuarios remotos conectar de manera segura la infraestructura de la empresa empleando el acceso local dial-up sobre el Internet.

Existen tres protocolos similares que cumplen este objetivo:

- El protocolo Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

2.7.1 El Protocolo Layer 2 Forwarding.- El protocolo Layer 2 Forwarding (L2F) fue creado por Cisco Systems. Permite tunelling en la capa de enlace – esto es, frames HDLC (High-Level Data Link Control), async HDLC, o Serial Line Internet Protocol (SLIP) – de protocolos de capa superior.

2.7.2 Layer 2 Tunneling Protocol.- Debido a que tanto L2F como PPTP proveen funcionalidad similar, Cisco y Microsoft, junto con otros vendedores, han colaborado en un único estándar: un protocolo dentro del IETF llamado Layer 2 Tunneling Protocol (L2TP). Como sigue, este protocolo será explicado en más detalle pues finalmente lo emplearemos en el diseño de red. Este protocolo enfoca los siguientes requirimientos del usuario final:

- Transparencia del sistema final. Ni el sistema final remoto ni los hosts del home site debería requerir algún software especial para usar este servicio de una manera segura:
- La autentificación es proveída por PPP dial-up CHAP, PAP, EAP, o a través de otros diálogos. Esto incluye soluciones TACACS+ y RADIUS y también soporta tarjetas inteligentes y passwords de un solo uso. La autentificación debe ser manejable por el usuario independientemente del ISP.

- El direccionamiento debería ser tan manejable como soluciones dial-up dedicadas. La dirección deberá ser asignada por el home site y no por el ISP.
- La autorización debería ser manejada por el home site como lo sería en una solución dial-up directa.
- El registro o accounting debería ser ejecutado tanto por el ISP (para propósitos de facturación) y por el usuario (para propósitos de auditoría).

De manera similar que PPTP, L2TP define dos entidades:

- L2TP Access Concentrator (LAC). Este dispositivo está conectado a la estructura de red switchada (PSTN o ISDN) o co-situadas con un sistema final PPP capaz de entender L2TP. El LAC solamente tiene que implementar el medio sobre el cual L2TP va a operar para pasar tráfico a uno o más LNS. El LAC puede tunelizar cualquier protocolo llevando dentro de PPP. El LAC es el iniciador de llamadas entrantes y el receptor de llamadas salientes.
- L2TP Network Server (LNS). Este servidor opera sobre cualquier plataforma capaz de terminación PPP. El LNS maneja el lado servidor del protocolo L2TP. Debido a que L2TP confia solamente en el medio sobre el cual los túneles L2TP llegan, el LNS puede tener solamente una única interface LAN o WAN aún siendo capaz de terminar llamadas entrantes sobre cualquier rango de interfaces PPP de LAC (ASYNC, ISDN síncrono, V.120). El LNS es el iniciador de llamadas salientes y el receptor de llamadas entrantes.

Hay dos componentes paralelos de L2TP operando sobre un tunel dado: mensajes de control entre cada par LAC-LNS y paquetes de data entre el mismo par LAC-LNS. Estos últimos son empleados para transportar paquetes PPP encapsulados en L2TP para sesiones de usuario entre el par.

Antes que la tunelización PPP pueda ocurrir entre un LAC y un LNS, mensajes de control deben ser intercambiados entre ellos. Los mensajes de control son intercambiados sobre el mismo tunel que será empleado para despachar data una vez que la información de gestión y control de llamada L2TP ha sido pasada. Los mensajes de control son responsables por el establecimiento, gestión y liberación de sesiones llevadas a través del tunel, así como del status del tunel mismo.

Un mecanismo de aviso de status operativo (keep-alive) es empleado por la capa superior L2TP para diferenciar cortes de túneles por tiempos extendidos de inactividad de data y control sobre un tunel.

Luego que un tunel ha sido establecido y los mensajes de control han completado la configuración del tunel, el tunel puede ser empleado para llevar paquetes PPP de sesión de usuario para sesiones implicando un par LNS-LAC dado. El campo Call ID en la cabecera L2TP indica la sesión a la cual un paquete PPP particular pertenece. De esta manera, los paquetes PPP son multiplexados y demultiplexados sobre un único tunel entre un para LNS-LAC dado. El valor del campo Call ID es establecido durante el intercambio de mensajes de control de configuración de llamada.

La figura 2.13 muestra un escenario ejemplo L2TP de un arreglo Internet genérico con acceso PSTN (PPP asíncrono empleando modems) y acceso ISDN (acceso PPP síncrono). Los usuarios remotos accesan la red LAN como si hubiesen marcando el ingreso a un LNS, sin embargo su conexión fisica dial-up es a través del NAS ISP (actuando como LAC).

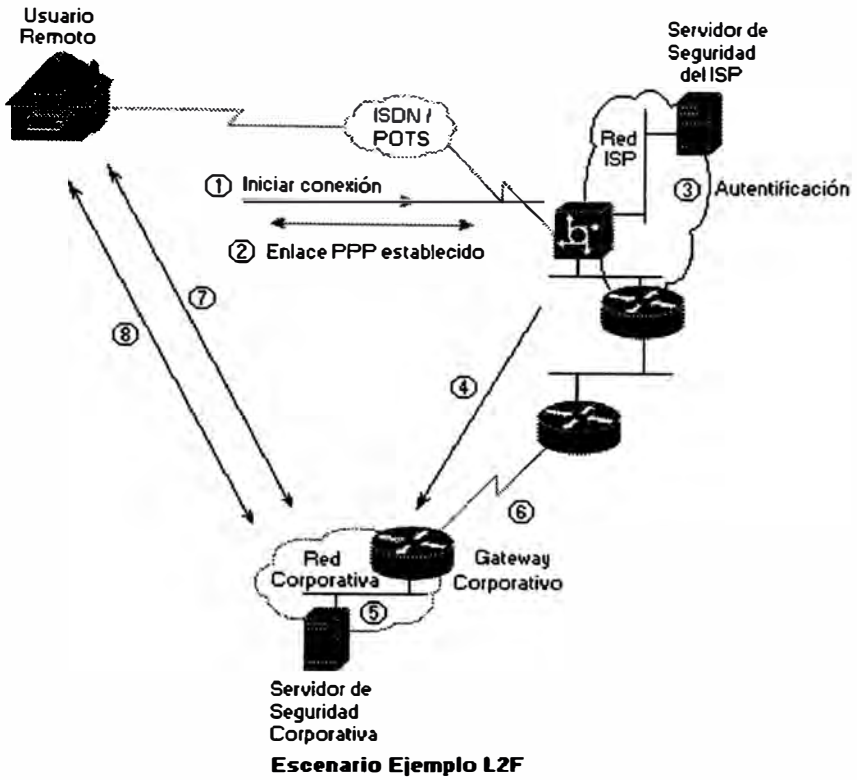


Figura 2.13: Escenario Ejemplo L2TP

2.7.3 Ventajas de las Tecnologías VPDN

Características	*Beneficios*
Soporte multiprotocolo	El ISP puede proveer servicios multiprotocolos sobre un backbone IP, fortaleciendo facilidades, técnicas de gestión, personal y capacitación aplicada de la infraestructura actual.
Autentificación de usuario ejecutada en la corporación del usuario remoto	No se requiere que el ISP mantenga una base de datos de autentificación por usuario. El ISP no tiene que responder a cambios organizacionales de la localidad corporativa. Las corporaciones no necesariamente se confían de los mecanismos de autentificación del ISP.
Autorización de usuario ejecutada en la corporación del usuario remoto	No se requiere que el ISP mantenga listas de acceso por usuario. Simplifica la gestión del firewall. Las corporaciones pueden imponer sus propias políticas de seguridad.

Soporte simultáneo para acceso local	El NAS puede ser usado por el ISP tanto para acceso al Internet estándar como para el servicio dial-up virtual, reduciendo requerimientos de costos, equipo e infraestructura.
Asignación de direcciones ejecutada por la corporación del usuario remoto empleando túneles end-to-end	No se requiere que el ISP mantenga el espacio de direcciones de la corporación dentro de la red ISP. Esto minimiza la tabla de enrutamiento llevada por el ISP, mejora la escalabilidad, y soporta el uso corporativo de direcciones no registradas a través del Internet y redes públicas.
No dependencia del medio	El ISP puede implementar cualquier medio (Frame Relay, ATM, PPP, X.25) en el backbone para soportar el servicio dial-up virtual.
Túnel dinámico	Los túneles son iniciados y la gestión separada basados en la gestión L2TP. Esta configuración provee una solución escalable debido a que los túneles son iniciados sólo cuando el tráfico de usuario está activo. Minimiza los recursos del NAS requeridos para mantener los túneles.
Múltiples sesiones de usuarios remotos son multiplexadas sobre un único túnel L2TP	Representa una solución escalable puesto que minimiza el número de túneles requeridos para ser abiertos en un instante dado. Infraestructuras de backbone basadas en PVCs, como Frame Relay, necesitan solamente un sólo PVC entre el NAS y el gateway corporativo para manejar las múltiples sesiones de usuarios remotos.
La seguridad del túnel mantiene claves aleatorias y números de secuencia	El establecimiento del túnel implica un proceso de autentificación NAS (ISP) – gateway corporativo, para protección contra ataques. Adicionalmente, L2TP previene el spoofing empleando números de secuencia.
No dependencia de protocolos de enrutamiento	No se requiere que ni el ISP ni el cliente corporativo manejen el dominio de enrutamiento de otros para proveer acceso y servicios, dándo la posibilidad a ambos de

	emplear los protocolos de enrutamiento cualesquiera que más les convenga.

CAPITULO III
PROYECTO DE DISEÑO DEL SISTEMA DE SEGURIDAD DEL CAMPUS DE LA RED CORPORATIVA

El presente capítulo explica las consideraciones de diseño de seguridad de red imprescindibles para el campus de una corporación. Cumple con los elementos de una arquitectura de seguridad: confidencialidad, integridad de la data, disponibilidad, consistencia, control y auditoría.

3.1 Seguridad del NOC

Como se mencionó en el primer capítulo, el NOC es el sistema nervioso de la red. El NOC se compone de estaciones y servidores de gestión. La presente sección se orienta, sobretodo, a la seguridad de estaciones UNIX (equipos de gestión de red por antonomasia).

La primera parte de esta sección, "Seguridad de las estaciones de gestión", describe brevemente los peligros a enfrentar (pues ya se describieron con detalle en el capítulo anterior) y cómo guardar la data sana y salva. Se explica en gran detalle cómo operan los mecanismos de seguridad de UNIX , cómo configurarlos y administrarlos para su máxima protección (contra amenazas internas y externas, intencionadas o casuales).

La segunda parte de esta sección, "Firewall del NOC", describe la estrategia de diseño, basada en la experiencia en detectar y defender contrar atacantes.

3.1.1 Seguridad de las estaciones del NOC

3.1.1.2 Usuarios y passwords.- Una política de elección de passwords adecuados es la primera línea de defensa contra abusos del sistema. La fuente de intentos de ingresos no autorizados al sistema es a menudo tratar de adivinar los passwords de usuarios legítimos. Dos maneras comúnes y relacionadas son el intentar un sinnúmero de passwords desde una base de datos de "passwords comunes" y, el robar una copia del archivo de passwords y desencriptarlo (crackearlo).

Algunas veces incluso buenos passwords (difíciles) no son suficiente. Estos pueden ser espiados (sniffed) cuando viajan por una red broadcast (por un hub, mas no por un switch). Como el acceso a los servidores del NOC será sólo desde la LAN interna y por ser una red switcheada (switched network), passwords UNIXs normales serán empleados y no será necesario el empleo de passwords de un solo uso, idóneos para acceso desde redes externas o desde el Internet.

En sistemas grandes distribuidos, no se puede asegurar que cada ordenador posea el mismo archivo /etc/passwd. Por esta razón, existen varios sistemas comerciales para hacer que la información almacenada en /etc/passwd esté disponible sobre la red. Se tiene, a saber: Sun Microsystems Network Information System (NIS), NIS+, Open Software Foundation´s DCE (Distributed Computing Environment). Sin embargo, un administrador se sentirá inquieto por miedo a que el sistema mismo se vea comprometido.

3.1.1.3 Protecciòn de las cuentas.- El título busca exponer las maneras en las que se puede hacer las cuentas más difíciles de atacar por un hacker.

Se debe descubrir las cuentas sin passwords. Por ejemplo, en UNIX SVR4 se ejecuta el comando:

```
# logins -p
```

También se puede emplear:

```
% cat-passwd | awk -F: 'length($2)<1 {print $1}'
```

El permitir que programas como who y finger sean ejecutados por alguien que no se ha autentificado es también un riesgo en la seguridad, debido a que estos comandos permiten conocer los nombres de las cuentas en el sistema. Tal información puede ser empleada como base para ataques posteriores.

En el caso de cuentas durmientes, es decir, no empleadas por un período de tiempo, se puede: cambiar el password de la cuenta, modificar el password de la cuenta de modo que no pueda ser usado, cambiar el shell de la cuenta.

El password de la cuenta puede ser cambiado por el superusuario. Cuando el usuario se halle inhabilitado de ingresar, contactará inmediatamente al administrador. Otra manera alternativa es insertando un asterisco en el campo de password de la cuenta de usuario, del modo siguiente:

```
efromm:*fdfi34kiur1824m:105:100:Erich Fromm:/home/efromm:/bin/csh
```

Sin embargo, aún colocando un asterisco, la cuenta será siendo de uso de su, o desde un ingreso remoto empleando los mecanismos de hosts confiables (~/.rhosts o /etc/hosts.equiv). También será necesario observar los trabajos at y job corridos por el usuario cuya cuenta se deshabilitó (ellos seguirán operando).

El método de variar el shell de usuario consiste en que el sistema simplemente imprime una mensaje informativo y escapa. Este cambio efectivamente deshabilita la cuenta.

Por ejemplo, la línea en /etc/password para el usuario jpsartre:

```
jpsartre:weri83&jk123:105:100:Jean Paul Sartre: /usr/users/jpsartre
: /bin/csh
```

Puede cambiarse a:

```
jpsartre:weri83&jk123:105:100:Jean Paul Sartre:  /usr/users/jpsartre

  /etc/disabled
```

El script shell /etc/disabled sería:

```
#!/bin/sh
/bin/echo Your account has been disabled because you seem to have
/bin/echo forgotten about it.  If you want your account back, please
/bin/echo call N OC´s administrator.
/bin/sleep 10
```

El siguiente script puede correrse el último día de cada mes para descubrir una lista de usuarios que no empleado sus cuentas el mes corriente.

```
#!/bin/sh
#
# not-this-month:
# Gives a list of users who ahve not logged in this month.
#
PATH = /bin:/usr/bin;export PATH
umask 077
THIS_MON TH=`date| awk ´{print $2}´`
/bin/last | /bin/grep $THIS_MON TH| awk ´{print $1)´ |
    /bin/sort -u > /tmp/users1$$
cat-passwd  |  /bin/awk  -F:  ´{print  $1}´  /bin/sort  -u  >
/tmp/users2$$
/bin/comm -13 /tmp/users[12]$$
/bin/rm -f /tmp/users[12]$$
```

Sin duda, la manera más fácil de eliminar las cuentas durmientes en el sistema es crear cada cuenta de usuario con una fecha de expiración fija. Los usuarios de cuentas activas deberán renovarlas periódicamente.

Bajo SVR4, se puede realizar esto con el comando usermod:

```
# usermod -e 15/10/2000 spaf
```

Para prevenir que un usuario pueda cambiar su password (pues es "propenso" a escoger passwords sencillos) es bueno manipular su parámetros de expiración apropiadamente. Por ejemplo, en UNIX SVR4, el comando:

```
# passwd -n 60 -x 50 acamus
```

hará que el password de acamus expire en 50 días y necesitará ser rehabilitado por alguien con acceso al superusuario.

Existen paquetes libremente disponibles en el Internet, como npasswd y passwd+, con el fin de descubrir passwords sencillos; ambos disponibles por coast.cs.purdue.edu. Otro sistema popular con más ventajas es anlpasswd, ubicado en info.mcs.anl.gov.

En una estación SVR4, se puede restringir la habilidad de los usuarios para ingresar con la cuenta root desde cualquier terminal que no sea la consola. Se logra editando el archivo /etc/default/login e insertando la línea:

```
CONSOLE=/dev/console
```

3.1.1.4 Integrity management.- Existen diferentes aspectos en la seguridad de red, y de ellos, la integridad es, en gran parte, el aspecto más importante: proteger la data contra modificación o borrado no autorizado. Integridad y confidencialidad van de la mano, pero la primera es más importante. Por ejemplo, respecto de los bancos, desean guardar los saldos de cuentas tanto correcta como secretamente. Pero, entre revelar los saldos y modificarlos, lo primero es preferible a lo segundo.

La misión de una buena gestión de integridad es el prevenir alteraciones (o borrados) de data, para detectar alteraciones (o borrados) si ocurren, y para recuperarse de los mismos. La relación con los backups es evidente.

Existen básicamente tres enfoques para detectar cambios sobre archivos e inodes (index node, la entrada básica del sistema de archivos). El primer medio es emplear copias de comparación de la data a ser monitoreada. Una segunda manera es monitorear la metadata sobre los items a proteger. Esto incluye monitorear la modificación del tiempo de entradas almacenadas por el sistema, y monitorear cualquier log o huellas de auditorías que muestre alteraciones de los archivos. La

tercera vía es emplear alguna forma de firma de la data a ser monitoreada, y recomputar periódicamente y comparar la firma contra un valor almacenado.

3.1.1.4.1 Comparación de copias.- El método más seguro y directo de detectar cambios de la data es almacenar una copia de la data no alterada, y realizar una comparación byte a byte cuando se necesite. La más leve diferencia indicará no sólo que un cambio ocurrió, sino lo que implica. Sin embargo, esto resulta poco manejable desde el punto de vista del almacenamiento y de los derechos de licencia. Por otro lado la copia de comparación necesita almacenarse en un lugar seguro.

Aún con estas deficiencias, las copias de comparación tienen un beneficio: si se descubre un cambio no autorizado, simplemente se reemplaza la versión alterada con la copia de comparación salvada, restituyendo el sistema a lo normal.

Un método estándar de copias locales son las copias on-disk. Por ejemplo se podría guardar una copia del directorio /usr/bin en /usr/adm/.hidden/.usr/bin. Adicionalmente, se podría comprimir y/o encriptar la copia para reducir el espacio en disco y resguardarla del espionaje. La desventaja radica en el tiempo de recuperación.

Otro método de emplear copias de comparación es almacenarlas en un sitio remoto y hacerlas disponibles remotamente de alguna manera. Por ejemplo, se podría colocar las copias de todos los archivos de sistemas en una partición de disco en un servidor seguro, y exportar dicha partición de solo lectura empleando NFS o protocolo similar. Todas las estaciones clientes podrían montar dicha partición y usar las copias en comparaciones locales. Se debe asegurar que los programas empleados en la comparación (como cmp, find y diff) sean tomados de la partición

remota y no del disco local. Un hacker podría modificar dichos archivos para no reportar los cambios.

Otro método de comparación remota sería el emplear un programa para hacer la comparación a través de la red. La utilidad rdist es un programa que sienta bien al respecto. La desventaja de emplear rdist, sin embargo, es la misma que con las copias de comparación total: la revisión byte tras byte. El problema se agrava pues se requiere de la transferencia de las copias a través de la red cada vez que se ejecuta una revisión. Otra deficiencia es que rdist depende del mecanismo de hosts confiables Berkeley para trabajar correctamente.

3.1.1.4.2 Listas de comprobación y metadata.- Primeramente mencionemos las desventajas de las copias de comparación. Requiere espacio substancial de disco y además, si ejecutadas a través de la red, via rdist o NFS, aumentarán la carga de red cada vez que las comparaciones se realicen.

Un método más eficiente sería almacenar un resumen de las características importantes de cada archivo y directorio. A la hora de comparar, las características son regeneradas y comparadas con la información salvada. Si dichas características son comprehensivas y de menor espacio que el contenido del archivo, entonces este método es sin duda más eficiente. Además este enfoque entra al detalle de los cambios en metadata tales como los propietarios de archivos y los modos de protección.

3.1.1.4.3 Checksums (comprobaciones de suma) y firmas.- El monitoreo mediante metadata puede ser burlado si un archivo es modificado escribiendo al dispositivo de disco en bruto luego que el bloque apropiado es conocido. También se podría

subrepticiamente alterar el reloj del sistema de manera que los tiempos de modificación no varíen y no se note el cambio.

La primera aproximación hacia una firma es el empleo del estándar checksum CRC, implementado por el comando sum. Los polinomios CRC son a menudo empleados para detectar alteraciones en la transmisión de mensajes; sin embargo, están diseñados para detectar cambios aleatorios más no intencionados (o concienzudamente elaborados).

Para generar un checksum más sólido se necesita un mecanismo más fuerte, tales como los mensajes digeridos (hash messages). Si se tuviese un programa para generar el hash MD5 de un archivo, se podría alterar el script de comprobación así:

```
#!/bin/sh
find `cat /usr/adm/filelist` -ls -type f -exec md5 { } \; > /tmp/now
diff -b /usr/adm/savelist /tmp/now
```

3.1.1.4.4 Tripwire.- El paquete Tripwire fue escrito por Gene Kim y Gene Spafford de Purdue con el fin de leer una archivo de configuración de archivos y directorios a monitorear, y luego sigue el rastro de cambios a la información de inode y contenidos. La base de datos es altamente configurable, y permite al administrador especificar atributos particulares a monitorear, y algoritmos hash particulares para cada archivo.

Un archivo de configuración típico luce así:

```
/.rhosts                R               # may not exist
/.profile               R               # may not exist
/.forward               R-12+78         # may not exist
/usr/spool/at           L
=/tmp                   L-n
```

En este ejemplo, todo respecto a los inodes será observado en /.rhots, /.profile y /.forward excepto el tiempo de acceso. Los dos primeros archivos son comprobados empleando las firmas MD5 y Snefru, y el archivo /.forward mediante

los algoritmos SHA y HAVAL. El directorio /usr/spool/at y su contenido es sometido a monitoreo de propietario, group, modos de protección y cuenta de enlace; los cambios a los contenidos son ignorados. El directorio /tmp es observado sobre los mismos cambios más no su contenido.

3.1.1.5 Auditoría y logging.- El proceso de auditoría consiste en el proceso de monitoreo del comportamiento del sistema. Los archivos log guardan una historia del pasado del ordenador, haciendo más fácil seguir el rastro de problemas intermitentes o ataques. A continuación sigue la descripción del manejo adecuado de archivos log importantes.

El archivo lastlog almacena la última vez que cada usuario ingresa al sistema. No existe una utilidad en UNIX que permite leer el archivo de modo inteligible e imprimir toda la información. El siguiente script de Perl resuelve la situación:

```
/var/adm/format.lastlog
#!/usr/local/bin/perl
$fname = (shift || "/var/adm/lastlog");
$halfyear = 60*60*24*365.2425/2;  # pedantry abounds
setpwent;
while (($name, $junk, $uid) = getpwent) {
    $names{$uid} = $name;
}
endpwent;
open(LASTL, $fname);
for ($uid = 0; read(LASTL, $record, 28); $uid++) {
(    $time, $line, $host) = unpack('l A8 A16', $record);
     next unless $time;
     $host = "($host)" if $host;
     ($sec, $min, $hour, $mday, $mon, $year) = localtime($time);
     $year += 1900 + ($year < 70 ? 100 : 0);
     print $names{$uid}, $line, " $mday/$mon ";
     print ((time - $time) > $halfyear) ? " $year " : " $hour  $min
";
     print "    $host\n";
}
close LASTL;
```

Mientras el archivo lastlog está diseñado para proveer rápido acceso a la última vez que una persona ingresó al sistema, éste no provee una historia detallada registrando el uso de cada cuenta. Para ello, UNIX emplea el archivo log wtmp.

El comando ps ofrece un reporte más preciso de quién está actualmente empleando el sistema que los comandos who, whodo, users y finger, debido a que bajo ciertas circunstancias, los usuarios pueden tener procesos corriendo sin que sus usuarios aparezcan en los archivos /etc/utmp o /var/adm/wtmp. Por ejemplo, un usuario puede tener un proceso corriendo y luego haber salido, o haber empleado el comando rsh en vez de rlogin.

Cuando se emplea el comando su, se crea un nuevo proceso con un UID real y otro UID efectivo. Esto da la habilidad para accesar los archivos de otros usuarios, y correr programas como el otro usuario. Aún cuando, su no modifica la entrada en los archivos /etc/utmp o /var/adm/wtmp, finger seguirá mostrando la cuenta donde uno ingresó, no hacia donde se aplicó su, produciendo confusión a otros usuarios y a algunas utilidades del sistema.

En adición a los ingresos y salidas, UNIX también puede registrar cada comando simple ejecutado por usuario. El archivo acct o pacct puede ser usado luego de un ingreso no autorizado para ayudar a determinar qué comandos un usuario ejecutó. El programa lastcomm o acctcom muestra los contenidos de este archivo en forma inteligible:

```
wsvill#lastcomm
ls         root       pts/13    0.02 secs  Wed Jun 28 22:55
test-url   cricket     __        0.39 secs  Wed Jun 28 22:55
pwd        cbmum      pts/13    0.01 secs  Wed Jun 28 22:55
touch      cricket    __        0.01 secs  Wed Jun 28 22:55
sh         barquillo  __        0.01 secs   Wed Jun 28
22:55
sh         blenda     __        0.00 secs  Wed Jun 28 22:55
lastcomm   tigrin     pts/13    0.05 secs  Wed Jun 28 22:54
```

```
update_h   analucha   pts/13    0.06 secs  Wed Jun 28 22:54
```

Desafortunadamente, el accounting de UNIX no registra los argumentos de los comandos tipeados por el intruso, ni el directorio en que el comando fue ejecutado. Como el archivo /var/adm/acct crece rápidamente, se tiene el comando sa o runacct (que produce /var/adm/savacct) para obtener un resumen.

Es importante revisar el archivo /usr/adm/messages o /var/adm/messages pues en el se sitúa cualquier mensaje impreso en la consola del sistema.

El archivo sulog registra los intentos de uso de la cuenta de superusuario exitosos y fallidos de los usuarios. Si se tiene decenas de ingresos su de un usuario particular que se supone no tiene acceso a la cuenta de superusuario, se debe indagar inmediatamente. Desafortunadamente, si un usuario realmente logra el acceso a la cuenta de superusuario, podrá eliminar los intentos fallidos, BADSU, del archivo log. Por esta razón, se podría enviar los intentos fallidos registrados hacia una impresora o hacia una computadora remota segura.

Existen otros archivos que son almacenados en una base por usuario que pueden ser de utilidad al analizar algo adverso en el sistema. Aún cuando no son archivos log propiamente dichos, pueden ser tratados como una posible fuente de información sobre comportamiento de usuario.

Muchos de los shells estándares, como csh, tcsh y ksh, pueden almacenar un archivo de history. Cuando el usuario edita comandos, el texto de cada comando y sus argumentos son almacenados en el archivo historia para rejecución posterior. Si se está tratando de recrear la actividad llevada en una cuenta, posiblemente por un intruso, los contenidos de este archivo pueden ser bastante útiles acoplados con la

información de log. Se debe observar la fecha de modificación del archivo para asegurar que fue empleada durante el tiempo que la actividad sospechosa ocurrió.

En adición a las varias facilidades de logging mencionadas, UNIX provee de una facilidad de logging de propósito general de nombre syslog. Programas individuales que necesitan tener información registrada (logged) envía la información a syslog. Los mensajes pueden ser registrados en varios archivos, dispositivos u ordenadores, dependiendo del emisor del mensaje y su severidad.

Por defecto, syslog aceptará los mensajes log desde hosts arbitrarios enviados sobre el puerto UDP syslog. Esto puede resultar en una ataque de denegación de servicio cuando el puerto sea inundado de mensajes más rápido de lo que puede tolerar el demonio syslog. Este deberá filtrarse adecuadamente en el firewall del NOC, permitiendo sólo enviar mensajes a estaciones autorizadas.

Se pueden registrar todos los mensajes de autorización de sistema sobre un impresora insertando la línea siguiente en el archivo syslog.conf:

```
auth.*                  /dev/ttya
```

El logging sobre un dispositivo de copia rígida es una muy buena idea si se piensa que el sistema está siendo visitado por intrusos en una base regular. El intruso puede borrar los archivos log, pero luego que algo es enviado a la impresora, no podrá tocar la salida de la misma sin irrumpir fisicamente en el establecimiento.

El logging hacia otra estación agrega más seguridad global: aún cuando se irrumpa sobre una estación y se borre sus archivos log, se tendrá todavía que lidiar con los mensajes log enviados a través de la red sobre la estación de log segura. Si de hecho se maneja una estación de logging, es recomendable restringir las cuentas

de usuarios en dicha máquina. Sin embargo, está única estación significa un único punto de fallo, por ello es mejor registrar sobre dos estaciones loghots1 y loghost2.

Respecto a la gestión de los archivos log, la primera recomendación es realizar backup de los mismos sobre una base regular, preferentemente diario. Lo segundo se refiere a la frecuencia de revisión de los archivos log. Al lo menos se debe realizar diariamente. Como tercera recomendación, se debe observar cómo se procesan los mensajes log. Se debe buscar filtrar la información primordial de la cotidiana (y aburrida). Estos filtros se deben actualizar también periódicamente. Finalmente, desgraciadamente no se puede confiar ciento por ciento en los logs. Ellos pueden ser alterados o borrados por un intruso con derechos de superusuario. Los mismos usuarios locales con acceso fisico o conocimiento apropiado del sistema pueden fácilmente burlar los mecanismos. Por otro lado, los errores de software y del sistema mismo pueden resultar en logs no apropiadamente coleccionados y grabados. Así, lo que se necesita es de mecanismos redudantes.

3.1.1.7 De la seguridad de los servicios de red.- La mayoría de servicios de red UNIX son proveídos por programas individuales llamados servidores. Para que un servidor opere, se le debe asignar un protocolo (TCP o UDP), un número de puerto, y ser iniciado cuando el sistema se pone en marcha o según se necesite.

3.1.1.7.1 Systat (TCP puerto 11).- El servicio systat provee información de estado sobre el ordenador. Las peticiones son respondidas con las salidas del comando who. Es recomendable comentar o remover la línea de servicio de /etc/inetd.conf pues la información de nombres de usuario, tiempos de utilización y hosts fuentes, puede ser empleada como objetivos para ataques.

3.1.1.7.2 File Transfer Protocolo FTP (TCP puertos 20 y 21).- Bajo circunstancias normales el servidor FTP inicia la conexión de retorno hacia el cliente FTP. Muchos servidores y clientes soportan un modo alternativo de operación llamado modo pasivo. En modo pasivo, el cliente FTP inicia la conexión que el servidor usa para enviar data de retorno al cliente.

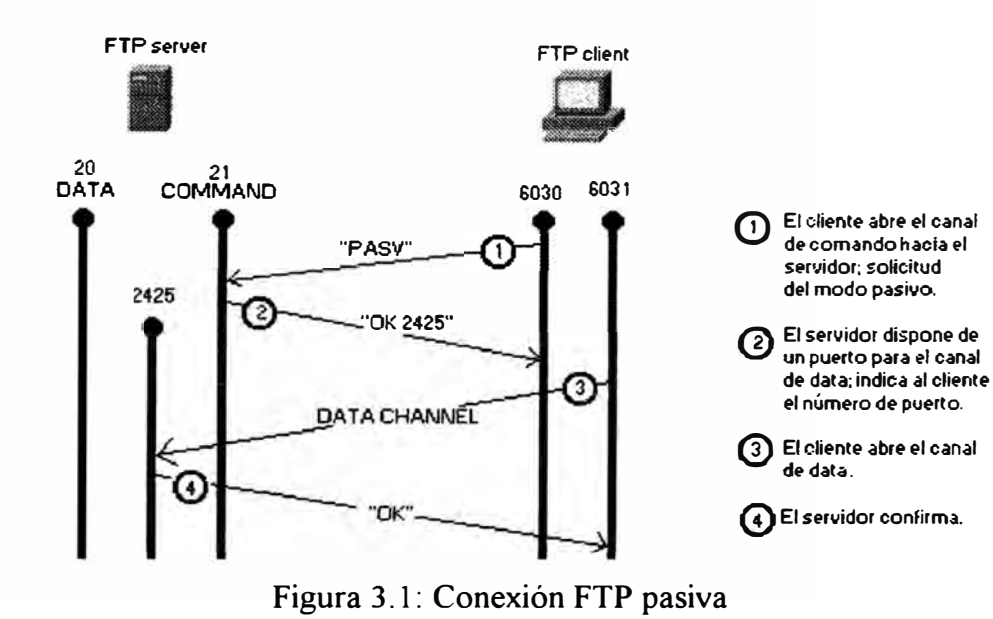


Figura 3.1: Conexión FTP pasiva

El modo pasivo es deseable porque simplifica la tarea de construir un firewall: el firewall simplemente permite que conexiones internas pasen a traves hacia el mundo exterior, pero no necesita permitir que las conexiones externas retornen. No todos los clientes soportan el modo pasivo. Si el software que se tiene lo incluye, deberá mejor realizarse un upgrade del mismo.

El archivo /etc/ftpusers contiene una lista de las cuentas que no son permitidas para usar FTP. Este archivo debe contener todas las cuentas que no corresponden a seres humanos reales:

```
# cat /etc/ftpusers
root
uucp
news
```

```
ingres
nobody
daemon
```

Si se tiene un directorio en un servidor FTP anónimo que es escribible por el usuario ftp, existe la posibilidad que piratas de software empleen pronto estos directorios como repositorios para programas copiados ilegalmente o archivos pornográficos. Esta información se conocen comúnmente como warez. Para crear un depósito protegido seguir lo citado:

- Crear un directorio escribible mas no leíble por el usuario ftp. La manera más sencilla es haciendo que el directorio sea de propiedad de la raíz y tenga modo 1733.
- Colocar una cuota de archivo sobre el usuario ftp para limitar el número total de bytes que pueden ser recibidos.
- Crear un script shell que automáticamente mueva los archivos dejados en el repositorio que han permanecido por más de 15 o 30 minutos sobre otros directorio no accesible por el usuario ftp. También se podría notificar al respecto (e-mail).
- Correr periódicamente el script agregándolo al archivo /usr/lib/crontab.

3.1.1.7.3 Telnet (TCP puerto 23).- El mayor peligro sobre sesiones Telnet es el espionaje de paquetes (packets sniffing). El medio más eficaz contra él es el uso de passwords de un solo uso y encriptación.

Un segundo peligro es que un atacante puede realizar un ataque secuestrando una sesión en transcurso (hijacking) . Así, luego que un usuario ha ingresado su password, el atacante puede tomar control de la sesión y tipear los comandos que

desee. La única manera de evitar el hijacking es mediante la encriptación (por ejemplo, empleando Telnet kerberizado).

Telnet es un servicio muy útil. Para hacerlo más seguro se deberá evitar emplear password reusados. También se puede asignar usuarios diferentes sobre diferentes ordenadores, de modo que si una cuenta se ve comprometida, otras no lo serán.

3.1.1.7.4 Simple Mail Transfer Protocol SMTP (TCP puerto 25).- El programa UNIX /usr/lib/sendmail usualmente implementa tanto el lado cliente como el lado servidor del protocolo, y parecer ser el software predominante usado en sistemas de correo UNIX.

Una dirección de correo legítima puede ser un nombre de usuario o una entrada en la base de datos alias. Los alias se hallan generalmente en los directorios /usr/lib, /etc, /etc/mail o /etc/sendmail sobre el archivo alias.

Sendmail ha sido la fuente de numerosas brechas de seguridad en sistemas UNIX. Por ejemplo:

- Versiones iniciales de sendmail permitían que el correo sea enviado directamente a cualquier archivo sobre el sistema, incluyendo archivos como /etc/passwd.
- Sendmail soporta un password "wizard", establecido en el archivo de configuración, que puede ser usado por conseguir un shell en un sistema remoto sin autenticarse.
- Sendmail permite a usuarios confiables el falsificar el correo enviado a la estación local.

- Sendmail puede ser compilado en modo debug, un modo empleado por usuarios externos invasores para ingresar al sistema sobre el cual está corriendo Sendmail.
- Sendmail solía aceptar correo con un programa como recipiente, permitiendo así a los usuarios invocar shells y otros programas sobre la estación remota.
- Sendmail ha hecho un trabajo pobre para validar sus argumentos, permitiendo así a los usuarios sobreescribir localizaciones arbitrarias en memoria, o proveer entrada que resulta en efectos colaterales dañinos.

Una de las principales razones de Sendmail es su diseño todo en uno. El programa es extremadamente complicado, corre como superusuario, acepta libremente conexiones desde cualquier ordenador en el Internet, y tiene un lenguaje de comandos riquísimo. Afortunamente, existe alternativas. En vez de tener un largo programa todo en uno que reciba mensajes desde el Internet y luego entregue el correo, se podría dividir esta funcionalidad en dos programas diferentes. El juego de seguridad Firewall Toolkit de Trusted Information Systems contiene un programa llamado smap que hace exactamente esto.

Si se corre Sendmail para recibir correo electrónico, se deberá tomar medidas extras para proteger la seguridad del sistema.

- Asegurarse que el programa Sendmail no soporta los comandos debug, wiz o kill; en su defecto reemplazar la versión.
- Borrar los alias "decode" del archivo alias. El alias decode es una simple línea que luce así:

  decode: "|/usr/bin/uudecode"

El alias decode permite que el correo sea enviado directamente al programa uudecode. Examinar cuidadosamente cada alias que apunta a un archivo o programa en vez de una cuenta de usuario. Recordar ejecutar newaliases luego de cambiar el archivo /etc/alias.

- Asegurarse que el archivo aliases está protegido de modo que no pueda ser modificado por terceros.
- Asegurarse que el password "wizard" esté deshabilitado en el archivo /etc/mail/sendmail.cf.
- Asegurarse que la última versión de Sendmail esté corriendo en el sistema. Observar con frecuencia las listas de correo del CERT relacionadas a problemas con Sendmail.
- Evitar cuentas fantasmas. El sistema operativo UNIX emplea cuentas que no corresponden a usuarios reales para ejecutar ciertas funciones. Ejemplos incluidos, uucp, news y root. Desafortunadamente el sistema de correo recibirá inocentemente correo de estos usuarios. Los archivos de correo en /var/spool/mail pueden crecer desmesuradamente y consumir recursos valiosos. Muchos programas que corren autónomamente enviarán correo a una dirección tal como news o uucp cuando encuentran un problema. Si este mail no es monitoreado el correo pasará por alto. La mejor manera de evitar el correo fantasma es creando alias para todas las cuentas de "usuarios inexistentes". Por ejemplo:

```
#
# System aliases
#
root:          simsong
Postmaster:    root
usenet:        root
```

```
news:           root
agent:          root
sybase:         root
```

3.1.1.7.5 TACACS (UDP puerto 49).- TACACS es un protocolo que es empleado para autentificar ingresos hacia servidores terminales. Los passwords no son encriptados entre el terminal y el equipo accesado; asì, ellos son susceptibles al espionaje de paquetes; mas la sesión entre el servidor TACACS y el equipo al cual se accesa si es encriptada.

3.1.1.7.6 Domain Name System DNS (TCP y UDP, puerto 53).- El proceso de transferencia de zona puede ser un riesgo en la seguridad debido a que entrega a terceros una completa lista de las computadoras conectadas a la red interna. Se puede bloquear las transferencias de zonas con un router que filtre las conexiones entrantes TCP sobre el puerto 53.

Debido a que muchas aplicaciones UNIX emplean nombres de hosts como base del control de acceso, un atacante puede hacer que el servidor ofrezca información incorrecta de dos modos: información incorrecta puede ser descargada sobre los servidores; el atacante puede modificar los archivos de configuración del servidor.

Para cambiar los archivos de configuración, un atacante debe tener acceso al sistema de archivos del ordenador sobre el cual el servicio está operando y ser capaz de modificar los archivos. Luego que los archivos son modificados, el servidor deber ser reinicializado (enviándole una señal kill –HUP).

Para minimizar la posiblidad de un atacante de modificar el servidor de nombres se debe seguir las siguientes recomendaciones:

- Correr el servidor de nombres sobre un ordenador especial que no posee cuentas de usuarios.
- Si se corre el servidores de nombres sobre un ordenador que es empleado por usuarios ordinarios, asegurarse que los archivos del servidor sean todos de propiedad del root y tengan su derecho de uso establecido en 444 o 400. La regla se aplica de igual manera a los directorios pero con modos 755 o 700.

Otra forma de protegerse contra ataques sobre el DNS es evitar emplear nombres de hosts en las listas de control de acceso. Desafortunadamente, muchos programas no permiten el uso de direcciones IP, como por ejemplo rlogind/rshd de Solaris, que no permite lo anterior en los archivos /etc/hosts.equiv o .rhosts.

3.1.1.7.7 Trivial File Transfer Protocol TFTP (UDP puerto 69).- Debido a que TFTP no ofrece seguridad, tftpd, el demonio TFTP, es normalmente restringido de modo que sólo pueda transferir archivos hacia o desde cierto directorio.

Para probar esta restricción realizar lo siguiente:

```
% tftp localhost
tftp> get /etc/passwd tmp
Error code 1: File not found
tftp> quit
```

Si tftp no responde así o simplemente se cuelga, es mejor conseguir otra versión del programa.

3.1.1.7.8 Simple Network Management Protocol SNMP (UDP puertos 161 y 162).- SNMP es de gran valor para los atacantes. Mediante mensajes SNMP construídos concienzudamente, un atacante puede aprender la estructura interna de la red, cambiar la configuración de la red e incluso desactivar sus operaciones. SNMP versión 2.0 se suponía incluir buenas características de seguridad pero

lamentablemente no se ha estandarizado. La primera recomendación obvia es cambiar la comunidad SNMP por defecto de "public" a cualquier otro valor.

3.1.1.7.9 rexec (TCP puerto 512).- El demonio de ejecución remota /usr/sbin/rexecd permite a los usuarios ejecutar comandos sobre otros ordenadores sin tener que ingresar sobre ellos. El cliente abre una conexión y transmite un mensaje que especifica el nombre de usuario, el password y el nombre del comando a ejecutar. Como rexecd no emplea el mecanismo de hosts confiable, éste puede ser editado desde cualquier host en la red. Sin embargo, debido a que rexecd requiere que el password sea transmitido sobre la red, es susceptible al snooping de passwords similar al Telnet.

Debido a esta debilidad, un cracker puede emplear rexecd para probar el sistema por nombres de cuentas válidas y luego dirigir sobre estas cuentas ataques de adivinación de passwords.

Si no se espera emplear este servicio, mejor deshabilitarlo en /etc/inetd.conf.

3.1.1.7.10 rlogin y rsh (TCP puertos 513 y 514).- El termino host confiable, trusted host, fue inventado por personas que desarrollaron el software UNIX Berkeley. Si un host confia en otro host, luego cualquier usuario que tiene el mismo nombre de usuario en ambos puede ingresar desde el host confiable hacia el otro ordenador sin tipear un password.

Debido a que no se necesita tipear un password cuando se emplea rlogin para ingresar en una computadora desde otra máquina que es un host confiable, rlogin es usualmente menos susceptible a espionaje que Telnet. Sin embargo, los hosts confiables introducen problemas de seguridad por dos razones: no se puede confiar siempre en un host, y no se puede confiar en los usuarios de dicho host.

Si un atacante logra romper la cuenta de alguien que tiene una cuenta en dos computadores – y los dos se tienen confianza – luego la cuenta de la persona en la segunda computadora también será comprometida.

Otro problema implica NFS. A menudo, el directorio home de un usuario es exportado con NFS hacia otras máquinas. Alguien capaz de escribir sobre el directorio home del usuario en dicha partición sobre una máquina remota puede agregar entradas arbitrarias al archivo .rhosts. Estas adiciones luego permite al atacante ingresar a dicha cuenta en cada máquina que importa el directorio home.

Los hosts confiables también son vulnerables a spoofing IP, una técnica en la cual un ordenador envía paquetes IP que parecen venir de una computadora diferente. Empleando una forma de spoofing IP, los usuarios en un host pueden enmascararse, y parecen que provienen de un segundo host. Ellos pueden luego ingresar al ordenador, si el segundo host es confiable.

El archivo /etc/hosts.equiv contiene una lista de hosts confiables para el ordenador. Luego de analizar éste, los programas rlogind y rshd analizan el directorio home del usuario por un archivo de nombre .rhosts.

Los archivos .rhosts son fácilmente explotados para propósitos no destinados. Por ejemplo, los crackers que rompen el sistema frecuentemente agregan sus nombres de usuarios de modo que puedan fácilmente en el futuro quebrantarlo una y otra vez.

La primera recomendación es mantener los archivos hosts.equiv y .rhosts con modo de protección 600.

Debido a los riesgos obvios expuestos por .rhosts, muchos administradores de red deciden deshabilitarlo completamente. Un primer enfoque es remover

(comentarlos) las entradas para rshd y rlogind en el archivo inetd.conf. Otro modo es empleando el paquete logdaemon de Wietse Venema. Una tercera opción es obtener el código fuente para los programs rshd y rlogind y remover las características directamente. Otra aproximación es analizar el sistema periódicamente para usuarios que tienen dichos archivos y tomar acción apropiada si se encuentran.

Se puede hallar los archivos .rhosts en el sistema empleando el siguiente script:

```
#!/bin/ksh
# Search for .rhosts files in home directories
PATH=/usr/bin
for user in $(cat passwd | awk -F: 'length($6) > 0 {print $6}' |
sort -u)
do
    [ [ -f $user/.rhosts ] ] && print "There is a .rhosts file in
$user"
done
```

Para borrar los archivos .rhosts automáticamente, agregar un comando rm al script shell:

```
#!/bin/ksh
# Search for .rhosts files in home directories
PATH=/usr/bin
for user in $(cat passwd | awk -F: 'length($6) > 0 {print $6}' |
sort -u)
do
    [ [ -f $user/.rhosts ] ] || continue
    rm -f $user/.rhosts
    print "$user/.rhosts has been deleted"
done
```

3.1.1.7.11 Routing Internet Protocol (RIP routed) (UDP puerto 520).- El demonio routed es en general un programa confiable: éste recibirá inocentemente cualquier paquete desde otro ordenador indicando que el mejor camino hacia el exterior es la estación emisora. Claramente, esta confianza presenta una manera simple para confundir la red. Aún peor: da la opción a usuarios sofisticados de husmear todas las comunicaciones.

Por estas razones, muchos sitios ya no corren el demonio routed. En su lugar, ellos emplean rutas estáticas.

3.1.1.7.12 finger (TCP puerto 79).- Finger hace fácil para los intrusos conseguir una lista de usuarios en el sistema, lo cual incrementa dramáticamente las chances del intruso para quebrar el sistema.

Existen dos maneras para deshabilitar el sistema finger.

- Remover la línea de servicio finger en el archivo /etc/inetd.conf. La deshabilitación mediante este modo puede causar problemas para tratar de determinar direcciones de correo y obviamente eso afecta la performance de las operaciones de red.
- Se puede reemplazar el servidor finger con un script que imprima un mensaje instruyendo a las personas como contactarse. Por ejemplo, podría lucir así:

```
#!/bin/sh
#
/bin/cat << 'XX'
Welcome to Zoo Station Inc.
For information on contacting a specific employee, please call
our company operator at 511-4366468 o send electronic mail to the
address postmaster@zoostation.com
Thank you.
XX
exit 0
```

Almacenar este script en un archivo ejecutable, tal como /usr/local/bin/no_finger.

Luego en el archivo /etc/inetd.conf, reemplazar el finger normal con la línea:

```
finger stream tcp nowait nobody /usr/local/bin/no_finger
no_finger
```

Luego reinicializar inetd.

3.1.1.7.13 Identification Protocol (auth) (TCP puerto 113).- Cuando un servidor desea conocer el "nombre real" de una persona iniciando una conexión TCP/IP, éste simplemente abre una conexión hacia el demonio identd de la máquina cliente y envía una descripción de la conexión TCP/IP en progreso.

En general, las respuestas a las peticiones ident son más útiles para los administradores del sitio que envía la respuesta que para el sitio que las recibe. Los sitios que tienen un número razonable de usuarios deberían usar ident para ayudar en el seguimiento de cuentas que han sido comprometidas durante un incidente.

3.1.1.7.14 Network News Transport Protocol NNTP (TCP puerto 119).- NNTP puede ser configurado con una lista de control de acceso para determinar que ordenadores están permitidos para usar ciertas características. La lista de control de acceso está basada en nombre de hosts; así, la seguridad de NNTP puede ser sobrepasada a través del spoofing IP o a través de ataques al DNS.

Existen dos circunstancias en las cuales el uso no autorizado de NNTP podría causar problemas:

- Si existe un grupo de noticias especial de las discusiones internas de la organización, hay la posibilidad que un servidor NNTP comprometido revele información confidencial al exterior.

- Si un invasor puede remitir desde el servidor NNTP propio, el invasor podría remitir un mensaje escandolo u ofensivo, con las implicancias de responsabilidad de la organización.

Con una configuración adecuada del firewall se puede evitar estos compromisos.

3.1.1.7.15 Network Time Protocol NTP (UDP puerto 123).- NTP no fue diseñado para resistir ataques, y varias versiones de ntpd, el demonio NTP, pueden ser burladas e introducir errores significativos en el reloj del sistema.

Una variedad de problemas puede surgir si un atacante puede cambiar el reloj del sistema:

- El atacante puede intentar un ataque de repetición. Por ejemplo, si el sistema emplea Kerberos, tickets Kerberos pasados pueden ser reutilizados.
- Los archivos log del sistema ya no indicarán con precisión el tiempo en el cual eventos tomaron lugar. Un atacante incluso podría borrar todos los archivos log como resultado de un procedimiento de eliminación quincenal o mensual.
- Los trabajos (jobs) corridos desde el demonio cron pueden no ser ejecutados si el reloj del sistema salta en el período especificado en el archivo crontab.

3.1.1.7.16 X Window System (TCP puertos 6000-6003).- Estaciones multiusuarios proveen un challenge para seguridad X. En implementaciones iniciales de X, los dispositivos lógicos para el teclado, pantalla, y dispositivos de sonido eran escribibles y leíbles por el mundo; esta disponibilidad ocasionaba problemas de seguridad, debido a que significaba que cualquiera podía leer los contenidos de la pantalla o teclado del usuario, o podía escuchar el micrófono en su oficina.

Algunas versiones de UNIX poseen un archivo especial que es empleado para resolver este problema El archivo de nombre /etc/logindevperm (sobre Solaris), especifica una lista de dispositivos que deberían tener su propietario cambiado a la cuenta que ha ingresado en la estación de trabajo UNIX. Este enfoque es similar a la manera que /bin/login cambia la propiedad de los dispositivos tty a la persona que ha ingresado en el dispositivo serial.

Bajo Solaris, el archivo es leído por el programa /bin/ttymon. Cuando una persona ingresa en el dispositivo que es listado en el primer campo, el programa establece el dispositivo listado en el tercer campo con el UID que el usuario ha ingresado. El modo del dispositivo es configurado con el valor contenido en el segundo campo:

```
/dev/console    0600    /dev/mouse:/dev/kbd
/dev/console    0600    /dev/sound/*            # audio devices
/dev/console    0600    /dev/fbs/*              # frame buffers
/dev/console     0600     /dev/rtvc0              # nachos capture
device 0
/dev/console     0600     /dev/rtvc2              # nachos capture
device 2
/dev/console     0400     /dev/rtvcctl2           # nachos control
device 2
```

El sistema X Window tiene un modelo de seguridad sencillo, todo o nada. Los mecanismos de seguridad X son empleados para determinar si un cliente puede o no conectarse al servidor X Window.

En vez de desarrollar un sistema que emplea listas de control de acceso y múltiples niveles de privilegio, los diseñadores del sistema X Window han trabajado meramente en refinar el control de acceso todo o nada. X Version 11, Release 6 tiene cinco mecanismos diferentes para implementar el control de acceso: xhost, MIT-MAGIC-COOKIE-1, XDM-AUTHORIZATION-1, SUN-DES-1 y MIT-KERBEROS-5.

X mantiene una lista de control de acceso de todos los hosts a quienes se les permite acceso al servidor X. La lista de hosts es mantenida via el comando xhost. La lista de hosts está siempre activa, no importa que otras formas de autentificación son usadas.

Aún cuando se emplee la facilidad xhost, el sistema X Window puede ser vulnerable a ataques desde computadoras que no están en la lista xhost. Algunos servidores X Window leen un pequeño paquete desde el cliente antes de determinar si el cliente está o no en la lista xhost. Si un cliente se conecta al servidor X pero no transmite este paquete inicial, el servidor X paraliza todas sus operaciones hasta un tiempo de vencimiento de 30 segundos.

Se puede determinar si el servidor X tiene este problema ejecutando el siguiente comando:

```
% telnet localhost 6000
```

Si se tiene este problema, la pantalla de la estación de trabajo se congelará. El cursor no se moverá y no se podrá tipear nada. En algunas implementaciones, el servidor X expirará luego de 30 segundos y reasumirá operaciones normales. Bajo otras implementaciones X, el servidor permanecerá bloqueado hasta que la conexión sea abortada.

A pesar que este ataque no puede ser usado para destruir información, puede ser usado para incapacitar cualquier estación de trabajo que corre uno de estos servidores y está conectado a la red. Si se tiene este problema con el software, es necesario consultar con el vendedor para una actualización correcta.

3.1.1.7.17 RPC rpc.rexd (TCP puerto 512).- El programa rpc.rexd es un servidor Sun RPC que permite ejecución remota de programas. Empleando rpc.rexd, cualquier usuario que puede ejecutar comandos RPC en la máquina puede correr comandos shell arbitrarios.

Es mejor inmediatamente comentar la línea que le corresponde en inetd.conf:

```
# The rexd server provides only minimal
# authentication and is often not run
#
# rexd/1     tli  rpc/tcp wait  root /usr/sbin/rpc.rexd rpc.rexd
```

3.1.1.7.18 HyperText Transfer Protocol (HTTP) (TCP puerto 80).- El World Wide Web es uno de los usos más excitantes del Internet. Pero también expone desafíos grandes de seguridad. En orden de importancia estos son:

- Un atacante puede tomar ventaja de los bugs del servidor Web o de scripts CGI para ganar acceso no autorizado a otros archivos del sistema, o incluso tomar control entero del ordenador.
- Información confidencial que está en el servidor Web puede ser distribuída a individuos no autorizados.
- Información confidencial transmitida entre el servidor Web y el browser puede ser interceptada.
- Bugs en el browser Web pueden permitir que información confidencial del cliente Web sea obtenido desde un servidor Web pirata.

- Debido a la existencia de tecnologías estándares y patentadas, muchas organizaciones encuentran necesario comprar software con licencia especial. Este, a su vez, puede crear vulnerabilidades únicas.

Para entablar un Web server seguro en cualquier plataforma, se debe ser capaz de asegurar una variedad de cosas, incluyendo:

- Los usuarios de red no deben nunca ser capaces de ejecutar programas arbitrarios o comandos de shell sobre el servidor.
- Scripts CGI que corren en el servidor deben ejecutar o la función esperado o retornar un mensaje de error. Los scripts deberán esperar y ser capaces de manejar cualquier entrada maliciosamente manipulada.
- En el caso que el servidor se vea comprometido, un atacante no deberá ser capaz de lanzar ataques adicionales contra la organización.

Es recomendable que la estructura de directorios del Web pertenezca a un grupo creado de nombre www y de propiedad del root, como se muestra:

```
drwx-x-x     8  root www        1024  Oct 16   23:45   cgi-bin/
drwx-------  2  root www        1024   Dec 25   12:00   conf/
drwxr-xr-x   2  root www        1024   Jan 1    17:32   htdocs/
-rwx------   1  root www      482168  Feb 6    01:05   httpd*
drwxrwxr-x   2  root www         1024  Dec 11   16:18   icons/
drwx------   2  root www         1024  Apr 22   23:06   logs/
drwxr-xr-x   2  root www         1024  Aug 6    14:34   support/
```

El directorio cgi-bin tiene modo de acceso 711; lo cual permite al servidor httpd correr programas que él contiene, pero no permite a una persona en el servidor ver los contenidos del directorio.

Debido a que los archivos de configuración pueden ser usados para subvertir el servidor o el sistema entero, se deberá proteger los scripts de modo que sólo puedan ser leídos y modificados por el superusuario:

```
-rw-------  1  root  www        918 Oct 16  23:45  access.conf
```

```
-rw-------  1  root www        2048 Oct 16  23:49  httpd.conf
-rw-------  1 root www         3450 Oct 16  23:33  mime.types
-rw-------  1 root www         4218 Oct 16  01:05  srm.conf
```

Además de establecer los permisos, es necesaria habilitar o deshabilitar las siguientes opciones de configuración:

- La mayoría de servidores Web listarán automáticamente los contenidos de un directorio si un archivo index.html no está presente en el directorio. Esta carácterística puede causar problemas de seguridad, sin embargo, pues da a terceros la habilidad de examinar archivos y vulnerabilidades del sistema.
- Algunos servidores permiten comprender enlaces simbólicos fuera del árbol de documentos del servidor Web. Esto hace que cualquiera que tiene acceso al árbol del Web server, tenga la posibilidad de poner a disposición otros documentos del ordenador para acceso Web. Por consiguiente, evitar los enlaces simbólicos fuera de rango.
- Los adjuntos server-side son directivas que pueden ser adecuadas en un documento HTML. Estos adjuntos son procesados por el servidor HTML antes que el documento sea enviado a un cliente solicitante. Los adjuntos server-side pueden ser usados para incluir otros documentos o ejecutar documentos, e imprimir la salida.

  He aquí dos ejemplos de adjuntos server-side que demuestran del porqué su uso es una mala idea:

```
<!--#include file="/etc/passwd">
<!--#exec cmd="rm -rf /&; cat /etc/passwd">
```

  El primer adjunto provee al atacante con los contenidos del archivo /etc/passwd, permitiéndole emprender un ataque de rotura de password. El segundo lanza un

proceso background que intenta borrar cada archivo escribible de la computadora. Luego provee al atacante de una copia de /etc/passwd.

Afortunadamente, los adjuntos se hallan por lo general deshabilitados por defecto.

Como regla general, no se debe permitir a los usuarios colocar scripts en el servidor a menos que un profesional calificado en seguridad haya leído personalmente los scripts y asegurado su inocuidad.

Cualquier script CGI puede ser ejecutado al requerir directamente al script URL; los atacantes no necesitan ir sobre la forma o emplear la interface que uno provee.

Tomar en cuenta lo siguiente:

- Si se crea una lista de selección, el valor que es retornado por el campo de entrada no necesariamente corresponde a los valores permisibles que se han definido.
- Si se especifica una longitud máxima para una variable, la longitud de la variable que es proveída al script puede ser significativamente más extensa.
- Los valores para variables que son proveídas pueden contener caracteres especiales.
- El usuario puede ver data que está marcada como "escondida".
- Si se emplea cookies o etiquetas especiales escondidas para mantener el estado del servidor, el script puede recibir cookies o etiquetas que nunca creó.

Una de las razones por la cual es sorprendentemente fácil crear un script CGI inseguro es que es muy dificil someter los scripts contra la amplia variedad de

clientes HTTP disponibles. Comprobar todos los valores que son proveídos al programa respecto a caracteres especiales y longitud apropiada.

Para asegurar no comprometer los scripts CGI, seguir lo siguiente:

- Configurar el Web Server de manera que todos los scripts CGI sean situados en un ùnico directorio (típicamente llamado cgi-bin).
- Emplear un programa tal como Tripwire para monitorear cambios no autorizados a estos scripts.
- Permitir acceso limitado a este directorio y sus contenidos. Los usuarios locales no deberán estar permitidos de instalar o remover scripts, o editar los scripts existentes sin revisión administrativa.
- Remover los archivos backup que son automáticamente generados por el editor. Por ejemplo, el editor Emacs deja archivos de extensiones tales como script_account~.
- Prevenir que los usuarios de red lean los contenidos de los scripts CGI. Esto mantendrá al atacante lejos de intentar analizar los scripts para descubrir errores de seguridad.
- Evitar el emplear el mismo directorio para almacenar documentos accesados tanto por FTP anónimo como por World Wide Web. El permitir el acceso FTP anónimo a los directorios HTTP da a los usuarios un medio para saltar las restricciones en acceso de documentos que el servidor Web pudiera estar proveyendo. Si un atacante descarga los scripts CGI via FTP, podrá buscar nuevas vias de ataque. Así mismo un usuario podría instalar un script via FTP para que corra en el servidor. El archivo /etc/passwd, presente para el servicio FTP, podría ser visible a alguien empleando el servicio WWW.

Existen otras muchas medidas que se pueden tomar para hacer más seguro el servidor. Por ejemplo, se puede limitar el empleo del ordenador de modo que sea solamente un servidor Web. Esto hará más difícil que un atacante quiebre el servidor, y si lo hace, limitará el daño causado en el resto de la red. En particular se puede escoger las siguientes opciones:

- Borrar todas las cuentas innecesarias.
- No exportar o montar ningún directorio por NFS.
- Borrar todos los compiladores.
- Borrar todas las utilidades que no son empleadas durante la inicialización o por el servidor Web.
- Proveer el menor número posible de servicios de red.
- No correr un servidor mail.

El servidor NCSA o el Apache permite colocar todas las restricciones de acceso global en un archivo simple llamado conf/access.conf. Los contenidos del mismo lucen como HTML. Por ejemplo, si se desea restringir el acceso a archivos de un directorio sólo para la red 209.58.61.*, se puede agregar las siguientes líneas al archivo access.conf:

```
<Directory /usr/local/etc/httpd/htdocs/special>
<Limit GET POST>
order deny, allow
deny from all
allow from 209.58.61.*
</Limit>
</Directory>
```

3.1.1.7.19 RPC, NIS y NIS+.- RPC, NIS y NIS+ fueron ampliamente responsables del éxito de Sun Microsystems como fabricante de computadoras: ellos hacen posible que cada usuario en una organización disfruta del poder y libertad de un sistema

dedicado, individual, mientras se ganaba los beneficios de emplear un sistema que era administrado centralmente.

El portmapper UNIX estándar asume que la seguridad será manejada por los servidores, sin embargo es mejor emplear el programa reemplazante portmapper de Wietse Venema, el cual tiene ingreso (logging) mejorado así como listas de control de acceso.

Por otro lado también se puede simplemente restringir el acceso a portmappers bloqueando los paquetes dirigidos a los puertos 111 sobre routers y firewalls.

El mecanismo de RPC permite que un programa corriendo en una computadora ejecute más o menos transparentemente una función que está realmente corriendo en otra computadora.

Cuando un servidor RCP inicia, éste dinámicamente obtiene un puerto TCP o UDP libre, luego se registra así mismo con el portmapper. Cuando un cliente desea comunicarse con un servidor en particular, contacta el proceso portmapper, determina el número de puerto empleado por el servidor y luego inicia la comunicación.

Existen varias formas diferentes de autentificación disponibles para RPC, a saber, AUTH_NONE, AUTH_UNIX, AUTH_DES y AUTH_KERB. AUTH DES o Secure RPC.

AUTH_NONE como su denominación reza no provee autentificación de usuario alguna. Debe ser empleada para servicios que proveen información no útil o crítica, como la fecha y hora. Las implicancias de seguridad saltan a la vista y es obvio evitar esta "autentificación".

AUTH_UNIX es el más empleado y es fundamentalmente inseguro. Cada petición RPC va acompañada con un UID y un juego de GIDs para autentificación. El servidor confia implícitamente en el UID y GIDs presentados por el cliente, y emplea esta información para determinar si la acción debiera ser permitida o denegada. Cualquiera con acceso a la red puede manipular un paquete RPC con valores arbitrarios de UID y GID. Obviamente, AUTH_UNIX no provee seguridad pues el cliente tiene libertad de aducir cualquier identidad, y no hay provisión de comprobación de parte del servidor.

AUTH_KERB es una modificación del sistema RPC de Sun que le permite interoperar con el sistema Kerberos del MIT para autentificación.

Secure RPC está basado en una combinación de criptografia de clave pública y criptografia de llave secreta.

Secure RPC representa un pequeño salto en seguridad respecto al estándar RPC de Sun. Sin embargo, Secure RPC no está libre de problemas:

- Cada cliente de red debe modificarse individualmente para uso por Secure RPC. Cada cliente que emplea un servicio de red debe tener especificado explícitamente y modificado individualmente para usar autentificación AUTH DES.
- Existe un costo en performance. El autentificador RPC debe ser descifrado empleando DES para verificar cada transmisión. Sobre transacciones NFS esta pena es de mayor consideración.
- Secure RPC no provee ni confidencialidad ni integridad de la data. Secure RPC autentifica el usuario mas no protege la data transmitida con encriptación o

firmas digitales. Es responsabilidad de los programas empleando Secure RPC en el encriptar empleando un algoritmo y una clave adecuados.

- Puede ser posible romper la clave pública. Cualquier pieza de información encriptada con el sistema de encriptación de clave pública de Diffie-Hellman empleada en RPC puede ser descifrada si un atacante puede calcular el algoritmo discreto de la clave pública.
- Puedes ser posible romper la llave secreta. La llave secreta de Secure RPC es encriptada empleando una clave DES de 56 bits y es hecha disponible públicamente sobre el servidor. Mientras las computadoras se tornan más veloces, la posibilidad de un ataque de fuerza bruta contra la clave secreta encriptada se hace más realidad.

Como análisis final, el empleo de Secure RPC provee mejor protección que otros enfoques, especialmente en máquinas multiusuarios. Desafortunadamente, como Secure RPC requiere del empleo de NIS o NIS+, esto genera desconfianza. Una ventaja se monta sobre una vulnerabilidad.

El Network Information Service (NIS) de Sun es un sistema de base de datos distribuído que permite a muchas computadoras compartir archivos de password, archivos de grupos, tablas de hosts y otros archivos sobre la red.

Cuando se configura un servidor NIS se debe especificar un dominio NIS. Es recomendable no emplear el dominio de Internet como dominio NIS, pues sería fácilmente adivinable. Las herramientas de hackers que intentan explotar errores en NFS o NIS prueban variaciones del dominio de nombre de Internet como dominio NIS antes de intentar otros ataques.

Los grupos de red (netgroups) NIS permiten crear grupos para usuarios o máquinas en la red. En el caso de organizaciones pequeñas, se podría crear simplemente dos grupos de red: uno para todos los usuarios y otro para todas las máquinas clientes. Estos grupos simplificarán la creación y administración de los archivos de configuración del sistema.

Existe errores de diseño en el código de las implementaciones de NIS que permiten a un usuario reconfigurar y engañar el sistema NIS. El spoofing se puede lograr por dos medios: engañar al sistema subyacente RPC, engañar al NIS.

Los clientes NIS obtienen información desde un servidor NIS a través de llamadas RPC. Un demonio local, ypbind, almacena la informaicón de contacto para el demonio servidor NIS apropiado, ypserv. El demonio ypserv puede ser local o remoto. Bajo ciertas versiones de SunOS se podía iniciar un programa que actuase como ypserv, lo que hacía que el atacante pueda proveer su propio archivo de passwords. Las implementaciones actuales de NIS proveen de una bandera –secure, la cual hará que el demonio ypbind no acepte cualquier información desde un servidor ypserv que no está corriendo en un puerto privilegiado.

Con el fin de prevenir la divulgación no autorizada de las bases de datos NIS se tiene:

- Emplear un firewall o router para no permitir paquetes UDP asociados a RPC. Desafortunadamente, debido a que RPC está basado en el portmapper, el puerto UDP real que es empleado no es fijo. En la práctica, la única estrategia segura es bloquear todos los paquetes UDP excepto aquellos especificados explícitamente.
- Otro enfoque es emplear el programa portmapper de Wietse Venema disponible libremente, el cual permite emplear una lista de ordenadores por nombre de host

o dirección IP que deberán ser permitidos o denegados de accesar a servidores RPC específicos.

- Algunas versiones de NIS soportan el uso del archivo /var/yp/securenets para servidores NIS. Este archivo puede ser usado para especificar una lista de redes que pueden recibir información NIS.

NIS+ fue diseñado para suplir las debilidades que NIS estaba empezando a mostrar en redes que crecían a miles de ordenadores, a saber:

- Los mapas NIS podían ser solo actualizados ingresando al servidor y editando archivos.
- Los servidores NIS podían ser solo actualizados en una operación batch única.
- Toda la información transmitida por NIS era transmitida sin encriptación, haciéndolo sujeto a espionaje.
- Las actualizaciones NIS mismas eran autentificadas empleando AUTH_UNIX.

Si es configurado apropiadamente, NIS+ puede ser un sistema muy seguro para autentificación y gestión de red. Sin embargo, como cualquier sistema de seguridad, es posible realizar un error en la configuración o en la gestión de NIS+ que torne a la red menos segura de lo absoluto. A continuación siguen recomendaciones a tomar en cuenta:

- No correr NIS+ en modo de compatibilidad NIS. Cualquier servidor NIS en la red tendría la habilidad de accesar cualquier pieza de información almacenada dentro del servidor NIS+. Típicamente, el acceso NIS es usado por atacantes para obtener una copia del archivo de passwords del dominio.
- Manualmente inspeccionar los permisos de los objetos NIS+ regularmente. Software para la comprobación de integridad de archivos no existe para NIS+.

En su ausencia, se debe inspeccionar manualmente las tablas, directorios y grupos NIS+ sobre una base regular.

- Proteger las computadoras donde los servidores NIS+ están corriendo. El servidor NIS+ es tan seguro como la computadora sobre la cual está corriendo.
- Asegurarse que los servidores NIS+ están operando en el nivel 2 de seguridad de los tres proveídos (autentificación de seguridad completa y control de acceso habilitado).

Existen varios problemas de seguridad básicos con NFS:

- NFS está construído en la cima de RPC, y en la mayoría de los casos emplea RPC para autentificación de usuario. A menos que una forma segura de RPC sea empleada, NFS puede ser fácilmente engañado.
- Aún cuando no sea usado Secure RPC, la información enviada por NFS sobre la red no está encriptada, y así está sujeta a monitoreo y espionaje.
- NFS emplea el sistema de archivos UNIX estándar para control de acceso, abriendo el sistema de archivos de red a muchos de los problemas que aquejan a un sistema de archivos local.

Recordar no exportar sistemas de archivos de retorno a la propia máquina si el portmapper RPC tiene proxy forwarding habilitado. No se deberá exportar las particiones al host local, por el nombre o por el alias localhost, y no se deberá exportar a ningún grupo de red en el cual el host es miembro. Si el proxy forwarding está habilitado, un atacante puede moldear cuidadosamente paquetes NFS y enviarlos al portmapper, el cual a su vez los direcciona hacia el servidor NFS. Como los paquetes provienen del proceso portmapper (el cual está corriendo como root), ellos

parecen venir de un sistema confiable. Esta configuración puede permite a cualquiera alterar y borrar archivos a voluntad.

Debido a que los archivos que un cliente monta aparecen en el sistema de archivos del cliente, un atacante que es capaz de modificar archivos montados puede comprometer directamente la seguridad del cliente.

El sistema primario que NFS emplea para autentificar servidores está basado en direcciones IP y nombres de hosts. Los paquetes NFS no son encriptados o firmados digitalmente en modo alguno. Así, un atacante puede engañar un cliente NFS bien presentándose como un servidor NFS o cambiando la data que está en curso entre un servidor y un cliente. De esta manera, un atacante puede forzar que una máquina cliente corra cualquier ejecutable montado por NFS.

A la hora de montar, el comando UNIX mount permite al sistema cliente especificar si archvios SUID serán tratados como tales en el sistema de archivos remoto. Esta capacidad es una de las razones del porqué el comando mount requiere de privilegios de root para ejecución. Si se proveyese facilidades para permitir que los usuarios monten sus propios sistemas de archivos, se deberá asegurar que la facilidad especifique la opción nosuid.

NFS puede también causar problemas de disponibilidad y performance sobre máquinas cliente. Si un cliente tiene un partición NFS montada y el servidor se torna indisponible, luego el cliente puede inmobilizarse hasta que el servidor NFS vuelva a hacerse disponible. Ocasionalmente, un servidor NFS dejará de operar y se reinicializará; los manejadores de archivos de los clientes NFS se tornaran inoperantes (stale). En este caso, se puede hallar imposible desmontar el sistema de

archivos NFS inoperante, y la única manera de retomar el curso es reinicializando la computadora cliente.

He aquí algunas directrices para hacer los clientes NFS más confiables y seguros:

- Asegurarse que la computadora es o un servidor NFS o un cliente NFS.
- En lo posible, no permitir que los usuarios ingresen al servidor NFS.
- No permitir que clientes NFS monten servidores NFS fuera de la organización.
- Minimizar el número de servidores NFS que cada cliente monta.
- En lo posible, deshabilitar el asignar archivos y dispositivos SUID en particiones montadas.

Existen muchas técnicas que pueden ser usadas para mejorar la seguridad NFS total:

- Limitar el uso de NFS limitando las máquinas sobre las cuales los sistemas de archivos son exportados, y limitar el número de sistemas de archivos que cada cliente monta.
- Exportar sistemas de archivos en modo de sólo lectura en lo posible.
- Emplear la pertenencia del root sobre archivos y directorios exportados. Establecer el modo 755 para programas y directorios, y 644 para archivos de data.
- Remover los permisos de escritura de grupo sobre archivos y directorios exportados.
- No exportar los ejecutables del servidor. Esto permite a un atacante determinar fácilmente la versión de cada ejecutable que el servidor está corriendo, lo cual le habilita de probar puntos débiles. Si existe un error en la configuración del

sistema, se puede exportar los binarios sobre un sistema de archivos escribible. Un atacante podría modificar los binarios propios del servidor y romper el sistema.

- No exportar directorios home. Un ataque simple consiste en que el atacante cree un archivo .rhosts en el directorio home de un usuario que específicamente permite acceso al atacante.
- Emplear el programa fsirand. El manejador de archivos de NFS empleado para referenciar un archivo consiste solamente de un ID, un número inode, y una cuenta de generación. Adivinar los dos primeros parámetros no es difícil. La dificultad viene en adivinar la cuenta de generación, sin embargo, para inodes importantes, se espera un valor muy pequeño. El programa fsirand incrementa la dificultad de adivinar un manejador de archivo válido haciendo aleatorio el número de generación de cada inode en un sistema de archivos.
- Configurar la variable portmon. Debido a que las peticiones NFS están supuestas a provenir de kernels de otras computadoras, y no de usuarios corriendo programas de nivel de usuario, una manera simple de mejorar la seguridad de los servidores NFS es programarlos para que rechacen peticiones NFS que no provienen de puertos privilegiados. En Solaris 2.5 se debe insertar la línea siguiente en /etc/system:

  set nfssrv:nfs_portmon =
- Emplear el comando showmount –e para verificar periódicamente que sólo se está exportando el sistema de archivos deseado a los hosts especificados con las banderas correctas.
- Emplear Secure NFS.

3.1.1.7.21 Recomendaciones.- A continuación siguen estrategias para proteger los servidores y la data:

- Emplear encriptación para proteger la data. Si es robada, la data no será de uso para el atacante. Además, cualquier modificación de la data que no se llegue a notar es dificil, sino imposible.
- Evitar autentificación basada en passwords y hosts.
- Emplear un firewall para aislar la red interna del mundo exterior.
- "Desconectar" la red interna del mundo exterior. Establecer redes específicas de estaciones que permitan el acceso Web, correo y otros servicios.
- Crear una segunda red interna para la información más confidencial.
- Deshabilitar todos los servicios que uno no está seguro de necesitar, y colocar wrappers sobre el resto para registrar las conexiones y restringir la conectividad.

Con el fin de monitorear la red, se puede emplear el comando netstat para listar todas las conexiones TCP/IP activas y pendientes entre la estación y cada otra estación externa. La salida del comando incluye el host y el número de puerto de cada extremo de la conexión, así como el número de bytes en las colas de recepción y transmisión. Si un puerto tiene un nombre asignado en el archivo /etc/services, netstat lo imprimirá en vez del número de puerto.

Una salida típica de netstat lucirá así:

```
localhost.32811      localhost.32773      32768      0  8192      0
ESTABLISHED
localhost.32773      localhost.32811       8192      0 32768      0
ESTABLISHED
localhost.32814      localhost.32773      32768      0  8192      0
ESTABLISHED
localhost.32773      localhost.32814       8192      0 32768      0
ESTABLISHED
svp1.32819           svp1.6000            32768      0  8192      0
ESTABLISHED
```

```
svp1.6000              svp1.32819             8192       0 32768       0
ESTABLISHED
```

Con la opción –a, netstat imprimirá también la lista de todos los sockets TCP y UDP sobre los cuales los programas están escuchando.

```
starfox% netstat -a -f inet
wsvil1.tacacs cTCI.telnet     974     0   9112  0   ESTABLISHED
wsvil1.41988 pelmob1.telnet   4096    0   0     0   ESTABLISHED
wsvil1.telnet  172.20.8.15.1060 8191 0   10192 0   ESTABLISHED
wsvil1.telnet  172.20.8.15.1069 8502 0   10192 0   ESTABLISHED
wsvil1.43049 pesfeb1.telnet   4096    0   9112  0   ESTABLISHED
wsvil1.telnet 172.20.8.10.4072 8299  0   8760  0   ESTABLISHED
wsvil1.80     cw1.4867        8760    0   8760  0   ESTABLISHED
```

Existe un número creciente de programas que pueden ser utilizados para examinar la red sobre problemas conocidos. Desafortunadamente, los atacantes pueden usar estas herramientas para examinar la red por vulnerabilidades. Así, sería bueno conseguirse estás herramientas y probarlas antes que el oponente lo haga. Herramientas conocidos a saber, tenemos SATAN, ISS y PingWare.

3.1.1.8 Wrappers y proxies.- Un wrapper es un programa que es empleado para control de acceso de un segundo programa. El wrapper literalmente enrolla (wrap) el segundo programa, permitiendo reforzar la seguridad del programa original.

El wrapper nació de la necesidad de modificar los sistemas operativos sin accesar el código fuente del sistema. Sin embargo, se ha convertido en un herramienta de seguridad bastante elegante por las siguientes razones:

- Debido a que la lógica de la seguridad está encapsulada en un solo programa, los wrappers son sencillos y fáciles de validar.
- Debido a que el programa sobre el cual se aplica el wrapper, permanece como una entidad separada, puede ser actualizado sin necesidad de certificar el programa que lo envuelve (wrapping it).

- Debido a los wrappers llaman al programa "envolvedor" vía la llamada de sistema estándar exec( ), un wrapper sencillo puede ser usado para controlar el acceso a una variedad de programas.

El Tcpwrapper, desarrollado por Wietse Venema, es una utilidad de fácil empleo que sirve para registrar e interceptar servicios TCP iniciados por inetd.

El Tcpwrapper ofrece entre otras cosas lo siguiente:

- Opcionalmente envía un banner al cliente conectándose. Los banners son útiles para mostrar mensajes legales o advertencias.
- Ejecutar una busqueda reversa de las direcciones IP, asegurándose que las entradas DNS para las direcciones IP y el nombre de host coincidan. Por defecto, tcp wrapper es compilado con al opción –DPARANOID, de modo que el programa automáticamente descartará la conexión entrante si los dos no se equiparan, bajo la suposición de alguien hackeando.
- Comparar el nombre de host entrante y el servicio requerido con una lista de control de acceso, para ver si el host o la combinación host-servicio ha sido explícitamente denegado. Si alguno es denegado, tcpwrapper suprime la conexión.
- Emplear el protocolo ident (RFC 1413) para determinar el nombre de usuario asociado con la conexión entrante.
- Registrar los resultados mediante syslog.
- Opcionalmente ejecutar un comando. Por ejemplo, se puede hacer que el tcpwrapper ejecute finger para obtener una lista de los usuarios en la computadora que está tratando de contactarse con uno.

- Pasa el control de la conexión al demonio real de red, o pasa el control a algún otro programa que toma medidas adicionales.
- Transferir ha un ambiente que funciona como trampa (jail) donde se estudia, con más tranquilidad, la actividad del usuario.

Para instalar el tcpwrapper se necesita decidir dónde colocar el programa tcpwrapper y dónde colocar los demonios de red reales. Se recomienda dejar los programas ejecutables donde actualmente se hallan, y modificar el archivo /etc/inetd.conf. La razón de esta recomendación es que el hacer cambios en la configuración del sistema claramente indicada en los archivos de configuración del sistema, es menos confuso que cambiar los nombres y/o ubicación de los programas del sistema. A largo plazo, esta opción es mucha más manejable. Esto es especialmente importante si los parches de los vendedores esperan encontrar los binarios donde se suponen deben hallarse.

Cuando una conexión entrante es manejada por tcpwrapper, el programa aplica las siguientes reglas:

- El archivo /etc/hosts.allow es buscado para ver si el par (host, protocolo) es permitido.
- Si no hay correspondencia, el archivo /etc/hosts.deny es consultado para ver si el par (host, protocolo) es denegado.
- Si no hay correspondencia, la conexión es permitida.

Cada línea sigue el formato:

```
daemon list    client host list      shell command
```

Se debe editar el archivo /etc/inetd.conf de modo que el programa tcpwrapper sea invocado por inetd para cada servicio del cual se quiere tener control y guardar registro.

Modificar el archivo /etc/inetd.conf es sencillo: simplemente cambiar el nombre de cada programa por la ruta absoluta del programa tcpwrapper, y editar el nombre de comando de cada programa de modo que refleje la ruta completa del demonio de red original.

Por ejemplo:

```
finger      stream  tcp nowait        nobody          /usr/etc/fingerd
fingerd
```

Será:

```
finger      stream  tcp nowait        nobody      /usr/local/bin/tcpd
/usr/etc/fingerd
```

Si se compila empleando la opción –DPROCCESS_OPTION, sólo el archivo /etc/hosts.allow será necesario desde que las palabras "allow" y "deny" son opciones según el nuevo formato:

```
daemon list : client_host list : option : option :
```

El siguiente archivo /etc/hosts.allow permitirá el uso de finger desde cualquier estación interna, y mostrará un mensaje a peticiones finger externas. Cualquier servicio solicitado desde la red pirate.net será denegado:

```
#
# /etc/hosts.allow:
#
# Allow anybody to connect to our machine except people from
pirate.net
#

in.fingerd : LOCAL : allow
in.fingerd : all : twist /usr/local/bin/external_fingerd_message
all   .pirate.net : deny
all : all : allow
```

3.1.1.9 Backups del sistema.- Errores, accidentes, desastres naturales y ataques al sistema no pueden ser predecidos. A menudo, a pesar de los mejores esfuerzos, ellos no pueden ser prevenidos. Pero si se tiene backups, se puede comparar el sistema actual y el sistema backed-up y se puede restaurar el sistema a un estado estable.

Existen dos escuelas de pensamiento respecto sobre qué tomar backup:

- Tomar backup de todo aquello único al sistema, incluyendo archivos de usuarios, bases de datos (tales como /etc/passwd y /etc/tty), y directorios importantes de sistema (tales como /bin y /usr/bin).
- Tomar backup de todo, debido a que la restauración de un sistema completo es más fácil que la de un sistema incompleto.

Es recomendable el segundo enfoque. A medida que transcurre el tiempo, programas son instalados en directorios reservados como /bin y /usr/bin, brechas en seguridad son descubiertas y parchadas, y otros cambios ocurren. Luego de un desastre, es más sencillo el proceso de recuperación cuando todo se halla en su lugar.

Existe tres tipos básicos de backups:

- Backup de día cero. Hacer una copia del sistema original. Cuando el sistema es instalado por vez primera, antes de usarla, tomar backup de cada archivo y programa en el sistema. Dichos backups pueden ser invalorables luego de una intromisión.
- Backup total. Hacer una copia de cada archivo de la computadora sobre el dispositivo backup. Este método es similar al backup de día cero, excepto que se hace regularmente.

- Backup incremental. Realiza un copia sobre el dispositivo de backup de sólo aquellos items en un sistema de archivos que han sido modificados luego de un evento particular (tal como la aplicación de un parche) o data.

Los backups totales e incrementales operan juntos. Una estrategia de backup común es:

- Hacer un backup total el primer día de cada semana.
- Hacer un backup incremental cada noche de todo aquello que ha sido modificado desde el último backup total.

Cuando se realice backups incrementales, emplear un juego rotativo de tapes. Idealmente, ejecutar un backup incremental cada noche, y tener un tape diferente por cada noche de la semana.

A lo menos una vez al año se deberá intentar restaurar completamente el sistema entero desde los backups, para asegurar que el sistema backup entero está funcionando apropiadamente. Empezar con una computadora desconfigurada diferente, observar si se puede restaurar todos desde los tapes y hacer que el nuevo ordenador opere. Es posible que el vendedor de la computadora pueda prestar o rentar una computadora con una configuración apropiada para realizar esta prueba.

Es necesario elaborar un índice o listado de nombres de archivos en los tapes de backup.

Los backups presentan un problema doble en la seguridad de red. Por un lado se tiene al tape backup completamente seguro: idealmente, está lejos del ordenador de modo que un desastre local no arruine a ambos. Por otro lado, el backup contiene una copia completa de cada archivo del sistema.

No debe almacenarse los tapes en el mismo ambiente que los ordenadores.

Luego que se ha removido un tape backup del drive, asegurar el dispositivo de protección contra escritura. Un tape protegido contra escritura no puede ser sobreescrito ni borrado por error.

El uso de encriptación reduce dramaticalmente el riesgo para tapes. Sin embargo, si se decide encriptar, asegurarse que la clave de encriptación es conocida por más de una persona.

Adicionalmente a la ejecución de backups rutinarios del sistema entero, se debe hacer copias separadas de archivos de sistema críticos regularmente. La tabla lista una serie de archivos a tomar en cuenta:

Nombre de archivo	Asunto crítico
• /etc/passwd	Cuentas nuevas
• /etc/shadow	Cuentas sin passwords
• /etc/group	Grupos nuevos
• /etc/rc*	Cambios en la secuencia de booteo del sistema
• /etc/ttys, /etc/ttytab o /etc/inittab	Cambios de configuración en terminales
• /usr/lib/crontab, /usr/spool/cron/crontabs/, o /etc/crontab	Nuevos comandos a ejecutarse regularmente
• /usr/lib/aliases	Cambios en el despacho de correo
• /etc/dfs/dfstab (SVR4)	Cambios en el sistema de archivos NFS
• /etc/netgroups	Cambios en los grupos de red

- /etc/vfstab (SVR4) Cambios en las opciones de montaje
- /etc/inetd.conf Cambios en los demonios de red

3.1.1.10 Ataques de denegación de servicio y soluciones.- Existe dos tipos de ataques de denegación de servicio. El primer tipo de ataque intenta dañar o destruir los recursos de modo que no se pueda emplearlos. El segundo tipo sobrecarga o fatiga algún servicio del sistema evitando que los usuarios accesen al mismo.

Casi todos los ataques destructivos pueden ser preveídos restringiendo el acceso a cuentas y archivos críticos, y protegiéndolos de usuarios no autorizados. Si se sigue una buena práctica en la protección de la integridad del sistema, también ser preveerá ataques de denegación de servicio destructivos. Por ejemplo, para evitar reformatear una partición del disco o la ejecución del comando newfs/mkfs se debe preveer el ingreso al modo de usuario único, proteger la cuenta de superusuario y fisicamente proteger contra escritura los discos empleados para solo lectura. Por otro lado para evitar el borrado de archivos críticos (como archivos de /dev y /etc) se debe proteger los archivo con modos apropiados (como 755 y 711), proteger la cuenta de superusuario y configurar con propiedad de root los archivos montados por NFS y exportar con solo lectura.

Los ataques de sobrecarga incluyen: sobrecarga de procesos, ataques al disco, problemas de espacio swap y del directorio /tmp.

En versiones modernas de UNIX, el usuario root puede aún detener el sistema con un ataque de proceso debido a que no hay límite en el número de procesos que él puede generar. Sin embargo, el superusuario puede también apagar la máquina o hacer "lo que le venga en gana", de modo que lo anterior no es nada nuevo.

Existe también la posibilidad que el sistema pueda alcanzar el número total de procesos permisibles debido a que demasiados usuarios han ingresado, aún cuando ninguno de ellos haya alcanzado su tope individual.

Otro posibilidad es que el sistema haya sido configurado incorrectamente. Puede que el límite de procesos por usuario sea igual o mayor que el límite de todos los procesos del sistema. En este caso, un solo usuario puede transtornar la máquina.

El tener demasiados procesos corriendo puede ser muy dificil de corregir sin rebootear el computador; hay dos razones de por qué:

- No se puede ejecutar el comando ps para determinar los números de proceso de los procesor a eliminar.
- Si no se es superusuario al corriente, no se puede emplear los comandos su o login debido a que estas funciones requieren la creación de un nuevo proceso.

Una manera de salvar lo segundo es emplear el comando shell exec para correr su sin tener que crear un nuevo proceso:

```
% exec /bin/su
```

Para elminar automáticamente todos los procesos y entrar a modo de usuario único cuando init muere, ejecutar:

```
# kill -TERM 1
```

Esto enviará una señal SIGTERM al proceso init.

Otro ataque común basado en procesos ocurre cuando un usuario origina muchos procesos que consumen grandes cantidades de CPU. La mejor manera de lidiar con estos problemas es educando a los usuarios sobre como compartir el sistema. Incitar el empleo del comando nice para reducir la prioridad de las tareas

background. También se puede emplear los comandos at o batch para retrasar la ejecución de tareas largas para una hora en que el sistema no esté atestado.

Respecto a los ataques sobre el disco, a veces éste repentinamente se llena cuando una aplicación o un usuario crea erróneamente demasiados archivos. Otras veces, los discos se llenan debido a que muchos usuarios incrementan lentamente el espacio usado.

El comando du permite encontrar los directorios en el sistema que contienen lo más de data. El comando find también ayuda a tal propósito. Por ejemplo para ubicar archivos de tamaño mayor a 100 bytes se tiene:

```
# find /usr -size +1000 -exec ls -l { } \;
-rw-r--r-- 1 root other 700528 Aug 21 1999
/usr/local/lib/expect5.28/
libexpect5.28.a
-rw-r--r-- 1 root other 700528 Aug 21  1999
/usr/local/lib/libexpect5.
28.a
-rw-r--r-- 1 root other 22675909 May  6 04:13
/usr/local/apache/logs/error_log
```

El comando quot (con la opción f) permite imprimir el número de archivos y el número de bloques usados por cada usuario:

```
# quot -f /usr/users
282818   1307  svplus
100972   2139  informix
38867    246   root
27560    3422  lponce
1166     41    mmacedo
```

Otra manera de hacer inutilizable el disco es consumiendo los inodes libre, de modo que archivos nuevos no puedan ser creados. El comando df con la opción -i informa sobre el número de inodes libres:

```
svp1# df -o i /usr/users
Filesystem          iused   ifree      %iused  Mounted on
/dev/dsk/c0t0d0s6   7383    1000489    1%      /usr/users
```

El número de inodes en un sistema de archivos es usualmente fijado a la hora del formateo inicial del disco. La única manera para reestructurar la disposición de inodes es salvando el disco en tape, reformatear con más inodes y restaurar los contenidos.

Una mejor manera de proteger el sistema contra ataques al disco es empleando el sistema de quotas. Con ellas, cada usuario puede tener asignado un límite para el número de inodes y bloques de disco que el usuario puede emplear. Existe dos tipos de quotas:

- Quotas rígidas son límites absolutos.
- Quotas suaves son advertencias. Se permite a los usuarios sobrepasarse por un período de gracia de varios días, luego de los cuales el usuario ya no está permitido de crear más archivos sin primero reducir el uso corriente.

Versiones de UNIX como Solaris 2.5.1 soportan una protección adicional contra el llenado de disco: el sistema de archivos reserva aproximadamente el 10% del disco y lo hace inutilizable para usuarios regulares. La razón para esta reserva es performance, y adicionalmente evitar sobrecargar el disco. El comando tunefs permite manipular este parámetro.

Los archivos abiertos no ligados continúan ocupando espacio hasta que son cerrados. El espacio que estos archivos ocupan no aparece con los comandos du o find debido a que no están en el árbol de directorio. Para recuperarse de está situación es necesario eliminar el proceso que mantiene el archivo abierto. Si no se logra ubicarlo se deberá matar todos los procesos y luego observar la consistencia del sistema de archivos mediante fsck, por ejemplo. Existe un programa de nombre lsof

para este fin específico (aparte de otros): identifica los procesos que tienen archivos abiertos y la posición del mismo.

La mayoría de sistemas UNIX son configurados con algo de espacio de disco para ser empleado como memoria en procesos cuando estos se ven escasos de memoria. Cuando el sistema no está configurado con espacio swap suficiente, luego los nuevos procesos, especialmente los extensos, no correrán debido a que no hay espacio swap para ellos.

Si un atacante malicioso ha llenado el espacio swap, la solución más rápida es identificar el proceso maligno y eliminarlo.

El directorio /tmp normalmente está configurado para que cualquier usuario pueda crear archivos sobre él. Consecuentemente, un usuario podría llenar la partición haciendo imposible que otros usuarios creen nuevos archivos. Citamos un para de maneras de minimizar el ataque sobre el directorio /tmp:

- Establecer quotas en /tmp de modo que un único usuario no pueda llenarlo. Una cuota recomendable es de 40%, de manera que más de dos usuarios lo llenarían en el peor de los casos.
- Tener un proceso (script) que monitoree /tmp regularmente y alerte al administrador de su capacidad.

Los ataques DoS de red incluyen: sobrecarga del servicio, inundación de mensajes (message flooding) y creación de conexiones semiabiertas (clogging).

La sobrecarga del servicio ocurre cuando torrentes de peticiones de red son hechos a un demonio servidor en un ordenador. Desafortunadamente es poco lo que un administrador puede hacer respecto de los protocolos y demonios para que el sistema sea más robusto. Lo primero es particionar la red local en subredes, así si

una subred es inundada como parte de un ataque o accidente, no todas las estaciones serán deshabilitadas. Otra acción es el monitoreo del tráfico de red. Es recomendable elaborar una lista con las direcciones fisicas de las estaciones cliente normales. Respecto a los servicios ofrecidos por inetd, si muchas peticiones son recibidas, éste empezará a rechazarlas y enviará un mensaje syslog anunciando que el servicio está fallando.

La inundación de mensajes ocurre cuando se realizan múltiples peticiones, cuyas respuestas consumen recursos. De este tipo es la tormenta de broadcast. Manipulando mensajes de red, se puede crear un mensaje especial que instruye a cada ordenador a responder o transmitirlo. Los broadcast storm pueden suceder por errores de hardware o software, intencionales o accidentales. Contra esto la estrategia recomendada es el monitoreo y la división de la red en subredes.

Finalmente se tiene el clogging, el cual consiste en generar conexiones TCP desde estaciones fantasma y por ende no concluídas. El servidor responde a estaciones no existentes o inalcanzables. Los parches disponibles por los fabricantes permiten limitar el número de conexiones semiabiertas y el tiempo de permanencia en tal estado. Es obviamente necesario limitar lo anterior también en el firewall.

3.1.2 Firewall del NOC.- Tradicionalmente, los firewalls son situados entre una organización y el mundo exterior. Pero una red corporativa también necesitará firewalls internos para aislar dominios de seguridad (security domains). Un dominio de seguridad es un juego de máquinas bajo un control administrativo común, con una política de seguridad y nivel de seguridad comunes. La red interna del NOC resulta ser un dominio de seguridad.

La red interna del NOC se compondrá de estaciones de gestión UNIX (servidores y workstations) y estaciones Windows que formarán parte de la red corporativa. Es decir, la red interna del NOC se divide en: red de administración (de equipos) y red corporativa.

El firewall del NOC deberá cumplir lo siguiente:

- Denegar servicios TCP/IP vulnerables (aquellos especificados en la sección "De la seguridad de los servicios de red").
- Asegurar la protección de las estaciones UNIX y su conectividad sólo dentro de la red de administración.
- Asegurar la protección de las estaciones Windows y su conectividad sólo dentro de la red corporativa.
- Restringir el número y tiempo de conectividad de sesiones TCP.

Tanto la red de administración como la corporativa estarán en el rango de redes privadas. Ellas no deben translaparse. Las estaciones Windows emplearán translaciones NAT dinámicas para accesar el exterior.

Por defecto el firewall PIX de Cisco excogido, deniega todas las peticiones entrantes (permite las conexiones entrantes pertenecientes a sesiones establecidas), por consiguiente se especificará los servicios permitidos a ser requeridos por el

exterior, a saber, TACACS+, Syslog, SNMP, etc. Las estaciones UNIX no emplearán NAT y no podrán ser accesibles (es bueno recalcarlo) por Telnet, FTP, mail o Web.

El firewall será administrado mediante TACACS+ y sus mensajes syslog enviados al servidor Syslog.

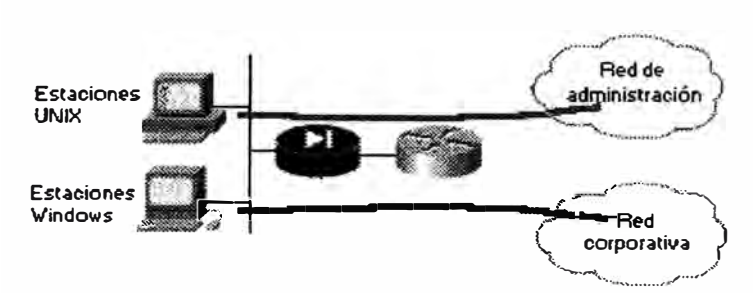


Figura 3.2: Firewall del NOC

3.2 Privilegios de acceso de los usuarios sobre los equipos de red

La mejor manera de ofrecer acceso a los usuarios es desde una plataforma centralizada. Entre sus ventajas se tiene escalabilidad, simplicidad y rápido troubleshooting.

Otro enfoque es el configurar los usuarios sobre cada equipo de comunicación. La dificultad que aparece es el manejo flexible de los mismos: actualizaciones, adiciones, modificaciones y eliminaciones de cuentas.

La plataforma empleada para la administración centralizada es el protocolo TACACS+. Este servidor se ubicará en la red del NOC y deberá manejar el acceso de los siguientes equipos:

- Firewall del NOC.
- Switch y routers del core.
- Routers de las sucursales.
- Firewalls de la red corporativa.

- Router del acceso remoto.

El router remoto del acceso dial a través del Internet (IPSec sobre túnel) no tendrá configurado TACACS+ debido a la lentitud ofrecida. Este tendrá configurado usuarios con diferentes niveles de privilegio. El de mayor privilegio será manejado por el NOC.

La comunicación (conectividad) de los equipos de telecomunicación con el servidor TACACS+ será exclusivamente sobre la red privada de administración.

Cuando el servidor TACACS+ se deshabilite o cuando se pierda conexión con el equipo, éste manejará un password de último recurso que deberá modificarse periódicamente.

El servidor TACACS+ será administrado por el Ingeniero de Seguridad de Red de la corporación; sólo él podrá configurar TACACS+ sobre los equipos (que al fin y al cabo se realiza una única vez, el resto es desde el servidor central) y tendrá configurado los siguientes usuarios:

- Usuarios de acceso privilegiado: pertenecerán a usuarios reales que podrán monitorear y configurar el equipo. Son usuarios permanentes y sus passwords deberán modificarse sobre una base regular (cada 3 meses).
- Usuarios de acceso restringido: pertenecerán a usuarios ficticios cuya función principal es la toma de backups de las configuraciones de los equipos de telecomunicación. Aún cuando sólo puedan monitorear deberán modificarse sobre una base regular (cada 4 meses por ejemplo).
- Usuario de acceso eventual: éste deberá configurarse o habilitarse sólo cuando se requiera el apoyo externo del servicio de asesoría técnica del fabricante de

equipos, en nuestro caso, el TAC (Technical Assistance Center) de Cisco Systems.

El demonio servidor (tacacsd) deberá ejecutarse con derechos de superusuario. El log del TACACS+ deberá protegerse como se especificó según la sección "Seguridad del NOC" (auditoría y logging).

Los routers Series 7200VXR, 2600 y 1600, y switches Catalyst 2924 y 5509 empleados en el diseño soportan TACACS+. El factor preponderante para que fuese preferido frente a Kerberos fue su log detallado (accounting), sobretodo por el registro de comandos de configuración y perfiles de usuario.

TACACS+ encripta el tráfico entre el equipo y el servidor mas no entre el equipo y el terminal remoto, por eso la sesión Telnet es encriptada empleando IPSec.

3.3 Confidencialidad de la data en el transporte. Encriptación

La principal función de la encriptación es hacer ininteligible la información que fluye por un circuito en el caso de espionaje. La encriptación dentro del campus corporativo será realizada por routers empleando IPSec. Lo ideal es encriptar la información, sinónimo de hermetismo completo; sin embargo, la encriptación consume recursos de memoria y CPU que si son abusados decrementan el performance del router. Otro factor importante es el costo económico. Las oficinas remotas tienen proyectadas routers de acceso Cisco 1600 y 2600, no ideales para aplicaciones de encriptación pesadas. El costo de emplear routers de mayor performance, como Cisco 7200 o 7500, supera con creces la probabilidad de riesgo ante la falta de encriptación.

El único servicio crítico a encriptar será el acceso por Telnet desde el NOC hacia los equipos de telecomunicaciones (desde el firewall del NOC hacia los routers centrales y remotos).

Otros servicios que podrían ser encriptados podrían ser el FTP y el SNMP. Debido al polling SNMP constante es mejor obviar éste. Por otro lado respecto al TFTP, el flujo de tráfico TFTP no representan un riesgo sino más bien la protección de la imagen residente en el servidor del NOC.

3.4 Integridad y control de conectividad

Es importante brindar integridad dentro del campus corporativo a nivel del grupo de trabajo. La serie de switches Catalyst 2900 y 5509 de Cisco puede emplear seguridad en los puertos para bloquear la entradas en un puerta Ethernet, Fast Ethernet o Gigabit Ethernet cuando la dirección MAC de la estación intentando accesar al puerto es diferente de la direcciones MAC especificadas para dicho puerto. Los puertos deben ser configurados en modo shutdown de modo que se deshabiliten permanentemente al detectar una violación; así mismo el switch debe enviar un trap SNMP hacia la estación de gestión. La dirección MAC del puerto puede ser configurada estáticamente o aprendida al inicio de la conexión.

3.5 Disponibilidad de red. Redundancia

Dentro del campus corporativo debido al acceso en tiempo real sobre los servidores centrales mediante aplicaciones interactivas, se debe asegurar la conectividad contínua de las oficinas remotas con el core.

La redundancia comprende:

- Dos routers de core: principal y secundario.
- Un switch de core o principal.

- Dos circuitos ATM desde el local remoto hacia los routers de core.
- Un enlace ISDN backup desde el local remoto hacia el router de core secundario.
- Dos circuitos de alimentación separados para los routers/switches primario y secundario.

La redundancia entrará a tallar en los siguientes casos:

- Cuando falle el router de core primario deberá entrar en funcionamiento el router de core secundario.
- Cuando fallen los circuitos ATM del local remoto deberá entrar en funcionamiento el circuito ISDN.

El dial backup será disparado desde las oficinas remotas empleando la característica DDR (dial-on-demand routing) de Cisco. En el caso que el dial backup opere y deje de fluir tráfico interesante (el que mantiene vivo el backup) las llamadas serán terminadas por los locales remotos.

En cuanto al diseño lógico se tiene las siguientes consideraciones de diseño:

- Deshabilitar la autosumarización EIGRP.
- Los enlaces ISDN emplearán un direccionamiento IP distinto del campus corporativo.
- CHAP será el método de autentificación sobre PPP empleado.
- Interfaces dialer ISDN serán empleadas y asignadas a interfaces fisicas BRI sobre el router remoto.
- El protocolo de enrutamiento dinámico será EIGRP debido a su rápida convergencia y gran flexibilidad y simplicidad de configuración.

- Las rutas estáticas serán redistribuídas.
- Los routers de core principal y secundario publicarán una ruta default (hacia el Internet, exactamente hacia el firewall de la red corporativa) sobre los routers sucursales. La ruta del router principal será de mayor peso que la del router secundario (menor distancia administrativa)
- Los routers remotos tendrán configurados una ruta por defecto de menor peso que aquellas aprendidas (redistribuídas) desde los routers de core. Esta es la ruta hacia la puerta ISDN backup.
- La interface LAN de los routers remotos no deberá publicar updates EIGRP.
- Existirá una red aparte que comunicará los routers centrales. Su misión se entiende en el caso que los circuitos ATM dejen de operar. A través de ella los routers principal y secundario publicarán que para llegar a los locales remotos remotos es necesario reenrutar hacia la interface ISDN del router secundario donde se halla la plataforma ISDN. De lo anterior se tiene que ambos routers de core tendrán configuradas rutas estáticas que apunten con distancia administrativa alta (pues la mejor ruta es aquella aprendida por EIGRP) hacia las LANs remotas.
- Para nuestro diseño el filtraje de rutas permite reducir la tabla de enrutamiento y aprender estrictamente lo necesario. Se tiene que los routers centrales bajo operación normal sólo deberán publicar la ruta por defecto y deberán sólo aprender los updates EIGRP de los locales remotos referentes a la LAN.
- Apaciguar interfaces (fisicas o virtuales) no participantes del proceso EIGRP.

La redistribución permite propagar información de enrutamiento aprendida via un protocolo de enrutamiento dentro de otro protocolo de enrutamiento, filtrando y haciendo ajuste de métricas de por medio.

Se empleará autentificación MD5 entre routers para evitar que formen nuevas adyacencias e intercambien información de enrutamiento (paquetes EIGRP falsos) con un dispositivo no confiable. La autentificación MD5 de EIGRP confía exclusivamente en un secreto compartido, el cual debe ser periódicamente cambiado. Este cambio puede ser automatizado empleando un script Expect, recordando que el acceso por Telnet está encriptado. MD5 es una algoritmo descrito en el RFC 1321 que toma un mensaje y genera 128 bits como huella digital.

3.6 Protección contra ataques de red

Una multitud de tipos de ataques pueden hacer colapsar una red. Muchos pueden ser evitados o detenidos mediante características que han sido específicamente diseñadas para ataques bien conocidos.

Aún cuando es muy dificil realmente reconocer paquetes spoofed o falsificados, algunos mecanismos son empleados para prevenirlos. Algunos de estos paquetes pueden ser causados por simples desconfiguraciones y lazos de enrutamiento. La red corporativa emplea un rango de direcciones privadas especificadas por el RFC 1918. El resto de direcciones deberá ser explícitamente denegados.

Es casi imposible detener un ataque de inundación TCP SYN. Lo que se puede hacer es constreñir su impacto en partes críticas de la red. Los firewalls y routers presentar una característica contra este ataque. El dispositivo chequea la conexión TCP entrante y responde en lugar del dispositivo final para asegurar que la

petición es válida antes de conectarse al servidor o destino. Luego que el dispositivo ha establecido una conexión genuina con el cliente y el servidor, une estas dos conexiones en una sesión fuente/destino única. El dispositivo, caso de peticiones vagas, puede ser configurado para establecer timeouts sobre conexiones semiabiertas; también tiene parámetros para establecer niveles umbrales para el número de peticiones entrantes y salientes.

Como medidas generales, en routers y firewalls es necesario:

- Deshabilitar el servicio finger.
- Eliminar los mensajes ICMP redirect.
- Deshabilitar el proxy ARP empleado para responder peticiones para sistemas que no pueden responder por sí mismos.
- Deshabilitar el protocolo MOP (Maintenance Operation Protocol).
- Descartar mensajes ICMP unreachables.
- Restringir el acceso por Telnet para sólo estaciones autorizadas del NOC.
- Deshabilitar broadcast directos (ataque SMURF).
- Deshabilitar mensajes ICMP source routing.

3.7 Bases de datos centrales

Respecto a las bases de datos centrales, ellas serán ubicadas en el switch del local principal (Cisco Catalyst 5509). Este switch como se verá deberá conectarse a ambas routers centrales del campus corporativa, despues de todo, el router secundario justamente cumple una función de redundancia.

La cuestión que surge es cómo hacer que el switch o mejor dicho las estaciones que se conectan a él, distingan como default gateway entre el router principal y secundario cuando uno de ellos está activo. La estaciones usualmente no

participan en los protocolos de enrutamiento y están configurados estáticamente con una única dirección IP como ruta por defecto. Así una vez que las estaciones pierdan comunicación con el router principal no habrá manera de que redireccionar su ruta por defecto al router secundario.

Una solución a lo anterior es emplear IRDP, ICMP Router Discovery Protocol, para encontrar un nuevo router cuando una ruta se halla inalcanzable. Una estación que corre IRDP escucha los mensajes multicast hello de su router configurado y emplea un router alternativo cuando deja de recibir dichos hello.

Para hosts que no soportan IRDP, HSRP (Hot Standby Routing Protocol) de Cisco ofrece una vía de mantener la comunicación cuando un router se torna inalcanzable. HSRP permite a dos o más routers HSRP, emplear la dirección MAC y la dirección IP de un router virtual. El router virtual no existe fisicamente; en su lugar, representa el objetivo común para routers que son configurados para proveer backup uno al otro. Por consiguiente, las estaciones serán configurados con la dirección IP del router virtual como default gateway.

3.8 Logging y auditoría

Todos los equipos de telecomunicaciones tienen configurados la opción de logging, la cual envía los mensajes Syslog al servidor para este fin. Cada equipo cuenta con un buffer interno que sirve como logging local.

Es importante mencionar la sincronización que debe existir en la red. El protocolo NTP asegura que los equipos compartan el mismo reloj, imprescindible a la hora de realizar auditorías y respuestas antes incidentes.

El logging implica la seguridad del servidor Syslog, específicamente de sus archivos de registro.

Se deberán elaborar auditorías llevadas a cabo por personal de la corporación o externos para evaluar la seguridad interna. Ha de aprovecharse el equipo de detección de intrusos descrito en el capítulo IV, si bien su ubicación permante es aquel de interconexión con el Internet. La figura muestra la disposición de dos escenarios de prueba.

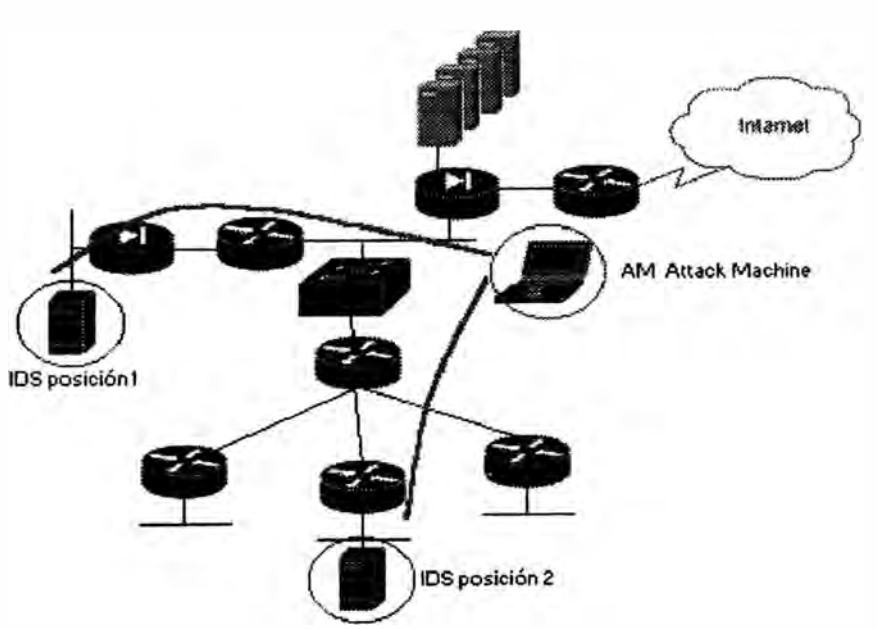


Figura 3.3: Escenarios de ataques de prueba dentro del campus corporativo

CAPITULO IV
PROYECTO DE DISEÑO DEL SISTEMA DE SEGURIDAD DEL ACCESO AL INTERNET DE LA RED CORPORATIVA

El presente capítulo explica la arquitectura del acceso al Internet escogida y las características de seguridad que serán soportadas por ella.

4.1 Arquitectura del acceso al Internet

La arquitectura de acceso al Internet más común es aquella que situa un dispositivo entre el Internet y el campus, tal como un router examinador, con capacidades de firewall limitadas.

En el capítulo I fueron mencionadas arquitecturas empleando proxy y bastión host. Este último generalmente va acompañado de un router examinador (packet-filter) y cumple, si analizamos la función del bastión host, cierta función de proxy.

La arquitectura escogida fue aquella de un firewall sólido junto a un router examinador. Desde que el firewall elegido fue un PIX Cisco, las habilidades de cut-through proxy están disponibles.

El firewall PIX fue escogido frente a otras plataformas por su gran versatilidad en el manejo del número de conexiones. Se trata pues de un sistema (hardware) propietario dedicado, que no depende de un sistema operativo necesario para soportar aplicaciones de servidor.

El router examinador externo actúa como filtro de primer nivel para permitir o denegar tráfico entrando del Internet hacia el campus corporativo. En esencia, un router de "screening" puede permitir o denegar un servicio, pero no puede proteger contra operaciones individuales dentro de un servicio. Este valida la mayor parte del tráfico antes de pasarlo al firewall.

El firewall luego provee la función que requiere más procesamiento, la inspección paquete por paquete. Por defecto, el PIX previene todas las conexiones externas del Internet de accesar los hosts o servidores corporativos internos. Habrá que ser explícito sobre los servicios internos. Adicionalmente las funcionalidades que serán explotadas serán la autentificación de la aplicación, encriptación y NAT.

El firewall cuenta con tres interfaces: una hacia el Internet, una hacia el campus y otra hacia la granja de servidores (DMZ).

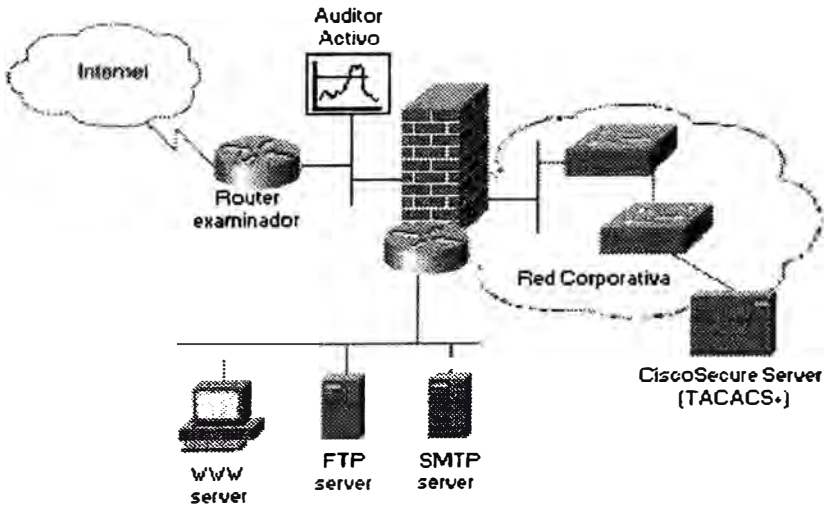


Figura 4.1: Arquitectura empleando router examinador y firewall

4.2 Filtraje de paquetes y DMZ

La red corporativa entera constituye un dominio de seguridad y como tal deberá ser protegida del mundo exterior.

Tanto el router como el firewall aplicarán filtraje de paquetes. El filtraje de paquetes opera descartando paquetes basado en sus direcciones o puertos fuente o destino. El administrador realiza una lista de las máquinas y servicios aceptables y una lista "negra" de máquinas y servicios inaceptables.

La mayoría de políticas de seguridad requieren control más fino que esto; ellas necesitan definir el acceso a servicios específicos para hosts que de otro modo son desconfiables. El filtraje de paquetes ofrece cierto control a este nivel, pero es un proceso peligroso y sujeto a error. Para operarlo correctamente se requiere conocimiento íntimo de la utilización de los puertos TCP y UDP en un número de sistemas operativos. Si un servicio deseable tiene operaciones inseguras, o si el servicio está normalmente proveído sobre un servidor inseguro, el filtraje de paquetes solo no podrá protegerlo.

La configuración de un filtro de paquetes es un proceso de tres etapas. Primero, por supuesto, se debe saber que debería ser y no debería ser permitido. Esto es, se debe tener una política de seguridad. Luego, los tipos de paquetes permitidos deben ser especificados formalmente, en términos de expresiones lógicas de los campos del paquete. Finalmente, las expresiones deben ser reescritas en la sintaxis del equipo.

La política de seguridad de la red corporativa a diseñar se especificará en el capítulo VI de implementación.

La filosofia a seguir es: todo lo que no está expresamente permitido está prohibido. Por otro lado, todas las sesiones iniciadas desde el interior están permitidas (se suponen confiables).

A lo menos tres servicios mayores no son bien manejados por filtros de paquetes: FTP, X11 y DNS. El problema con FTP ya fue mencionado en los capítulos II y III: debido a que la transferencia de data es iniciada desde el servidor éste puede ser manipulado como un port-scanner (empleando la opción PORT); es decir, la regla de que el servicio es "iniciado" por el cliente ya no se cumple. Yendo más al detalle ya no sería posible diferenciar paquetes entrantes pertenecientes a sesiones establecidas desde estaciones internas.

El problema con X11 es similar al del FTP en cuanto a que el uso debido requiere de una llamada entrante. Esto es, la visualización –pantalla, teclado y ratón- es un servidor; las aplicaciones X11 se conectan a ella via TCP. Si las aplicaciones son ejecutadas en estaciones externas, la conexión hacia el servidor implica una llamada hecha desde el exterior, lo cual es bloqueado por una política de seguridad típica. Una recomendación usual es bloquear cualquier llamada entrante a los números de puerto 6000 a 6100, a lo menos. Existe un efecto secundario: si se bloquea todo el tráfico a estos puertos, en vez de las llamadas entrantes, se corre el riesgo de estropear programas clientes que escogen aleatoriamente estos puertos. Por otro lado, cabe mencionar que la ejecución de una aplicación en una máquina interna desde el exterior implica una llamada saliente, lo cual normalmente no es problema. Sin embargo, las características del servidor X11 hacen esto algo peligroso. El compromiso de un servidor interno afecta obviamente la seguridad de su alrededor.

Respecto al DNS, supondremos una red corporativa que no posee un DNS propio. Este es aquél proveído por el ISP. Los problemas referidos al DNS implican desconcordancia entre hostname y direcciones IP (double-reverse lookups), intentos no autorizados de transferencias de zonas, revelación de demasiada información y respuestas vagas a peticiones DNS. Las dos primeras escapan del ámbito administrativo de la red corporativa y su seguridad es manejada por el ISP (deberá ser exigida y garantizada en todo caso). La revelación de información depende claro está de la data proveída al ISP respecto al dominio de la red. Respecto a lo último, las respuestas vagas afectan aplicaciones dependientes del hostname como mecanismo de autentificación (como rlogin).

Los filtros aplicados a la salida del router pueden incrementar la eficiencia, desde que la búsqueda y la aplicación de la regla del filtro pueden a menudo ser combinadas con la búsqueda en la tabla de enrutamiento. Por otro lado, cierta información ha sido descartada, como el saber la interface física donde el paquete arribó. Esto es especialmente importante a la hora de preveer ataques spoofing. El filtraje en la entrada puede proteger al router mismo del ataque.

Una función distintiva del router examinador es la ejecución de filtros anti-spoofing, denegando paquetes falseados provenientes del exterior con direcciones fuentes en el rango de la red corporativa. El firewall también cumple esto, pero no puede decir si los paquetes que claman ser de la red DMZ son falseados.

La zona perimetral o DMZ es un buffer entre la red corporativa y el mundo exterior. Los servicios públicos, como correo, FTP y servidor Web tiene su lugar allí. La DMZ posee un número de red único que es diferente del número

de red corporativo. Solo la DMZ resulta visible desde el exterior. El firewall PIX de Cisco asigna un valor número a cada una de las tres interfaces y especifican un nivel de seguridad (que va de 0 a 100). El comportamiento es como sigue:

- El tráfico que va desde una interface con un mayor nivel de seguridad hacia una interface destino con menor nivel de seguridad: Permitir todo el tràfico basado en IP a menos que estè restringido por listas de acceso, autentificación o autorización.
- El tráfico que va desde una interface con un nivel menor de seguridad hacia una interface destino con mayor nivel de seguridad: Descartar todos los paquetes a menos específicamente permitidos por el comando conduit. Se necesita implementar restricción adicional si se emplea autentificación y autorización.
- Tráfico yendo de un interface con el mismo nivel de seguridad que la interface destino: No hay comunicación entre las dos redes.

Adicionalmente el PIX ofrece protección contra el ataque SYN, ataque de fragmentación, filtraje Java, juego seguro de comandos SMTP.

La configuración propuesta es similar a la arquitectura de subred examinadora (subnet screened architecture, "Building Internet Firewalls" de Brent Chapman y Elizabeth Zwicky), donde el router interior y exterior se mezclan, conservando la red perimetral. Un hacker deberá primero lidiar con el software Cisco IOS del router examinador, y luego, en caso de éxito, enfrentarse al PIX.

4.3 Network Address Translation

Los slots de translación dinámicos son útiles para estaciones que no necesitan direccciones constantes en el Internet. Hosts internos con direcciones IP no registradas en el NIC (Network Information Center) pueden accesar directamente el Internet empleando software TCP/IP estándar. No se requiere software cliente especial. El PIX soporta NAT para asignar una dirección globalmente única para cada host interno, y PAT para compartir una sola dirección globalmente única para hasta 64000 hosts accesando simultáneamente.

Otro tipo de translación de direcciones es la translación estática. Esto es útil para máquinas internas que necesitan ser direccionadas desde los gateways exteriores en el Internet; por ejemplo, un servidor Web.

Para nuestro diseño de red, todas las estaciones internas accesarán al Internet empleando NAT. Los servidores en la DMZ serán direccionados con NAT estático.

NAT es a menudo visto falsamente como una característica de seguridad. NAT fue originalmente creado para ayudar a resolver el problema de una corporación extensa al tener que renumerar sus miles de estaciones al conectarse al Internet con una dirección ilegal. La manera en que NAT sirve como una característica de seguridad es que nadie sabe la dirección IP corporativa interna traducida en una dirección legalmente válida.

4.4 Redundancia de firewalls

La protección de los servicios incluye que estos no se vean degradados o se tornen indisponibles sin autorización o por accidente. El servicio del Internet es imprescindible para el contacto con el mundo exterior. Su ausencia implica aislamiento.

La redundancia de firewalls busca no solo reponer, obviamente, el servicio del Internet (para su uso en nuestro caso), sino ser una redundancia nuevamente invulnerable y automática.

La instalación y configuración iniciales hacen que la unidad activa automáticamente descargue su configuración sobre la unidad stand-by.

Ambos PIX deben tener idéntica configuración. Los comandos ingresados en la unidad activa son automáticamente replicados en la unidad stand-by. Si se editan cambios en la unidad stand-by, ésta muestra una advertencia y no actualiza la unidad activa.

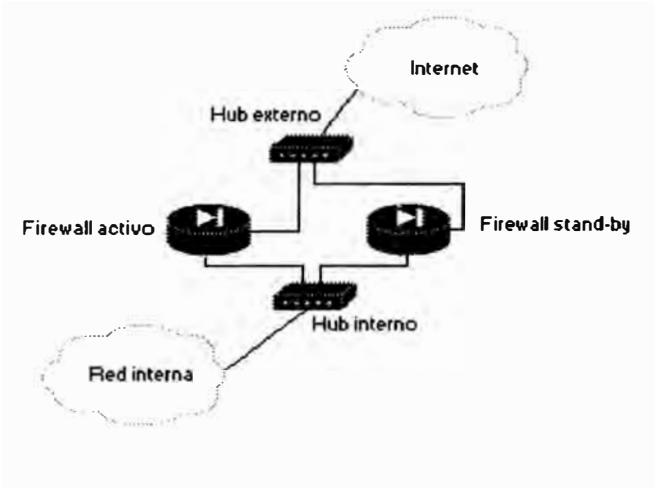


Figura 4.2: Redundancia del firewall

La configuración anterior muestra el uso de hubs en vez de switchs para saltar los problemas por reconocimiento de direcciones MAC ligadas a direcciones IP.

4.5 Auditoría: monitoreo, logging y detección de intrusos.

La función de auditoría asegura que la infraestructura de red esté configurada como se esperaba (hablando desde el punto de vista de la seguridad).

La función de logging se relaciona estrechamente con aquella de monitoreo. Se busca monitorear el uso del sistema y patrones de tráfico para ayudar a determinar el comportamiento normal. Todos los equipos deberán estar configurados para enviar sus mensajes log al servidor Syslog del NOC. Este se convertirá en un punto de fallo único de allí la importancia de su protección, abarcada en la sección "Seguridad de las estaciones del NOC".

La auditoría implica generar:

- Topología de la red al corriente
- Identificar los servicios en las estaciones
- Desarrollar escenarios de prueba ("what-if") para detectar problemas de filtraje
- Ejecutar escenarios de ataques simulados para hallar vulnerabilidades

Existe herramientas en el mercado para realizar intrusiones y medir la seguridad de la red, a saber, CyberCop Scanner de Network Associates, IIS Internet Scanner, NetSonar de Cisco, entre otros.

Su contraparte, el sistema de detección de intrusos, debe cumplir las siguientes características:

- Debe correr contínuamente sin supervisión humana.
- Debe resistir ataques, es decir, tener la capacidad de monitorearse a sí mismo y detectar ataques a él.
- Debe suponer mínimo overhead en el sistema

El sistema IDS NetRanger de Cisco, se compone de un equipo Director y otro Sensor. El director muestra eventos, monitorea Sensores, y analiza la data. Se comunica con uno o más Sensores a través del Sistema de Comunicación de

NetRanger (ver Figura 4.3). Las capacidades del Sensor son detección de red, respuesta ante ataques y gestión del dispositivos (permitiendo reconfigurar equipos terceros).

El Sensor será configurado de manera que capture el tráfico directamente de la red (es decir, que no lo reciba de un tercer equipo).

El IDS se colocará en cuatro posiciones rotativas: en la puerta Wan del router examinador del Internet, en la DMZ y en las interfaces interna y externa del firewall de la red corporativa. El Intrusion Detection System deberá permanecer la mayor parte del tiempo en la primera posición. Se trata de analizar el tráfico que llega directamente sin influencia alguna del sistema de seguridad corporativo (raw traffic).

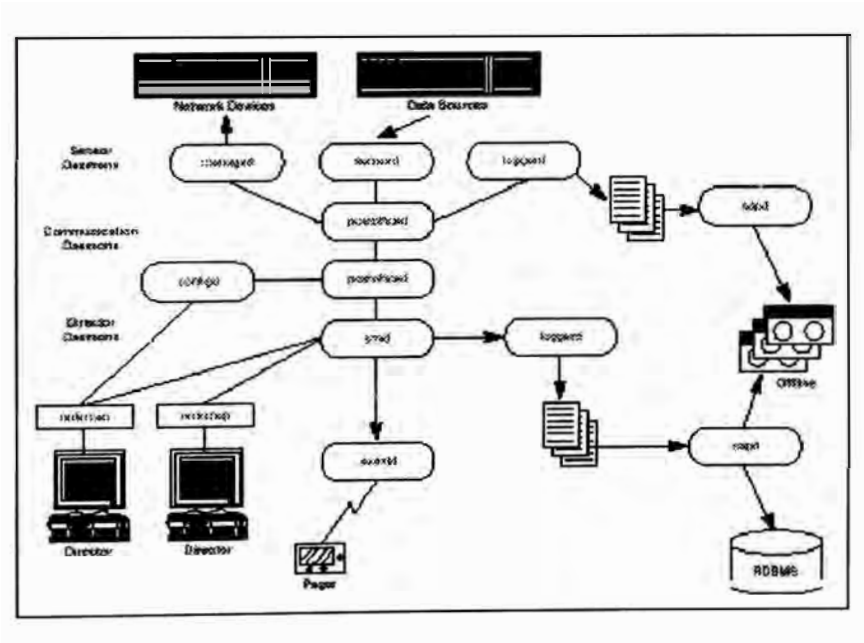


Figura 4.3: Arquitectura del NetRanger de Cisco

Las posiciones que seguirán aseguran la correcta configuración y eficiencia del router examinador y firewall de la red corporativa. Las acciones disparadas y los

logs deberán compararse con aquellos de la primera posición. Estos logs servirán para depurar y afinar los filtros en los equipos arriba mencionados.

El Director muestra eventos, monitorea el Sensor y analiza la data. Su ubicación idónea será el NOC.

Aún cuando el NetRanger permite reconfigurar un equipo ante un eventual ataque, evitaremos esta complicación sobre los equipos que lo soportan (dispositivos Cisco 2500, 4500, and 7500 series routers). Se ha visto la generación frecuente de los denominados falsos positivos que saturan el log. Como el Sensor eventualmente envia información pertinente al Director, debe asegurarse no sobrecargar el enlace hacia el Director, eso significa ser muy minucioso y específico en la información a enviar para análisis. Será necesario realizar un estudio de este tráfico generado para sintonizar el perfil del Sensor - generación de patrones de paquetes y pruebas con aplicaciones típicas de uso de la red corporativa.

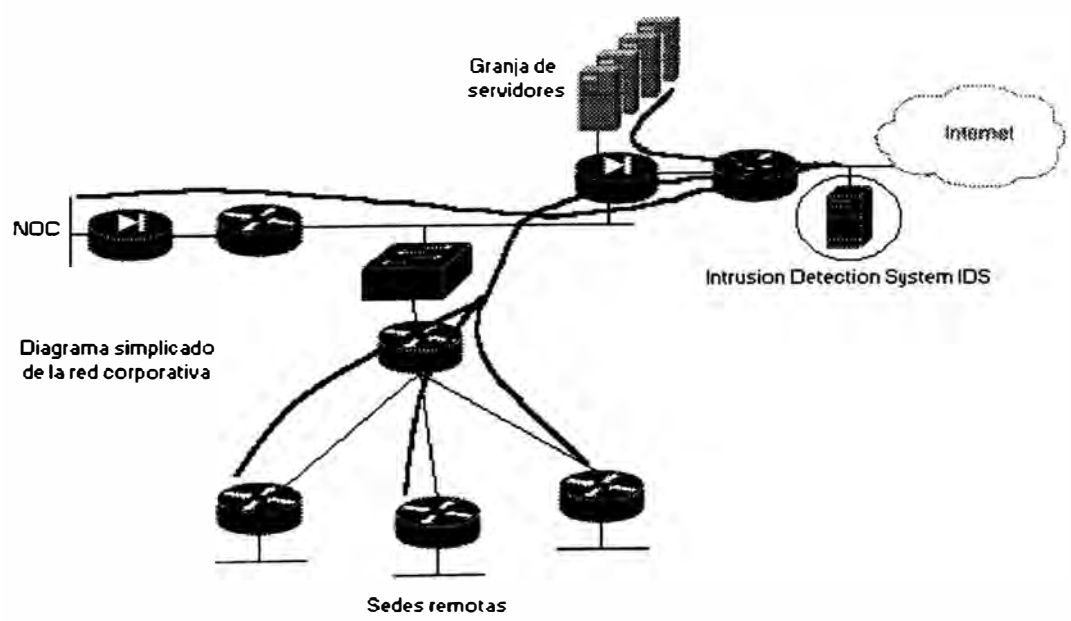


Figura 4.4: Ubicación Permanente del IDS

Todos los usuarios que debieran tener acceso a información de seguridad del NOC deberán pertenecer al grupo netrangr del Director. El servicio de notificación por e-mail conteniendo información de alarmas, será habilitado. El empleo de detección de patrones por expresiones regulares será empleado con precaución para no afectar el performance.

CAPITULO V
PROYECTO DE DISEÑO DE LA INFRAESTRUCTURA DE SEGURIDAD DEL ACCESO REMOTO DE LA RED CORPORATIVA

El presente capítulo tiene como objetivo la descripción de nuevas alternativas para los accesos remotos convencionales de la red corporativa, aquellos a que estamos acostumbrados, que provean implícitamente la seguridad del circuito como parte de su implementación.

5.1 Tunelización L2TP

El sistema de acceso remoto tradicional es dividido en dos mitades. Una mitad es responsable por terminar las conexiones fisicas, y la otra mitad provee el acceso a la red privada. Con L2TP, modems análogos y líneas ISDN pueden ser fisicamente terminados por un ISP, y la data del usuario puede ser llevada a un dispositivo en el extermo de la red privada de una organización.

L2TP fue descrito en el capítulo II. La filosofia detrás de L2TP es llevar tráfico Point-to-Point Protocol, PPP, sobre redes que no son punto a punto. PPP es el protocolo más comúnmente usado para proveer acceso remoto sobre líneas dial-up tales como líneas telefónicas e ISDN. L2TP provee acceso remoto virtual al tunelizar PPP.

Un acceso remoto tradicional emplea un NAS, Network Access Server, ubicado en el border de la red privada. Una sesión se establece sobre una PSTN empleando PPP. El protocolo L2TP es empleado para explotar el trabajo hecho por

el NAS en dos piezas (LAC y LNS) y proveer un mecanismo de comunicación entre los dos dispositivos manejando cada pieza de funcionalidad. Como resultado, el dispositivo en el borde de la red privada, LNS, L2TP Network Server, que el usuario remoto está accesando, no necesita soportar el tipo de conexión fisica particular del usuario remoto.

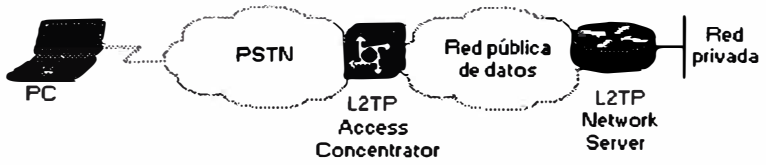


Figura 5.1: Acceso remoto empleando L2TP

Nos encontramos pues ante una VPN, Virtual Private Network, que deberá ofrecer las mismas características de un red privada, a saber:

- Protección contra espionaje fisico. El servicio VPN proveerá encriptación criptográfica para esconder la data, empleando IPSec.
- Control sobre la conectividad. L2TP provee autentificación de tráfico y sesión.

La sensación final que se tiene es la de un usuario remoto manejando PPP con el servidor LNS.

El servidor LNS será ubicado en las instalaciones de la red corporativa y el LAC será de responsabilidad del ISP. Este LAC (NAS) requiere de un router de forwarding encargado de transportar el tráfico VPDN. Esta función será cumplida por el POP del ISP. Servidores RADIUS o TACACS+ acompañarán a ambos. Aquél del lado del LAC controlará la identificación y autentificación del tunel. Aquél del lado del LNS, completará la autentificación del tunel y manejará el control de acceso final de usuarios y sesiones.

El ISP provee de un concentrador de acceso L2TP que soporta clientes PPP sobre un número de plataformas, incluyendo Windows, UNIX, Linux y Macintosh. Ha de asegurarse que el LAC soporte IPSec para la encriptación de la información entre éste y el LNS.

La red pública de transporte empleada entre el LAC y el LNS no será sino el Internet.

La información que sigue deberá recabarse para el diseño adecuado:

- Volumen de tráfico que el sitio remoto generará (capacitiy planning).
- Aplicaciones a correrse.
- Número de usuarios y de sesiones simultáneas.
- Medios de acceso dial: PSTN, ISDN.
- Empleo de PAP o CHAP para la autentificación del tunel.
- Si el servidor LNS será de propiedad de la corporación o será alquilado del ISP.
- Espacio de direcciones IP manejados por el ISP y por la red corporativa.

Como siempre, los reportes y la contabilidad son importantes para monitorear el acceso L2TP. Averiguar si el ISP provee reportes de utilización para el tráfico VPN y con qué frecuencia. Asimismo, exigir un expediente de Service Level Agreement para documentar las expectaciones del servicio recibido. Mientrás más nivel de outsourcing se cuente, se tendrá necesidad de un SLA más fuerte.

5.2 Tunelización IPSec

La iniciativa de IPSec ha sido propuesta para ofrecer una vía estándar de establecer servicios de autentificación y encriptación entre puntos remotos. Esto no significa solamente algoritmos y transformaciones estándares, sino también mecanismos de negociación y gestión de clave estándares. Los servicios de

seguridad incluyen control de acceso, integridad en circuitos no orientados a conexión, autentificación del origen de la data, protección contra ataques de repetición, confidencialidad (encriptación) y confidencialidad de flujo de tráfico limitada.

AH provee autentificación para lo más que sea posible de la cabecera IP, así como para todos los protocolos de las capas superiores de un datagrama IP. Debido a que nuestra preocupación principal es la confidencialidad no emplearemos AH y evitaremos también el overhead adicional.

El modo de transporte en IPSec tiene la ventaja de añadir sólo unos cuantos bytes a la cabecera de cada paquete. Con esta opción, la cabecera original no es protegida. Esta configuración permite que las direcciones fuente y destino sean vistas por dispositivos intermedios. Como lo que se desea ocultar son las estaciones finales evitaremos este modo a costa de evitar el bajo overhead.

El modo tunel es empleado entre dos dispositivos gateways. En modo tunel, el paquete IP original entero es encriptado y se convierte en la data de un nuevo paquete IP. La nueva cabecera IP tiene la dirección destino de su par IPSec. Una de las ventajas del modo tunel es que los dispositivos intermedios, tales como routers, pueden hacer la encriptación sin modificar los sistema finales. Este modo se adecúa a lo requerido.

El modo tunel ESP provee la mayor seguridad para cada paquete IP individual al encriptar el paquete entero. Luego que los contenidos del paquete (incluyendo la cabecera original) son encriptados, ESP en modo tunel genera una nueva cabecera IP para enrutar el datagrama protegido del emisor al receptor.

Para que dos routers manejen una Asociación de Seguridad es necesario que antes se autentifican, es allí donde empezamos a hablar de la gestión de clave. Debido a que tratamos sólo de un par de routers no es obviamente idóneo manejar todo un PKI (Public Key Infraestructure) y de un servidor CA (Certificate Authority). Una solución manual es sencilla más no tan confiable. De las soluciones manuales escogeremos la más segura, la autentificación empleando claves públicas RSA. Estas deberán renovarse periódicamente, a lo menos cada dos meses. Para ello se debe compartir inicialmente las llaves públicas RSA.

Las claves RSA se generan inicialmente por comando en los routers y se copia al router par.

La gestión de clave IPSe permite incorporar facilidad para especificar:

- La granularidad sobre la cual un nivel de seguridad dada deberá ser aplicado.
- Qué servicios de seguridad emplear y en qué combinaciones.
- Los algoritmos empleados para llevar a cabo la seguridad criptográfica.

Debido a que la política de cifrado y descifrado es simétrica, la política emplea información idéntica.

Un asunto a tomar en cuenta es que IKE, IPSec, ICMP, NTP y varios protocolos de enrutamiento emplean UDP. Existen dos temas al respecto. Al emplear listas de acceso en la manera normal permit/deny, asegurarse que no se bloquean los puertos UDP IKE o IPSec. IKE emplean el puerto UDP 500 para negociación. La cabecera IPSec AH contiene 51 en el Campo de Protocolo y la cabecera IPSec ESP contiene 50 en el Campo de Protocolo. Asegurarse que no se están filtrados estos puertos UDP u otros que son requeridos.

Otra sugerencia a la hora de configurar IPSec es no emplear la construcción "any" en una lista de acceso. Los mapas criptográficas (lista de acceso en donde permitir/denegar significa encriptar/no encriptar), en efecto, tienen dos propósitos: clasificación de tráfico y determinación de la política para un flujo de tráfico dado. La construcción "any" puede abarcar demasiados datagramas no relacionados y, por consiguiente, resultados inesperados pueden ocurrir.

Un principio general en criptoanálisis es que, dado un tiempo o tráfico protegido suficientes bajo una clave única, un atacante puede romperla. El manejo del tiempo de vida de la clave simétrica se maneja por tiempo transcurrido y por volumen de tráfico. Antes de la expiración de una clave, IKE negociará otra para permitir una transición sutil de clave a clave sin tener que cortar conexiones.

Tanto el router que se ubica en la red corporativa como aquél remoto emplearán un sistema operativo con características de firewall y un juego ceñido de sentencias de filtraje.

Como en el caso del tunel L2TP la red pública de transporte no será sino el Internet.

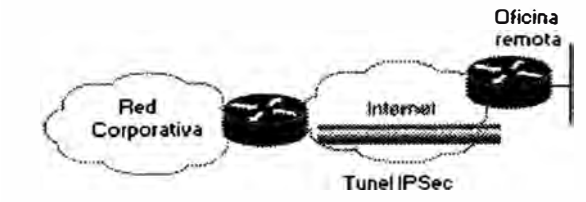


Figura 5.2: Acceso Remoto Empleando un Tunel IPSec

5.3 Acceso dial empleando autentificación SSH

El acceso dial que se propone es bastante simple pero seguro. El cliente es una laptop LINUX y el servidor es una estación LINUX ubicada en la LAN del

NOC. La función de este acceso será para efectos de troubleshooting remoto sobre los servidores del NOC.

La primera fase es un acceso dial común empleando PPP y autentificación CHAP. Hasta aquí no hay nada nuevo.

La segunda fase es la que ofrece la seguridad necesaria para el acceso. Esta fase asegura que dicho cliente inicie automáticamente, sólo y únicamente, una sesión SSH sobre el mismo servidor. El SSH será configurado de manera que solicite un passphrase a la hora de autentificar. La autentificación SSH se realizará empleando claves públicas RSA y un passphrase. No es que la seguridad resida en el passphrase sino en la autentificación mediante clave asimétrica empleada. Como se sabe, inicialmente se generan las claves pública y privada, en servidor y cliente. Posteriormente se intercambian las claves públicas. Este paso se puede realizar al principio localmente por el administrador conectando la laptop a la LAN del servidor. Como se ve, la seguridad reside en contar con la clave privada cliente correcta, en general, y conocer el passphrase (el passphrase protege la clave privada). Esta frase-password es diferente que aquella que se tipea al ingresar a la cuenta – es lo que se ingresa cuando el par de claves es generado.

La configuración del servidor será tal que se manejarán varios usuarios dial que manejarán un proceso de autentificación SSH similar (por manejarse un único par de claves).

El script /etc/ppp/ip-up ofrecida por las plataformas LINUX como Red Hat es ejecutado una vez se establece el enlace. Este script abrirá una sesión SSH sobre el servidor al cual se está accesando cada vez que PPP sea activado. Virtualmente este script puede contener lo que sea.

CAPITULO VI
PROYECTO DE IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA RED CORPORATIVA

El presente capítulo tiene como objetivo especificar la plataformas que conforman la infraestructura de seguridad de la red corporativa, sus características de hardware y software, sus configuraciones y los costos asociados. Las tablas descriptivas figuran al final del capítulo.

6.1 Implementación del sistema de seguridad del campus de la red corporativa

6.1.1 Servidores del NOC y configuración de los mismos.- Probablemente el modelo más común para la seguridad de redes de ordenadores es la seguridad a nivel de host. La seguridad a nivel de host no escala en grandes proporciones y debe ser manejada por los equipos intermedios entre redes. La red nuestra no es el caso y exige conocimiento adecuado de la administración y servicios del sistema.

La seguridad a nivel de host depende claro está de la complejidad y diversidad de los ambientes, donde se incluye estaciones de diversos vendedores. Las plataformas manejadas para nuestras especificaciones son Sun Microsystems con sistema operativo Solaris.

El NOC consistirá de las siguientes estaciones UNIX:

- Servidor de gestión de red (NNM, network node manager) como el CiscoWorks 2000.

- Servidor de control de acceso (ACS, Access Control Server) como el Cisco Secure.
- Workstation Windows.

A continuación sigue lo configurado y las recomendaciones a seguir referenciándonos por el capítulo III del Informe:

- Emplear passwords UNIX normales.
- Generación de una política de elección de passwords adecuados empleando diccionarios disponibles para detectar vulnerabilidades. Aplicación de expiración y aviso de advertencia.
- La actualización de la base de datos /etc/passwd se realizará empleando un script Expect dado el número reducido de servidores. Identificar y eliminar las cuentas sin passwords.
- Empleo de who y finger entre servidores (por ende denegados hacia y desde el exterior por el firewall).
- Control de cuentas durmientes: expiración y script de búsqueda de cuentas durmientes.
- Restringir el ingreso empleando la cuenta root sólo desde la consola.
- Respecto a la integridad, los archivos originales y actualizados son almacenados en el servidor ACS (función adicional del mismo), el cual los exporta "read-only", para efectos de comparación con los archivos existentes en los demás servidores.
- Instalar y configurar Tripwire (para integridad del filesystem) y monitorear los siguientes archivos: /etc/passwd, /etc/hosts, /etc/services, /etc/dfs/dfstab/, /etc/vfstab, /etc/inetd.conf, /etc/rc*, /etc/hosts.allow, /etc/hosts.deny, /etc/dev,

~/.cshrc, ~/.login, /var/spool/cron/crontab/*, /var/adm/sulog, /var/log/tac.log, alias, /opt/tacacs/tacacs_usersdb, ~/history (csh), ~/.emacs, archivos CGI del servidor Web, archivos de automatización de tareas, librerías /lib, /usr/lib y /usr/local/lib. Los atributos a ser monitoreados deberán ser: firmas MD5 y Snefru, propietario, grupo, modos de protección y cuenta de enlace.

- Observar regularmente los usuarios ingresados a través de los archivos: lastlog, who y finger.
- Activar restringídamente durante una ventana de tiempo, el accounting de comandos (/var/adm/pacct leído con acctcom), cuando sea menester
- Revisar periódicamente los procesos ejecutados por los usuarios en busca de: trabajos idénticos ejecutados por el mismo usuario (esto podría resultar en alguien corriendo un script que inicia una serie de trabajos background sin que ninguno de los trabajos culmine), observar el campo TIME para procesos que han acumulado una gran cantidad de tiempo de CPU (es posible que hayan entrado en una secuencia recursiva infinita), observar el campo C para encontrar procesos sin importancia que consumen un gran porcentaje de tiempo de CPU (para manejarlos mejor con menor prioridad), observar el campo SZ de procesos que consumen demasiado porcentaje de memoria.
- Observar periódicamente el archivo /var/adm/sulog (intentos de uso exitosos y fallidos de la cuenta de superusuario).
- Enviar los mensajes de autorización de sistema a la impresora del servidor Syslog.
- Analizar y filtrar la información primordial de los archivos log y llevarlos a tape backup diariamente (estación Syslog).

- Instalar y probar software nuevo (de fuentes confiables) en una estación de pruebas.
- Establecer los permisos de comandos a modos 555 o 511
- Asegurar que los directorios de usuarios sean escribibles por el usuario y no por el grupo o el mundo.
- Llevar un registro de instituciones y contactos de seguridad para aviso y asesoría en caso de ataques o presunción de ataques.
- El directorio actual, identificado por un punto, no deberá ser incluído en la ruta de búsqueda de ejecución de comandos o PATH.
- Deshabilitar Systat.
- Acceso por telnet sólo entre estaciones de la LAN del NOC y protegido por TCP wrappers.
- Permitir FTP sólo entre servidores del NOC y restringir empleando TCP wrappers.
- Crear el archivo que contiene las cuentas que no son permitidas de usar FTP: /etc/ftpusers.
- Ningún servidor FTP anónimo será levantado.
- El correo será configurado sólo para uso interno. Será empleado el Sendmail como programa en todas las estaciones salvo en la NNM, donde será levantado como demonio.
- Instalar la versión más actualizada de Sendmail.
- Asegurarse que el Sendmail no soporta los comandos debug, wiz o kill.
- Borrar los alias "decode" del archivo alias.

- Deshabilitar el password "wizard" en sendmail.cf.
- El servicio DNS no deberá ser configurado.
- TFTP será empleado sólo para uso desde el exterior (descarga de imágenes, sistemas operativos, etc) hacia los equipos de comunicación. El directorio repositorio /tftpboot deberá ser de propiedad del superusuario con los derechos adecuados 700, 711. El servidor ACS albergará también el servidor TFTP.
- El archivo finger no será deshabilitado por sus implicaciones con otros servicios de red, como el correo. Reemplazarlo por safe_finger que viene con el TCP wrapper.
- El servicio POP será deshabilitado.
- Reemplazar el portmapper por aquel de Wietse Venema.
- Habilitar el servicio Identification Protocol.
- Habilitar el servicio NTP, Network Time Protocol, en el servidor NNM, que ofrecerá la sincronización necesaria a todos los equipos de telecomunicaciones. El servidor ACS albergará el servicio NTP.
- Deshabilitar rexec.
- No emplear rlogin ni rsh. Vigilar que no exista archivos .rhosts en el sistema periódicamente.
- Indagar si existe el demonio routed (RIP) y deshabilitarlo. Rutas estáticas deberán ser manejadas.
- X Windows será permitido sólo para uso interno de la LAN del NOC empleando el mecanismo de autentificación xhost. Xauthority magic cookies se descarta

pues requiere de rhost; de igual manera SUN-DES-1 que usa RPC, sólo disponible en X11R5. El firewall del NOC evitará intrusiones desde el exterior.

- Deshabilitar RPC rpc.rexd.
- Un servidor WWW será hablitado en el servidor NNM y empleará la utilidad cricket para monitorear el performance (CPU, memoria) y utilización de los equipos (kpbs in, out; errors in, out; CRCs, etc). El servidor Apache a emplear determinará en su archivo access.conf las estaciones que pueden accesar a los archivos en /usr/local/apache/htdocs. Será sólo de uso interno de la LAN del NOC.
- La estructura de directorios del Web pertenecerá a un grupo creado de nombre www y de propiedad del root. Los derechos de los archivos de configuración serán 600.
- Seguir las recomendaciones respecto a scripts CGI según el capítulo III.
- NIS ni NIS+ serán configurados dado el reducido número de estaciones. Un script Expect mantendrá actualizada la base de datos de passwords.
- Exportar por NFS sólo con derecho de lectura y especificando las estaciones que tienen derecho de montar.
- El servidor de control de acceso será aprovechado para exportar aplicaciones como Emacs, Netscape, Perl, Tcl y Expect. No deberá exportarse directorios home.
- Configurar la variable portmon de NFS.
- Vigilar periódicamente los archivos exportados con el comando "showmount –e".
- Configurar Secure NFS.

- Monitorear y realizar un análisis de las conexiones TCP/IP activas y pendientes mediante el comando netstat.
- Tomar backup de los archivos especificados en el capítulo III, sección de backups, y llevar a tape mensualmente, encriptados y autentificados por un hash. Más de una persona deberá conocer las llaves de decodificación.
- Realizar backup de día cero.
- Realizar backup del sistema entero una vez al año.
- Intentar en una máquina de prueba o prestada de un proveedor restaurar un sistema entero desde los backups para fines de comprobación de la contingencia.
- Elaborar un listado de los archivos en los tapes de backup.
- Analizar periódicamente el crecimiento del filesystem (df –k), o mediante el comando du (encontrar los directorios en el sistema que contienen lo más de data).
- Habilitar en el servidor NNM el monitoreo del performance del sistema de las estaciones: disco, memoria RAM, paginación, memoria SWAP, CPU, paquetes por segundo.

La Tabla 6.1 resume las especificaciones de los servidores del NOC de Enterprise.com.

6.1.2 Plan de direccionamiento, enrutamiento y redundancia de red.- Las secciones que siguen a ésta especifican configuraciones de equipos y antes de ello es necesario el plan de direccionamiento IP pertinente, incluso antes del enrutamiento. Las Tablas 6.2 y 6.3 muestran el plan de direccionamiento de la red corporativa. A grandes rasgos diremos que la red 10.0.0.0 es para administración y enlaces WAN, mientras que la red 172.20.0.0 para subredes LAN de la red corporativa.

Así como para definir la política de seguridad de los firewalls, de igual forma procederemos con las configuraciones de los routers. Primero expresiones gramaticales explicando la función a llevar a cabo, seguido de la sintaxis de los routers.

Los routers Cisco soportan "routing" y "bridging" integrado, lo cual permite rutear un protocolo específico entre interfaces ruteadas y grupos bridge. Cisco introduce lo que se conoce como una interface virtual bridgeada o BVI; ésta es una interface ruteada normal que no soporta bridging pero que de hecho representa un grupo bridge correspondiente a la interface ruteada. La BVI tiene todos los atributos de una interface fisica, dirección de red y la habilidad de desarrollar filtros. La sintaxis que sigue es:

```
bridge irb
interface ATM6/0.101 point-to-point
pvc LocalUno 0/101
  abr 283 283
  oam-pvc manage
  encapsulation aal5snap
  bridge-group 1
interface BVI 1
 ip address 10.10.10.9 255.255.255.248
bridge 1 protocol ieee
 bridge 1 route ip
```

Cada sucursal pues tendrá asociada una interface virtual BVI. Los extremos del PVC ATM creado son la subinterface del router 7206 VXR y la subinterface del switch del POP del proveedor.

Cada subinterface ATM tendrá configurada gestión OAM (Operations, Administration & Maintenance). Estas celdas especiales OAM proveen un medio para detectar la degradación de performance en la red ATM. Ellas son generadas por todo equipo con soporte ATM (como los Cisco BPXs 8600), y ejecutan monitoreo, detección y reporte de errores.

Sin OAM la pérdida del enlace de fibra (switch del proveedor – local sucursal) sería imperceptible a nivel OAM (la subinterface ATM permanece activa). Sólo sería perceptible a nivel IP, como pérdida de una ruta directamente conectada y como pérdida de un vecino EIGRP.

Una configuración OAM en el router Cisco 7206 VXR luce:

```
interface ATM6/0.101 point-to-point
 description rPrincipalRC > Local Uno
 pvc LocalUno 0/101
    abr 283 283
    oam-pvc manage
   encapsulation aal5snap
```

El IOS requerido para OAM debe ser mayor o igual a la 12.0. En general, los requerimiento de un IOS pueden ser observados en la página web de Cisco.

La figura 6.1 muestra el circuito ATM del router central de la red corporativa a un router sucursal.

La redistribución de rutas estáticas por EIGRP fue aprovechada para proveer de dos rutas default a cada router sucursal, pero con diferentes pesos. Tendrá

preponderancia claro está la del router principal. La única manera de comparar rutas recibidas a través de diferentes procesos de enrutamiento es comparando las distancias administrativas de las rutas; sin embargo, EIGRP permite "asignar" las métricas EIGRP con las que serán enviadas las rutas estáticas default hacia un router sucursal, según el comando:

`redistribute static metric` *`delay bandwidth minimum reliability máximum load minimum MTU`*

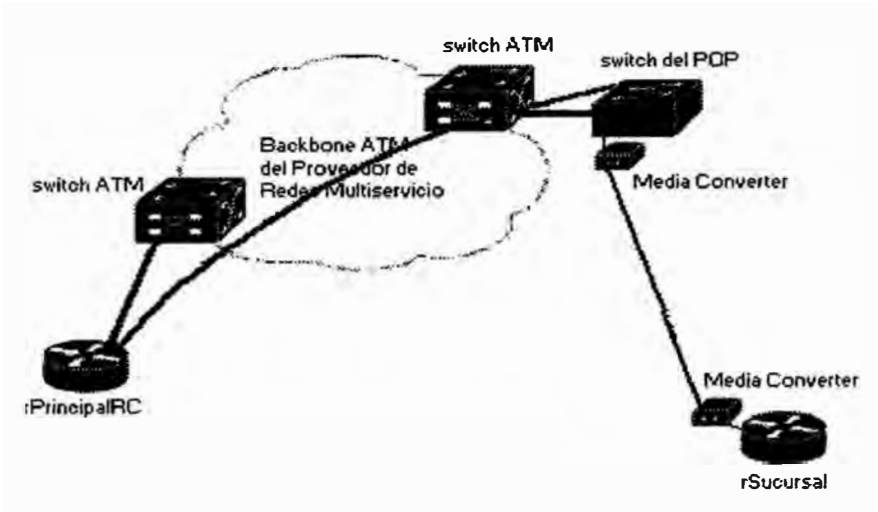


Figura 6.1: Circuito de Red entre el Router Principal de la Red Corporativa y un Router Sucursal

La métrica compuesta EIGRP sigue la ecuación (obsérvese las relaciones directa e inversamente proporcional del ancho de banda y la carga, respectivamente):

Composite metric = K1*BW+K2*BW/(256-load)+K3*DLY, donde

BW = ancho de banda expresado en decenas de Gbps

DLY = retardo en decenas de microsegundos

Según las configuraciones agregadas, el router principal tiene configurado una métrica de ancho de banda mayor en 10 veces a la del router secundario.

Las rutas default de los routers centrales apuntan al firewall de la red corporativa. Lo que se gana con la redistribución es que finalmente la ruta default del router sucursal "no apunte a la direccion del firewall" sino a la dirección IP de la interface por donde aprendió la ruta (las interfaces BVI Wan de los routers centrales).

Ahora bien, es necesario indicar explícitamente que redistribuir:

- El router principal aceptará las subnets loopback y corporativa de los routers sucursales. El router principal publicará sólo la ruta default.
- El router secundario aceptara subnets redistribuídas por el router principal, a excepción de la default, y las subnets loopback y corporativa de los routers sucursales, sea desde la interfaces Ethernet Wan o desde las interfaces Dialer cuando ISDN actúe. El router secundario publicará sólo la ruta default hacia los routers sucursales, ora a través de la interface virtual BVI Wan, ora a través de la interface Dialer cuando ISDN levante.

La pregunta que surge es ¿qué ruta por defecto aprenderá el router sucursal si a perdido conectividad ATM? Obviamente no aprenderá ninguna ruta default de las publicadas por los routers centrales a través de ATM. Es por ello que cada router central tiene configurado localmente una ruta default de distancia administrativa elevada que lo hace el último recurso y que apunta a la interface Dialer.

El comando distribute-list permitir especificar las rutas redistribuídas publicadas y recibidas según:

`distribute-list` *`distribute-list-number`* `in|out` *`interface`*

donde ***distribute-list-number*** se asocia a una lista de acceso, ACL, que especifica las subredes manejadas.

En cuanto a la autentificación MD5, ella asegura que los routers accepten paquetes EIGRP sólo de fuentes confiables. Luego que la autentificación MD5 es configurada en una interface, cada paquete EIGRP enviado por un router sobre una interface es firmado con una huella digital MD5. El proceso completo de intercambio protegido de información es:

- El router emisor genera información EIGRP a ser enviada.
- MD5 es computado sobre la información EIGRP y el secreto compartido.
- El valor "hash" MD5 resultante es agregado al paquete y enviado al router vecino.
- El router receptor computa MD5 sobre la información EIGRP y el secreto compartido. Si el valor MD5 computado iguala el de la huella digital agregada al paquete, el paquete es genuino y es aceptado para procesamiento adicional.

La configuración básica consiste en:

- Especificar el secreto compartido entre routers adyacentes:

```
ip authentication key-chain eigrp <as-number><key-chain-name>
```

- Activar la autentificación MD5 propiamente dicho:

```
ip authentication mode eigrp <as-number> md5
```

Finalmente para la configuración ISDN se ha considerado 8 interfaces BRI. En el peor de los casos dos sucursales quedarían sin la redundancia correspondiente. Emplearemos Dial-on-Demand Routing, una colección de características de Cisco que permite a dos o más routers Cisco establecer una conexión dinámica sobre facilidades dialup sencillas para rutear paquetes e intercambiar actualizaciones de enrutamiento según se necesite.

Para asociar llamadas según se requiere a una interface BRI fisica se emplea las interfaces virtuales Dialer. Los perfiles Dialer permiten que la configuración de interfaces fisicas sea separada de la configuración lógica requerida para una llamada, y también permiten que las configuraciones fisica y lógica sean atadas juntas dinámicamente según la llamada. Un perfil Dialer consiste de los siguientes elementos:

- Una configuración de interface dialer (una entidad lógica) incluyendo una o más cadenas dial (cada una de las cuales es empleada para alcanzar una subred destino).
- Una clase "dialer map" que define todas las características para cualquier llamada a la cadena dial especificada.
- Un pool ordenada dialer de interfaces fisicas a ser usadas por la interface dialer.

La configuración de una interface Dialer en un router sucursal es:

```
interface Dialer1
 bandwidth 64
 ip address 10.10.20.10 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer remote-name rSecundarioRC
 dialer string 2248514 class Enterprise
 dialer pool 1
 dialer-group 1
 ppp authentication chap
```

Donde el Dialer goza de atributos de interface fisica (similar a una BVI) y se defina encapsulación PPP y autentificación CHAP. Se define la cadena dialer, el número telefónico, para generar la llamada y la clase aplicada, de nombre "Enterprise".

El transfondo de la clase es simplificar la configuración agrupando características comunes a las interfaces, sea fisica o virtual en general. La clase estipula lo siguiente:

- Cuando ocurre contensión, es decir, cuando una línea está en uso y ocupada y se requiere enviar un paquete de respuesta, el tiempo de expiración "fast-idle" define cuanto ha de esperar el router hasta que la línea se desocupe y el paquete alcance el destino.
- El tiempo expiración "line-idle" define la cantidad de tiempo que una línea permanecerá desocupada (sin tráfico interesante) antes de ser desconectada.
- "wait-for-carrier-time" define el tiempo que una interface esperará por el servicio telefónico (carrier).

Cada interface Dialer emplea un pool Dialer, un juego de interfaces fisicas ordenadas en base a la prioridad asignada a cada interface (en nuestro caso, por orden de llegada pues todos tienen la misma prioridad configurada). Esta interface pertenece al pool Dialer número 1. Será esto lo que define su pertenencia a un grupo de interfaces fisicas según se ve en la configuración de la interface BRI:

```
interface BRI0/0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer pool-member 1 priority 200 max-link 1
 isdn switch-type basic-net3
 ppp authentication chap
```

Finalmente la lista de acceso dialer-list se asocia al tráfico interesante (todo tráfico IP a excepción de EIGRP), en cuya ausencia, será disparada la llamada ISDN.

6.1.3 Firewall del NOC.- Lo primero que debemos realizar es implementar la política de seguridad del firewall, es decir, la estrategia del filtraje de paquetes (el PIX de Cisco sigue esta arquitectura).

Se tiene la siguiente política expresada gramaticalmente:

- Toda sesión iniciada desde el interior será permitida, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.
- Toda sesión iniciada desde el exterior será denegada, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.
- Traducir direcciones de las estaciones Windows del rango del NOC al rango de la red corporativa.
- Permitir acceso desde el exterior hacia el servidor de control de acceso desde rangos privados de la administración.
- Permitir acceso desde el exterior hacia el servidor Syslog desde rangos privados de la administración.
- Permitir acceso desde el exterior al servidor NNM desde rangos privados de la administración.
- Permitir acceso desde el exterior al servidor de control de acceso mediante el protocolo ICMP desde rangos privados de la administración.
- Limitar sesiones TCP sobre los servidores del NOC.
- Proteger contra el ataque SYN.
- Denegar (explícitamente) la salida Web de las estaciones UNIX (servidores y workstation).
- Permitir acceso al servidor TFTP desde rangos privados de la administración.

- Denegar (explícitamente) el correo saliente desde las estaciones UNIX hacia el exterior.
- Permitir acceso a servidor NTP desde rangos privados de la administración.
- El acceso por Telnet al firewall será permitido sólo desde el servidor ACS.

A continuación, los tipos de paquetes permitidos deben ser especificados formalmente, en términos de expresiones lógicas:

- From inside to outside translate: 172.20.100.1 --> 10.10.60.10, 172.20.100.2 --> 10.10.60.11.
- From outside to inside: permit TCP packet, source address=10.10.0.0/24, destination address=10.10.60.4, destination port=tacacs.
- From outside to inside: permit UDP packet, source address=10.10.0.0/24, destination address=10.10.60.3, destination port=syslog.
- From outside to inside: permit UDP packet, source address=10.10.0.0/24, destination address=10.10.60.2, destination port=snmptrap OR source port=snmp.
- From outside to inside: permit all ICMP packet types, source address=10.10.0.0/24, destination address=10.10.60.3 from inside to outside: deny TCP packet, source address=10.10.60.(2,3,4,5), destination port=http.
- From outside to inside: permit UDP packet, source address 10.10.0.0/24, destination address=10.10.60.4, destination port=tftp.
- From inside to outside: deny TCP packet, source address=10.10.60.(2,3,4,5), destination port=smtp.

- From outside to inside: permit UDP packet, source address=10.10.0.0/24, destination address=10.10.60.4, destination port=ntp.
- From inside to firewall: permit TCP packet, source address=10.10.60.4, destination address=10.10.60.1, destination port=telnet.

Finalmente llevaremos las sentencias lógicas a la sintaxis del PIX de Cisco. Anotaremos la configuración total del mismo en la Tablas 6.4 y 6.5.

6.1.4 Switch principal, integridad y control de conectividad.- El switch considerado es el Catalyst 2924 CXL de Cisco con 2 tarjetas ATM. Un par de fibras se conecta al router central Principal y el otro par al router central Secundario.

La gráfica muestra las disposición fisica del switch principal, no la disposición lógica. Esta última será expuesta y entendible en la siguiente sección, de plan de direccionamiento IP.

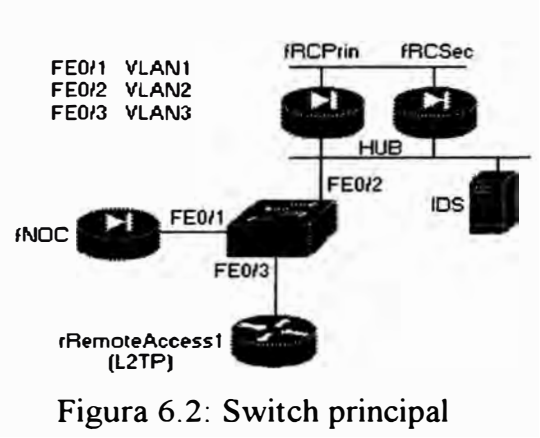


Figura 6.2: Switch principal

La configuración que cumple el switch será:

- Autentificación, autorización y contabilidad TACACS+.
- Control de paquetes broadcast: activarlo cuando se supera los 550 paquetes y retornar a lo normal al rebajarse por debajo de 250.
- Desactivación y alarma de puerto ante direcciones MAC intrusas.

- Activar protección de puertos Fast Ethernet y restringir su uso a un grupo de estaciones definidas por el administrador. La gráfica instruye sobre el número de direcciones MAC a conocer. En caso de violación de la regla anterior el puerto deberá desactivarse (la opción de enviar un trap es excluyente con lo anterior).
- Habilitar trunking (un trunk es un enlace punto a punto entre dos switches o un switch y un router).
- Gestión SNMP.
- NTP.
- Los enlaces ATM routers-switch son de 10M.

6.1.5 Confidencialidad de la data en el transporte.- Como se vió en la parte de diseño las sesiones Telnet desde el NOC hacia los locales remotos serán encriptadas. Los routers principales confian la seguridad de la confidencialidad en el bloqueo de puertos del switch, en el protocolo TACACS+ y listas de acceso que indican que sólo desde el NOC se puede ingresar por Telnet.

En el proceso de encriptación IPSec hay que diferencias dos subprocesos principales: una etapa de autentificación inicial, y otra etapa de intercambio de clave(s) y algoritmos soportados (acuerdo mutuo entre los peers).

IKE es el facilitador y gestor de las conversaciones basadas en IPSec. IKE comprende el establecimiento de las Asociaciones de Seguridad y el manejo de claves.

La Asociación de Seguridad es empleada para llevar registro de todos los detalles de la negociación para una sesión IPSec única. De hecho, una de las principales funciones de IKE es establecer y mantener SA.

La autentificación escogida fue la de claves pre-compartidas (pre-shared keys). Es sinónimo de simpleza y escalabilidad, más es la menos segura. Debido al número reducido de locales y a la necesidad de cambiar periódicamente la clave compartida es idónea para nuestros fines.

La configuración del firewall del NOC y de las sedes remotas comprenderá:

- Operación en modo de transporte (se conservará las direcciones fuente originales).
- El hash MD5 será el algoritmo empleado para autentificar el peer.
- Autentificación por clave pre-compartida.
- Manejar sólo ESP (no hay autentificación, integridad) para confidencialidad.

6.1.5.1 Configuración del firewall del NOC.- Por defecto, IPSec y todos los paquetes que atraviesan el PIX Firewall están sujetos al bloqueo especificado por los comandos conduit, outbound y listas de accesos. Para habilitar que los paquetes IPSec atraviesen el PIX Firewall, hay que asegurarse que sentencias conduit, outbound y listas de accesos así lo permitan explícitamente. Opcionalmente el comando "sysopt connection permit-ipsec" justamente cumple este objetivo y reemplaza los comandos anteriores.

```
sysopt connection permit-ipsec
isakmp enable outside
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 authentication pre-share
isakmp policy 20 lifetime 5000
crypto isakmp key iketest address <direccionIPSucursal>
crypto ipsec transform-set encrypt-des esp-des
  mode transport
crypto map combined 30 match address 105
set peer
set peer <direccionIPSucursal>
set transform-set encrypt-des
access-list 105 permit tcp host 10.10.60.4  10.10.30.0 0.0.0.255 eq
telnet
```

6.1.5.2 Configuración de un Router Sucursal.- Se define la clave compartida y la lista de acceso para definir los paquetes a encriptar es complementaria a la del firewall del NOC.

```
crypto isakmp policy 4
hash md5
authentication pre-share
group 2
lifetime 5000
crypto isakmp key iketest address 10.10.60.4
crypto ipsec transform-set encrypt-des esp-des
crypto map combined 7 ipsec-isakmp
set peer 10.10.60.4
set transform-set encrypt-des
match address 105

interface Ethernet0/0
 description Enlace Sucursal Uno > Campus Corporativo
 ip address 10.10.10.9 255.255.255.248
 ntp broadcast client
 crypto map combined

access-list 105 permit tcp host <DireccionIPSucursal>
      eq telnet host 10.10.60.4
```

6.1.6 Protección contra ataques de red.- Los siguientes comandos deberán incluirse en los routers Cisco siguiendo las recomendaciones de la sección del mismo nombre del capítulo III.

- no service finger
- no ip redirects
- no ip route-cache
- no ıp proxy-arp
- no mop enabled
- no ip unreachables
- En las interfaces LAN y WAN: no ip directed-broadcast
- Protección contra el ataque SYN mediante el feature TCP intercept

```
ip tcp intercept finrst-timeout 5
ip tcp intercept watch-timeout 20
ip tcp intercept max-incomplete low 700
ip tcp intercept max-incomplete high 950
ip tcp intercept one-minute low 950
ip tcp intercept one-minute high 700
ip tcp intercept mode watch
```

El modo configurado es "watch" de manera que las peticiones de conexión son permitidas de atravezar el router pero son observadas hasta que se establezcan. Si éstas fallan en establecerse dentro de 20 segundos, el software envía un Reset al servidor.

6.1.7 Bases de datos centrales.- Como mencionamos en la parte de diseño, el protocolo HSRP será configurado en ambos routers centrales, principal y secundario, de manera que ofrezcan una única dirección IP, virtual, como default gateway para las estaciones y bases de datos del local principal.

La configuración básica es como sigue. En el router principal:

```
interface FastEthernet4/1
    description rPrincipalRC - Switch del Local Principal
    ip address 172.20.50.1 255.255.255.0
    no ip redirects
    no ip directed-broadcast
    standby 1 timers 3 6
    standby 1 priority 170
    standby 1 preempt
     standby 1 ip 10.192.16.3
```

En el router secundario:

```
interface FastEthernet4/1

    description rSecundarioRC-Switch del Local Principal
    ip address 172.20.50.2 255.255.255.0
    no ip redirects
    no ip directed-broadcast
    standby 1 timers 3 6
    standby 1 priority 160
    standby 1 preempt
    standby 1 ip 10.192.16.3
```

Especificamos un intervalo de 3 segundos para el "hello time", el tiempo entre mensajes hello, y de 6 segundos el "hold time", el tiempo que espera un router antes que se declare como router activo.

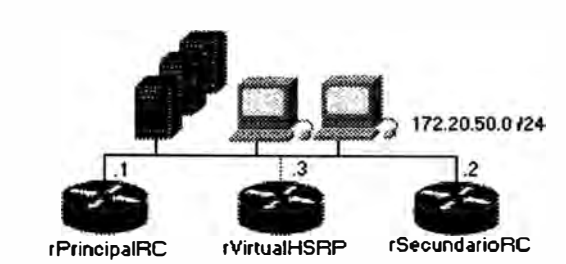


Figura 6.3: HSRP para Tolerancia a Fallos de las Bases de Datos en el Local Principal

6.1.8 Control de acceso sobre los equipos de red.- El software escogido es el Cisco Secure versión 2.3. No iremos a la configuración de los usuarios y grupos a través de las ventanas como es usual ver en los manuales de usuarios. Se ha considerado mejor mostrar la base de datos del Cisco Secure mediante texto plano, así se podrá apreciar la sintaxis del mismo.

Según lo previsto en el diseño, la base de datos plana contemplará:

- Especificación del archivo de logging.
- Clave de encriptación.
- Especificación del password de configuración o acceso privilegiado.
- Configuración de la cuenta del administrador con privilegios de configuración.
- Configuración de las cuentas de operadores del NOC con privilegios de configuración.
- Configuración de una cuenta para monitoreo, backups y aplicaciones de automatización por Expect, Perl, etc.

- Configuración de una cuenta durmiente para acceso de ingenieros del TAC (Technical Assistance Center).

```
key=Panzerkampfwagen
#set up accounting file if enabling accounting on NAS
##############
accounting file = /var/log/tac.log

#enable password setup for everyone:
user=$enable$ {
      login=cleartext "On/va/Enrr"
}

############################
# Network Operation Center #
############################

group = NOC {
      default service=permit
}

user=Admin {
      login = cleartext "Gio/6ch"
      expires = "Feb 06 2001"
      member = NOC
}
user=mmacedo {
      login = cleartext "tei&%la"
      expires = "Jan 01 2001"
      member = NOC
}
user=t_green {
      login = cleartext "qiwe125"
      expires = "Jan 01 2001"
      member = NOC
}

###################
# NOC restringido #
###################

# the group name means "restricted NOC"
group=restrictedNOC {
      cmd = show {
      deny runn
      deny conf
      permit .*
      }
      cmd = telnet {
      deny 10\..*
      permit .*
      }
      cmd = traceroute {
      deny 10\..*
      permit .*
      }
```

```
        cmd = ping {
        deny 10\..*
        permit .*
        }
}

user=ApplUser {
        login = cleartext "NS/4271"
        expires = "Jan 01 2001"
        member = restrictedNOC
}

########################################
# Exceptional privilege users like TAC #
########################################

#user = T/KyuzR {
#       default service = permit
#       login = cleartext "tmp?entrance"
#}
```

El usuario restringido sólo podrá ejecutar comandos "show" a excepción de "show running-configuration" y "show configuration". Una vez ingresado podrá hacer Telnet, ping y traceroute a cualesquiera dirección que no esté dentro de la red de administración (la red 10.0.0.0).

El software será siempre levantado sólo y únicamente por el root.

La configuración de TACACS+ en los equipos de comunicación es tal que:

- El acceso por consola y por terminales virtuales tiene como primer método de autentificación el TACACS+. En caso de ausencia de éste entrará a operar el password "enable secret" configurado en el equipo mismo, según:

  ```
  aaa authentication login default tacacs+ enable
  ```

- El acceso al modo privilegiado tiene como primer método de autentificación el TACACS+. En caso de ausencia de éste entrará a operar el password "enable secret" configurado en el equipo mismo, según:

  ```
  aaa authentication enable default tacacs+ enable
  ```

- La autorización a comandos de mayor nivel (15) se hará sólo por TACACS+, en su defecto el usuario estará autorizado directamente:

```
aaa authorization commands 15 tacacs+ none
```

- Se tomará accounting de los siguientes eventos: sesiones EXEC, comandos de nivel de configuración privilegiado, conexiones outbound, eventos del sistema. Registros de inicio y fin son enviados al servidor, según:

```
aaa accounting exec start-stop tacacs+
aaa accounting commands 15 start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting connection start-stop tacacs+
```

6.2 Implementación del sistema de seguridad del acceso al Internet

6.2.1 Firewall de la red corporativa y router examinador.- De manera similar a como se actuó con el firewall del NOC, lo primero que debemos realizar es implementar la política de seguridad del mismo.

El firewall de la red corporativa maneja tres interfaces: outside, inside y dmz. En la zona demilitarizada se coloracarán los servidores públicos, a saber, Mail, FTP y Web. La interface inside se liga al campus corporativo.

Se tiene la siguiente política expresada gramaticalmente:

- Toda sesión iniciada desde el interior y la dmz será permitida, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.
- Toda sesión iniciada desde el exterior será denegada, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.
- Crear un pool de direcciones globales para las interfaces outside y dmz. Aparte de las 10 direcciones externas manejadas se adiciona una direccional global PAT al final del rango para manejar el overflow. Debido a que el PIX lee las

direcciones globales desde el número más alto hasta el menor, el PAT es situado al inicio del rango.

- Permitir a los usuarios internos establecer conexiones en las interfaces dmz y outside, y permitir que usuarios en la dmz inicien conexiones a través de la interface outside.
- Permitir que cualquier usuario en la interface outside accese el servidor Mail en la interface dmz.
- Permitir que cualquier usuario en la interface outside accese el servidor FTP en la interface dmz.
- Permitir que cualquier usuario en la interface outside accese el servidor Web en la interface dmz.
- Proteger contra el ataque SYN.
- El acceso por Telnet al firewall será permitido sólo desde el servidor ACS.

Sigue especificar los tipos de paquetes permitidos y denegados en términos de expresiones lógicas:

- from inside or dmz to outside translate to: 192.150.50.34-192.150.50.43, 192.150.50.33 (PAT)
- from inside (172.20.0.0/16) and dmz (192.168.0.0/24) permit to outside
- from outside to dmz: permit TCP packet, source address=any, source port=any, destination address=192.168.0.1, destination port=smtp
- from outside to dmz: permit TCP packet, source address=any, source port=any, destination address=192.168.0.2, destination port=ftp, ftp-data

- from outside to dmz: permit TCP packet, source address=any, source port=any, destination address=192.168.0.3, destination port=www
- from inside to firewall: permit TCP packet, source address=10.10.60.4, destination address=10.10.60.1, destination port=telnet

Finalmente llevaremos las sentencias lógicas a la sintaxis del PIX de Cisco.

La Tabla 6.6 anota lo anteriormente descrito.

Conste que se ha anotado la configuración del firewall principal; después de todo la configuración del secundario es una réplica. En la sección de redundancia agregaremos los comandos adicionales de failover.

El router examinador tiene como misión principal el enrutamiento (no la seguridad) y tendrá configurado filtros antispoofing. Valida la mayor parte del tráfico entrante antes de pasarlo al firewall. El firewall provee la función de mayor intensidad en CPU en la inspección paquete por paquete.

El router examinador deberá seguir las reglas siguientes (Tabla 5.7):

- Acceso autentificado y autorizado por el servidor ACS.
- Filtros antispoofing de entrada y salida.
- Denegar servicios ICMP entrantes.
- Enviar mensajes de alarma al servidor Syslog.

6.2.2 Failover.- La primera consideración es emplear un par de dispositivos PIX idénticos (modelo, memoria, tarjetas de red, versiones de sistema operativo).

El cable de failover en el único hardware adicional requerido para este soporte. El cable de failover es un cable serial RS-232 modificado con una velocidad soportada de 9600 baudios.

La comunicación failover básica es a través del cable failover; ésta está basada en mensajes y necesita ser confiable. Cada mensaje enviado es confirmado (ACKed). Si un mensaje no es confirmado por el otro PIX en 3 segundos, el mensaje es retransmitido. Luego de 5 retransmisiones si una confirmación (para un total de 15 segundos), una condición de failover es disparada por el PIX standby.

Las dos unidades deben tener exactamente la misma configuración y deben correr la misma versión de software. Esto se cumple fácilmente, desde que la replicación de la configuración ocurre sobre el cable failover de la unidad activa a la standby de las siguientes maneras:

- Cuando la unidad standby completa su booteo inicial, la unidad activa replica su configuración entera a la unidad standby.
- Mientras comandos son ingresados en la unidad activa, ellos son enviados a la unidad standby.
- Cuando se ingresa el comando "write standby" en la unidad activa, se fuerza la configuración entera en memoria a la unidad standby.

La replicación de la configuración realiza una copia "de memoria a memoria". Una vez que es completada, se debe editar el comando "write memory" en la unidad activa para escribir la configuración en la memoria flash de la unidad standby. Los mensajes de consola "sync started" y "sync completed" se muestran durante esta operación. La replicación de la configuración sólo ocurre de la unidad activa a la standby. Los cambios hechos a la unidad standby no pasan a la activa.

Los comandos adicionales que deben agregarse son:

```
failover timeout 0:00:00
failover ip address inside 10.10.50.19
failover ip address outside 192.150.50.1
failover ip address dmz 192.168.0.100
```

"Failover timeout seconds" define la ventana de tiempo para reconectar luego de un failover, es decir, especifica la ventana de tiempo para reconstruir conexiones TCP (tablas de translación).

6.2.3 Auditoría: monitoreo, logging y detección de intrusos.- Si Todos los equipos Cisco empleados registran sus eventos Syslog al servidor del NOC según la sintaxis:

```
logging <Syslog server ip address>
```

La sincronización empleando NTP es importantísima. A la hora de un evento de seguridad permitirá seguir los pasos y correlacionar los eventos en diferentes equipos. La sintaxis que sigue es:

`service timestamps logging datetime localtime` (activar las marcas de tiempo)

`ntp broadcast client` (cliente NTP)

La respuesta ante ataques del IDS será:

- Generar una alarma
- Registrar el evento de alarma
- Reiniciar conexiones TCP tras un ataque

El Director será instalado en el servidor ACS y deberá tomarse en cuenta las siguientes especificaciones: basado en UltraSPARC, 64MB de RAM, 2.1GB de Disco Duro y sistema operativo Solaris 2.5.1.

Los eventos generados poseen dos atributos de estado: Minimum Critical Status Severity y Minimum Marginal Status Severity. Lo primero describe la severidad más baja que un evento puede tener antes que una alarma crítica (roja) sea

creada para representar dicho evento. Lo segundo describe la severidad más baja que un evento puede tener antes que una alarma marginal (amarilla) sea creada para representar dicho evento. Ambos valores serán dejados por defecto para todos los eventos existentes.

De los demonios que conforman la arquitectura del NetRanger, es el packetd el corazón del IDS. Packetd soporta reinicializar conexiones TCP individuales luego de un ataque. El servicio packetd es esencialmente una copia de sensord que comprende tanto como capturar como analizar el tráfico de red.

Se deberá definir las redes a analizar:

```
RecordOfInternalAddress 172.20.0.0 255.255.0.0
RecordOfInternalAddress 10.10.0.0 255.255.0.0
```

El NetRanger cuenta con un sinnúmero de firmas de ataques o patrones de maluso, descritas en el manual del NetRanger y divididas en los grupos ICMP, TCP y UDP.

NetRanger permitir definir patrones de comparación (matching patterns) para afinar la búsqueda, pero se debe tener experiencia en protocolos de red. Patrones definidos por defecto son:

```
#                Str     TCP      Traffic      Num
#                ID      Port    Direction    Occurs    String
#-------------------------------------------------------------
RecordOfStringName  2101  21  1  1  "[Rr][Ee][Tt][Rr].*[     \t/]passwd[
\t\n]*"
RecordOfStringName 2301 23 3 1 "IFS[=          ]+[/]"
RecordOfStringName 2302 23 1 1 "[/]etc[/]shadow"
RecordOfStringName 2303 23 1 1 "[+][  ]+[+]"
RecordOfStringName 51301 513 3 1 "IFS[=          ]+[/]"
RecordOfStringName 51302 513 1 1 "[/]etc[/]shadow"
RecordOfStringName 51303 513 1 1 "[+][  ]+[+]"
```

La disposición básica del IDS será como muestra la figura 6.4:

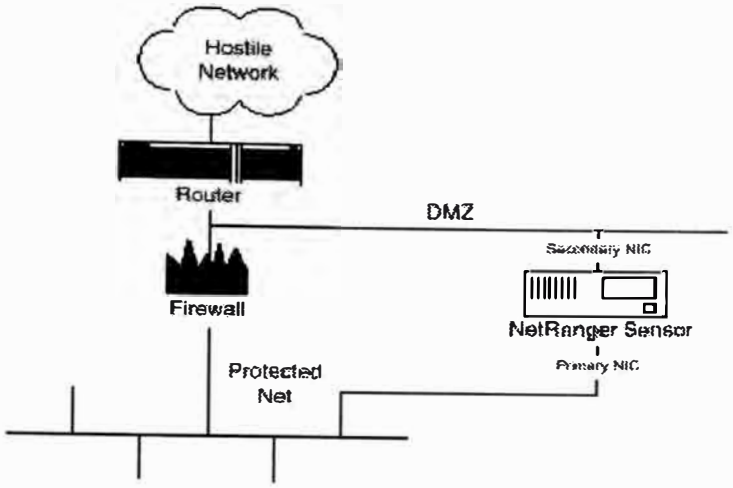


Figura 6.4: Disposición del IDS

6.3 Implementación del sistema de seguridad del acceso remoto.-

6.3.1 L2TP.- Para comprender mejor la dinámica L2TP esta sección se divide tres:

- El acceso L2TP propiamente dicho
- La tunelización IPSec
- Control de acceso AAA

El acceso L2TP propiamente dicho abarca las configuraciones del LAC, router de forwarding y LNS.

6.3.1.1 ISP-LAC.- La configuración básica incluye definir el grupo vpdn, asociar las interfaces E1 a grupos de interfaces asíncronas (llamadas dial). La puerta de salida del LAC es el router de forwarding, el router del POP.

```
hostname ISP-LAC-1
logging buffered 100000 debugging
enable password cisco
username isp-admin password 0 cisco
resource-pool disable
ip subnet-zero
!Turns on VPDN.
vpdn enable
vpdn search-order domain
vpdn-group 1
request-dialin
protocol l2tp
domain service.com
```

```
initiate-to ip 10.10.50.25 priority 1
local name ISP-LAC-1
l2tp tunnel password 7 tunnel4me
async-bootp dns-server 200.14.35.1 200.14.35.2
isdn switch-type primary-5ess
cns event-service server
mta receive maximum-recipients 0
!
controller E1 0
clock source line primary
linecode b8zs
cas-group 0 timeslots 1-32 type e&m-fgb
controller E1 1
framing esf
clock source line secondary 1
linecode b8zs
cas-group 0 timeslots 1-32 type e&m-fgb
interface FastEthernet0
description to ISP-RTR-1 for forwarding of VPDN traffic
ip address 192.168.10.1 255.255.255.252
duplex full
speed 100
!
interface Group-Async1
!Specifies that the asynchronous interfaces will use the IP address
of FastEthernet0.
ip unnumbered FastEthernet0
encapsulation ppp
async mode interactive
group-range 1 60
!
ip default-gateway 192.168.10.2
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.2
no ip http server
!
line con 0
transport input none
!Specifies the range of modems.
line 1 60
autoselect ppp
transport output pad telnet rlogin udptn v120 lapb-ta
line aux 0
line vty 0 4
password password
ntp server ntpserver_del_ISP
```

6.3.1.2 Router de forwading .- El router de forwarding permitirá que el LAC conozca el extremo del tunel (enrutamiento) y encripta el tunel L2TP entre interfaces túneles del router de forwarding y el router LNS de la red corporativa.

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
```

```
hostname ISP-RTR-1
logging buffered 100000 debugging
enable password password
username isp-admin password 0 password admin
ip subnet-zero
!
!Configures the IP addresses of DNS servers that translate hostnames
to IP addresses.
async-bootp dns-server 200.14.35.1 200.14.35.2
!
interface Tunnel100
  description tunnel to Enterprise
  ip unnumbered FastEthernet 0/0
  no ip directed-broadcast
  tunnel source serial2/0
  tunnel destination 150.31.5.129
interface FastEthernet0/0
ip address 192.168.10.2 255.255.255.252
full-duplex
!
!This interface is dedicated to forwarding VPDN traffic to the
service provider network.
interface Serial2/0
 description to Internet
 ip unnumbered FastEthernet0/0
 ip address 200.14.241.9 255.255.255.252
  ip access-group IntSecurity in
  ip access-group IntSecurityOut out
  no ip directed-broadcast
  encapsulation frame-relay IETF
  no ip mroute-cache
  frame-relay lmi-type ansi
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.14.241.10
!This static route is to the enterprise device subnet.
ip route 10.10.50.24 255.255.255.248 Tunnel100
!This static route is to the enterprise IP address pool subnet.
ip route 172.20.20.0 255.255.255.0 Tunel100
!This static route is to the service provider device subnet.
no ip http server
!
! ACL to block particular servcies and networks, inbound from the
ISP.
ip acccess-list extende IntSecurity
  deny ip 127.0.0.0 0.255.255.255 any
  deny ip 10.0.0.0 0.255.255.255 any
  deny ip 172.16.0.0 0.15.255.255 any
  deny ip 192.168.0.0 0.0.255.255 any
  deny udp any any eq snmp
  deny tcp any any eq 2000
  deny udp any any eq tftp
  deny udp any any eq sunrpc
  deny udp any any eq 2049
  deny tcp any any eq 2049
  deny tcp any any eq sunrpc
  deny tcp any any eq 87
```

```
  deny tcp any any eq exec
  deny tcp any any eq login
  deny tcp any any eq cmd
  deny tcp any any eq lpd
  deny tcp any any eq uucp
  permit ip any any
! ACL to prevent packets from private networks leaving by the ISP
interface
ip access-list extended IntSecurityOut
  deny ip 127.0.0.0 0.255.255.255 any
  deny ip 10.0.0.0 0.255.255.255 any
  deny ip 172.16.0.0 0.15.255.255 any
  deny ip 192.168.0.0 0.0.255.255 any
  permit ip any any
!
logging servidor_syslog_del_ISP
ip access-list 75 permit estaciones que pueden accesar por tftp
tacacs-server host 10.192.17.2
tacacs-server key Panzerkampfwagen
!
snmp-server community comunnityRWdelISP RW
snmp-server community comunidadROdelISP RO
snmp-server trap-source Loopback0
snmp-server location Centro de Computo
snmp-server contact FirstCom S.A. tlf: 0-800-11911
snmp-server chassis-id n/s SHN
snmp-server enable traps snmp
snmp-server enable traps frame-relay
snmp-server enable traps syslog
snmp-server host 10.192.17.2 traps communityROdelISP
snmp-server tftp-server-list 75
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
```

6.3.1.3 ENT-LNS.- Se define la terminación del tunel y de la encriptación del mismo. Se define el pool de direcciones para los hosts remotos.

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
hostname ENT-LNS-1
logging buffered 100000 debugging
enable password enablepassword
username ent-pass-1@enterprise.com password 7 ent-pass-1
ip subnet-zero
ip name-server 171.68.10.70
vpdn enable
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
```

```
terminate-from hostname ISP-LAC-1
l2tp tunnel password 7 tunnel4me
source-ip 10.10.50.25
async-bootp dns-server 200.14.35.1 200.14.35.2
interface Tunnel100
  description tunnel to remote ISP POP (router forwarding)
  ip unnumbered FastEthernet5/0
  no ip directed-broadcast
  tunnel source serial2/0
  tunnel destination 200.14.241.9
!
interface Serial 2/0
  description connection to ISP
  ip address 150.31.5.129 255.255.255.252
  no ip directed-broadcast
  ip access-group IntSecurity in
  ip access-group IntSecurityOut out
  no ip directed-broadcast
  framing c-bit
  cablelength 50
  dsu bandwidth 44210
!
!Configures the IP address of FastEthernet 0/0, through which all
VPDN traffic passes.
interface FastEthernet0/0
ip address 10.10.50.25 255.255.255.248
media-type MII
full-duplex
interface Virtual-Template1
ip unnumbered FastEthernet0/0
peer default ip address pool default
ppp authentication chap
encapsulation ppp
ip local pool default 172.20.20.1 172.20.20.60
ip classless
ip route 192.168.10.0 255.255.255.252 Tunnel100
no ip http server
line con 0
transport input none
line aux 0
line vty 0 4
password 7 password
!
ntp update-calendar
ntp server 172.22.16.9
```

6.3.1.4 IPSec en router de forwarding.- Se citan los comandos que se agregan a la configuración y que ya fueron comentados en la parte de encriptación dentro del campus corporativo.

```
crypto isakmp policy 4
hash md5
authentication pre-share
group 2
```

```
lifetime 5000
crypto isakmp key iketest address 150.31.5.129
!
!
crypto ipsec transform-set encrypt-des esp-des
  mode transport
!
crypto map combined 7 ipsec-isakmp
set peer 150.31.5.129
set transform-set encrypt-des
match address VPN_tunnel
!
Interface tunnel 100
  crypto map combined
!
ip access-list extenden VPN_tunnel
  permit ip host 150.31.5.129 host 200.14.241.9
```

6.3.1.5 IPSec en LNS.-

```
crypto isakmp policy 4
hash md5
authentication pre-share
group 2
lifetime 5000
crypto isakmp key iketest address 200.14.241.9
!
!
crypto ipsec transform-set encrypt-des esp-des
  mode transport
!
!
crypto map combined 7 ipsec-isakmp
set peer 200.14.241.9
set transform-set encrypt-des
match address VPN_tunnel

Interface tunnel 100
  crypto map combined
!
ip access-list extenden VPN_tunnel
  permit ip host 200.14.241.9 host 150.31.5.129
```

6.3.6.1 LNS TACACS+ .- La configuración del router LNS será:

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa authorization commands 15 default tacacs+ none
aaa accounting exec default start-stop tacacs+
aaa accounting commands 15 default start-stop tacacs+
aaa accounting network default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password somethingSecret
```

```
tacacs-server host 10.10.60.4
tacacs-server key PersonneNeLeSait
```

En el archivo de configuración del servidor TACACS+ de la red corporativa se deberá agregar lo que sigue para definir los usuarios finales PPP y la autentificación del NAS.

```
key = not2difficult
# Password for tunnel authentication
user = anonymous {
          chap = cleartext not2tell
        }
user = santiago {
          chap = cleartext letmein
          service = ppp protocol = lcp { }
          service = ppp protocol = ip { }
        }
user = santiago@cisco.com {
          global = cleartext jeveuxentrer
          service = ppp protocol = lcp { }
          service = ppp protocol = multilink { }
          service = ppp protocol = ip { }
        }
```

6.3.1.7 NAS/LAC TACACS+ .- El archivo de configuración define la terminación del tunel y su autentificación.

```
key = 2easy
# Use L2TP tunnel to 10.10.50.25 when 3462877 is dialed
user = remoteuser {
       service = ppp protocol = vpdn {
         tunnel-id = anonymous
         ip-addresses = 10.10.50.25
         tunnel-type = l2tp
       }
     }

# Password for tunnel authentication
user = anonymous {
       chap = cleartext not2tell
     }
```

6.3.2 Tunelización empleando IPSec.- La tunelización IPSec será bastante similar a la configuración del router LNS en el caso de la tunelización L2TP. De hecho se aprovechará dicho router para configurar otro tunel dedicado a esta

solución. Este LNS finalmente será dedicado sólo para proveer los túneles, no para accesar al Internet.

La sede remota de la red corporativa empleará un tunel de manera que tenga acceso al Internet por la interface serial y acceso a la red corporativa por el tunel. En la puerta serial se empleará NAT para ocultar las estaciones privadas.

Se indica la configuración adicional del router LNS y la configuración de la sede remota.

6.3.2.1 ENT-LNS .-

```
crypto isakmp policy 4
hash md5
authentication pre-share
group 2
lifetime 5000
crypto isakmp key hawai address 141.10.23.13
crypto ipsec transform-set encrypt-des esp-des
  mode transport
!
crypto map combined 7 ipsec-isakmp
set peer 150.31.5.129
set transform-set encrypt-des
match address IPSec_tunnel
!
interface Tunnel110
  description tunnel to remote local
  ip unnumbered FastEthernet5/0
  no ip directed-broadcast
  tunnel source serial2/0
  tunnel destination 150.31.5.129
  crypto map combined
ip access-list extenden IPSec_tunnel
  permit ip host 150.31.5.129 host 150.31.5.129
ip route 172.20.30.0 255.255.255.0 Tunnel110
```

6.3.2.2 Router de la Sede Remota de Enterprise.com.-

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
hostname rSedeRemtoa
logging buffered 100000 debugging
enable password password

username ent-admin password 7 pass2me
crypto isakmp policy 4
hash md5
authentication pre-share
```

```
group 2
lifetime 5000
crypto isakmp key ipsecsecret address 150.31.5.129
!
!
crypto ipsec transform-set encrypt-des esp-des
  mode transport
!
crypto map combined 7 ipsec-isakmp
set peer 200.14.241.9
set transform-set encrypt-des
match address IPSec_tunnel
!
interface Tunnel100
  description tunnel to LNS
  ip unnumbered Ethernet0/0
  no ip directed-broadcast
  tunnel source serial2/0
  tunnel destination 200.14.241.9
  crypto map combined
!
ip access-list extenden IPSec_tunnel
  permit ip host 200.14.241.9 host 150.31.5.129
!
interface Serial 2/0
  description connection to ISP
  ip address 150.31.5.129 255.255.255.252
  no ip directed-broadcast
  ip access-group IntSecurity in
  ip access-group IntSecurityOut out
  no ip directed-broadcast
  ip nat outside
  framing c-bit
  cablelength 50
  dsu bandwidth 44210
interface Ethernet0/0
ip address 172.20.30.1 255.255.255.0
ip nat inside
media-type MII
full-duplex
!
ip nat inside source list 50 inteface serial2/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 serial2/0
ip route 172.20.0.0 255.255.0.0 Tunnel100
no ip http server
access-list 50 permit 172.20.30.0 0.0.0.255
line con 0
transport input none
line aux 0
line vty 0 4
password 7 password
ntp server 172.22.16.9
```

6.3.3 Acceso dial empleando autentificación SSH.-

6.3.3.1 Configuración del Secure Shell en el cliente y el servidor.- La versión de LINUX empleada será RedHat 6.2 con versión de kernel 2.2.12.

La versión de SSH es SSH1, disponible en el site oficial: ftp://ftp.cs.hut.fi/pub/ssh.

El proceso de instalación es similar a la descarga de cualquier software de UNIX. La descarga inicial se realiza en el directorio /usr/local/src. Sin embargo luego de ella es necesario configurar las siguientes opciones para modificar el Makefile (archivo base de instalación que se adecua a la plataforma y requerimientos últimos de usuario), directamente o empleando "configure options host":

- Los cifradores por defecto son IDEA, Blowfish y Triple DES. Se puede habilitar también DES y arcfour, aún cuando no son muy recomendados.
- Deshabilitar "login –f" para completar la conexión de ingreso, lo cual permite al usuario ingresar a su cuenta sin tener que especificar un password dado que la autentificación propia ya ha sido llevada a cabo.
- Instalar la herramienta de encriptación RSAREF, disponible en ftp://ftp.rsa.com, la cual contiene el algoritmo RSA, así como otros cifradores.

Una vez instalado el SSH1, el proceso general de conectividad luce así:

- Solicitud de conexión sobre el puerto TCP 22 del servidor.
- El servidor engendra un proceso hijo.
- Intercambio de claves públicas entre cliente y servidor.
- Clave de sesión encriptada por llave privada intercambiada desde el cliente.
- Cifrador soportado decidido entre cliente y servidor.
- Data encriptada transferida.

- Conexión concluída.

En el sistema local cliente se genera un par de claves RSA de 1024 bits: la privada y la pública, almacenadas localmente en disco. Por defecto, se almacenan en /etc/ssh_host_key y /etc/ssh_host_key.pub, respectivamente.

En el sistema servidor se halla otro par de claves RSA de 768 bits, que es regenerada cada hora si ha sido empleada. Ellas no se almacenan en disco sino en memoria.

Luego que las llaves públicas son intercambiadas y validadas, ya no son necesitadas para cualquier otra función de encriptación. Lo que SSH hace a continuación es iniciado por el cliente, enviando unos bytes de check al servidor remoto, los cuales deberán ser comprobados por el host en el paquete de respuesta del servidor. Este paquete contiene los bytes de check y la clave de sesión.

SSH no será iniciado al reinicializar la laptop con LINUX, es decir, como un demonio. Resultará más práctico correrlo como programa ejecutando "sshd".

Lo que sigue indica nuestros requisitos para cliente y servidor respecto al archivo de configuración del demonio "sshd_config":

- Permisos por usuario y por nombre de host: AllowUsers/DenyUsers, AllowHosts/DenyHosts.
- Fecha de advertencia de expiración de cuentas: AccountExpireWarningDays.
- Autentificación RSA haciendo uso del passphrase de usuario empleado al generar las claves de usuario (este passphrase de usuario hará pues las veces de password de la cuenta de usuario y debe ser escogido cuidadosamente). Deshabilitar esta opción para el passphrase de host (que tienen un tiempo de vida de 3 a 6 meses): PasswordAuthentication.

- Mensajes keepalive para dar aviso al servidor si la conexión sigue con vida: KeepAlive.
- Habilitar facilidad syslog: SyslogFacility.
- Número de intentos de conexión del cliente: ConnectionAttempts.

De igual manera un usuario del sistema cliente deberá generar un par de claves de usuario, pública y privada (~/.ssh/identity y ~/.ssh/identity.pub), empleadas para la identidad del usuario y del host servidor al cual ingresan.

SSH1 emplea un programa llamado ssh-keygen para generar el par de claves de autentificación RSA. El administrador del sistema deberá generar, como root, el par de claves de hosts. Un usuario particular hace uso de ssh-keygen para generar su par de claves de identidad.

6.3.3.2 Configuración PPP del cliente.- Un único commando pppd configura un enlace dedicado para nuestro sistema Linux. Este se coloca en el archivo /etc/rc.d/rc.inet1:

```
pppd /dev/cua2 56000 crtscts defaultroute :
```

Donde /dev/cua2 selecciona el dispositivo al cual PPP está ligado, es decir, el puerto serial conectado al modem del servidor (COM2). Luego sigue la velocidad en bits por segundo. La opción crtscts activa el control de flujo por hardware. La opción defaultroute crea una ruta por defecto empleando el servidor remoto como la puerta de enlace o gateway.

Las direcciones local y remotas se especifican al final. Dado que la laptop cuenta con un puerto Ethernet es necesario asignar una dirección local diferente a ésta del puerto Ethernet. A uno y otro lado del dos puntos se ubican las direcciones

IP local y la del servidor. Ambas se dejan en blanco pues serán configuradas y recibidas desde el servidor.

En realidad PPP lee sus opciones del archivo /etc/ppp/options, luego de ~/.ppprc y finalmente de la línea de comando. El orden es tal que la línea de comando tiene mayor jerarquía.

Todos los scripts asociados con las interfaces de red son guardados en /etc/sysconfig/network-scripts. Aquellos asociados con PPP son:

chat-ppp0 Secuencia "esperar/enviar" para el proceso dial/ingreso.

ifcfg-ppp0 Las variables y configuraciones para la interface.

ifdown-ppp Script en shell para desactivar el link.

ifup-ppp Script en shell para activar el link.

También se puede emplear el paquete "dip" (Dial-up IP) para simplificar el proceso de marcar hacia el servidor remoto (por ejemplo, dip start-ppp).

Para solicitar autentificación CHAP agregar la opción "auth" en el archivo /etc/ppp/options. Un archivo ejemplo chaps-secrets en la estación local luce así:

```
RemoteServer      localhost         DasWeissIchNicht
10.10.60.3
localhost         RemoteServer      PromeneurSolitaire
10.10.60.15
```

Donde RemoteServer especifa el servidor PPP remoto. La clave secreta es DasWeissIchNicht y 10.10.60.3 es la dirección IP asignada a RemoteServer en la tabla de hosts. La primera entrada valida el sistema remoto y la otra responde al challenge de tal sistema remoto.

6.3.3.3 Configuración del cliente PPP para automatizar la llamada a SSH.- Luego que un enlace PPP se establece, pppd busca el archivo /etc/ppp/ip-up. Si este

script existe y es ejecutable, el demonio PPP ejecuta el script. Justamente este script contiene el llamado de la sesión SSH y lucirá así:

#!/bin/bash

#

Script that automates SSH startup.

#

if ( ) {ssh *server_hostname*} else exit 0

6.3.3.4 Configuración del servidor PPP sobre la estación Solaris.- Primero asegurarse que el software PPP y UUCP están instalados. También asegurar la comunicación con el modem:

tip ttya

Tanto servidor como la estación remota deben agregarse en la lista de hosts /etc/hosts:

```
SERV ADDR          SERV NAME    SERV_NAME.enterprise.com

REM ADDR           REM NAME           REM_NAME.enterprise.com
```

Generar una cuenta PPP en el archivo /etc/passwd:

ppp_user:x:115:10:PPP user: /:/usr/sbin/aspppls.

El archivo /etc/asppp.cf deberá contener en su línea inicial:

```
ifconfig ipdptp0 plumb SERV NAME REM NAME netmask +
path
    ipcp async_map 0
    inactivity_timeout 0
    interface ipdptp 0
    peer system_name ppp_user
    peer_ip_address REM NAME
```

Las direcciones MAC también deben ser listadas y se agregan en /etc7rc2.d/S99proxyarp según:

ndd –set 7dev/ip ip_forwarding 1

arp –s REM_NAME SERV_ETHER pub

Se agrega una entrada arp por cada cliente PPP.

6.4 Plataformas y Costos

6.4.1 Firewalls del NOC y de la Red Corporativa.- Los firewalls considerados para el NOC y la red corporativa son PIX 515. La ventaja en la serie PIX Firewalls es que se trata de un equipo de hardware/software integrado, no basado en UNIX, en tiempo real y especializado para seguridad, a diferencia de servidores proxy de actividad intensa en CPU y dependientes de un sistema operativo tercero (como Windows NT en el caso de Checkpoint). Entre otras características, el PIX ofrece un performance de hasta 250000 conexiones simultáneas, 6500 conexiones por segundo, y cerca de 170 megabits de throughput.

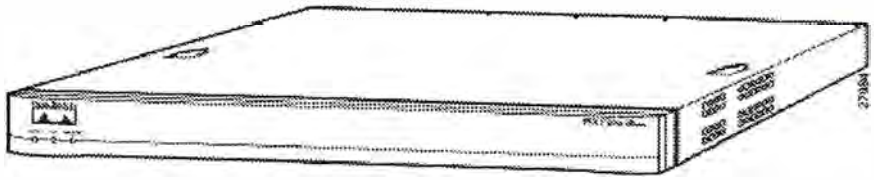


Figura 6.5 Vista frontal del Cisco Secure PIX Firewall 515

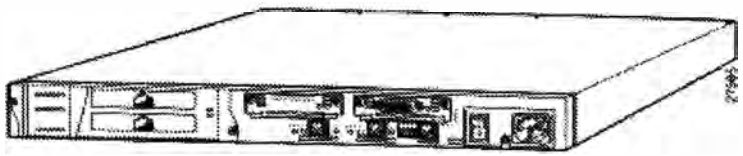


Figura 6.6 Vista trasera del Cisco Secure PIX Firewall 515

Las tarjetas de red estándares soportadas incluyen tarjetas Ethernet 10/100 de uno a cuatro puertos, tarjetas Token Ring 4/16 y tarjetas dual-attached multimode FDDI cards.

Los firewalls PIX 515 soportan sólo licencias no restringidas (unrestricted), e decir, de hasta 250000 conexiones simultáneas. El firewall del NOC posee 2 tarjetas Ethernet 10/100 y 32M de RAM. El firewall de la red corporativa deberá soportar 3 tarjetas Ethernet 10/100, failover y 64M de RAM.

El sistema operativo PIX-VPN-DES 5.2.2 es el mínimo disponible con soporte de IPSec para encriptación.

6.4.2 Routers Principal y Secundario de la Red Corporativa.- Desde que los routers deben soportar dos interfaces ATM la opción de Cisco Systems disponible fue el router 7206 VXR.

Los routers Cisco 7200 Series son plataformas multifuncionales de alto rendimiento y soportan:

- Alta densidad de interfaces LAN y WAN
- Agregación de servicios Subscriptor de Banda Ancha – incluyendo PPP, terminación RFC 1473 y tunelización L2TP
- Conectividad CODEC de video y conectividad digital de voz PBX T1/E1
- ATM y Packet sobre conectividad SONET
- Conectividad ATM CES (Circuit Emulation Standard) para servicios de voz, video y data

Un Cisco router 7206 VXR consiste de 6 slots. Las interfaces manejadas serán 2 ATM OC3, 1 puerto FastEthernet y una tarjeta de 8 BRIs ISDN.

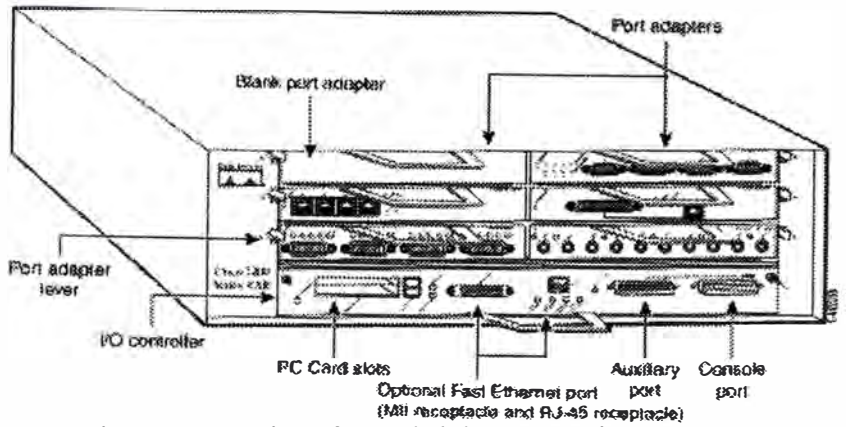


Figura 6.7: Vista frontal del router Cisco 7206 VXR

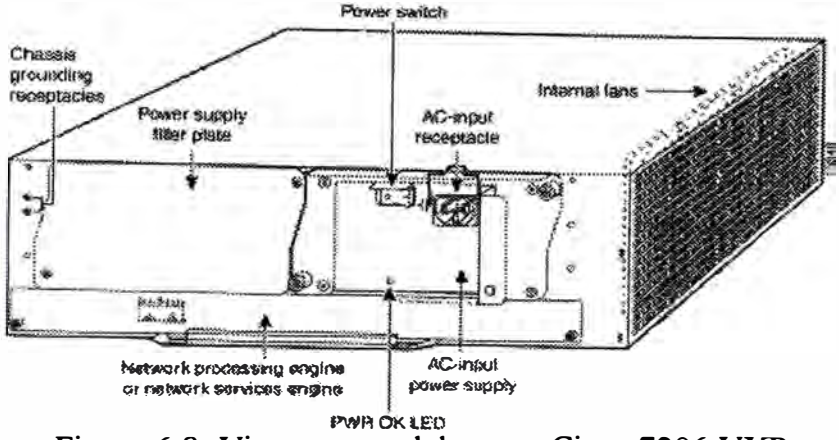


Figura 6.8: Vista trasera del router Cisco 7206 VXR

El sistema operativo IOS 12.0 IP es una versión estable. Anotamos las características que nos interesan en la tabla que sigue:

Características del IOS 12.0 IP
IP Routing
Expanded IP Access Lists
MAC Address and Precedence Accounting
OSPF Point to Multipoint
Management
Cisco IOS File System
Entity MIB
Expression MIB
Conditionally Triggered Debugging
SNMP Inform Request
SNMP Manager
Security
Named Method Lists for AAA Authentication
WAN Services

Multiple ISDN Switch Types
Multiprotocol over ATM
National ISDN Switch Types

6.4.3 Switch Principal de la Red Corporativa y Switches de las Sucursales.- El switch Cisco Catalyst 2924 XL es una solución efectiva en costo (densidad de puertos/costo), por su alto performance y ancho de banda de 10-100 Mbps para usuarios y servidores.

El switch Cisco Catalyst 2924 XL provee puertos autosensitivos 10/100. Permite una mejor gestión y control de tráfico broadcast y multicast. Provee a los administradores escoger el nivel de seguridad, notificación y acciones correctivas. Provee protección contra cambios de configuración no autorizados.

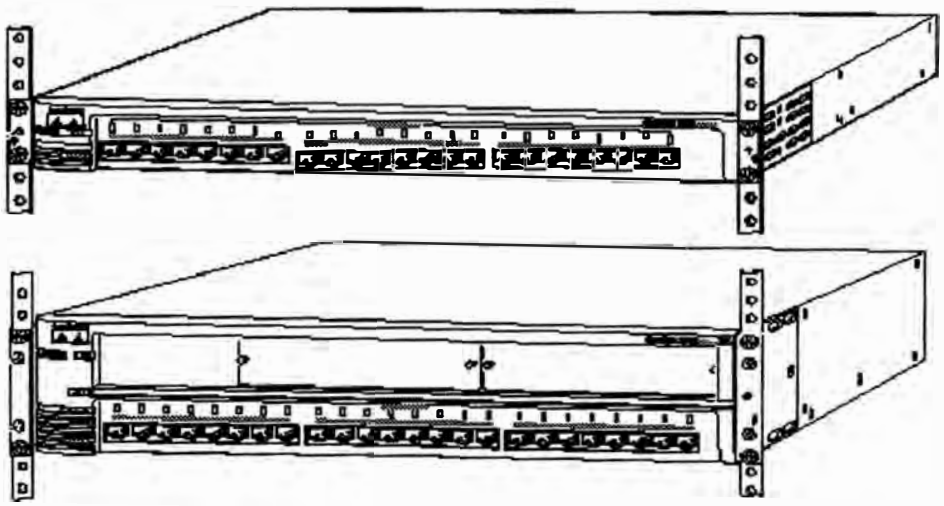


Figura 6.9: Vista frontal del switch Catalyst 2924 XL (con y sin módulos ATM)

Las versiones más recientes de IOS son la 12.0.5.2, para el sistema, y la 12.0.7 XF para el módulo ATM.

6.4.4 Routers de las Sucursales.- Una solución efectiva en costo la ofrece el router de acceso modular Cisco 2600. Este equipo provee gran versatilidad e integración a las oficinas sucursales.

Entre otras características se tiene:

- Acceso seguro Internet/intranet con protección de IOS firewall.
- Integración voz/data multiservicio.
- Servicios de acceso dial análogo y digital.
- Acceso VPN (Virtual Private Network)
- Routing con Manejo de Ancho de Banda

Los routers Cisco 2600 Series ofrecen interfaces LAN únicas y duales, un slot de módulo de red, dos slots de interfaces WAN y un nuevo slot AIM (Advanced Integration Module). El soporte LAN incluye opciones de Ethernet autosensing 10/100; mixtura Token-Ring y Ethernet; versión de chasis sólo Token-Ring. Las tarjetas WAN soportadas incluyen BRI ISDN, opciones integradas CSU/DSU para conectividad WAN primaria y backup. El slot AIM soporta integración de servicios avanzados tales como compresión de data asistida por hardware y en el futuro, encriptación.

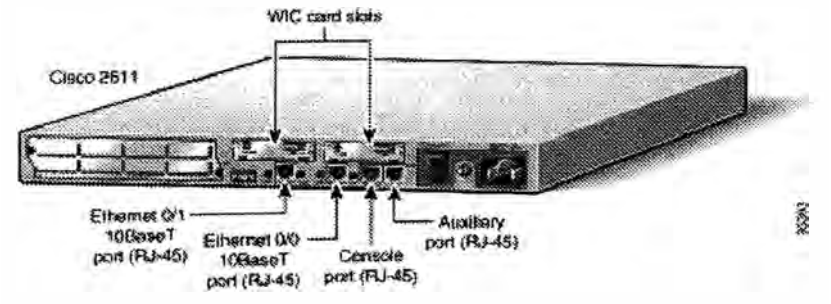


Figura 6.10: Vista trasera del router Cisco 2611

Dado que el router soportará tanto IPSec como ISDN el sistema operativo adecuado es la versión estable 12.0 IP Plus IPSec 56, cuyas características figuran en la tabla que sigue:

Características del IOS 12.0 IP Plus IPSec 56
Management
Cisco IOS File System
Entity MIB
Expression MIB
Conditionally Triggered Debugging
SNMP Inform Request
SNMP Manager
Multimedia/Voice
Voice Over IP
Security
Additional Vendor-Propietary RADIUS attributes
Authenticating ACLs
Internet Key Exchange Security Protocol
IPSec Network Security
MS-CHAP Support
Named Method Lists for AAA Authentication and Accounting
WAN Services
8/16 Analog/Digital Network Module
MPPC-MSPPP Compression
MS Callback
Multiple ISDN Switch Types
National ISDN Switch Type

6.4.5 Router para Accesos Remotos.- El diseño exige un router que soporte configuraciones túnel, L2TP y IPSec; 5 sesiones concurrentes L2TP y 5 sesiones concurrentes IPSec. Un Cisco 1600 Series es una caja adecuada para estas demandas no exigentes.

El sistema operativo IOS 12.1 IP/FW PLUS IPSEC 56 ofrece adicionalmente carácterísticas de firewall para restringir el acceso a los túneles. Como se mencionó este router no tendrá salida al Internet, su función es única y exclusivamente de tunelización.

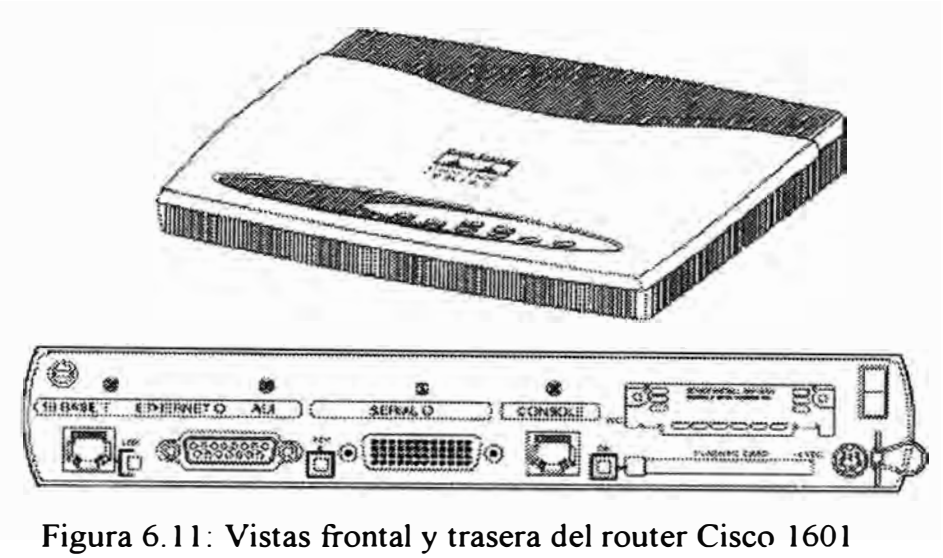


Figura 6.11: Vistas frontal y trasera del router Cisco 1601

El router Cisco 2601 soporta 2 interfaces LAN, una Ethernet y otra AUI. La interface WAN serial soporta modos síncronos para líneas Frame Relay, X.25, SMDS, servicios de 56kbps; y conexiones asíncronas de hasta 115.2kbps.

6.4.6 Switch del Campus Corporativo.- La escogencia del equipo se debió a dos factores: capacidad y seguridad. La solución más adecuada en costo es la de un Cisco Catalyst 5509 con 8 tarjetas de 24 puertos Ethernet 10/100, suficiente para dar cabida a los 150 usarios del campus y al menos 5 servidores de bases de datos. Soporta las características mencionadas para ei Catalyst 2924 XL y ofrece adicionalmente una arquitectura de crecimiento Gibabit Ethernet y características multicapa avanzadas (como end-to-end QoS o mejoras en multicast). La versión de IOS más reciente es la 6.1.

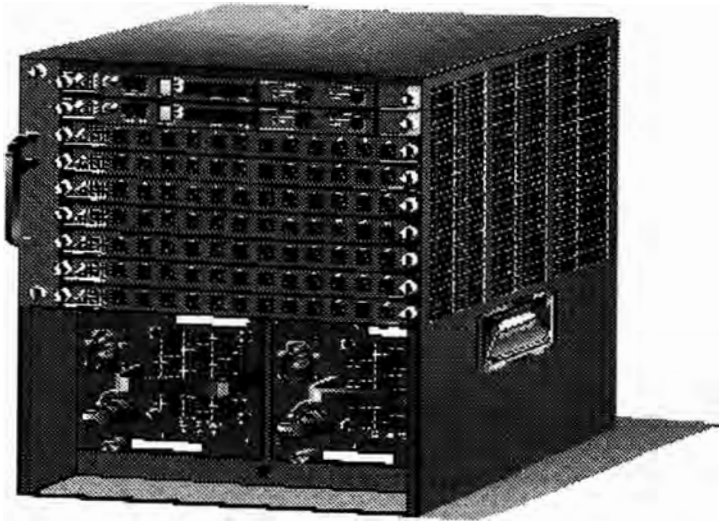


Figura 6.12: Vista frontal del Switch Cisco Catalyst 5509

6.5 Consideraciones restantes.- Habíamos mencionado al inicio del primer capítulo y como veremos en las conclusiones, que el Ingeniero de Seguridad de Red deberá consultar sobre las características de seguridad ofrecidas por el proveedor de servicios de transporte y el ISP en lo que respecta al Internet.

Las exigencias a solicitar deberán agruparse en las ramas de la seguridad de red, a saber, confidencialidad, integridad, disponibilidad, consistencia, control y auditoría.

Hemos mencionado también un carrier con un backbone ATM para el transporte. Las consideraciones a tomar en cuenta son:

- Realizar una inspección al POP y a los nodos para observar las condiciones físicas (cableado estructurado, UPS) y ambientales de los equipos de acceso y switches ATM, respectivamente.
- Exigir detalles sobre las labores de mantenimiento a POPs de la red de acceso y nodos del backbone.

- Solicitar diagramas sobre la redundancia fisica (fibra óptica y cobre) y lógica de la red del carrier.
- Documentación sobre la seguridad de red en POPs y switches ATM. Descripción del sistema de control de acceso del carrier o proveedor.
- Documentación sobre respuesta ante incidentes, tiempo de respuesta, disponibilidad y tiempo de downtime, a nivel de acceso y a nivel de backbone.
- Reportes de utilización de tráfico y de averías.
- Descripción del sistema de Help Desk y Trouble Ticket.
- Auditorías realizadas a la red del proveedor o carrier.
- Documentación sobre el manejo de backups de configuraciones e inventario (no detallado) de partes para redundancia y contingencia.
- Planes de contingencia.

Figura 6.13: Diagrama Simplificado de la Red Corporativa Enterprise.com

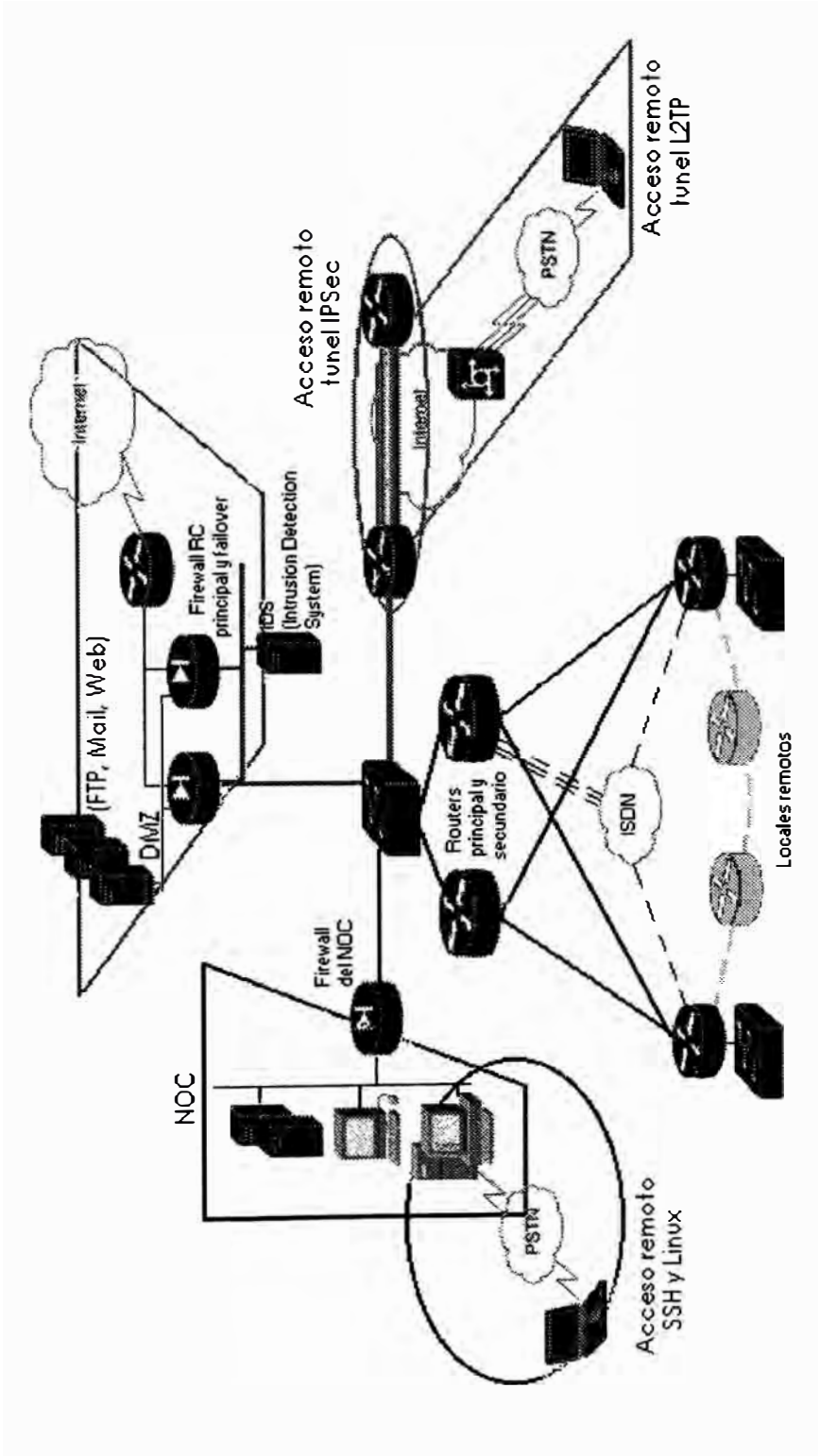
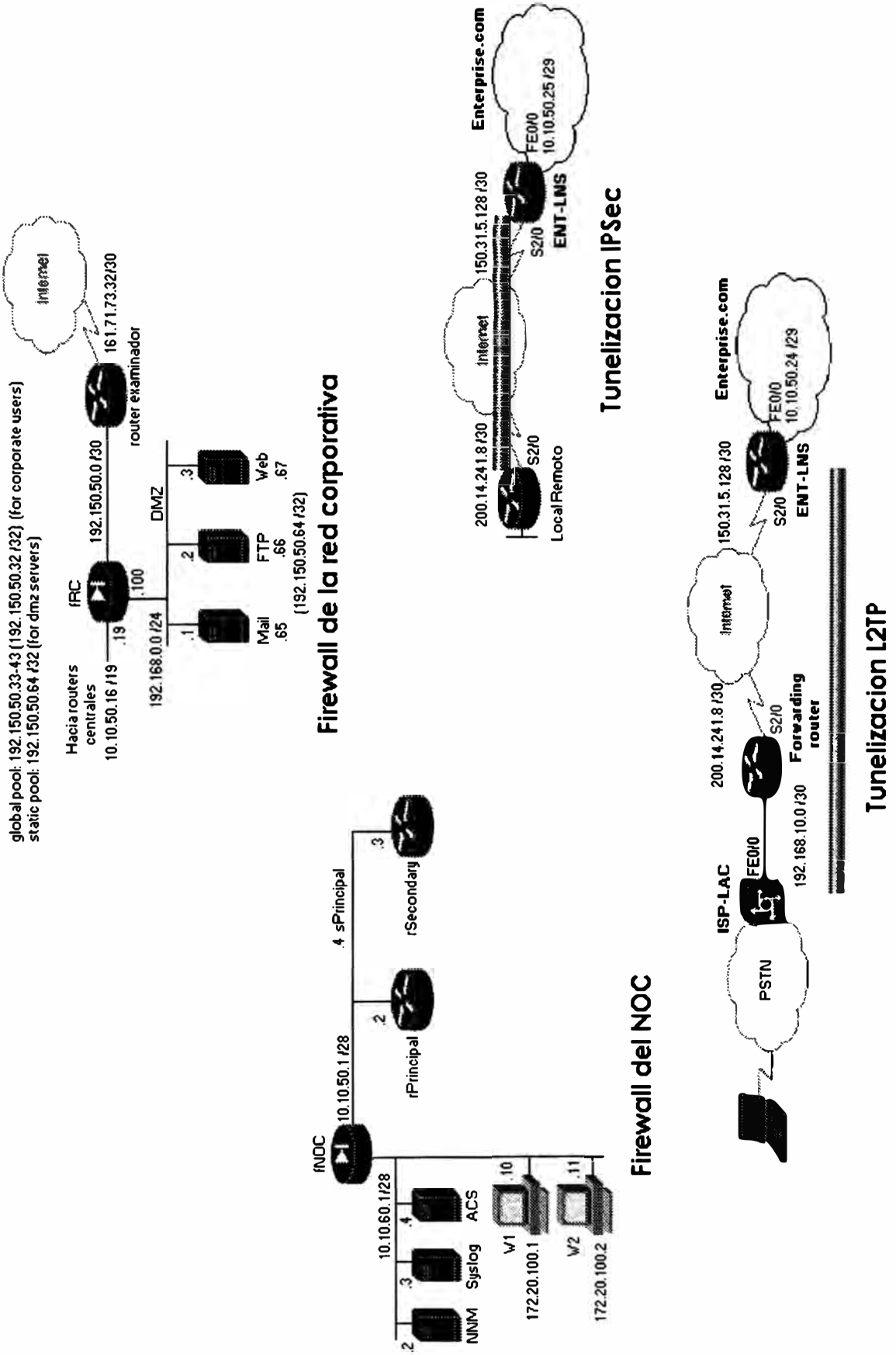


Figura 6.14: Direccionamiento IP por Secciones de la Red Corporativa



Especificación / Recomendacion	NNM	ACS	Syslog	Manejado por el firewall	Administración del NOC
Passwords UNIX normales.	x	x	x		
Política de passwords. Expiración y advertencia.	x	x	x		
/etc/hosts update con script Expect		x			
Who y finger de uso interno.				x	
Control de cuentas durmientes.		x			
Acceso root sólo por consola.	x	x	x		
Exportación RO de archivos originales.		x			
Tripwire para filesystem integrity.	x	x	x		
Observar regularmente lastlog, who y finger.	x	x	x		
Command accounting según sea menester.	x	x	x		
Análisis periódico de procesos.	x	x	x		
Revisión de sulog.	x	x	x		
Mensajes de autorización a printer.			x		
Análisis de logs y backup diario.		x	x		
No probar ni instalar software nuevo	x	x	x		
Permisos de comandos 555, 511.	x	x	x		
Directorios home sólo escribibles por el propietario.	x	x	x		
Contactos para reportes de ataques.					x
Excluir directorio actual del PATH.	x	x	x		
Deshabilitar Systat.	x	x	x		
Telnet y FTP de uso interno mediante TCP wrapper.	x	x	x	x	
Restricción por usuario de FTP.	x	x	x		
No emplear FTP server anónimo.					x
Servidor de correo interno (daemon).	x				
Correo para uso interno (program mode)		x	x		
Versión actualizada de Sendmail y verificar que no soporte debug, wiz o kill.	x	x	x		
Borrar alias "decode".	x	x	x		
Deshabilitar password wizard.	x	x	x		
Seguridad del servidor TFTP.		x			
Reemplazar finger por safe_finger.	x	x	x		
Deshabilitar POP.	x	x	x		
Portmapper.					
Habilitar Identification Protocol.	x	x	x		
Habilitar NTP.		x			
Deshabilitar rexec.	x	x	x		
No emplear ni rlogin ni rsh.	x	x	x		
Deshabilitar routed.	x	x	x		
xhost para X-windows	x	x	x	x	
Deshabilitar rpc.rexd.	x	x	x		
Uso interno del servidor Web.	x				
Estructura de directorio del servidor Web protegida.	x				
Seguridad CGI.	x				
Servidor NFS (exportar sólo RO).		x			
Configurar portmon (NFS)		x			
Comprobar archivos exportados.		x			
Secure NFS	x	x	x		
Monitoreo netstat	x	x	x		
Cronograma de backups					x
Backup de día cero.	x	x	x		x
Backup anual.	x	x	x		x
Prueba de restauración a partir de backups					x
Lista de archivos por backup.					x
Análisis del crecimiento del filesystem	x	x	x		x
Monitoreo del performance.	x				
Servidor PPP			x		

Tabla 6.1 Especificación de los servidores del NOC de Enterprise.com

Tabla 6.2: plan de direccionamiento de Enterprise.com

Descripción	Subnet asociada		Función asociada	Detalles adicionales
Routers centrales - firewall NOC	10.10.50.0 / 28	.1	fNOC	
		.2	rPrincipalRC	
		.3	rSecundarioRC	
		.4	sPrincipalRC	
Routers centrales - firewall RC	10.10.50.16 / 29	.17	rPrincipalRC	
		.18	rSecundarioRC	
		.19	fRCPrincipal	
Routers centrales - Remote Access router	10.10.50.24 / 29	.25	ENT-LNS	
		.26	rPrincipalRC	
		.27	rSecundarioRC	
Base de datos y hosts del Local Principal	172.20.50.0 /24		ligado a routers centrales	
		.1	rPrincipalRC	
		.2	rSecundarioRC	
		.3	rVirtual HSRP	
LAN del NOC	10.10.60.0 / 28			global translation
		.1	gateway	
		.2	NNM	10.10.50.11
		.3	Syslog	10.10.50.10
		.4	ACS	10.10.50.9 (TACACS+); .12 (ICMP); .13 (TFTP); .14 (NTP)
Windows del NOC	172.20.100.0 / 24			nat translation
		.1	RC Windows 1	10.10.60.10
		.2	RC Windows 2	10.10.60.11
fRC - rExaminador	192.150.50.0 /30			
Nat de las estaciones internas de la Red Corporativa	192.150.50.33-45 /27			
DMZ	192.168.0. 0 /24			global translation
		.1	Mail server	192.150.50.65 /32
		.2	FTP server	192.150.50.66 /32
		.3	Web server	192.150.50.67 /32
		.100	Interface DMZ	
Pool de direcciones para acceso L2TP	172.20.20.0/24			
LAN de la sede remota del acceso tunel IPSec	172.20.30.0 /24			
Servidores DNS de Enterprise.com	200.14.35.1 200.14.35.2			Dados por el ISP

Notas
Enlaces locales - central de 256 kbps
Switch - : fNOC, fRC Prin y Sec, rAccesoRemoto de 10 M

Tabla 6.3: Plan de direccionamiento de la red corporativa Enterprise.com

	Locales remotos				Router principal (loopbak 10.10.40.1 /30)				Router secundario (loopback 10.10.40.5 /30)							
Item	Enlace	IP Wan	loopback	LAN subnet	IPWan	Sub-int ATM	VCI	Bridge-group	IPWan	Sub-int ATM	VCI	Bridge-group	EIGRP`s ACL	#Int Dialer	Distribute-list	ISDN subnet
1	local 1	10.10.10.9 / 29	10.10.30.9 / 30	172.20.1.0 / 24	10.10.10.10 / 29	0.101	101	1	10.10.10.11 / 29	0.101	101	1	11	1	51	10.10.20.8 / 30
2	local 2	10.10.10.17 / 29	10.10.30.13 / 30	172.20.2.0 / 24	10.10.10.18 / 29	0.102	102	2	10.10.10.19 / 29	0.102	102	2	12	2	52	10.10.20.12 / 30
3	local 3	10.10.10.25 / 29	10.10.30.17 / 30	172.20.3.0 / 24	10.10.10.26 / 29	0.103	103	3	10.10.10.27 / 29	0.103	103	3	13	3	53	10.10.20.16 / 30
4	local 4	10.10.10.33 / 29	10.10.30.21 / 30	172.20.4.0 / 24	10.10.10.34 / 29	0.104	104	4	10.10.10.35 / 29	0.104	104	4	14	4	54	10.10.20.20 / 30
5	local 5	10.10.10.41 / 29	10.10.30.25 / 30	172.20.5.0 / 24	10.10.10.42 / 29	0.105	105	5	10.10.10.43 / 29	0.105	105	5	15	5	55	10.10.20.24 / 30
6	local 6	10.10.10.49 / 29	10.10.30.29 / 30	172.20.6.0 / 24	10.10.10.50 / 29	0.106	106	6	10.10.10.51 / 29	0.106	106	6	16	6	56	10.10.20.28 / 30
7	local 7	10.10.10.57 / 29	10.10.30.33 / 30	172.20.7.0 / 24	10.10.10.58 / 29	0.107	107	7	10.10.10.59 / 29	0.107	107	7	17	7	57	10.10.20.32 / 30
8	local 8	10.10.10.65 / 29	10.10.30.37 / 30	172.20.8.0 / 24	10.10.10.66 / 29	0.108	108	8	10.10.10.67 / 29	0.108	108	8	17	8	58	10.10.20.36 / 30
9	local 9	10.10.10.73 / 29	10.10.30.41 / 30	172.20.9.0 / 24	10.10.10.74 / 29	0.109	109	9	10.10.10.75 / 29	0.109	109	9	19	9	59	10.10.20.40 / 30
10	local 10	10.10.10.81 / 29	10.10.30.45 / 30	172.20.10.0 / 24	10.10.10.82 / 29	0.110	110	10	10.10.10.83 / 29	0.110	110	10	20	10	60	10.10.20.44 / 30

Tabla 6.4: Política de seguridad del firewall del NOC de la red coporativa Enterprise.com

Sentencias gramaticales	Sentencias lógicas	Sintaxis del PIX firewall
Toda sesión iniciada desde el interior será permitida, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.		
Toda sesión iniciada desde el exterior será denegada, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.		
Traducir direcciones de las estaciones Windows del rango del NOC al rango de la red corporativa	from inside to outside translate: 172.20.100.1 --> 10.10.60.10 172.20.100.2 --> 10.10.60.11	nat (inside) 1 10.10.60.10 255.255.255.255 100 70 nat (inside) 1 10.10.60.11 255.255.255.255 100 70 global (outside) 1 172.20.100.1-172.20.100.2 netmask 255.255.255.224
Permitir acceso desde el exterior hacia el servidor de control de acceso desde rangos privados de la administración.	from outside to inside: permit TCP packet, source address=10.10.0.0/24, destination address=10.10.60.4, destination port=tacacs	static (inside,outside) 10.10.50.15 10.10.60.4 netmask 255.255.255.255 55 100 70 conduit permit tcp host 10.10.50.9 eq tacacs+ 10.10.0.0 255.255.0.0
Permitir acceso desde el exterior hacia el servidor Syslog desde rangos privados de la administración.	from outside to inside: permit UDP packet, source address=10.10.0.0/24, destination address=10.10.60.3, destination port=syslog	static (inside,outside) 10.10.50.10 10.10.60.3 netmask 255.255.255.255 55 100 70 conduit permit udp host 10.10.50.10 eq syslog 10.10.0.0 255.255.0.0
Permitir acceso desde el exterior al servidor NNM desde rangos privados de la administración.	from outside to inside: permit UDP packet, source address=10.10.0.0/24, destination address=10.10.60.2, destination port=snmptrap OR source port=snmp	static (inside,outside) 10.10.50.11 10.10.60.2 netmask 255.255.255.255 55 100 70 conduit permit udp host 10.10.50.11 eq snmptrap 10.10.0.0 255.255.0.0 conduit permit udp host 10.10.50.11 10.10.0.0 255.255.0.0 eq snmp
Permitir acceso desde el exterior al servidor de control de acceso mediante el protocolo ICMP desde rangos privados de la administración	from outside to inside: permit all ICMP packet types, source address=10.10.0.0/24, destination address=10.10.60.3	static (inside,outside) 10.10.50.12 10.10.60.3 netmask 255.255.255.255 55 100 70 conduit permit icmp host 10.10.50.12 10.10.0.0 255.255.0.0
Limitar sesiones TCP sobre los servidores del NOC		Los comandos nat y static incluyen esto
Proteger contra el ataque SYN.		
Denegar (explícitamente) la salida Web de las estaciones UNIX (servidores y workstation).	from inside to outside: deny TCP packet, source address=10.10.60.(2,3,4,5), destination port=http	outbound 1 deny 10.10.60.2 255.255.255.255 80 tcp outbound 1 deny 10.10.60.3 255.255.255.255 80 tcp outbound 1 deny 10.10.60.4 255.255.255.255 80 tcp outbound 1 deny 10.10.60.5 255.255.255.255 80 tcp apply (inside) 1 outgoing_src
Permitir acceso al servidor TFTP desde rangos privados de la administración.	from outside to inside: permit UDP packet, source address 10.10.0.0/24, destination address=10.10.60.4, destination port=tftp	static (inside,outside) 10.10.50.13 10.10.60.4 netmask 255.255.255.255 55 100 70 conduit permit udp host 10.10.50.13 eq tftp 10.10.0.0 255.255.0.0
Denegar (explícitamente) el correo saliente desde las estaciones UNIX hacia el exterior.	from inside to outside: deny TCP packet, source address=10.10.60.(2,3,4,5), destination port=smtp	outbound 2 deny 10.10.60.2 255.255.255.255 25 tcp outbound 2 deny 10.10.60.3 255.255.255.255 25 tcp outbound 2 deny 10.10.60.4 255.255.255.255 25 tcp outbound 2 deny 10.10.60.5 255.255.255.255 25 tcp apply (inside) 2 outgoing_src
Permitir acceso a servidor NTP desde rangos privados de la administración	from outside to inside: permit UDP packet, source address=10.10.0.0/24, destination address=10.10.60.4, destination port=ntp	static (inside,outside) 10.10.50.14 10.10.60.4 netmask 255.255.255.255 55 100 70 conduit permit udp host 10.10.50.14 eq ntp 10.10.0.0 255.255.0.0
El acceso por Telnet al firewall será permitido sólo desde el servidor ACS.	from inside to firewall: permit TCP packet, source address=10.10.60.4, destination address=10.10.60.1, destination port=telnet	telnet 10.10.60.4 255.255.255.255 inside telnet timeout 15 tacacs-server (inside) host 10.10.60.4 tacacs_key timeout 5 aaa authentication telnet outbound 10.10.60.1 255.255.255.255 10.10.60.4 255.255.255.255 tacacs+ aaa authorization telnet outbound 10.10.60.1 255.255.255.255 10.10.60.4 255.255.255.255 tacacs+ aaa accounting telnet outbound 10.10.60.1 255.255.255.255 10.10.60.4 255.255.255.255 tacacs+

Tabla 6.5: Configuración del switch principal de la red corporativa Enterprise.com

```
sPrincipal#sh runn
Building configuration...
Current configuration:
! Last configuration change at 19:16:25 GMT Tue Sep 26 2000
! NVRAM config last updated at 18:03:31 GMT Tue Sep 26 2000
service timestamps log datetime localtime
service password-encryption
no service udp-small-servers
no service tcp-small-servers
hostname sPrincipal
clock timezone GMT -5
interface VLAN1
 ip address 10.10.50.2 255.255.255.248
 ntp broadcast-client
 no ip route-cache
interface FastEthernet0/1
 port storm-control broadcast threshold rising 550 falling 250
 port storm-control trap
 port security max-mac-count 1
 port security action shutdown
 port storm-control trap
 port storm-control threshold rising 550 falling 250
 switch port mode trunk
 switchport access vlan 1
interface FastEthernet0/2
 port storm-control broadcast threshold rising 550 falling 250
 port storm-control trap
 port security max-mac-count 3
 port security action shutdown
 port storm-control trap
 port storm-control threshold rising 550 falling 250
 switch port mode trunk
 switchport access vlan 2
interface FastEthernet0/3
 port storm-control broadcast threshold rising 550 falling 250
 port storm-control trap
 port security max-mac-count 2
 port security action shutdown
 port storm-control trap
 port storm-control threshold rising 550 falling 250
 switch port mode trunk
 switchport access vlan 3
interface FastEthernet0/5-24
vlan 1 name VLAN-fNOC
vlan 2 name VLAN-fRC
vlan 3 name VLAN-RemoteAccess
ip default-gateway 10.10.50.9
logging buffered 10000 debugging
mac-address-table secure hw-addr-fNOC fe0/1 vlan 1
mac-address-table secure hw-addr-fRC fe0/2 vlan 2
mac-address-table secure hw-addr-RCIDS fe0/2 vlan 2
mac-address-table secure hw-addr-rRemoteAccess1 fe0/3 vlan 3
mac-address-table secure hw-addr-rRemoteAccess2 fe0/4 vlan 3
```

```
snmp-server community ROCommunity RO
snmp-server community RWCommunity RW
snmp-server chassis-id 0x0E
snmp-server host 10.10.60.2 traps1 snmp vlan-membership config
tty c2900
line con 0
 password 7 072C205F4706090016
 login authentication default
 stopbits 1
line vty 0 4
 password 7 072C205F4706090016
 login authentication default
ntp source FastEthernet0/14
ntp peer 10.10.60.4
end
```

Configuración de las tarjetas ATM

```
session 0
interface atm0.1 point-to-point
  description fNOC - rPrincipal
  atm pvc 201 0 201 aal5snap 11680 11680
  atm bind pvc vlan 1
interface atm0.2 point-to-point
  description fRC - rPrincipal
  atm pvc 202 0 202 aal5snap 11680 11680
  atm bind pvc vlan 2
interface atm0.3 point-to-point
  description rAccesoRemoto - rPrincipal
  atm pvc 203 0 203 aal5snap11680 11680
  atm bind pvc vlan 3
session 1
interface atm1.1 point-to-point
description fNOC - rSecundarioRC
  atm pvc 201 0 201 aal5snap 11680 11680
  atm bind pvc vlan 1
interface atm1.2 point-to-point
description fRC - rSecundarioRC
  atm pvc 202 0 202 aal5snap 11680 11680
  atm bind pvc vlan 2
interface atm1.3 point-to-point
description rAccesoRemoto - rSecundarioRC
  atm pvc 203 0 203 aal5snap 11680 11680
  atm bind pvc vlan 3
```

Tabla 6.6. Política de Seguridad del Firewall de la Red Corporativa

Sentencias gramaticales	Sentencias lógicas	Sintaxis del PIX firewall
Toda sesión iniciada desde las interfaces outside y dmz serán permitidas, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.		
Toda sesión iniciada desde el exterior hacia las interfaces inside y dmz serán denegadas, salvo indicación expresa. El firewall opera por defecto bajo esta premisa.		
Crear un pool de direcciones globales para las interfaces outside y dmz. Aparte de las 10 direcciones externas manejadas se adiciona una direccional global PAT al final del rango para manejar el overflow. Debido a que el PIX lee las direcciones globales desde el número más alto hasta el menor, el PAT es situado al inicio del rango.	from inside or dmz to outside translate to: 192.150.50.34-192.150.50.43, 192.150.50.33 (PAT)	global (outside) 1 192.150.50.34-192.150.50.43 global (outside) 1 192.150.50.33 global (dmz) 1 192.150.50.44-192.150.50.45
Permitir a los usuarios internos establecer conexiones en las interfaces dmz y outside, y permitir que usuarios en la dmz inicien conexiones a través de la interface outside.	from inside (172.20.0.0/16) and dmz (192.168.0.0/24) permit to outside	nat (inside) 1 172.20.0.0 255.255.0.0 100 70 nat (dmz) 1 192.168.0.0 255.255.255.0 100 70
Permitir que cualquier usuario en la interface outside accese el servidor Mail en la interface dmz.	from outside to dmz: permit TCP packet, source address=any, source port=any, destination address=192.168.0.1, destination port=smtp	static (dmz,outside) 192.150.50.65 192.168.0.1 netmask 255.255.255.255 100 70 conduit permit tcp host 192.150.50.65 eq smtp any
Permitir que cualquier usuario en la interface outside accese el servidor FTP en la interface dmz.	from outside to dmz: permit TCP packet, source address=any, source port=any, destination address=192.168.0.2, destination port=ftp, ftp-data	static (dmz,outside) 192.150.50.66 192.168.0.2 netmask 255.255.255.255 100 70 conduit permit tcp host 192.150.50.66 eq ftp any conduit permit tcp host 192.150.50.66 eq ftp-data any
Permitir que cualquier usuario en la interface outside accese el servidor Web en la interface dmz.	from outside to dmz: permit TCP packet, source address=any, source port=any, destination address=192.168.0.3, destination port=www	static (dmz,outside) 192.150.50.67 192.168.0.3 netmask 255.255.255.255 100 70 conduit permit tcp host 192.150.50.67 eq www any
Permitir que el router examinador accese al servidor ACS.	from outside to inside: permit TCP packet, source address=192.150.50.2, source port=any, destination address=192.150.50.70, destination port=tacacs	static (inside,outside) 192.150.50.70 10.10.60.4 netmask 255.255.255.255 100 70 conduit permit tcp host 192.150.50.70 eq tacacs any
Permitir que el router examinador accese al servidor Syslog.	from outside to inside: permit TCP packet, source address=192.150.50.2, source port=any, destination address=192.150.50.71, destination port=syslog	static (inside,outside) 192.150.50.71 10.10.60.3 netmask 255.255.255.255 100 70 conduit permit tcp host 192.150.50.71 eq syslog any
Limitar sesiones TCP sobre los servidores del NOC.		Los comandos nat y static incluyen esto.
Proteger contra el ataque SYN.		Los comandos nat y static incluyen esto.
El acceso por Telnet al firewall será permitido sólo desde el servidor ACS.	from inside to firewall: permit TCP packet, source address=10.10.60.4, destination address=10.10.60.1, destination port=telnet	telnet 10.10.60.4 255.255.255.255 inside telnet timeout 15 tacacs-server (inside) host 10.10.60.4 tacacs_key timeout 5 aaa authentication telnet outbound 10.10.60.1 255.255.255.255 10.10.60.4 255.255.255.255 tacacs+ aaa authorization telnet outbound 10.10.60.1 255.255.255.255 10.10.60.4 255.255.255.255 tacacs+ aaa accounting telnet outbound 10.10.60.1 255.255.255.255 10.10.60.4 255.255.255.255 tacacs+

Tabla 6.7: Configuración del Router Examinador de la Red Corporativa Enterprise.com

```
service password-encryption
no service udp-small-servers
hostname RouterExaminador
enable secret 5 lLD&77$QRE.222T55Y6xxyM.aRh71
no service finger
no service pad
no ip bootp server
no ip source-route
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa authorization commands 15 default tacacs+ if-authenticated
aaa accounting exec default start-stop tacacs+
aaa accounting commands 15 default start-stop tacacs+
aaa accounting network default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
interface Serial 0/0
  description To the Internet
  ip address 161.71.73.33 255.255.255.252
  ip access-group 111 in
interface Ethernet 1/0
  description To Corporate Network
  ip address 192.150.50.2 255.255.255.252
  no ip directed-broadcast
  no ip proxy-arp
  ip access-group 101 in
  ip access-group 102 out
  no ip route-cache
  no cdp enable
ip classless
ip route 0.0.0.0 0.0.0.0 serial0/0
ip route 192.150.50.32 255.255.255.224 192.150.50.1
ip route 192.150.50.64 255.255.255.224 192.150.50.1
access-list 101 permit tcp 192.150.50.32 0.0.0.31 any
access-list 101 permit tcp 192.150.50.64 0.0.0.31 any
access-list 101 permit udp 192.150.50.32 0.0.0.31 any
access-list 101 permit udp 192.150.50.64 0.0.0.31 any
access-list 101 permit icmp 192.150.50.32 0.0.0.31 any
access-list 101 permit icmp 192.150.50.64 0.0.0.31 any
access-list 101 deny ip any any
access-list 102 permit ip any 192.150.50.32 0.0.0.31
access-list 102 permit ip any 192.150.50.64 0.0.0.31
! anti-spoof filters
access-list 111 deny ip 127.0.0.0 0.255.255.255 any
access-list 111 deny ip 10.0.0.0 0.255.255.255 any
access-list 111 deny ip 172.16.0.0 0.240.255.255 any
access-list 111 deny ip 192.168.0.0 0.0.255.255 any
!
!  Sometimes Enhanced IGRP is run on the Internet link. When you
use
! an input access list, you have to explicitly allow control
! traffic.  This could be more restrictive, but there would have
to be
```

```
! entries for the Enhanced IGRP multicast as well as for the
! corporation´s own unicast address.
access-list 111 permit eigrp any any
!
! These are the ICMP types actuallly used...
! administratively-prohibited is useful when you´re trying to
figure out
! why you can´t reach something you think you should be able to
reach.
access-list 111 deny icmp any 192.150.50.0 0.0.255.255 echo
!
! Deny incoming traceroute
access-list 111 deny icmp any 192.150.50.0 0.0.255.255
traceroute
access-list 111 permit ip any any
no cdp run
!
tacacs-server host 192.150.50.70
tacacs-server key PersonneNeLeSait
!
line con 0
  exec-timeout 2 30
  login authentication default
!
line aux 0
  no exec
  transport input none
line vty 0 4
  exec-timeout 2 30
  login authentication default
!
service timestamps log datetime localtime show-timezone
!
logging on
logging 192.150.50.71
logging console information
```

Tabla 6.8: Costos de las plataformas empleadas en la red corporativa Enterprise.com

150 personas en la sede principal
20 personas en cada uno de los 10 locales sucursales
5 personas accediendo concurrentemente por IPSec
5 personas accediendo concurrentemente por L2TP

Firewall del NOC — **Cisco Secure PIX Firewall 515**

Producto	Descripción	Cantidad	Precio ($)
PIX-515	PIX 515 Chassis only	1	2,500.00
CAB-AC	Power Cord, 110V	1	0
PIX-515R-SW	PIX 515 Restricted Function software license	1	3,000.00
SF-PIX-5.2	PIX v5.2 Software for the PIX Chassis	1	0
PIX-VPN-DES	56-bit DES IPSec software license for PIX	1	0
CON-OSP-PIX515RS	24x7x4 Onsite Svc, PIX-515R-SW Software License	1	500
CON-OSP-PIX515	24x7x4 Onsite Svc, PIX-515 Chassis. Add service for S/W Lic	1	500
	Total		6,500.00

Firewall de la Red Corporativa — **Cisco Secure PIX Firewall 515**

Producto	Descripción	Cantidad	Precio ($)
PIX-515	PIX 515 Chassis only	1	2,500.00
CAB-ACE	Power Cord Europe	1	0
PIX-515UR-SW	PIX 515 Unrestricted Function software license	1	9,500.00
PIX-VPN-DES	56-bit DES IPSec software license for PIX	1	0
SF-PIX-5.2	PIX v5.2 Software for the PIX Chassis	1	0
PIX-1FE	ONE 10/100 Mbps ETHERNET INTERFACES, RJ45	1	200
	Total		12,200.00

Routers Principal y Secundario de la Red Corporativa — **Routers 7206 VXR**

Producto	Descripción	Cantidad	Precio ($)
CISCO7206VXR/300	7206VXR Bundle with NPE-300 and I/O Controller with FE	1	17,000.00
PWR-7200	Cisco 7200 AC Power Supply Option	1	0.00
CAB-AC	Power Cord, 110V	1	0.00
S72C-12103T	Cisco 7200 Series IOS IP	1	0.00
MEM-I/O-FLC20M	Cisco 7200 I/O PCMCIA Flash Memory, 20 MB Option	1	0.00
MEM-SD-NPE-32MB	32MB Memory for NPE-300/NPE-225/NPE-175 in 7200 Series	1	0.00
PA-A3-OC3SMI	1-Port ATM Enhanced OC3c/STM1 Singlemode(IR)Port Adapter	2	20,000.00
CON-OSP-7206	CISCO7206 On-Site Premium Maintenance	1	6,000.00
	Total		43,000.00

Producto	Descripción	Cantidad	Precio ($)
CISCO7206VXR/300	7206VXR Bundle with NPE-300 and I/O Controller with FE	1	17,000.00
PWR-7200	Cisco 7200 AC Power Supply Option	1	0.00
CAB-AC	Power Cord, 110V	1	0.00
S72C-12103T	Cisco 7200 Series IOS IP	1	0.00
MEM-I/O-FLC20M	Cisco 7200 I/O PCMCIA Flash Memory, 20 MB Option	1	0.00
MEM-SD-NPE-32MB	32MB Memory for NPE-300/NPE-225/NPE-175 in 7200 Series	1	0.00
PA-8B-S/T	8-Port BRI Port Adapter, S/T Interface	1	2,000.00
PA-A3-OC3SMI	1-Port ATM Enhanced OC3c/STM1 Singlemode(IR)Port Adapter	2	20,000.00
CON-OSP-7206	CISCO7206 On-Site Premium Maintenance	1	6,000.00
	Total		45,000.00

Switch Principal de la Red Corporativa — **Switch Catalyst 2924 XL**

Producto	Descripción	Cantidad	Precio ($)
WS-C2924-XL-EN	24-port 10/100 Switch (Enterprise Edition)	1	1,995.00
CAB-AC	Power Cord, 110V	1	0
WS-X2971-XL	Catalyst 2900 XL Series ATM 155 SM Fiber Medium Reach Module	2	7,990.00
	Total		9,985.00

Switches de Sucursales — **Switch Catalyst 2924 XL**

Producto	Descripción	Cantidad	Precio ($)
WS-C2924-XL-EN	24-port 10/100 Switch (Enterprise Edition)	1	1,995.00
CAB-AC	Power Cord, 110V	1	0
	Total		1,995.00

Routers de Sucursales

Router Cisco 2600 Series

Producto	Descripción	Cantidad	Precio ($)
CISCO2611	Dual Ethernet Modular Router w/ Cisco IOS IP Software	1	2,495 00
CAB-AC	Power Cord,110V	1	0
S26CL-12104	Cisco 2600 Series IOS IP PLUS IPSEC 56	1	1,200 00
MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series	1	1,000 00
MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series	1	700
WIC-1B-S/T	1-Port ISDN WAN Interface Card(dial and leased line)	1	500
		Total	5,895 00

Router de Accesos Remotos

Router Cisco 1600 Series

Producto	Descripción	Cantidad	Precio ($)
CISCO1601-R	Cisco 1601 R Ethernet/Serial Modular Router	1	1,495 00
S16RCHL-12104	Cisco 1600R Series IOS IP/FW PLUS IPSEC 56	1	1,200 00
MEM1600R-8U24D	8MB to 24MB DRAM Factory Upgrade for Cisco 1600 R	1	1,000 00
MEM1600R-4U8FC	4MB to 8MB Flash Factory Upgrade for Cisco 1600 R	1	400
PWR-1600-WW1	Cisco 1600 AC Power Supply - WORLD-WIDE	1	0
CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet	1	100
CAB-AC	Power Cord,110V	1	0
		Total	4,195 00

Switch del Campus Corporativo (Local Principal)

Switch 5509

Producto	Descripción	Cantidad	Precio ($)
WS-C5509	Catalyst 5509 Chassis	1	2,495 00
WS-C5518	Catalyst 5509 AC Power Supply	1	2,995 00
CAB-7KAC-15	AC Power Cord North America, 15A	1	0
SC5K-SUPG-6 1 1	Catalyst 5K Supervisor 2G & 3G, Flash Image, Release 6 1 1	1	0
WS-X5540	Catalyst 5500/5000 Supervisor IIG	1	8,995 00
WS-X5234-RJ45	24-port 10/100TX Switch Module (FEC,WRED,802 1Q/ISL,RJ-45)	8	39,960 00
		Total	54,445 00

Intrusion Detection System

Netranger v. 2.1.1

Producto	Descripción	Cantidad	Precio ($)
IDS-4230-FE	Cisco Secure IDS Fast Ethernet Sensor	1	$19,000
IDS-DIR	Cisco Secure IDS Director Software	1	$4,995
		Total	$23,995

CONCLUSIONES

A la culminación del presente Informe de Ingeniería, y luego de evaluar el diseño y la implementación, es posible dar las siguientes conclusiones:

- Es imprescindible que un Ingeniero de Seguridad de Red posea conocimientos sólidos de arquitectura de redes y enrutamiento ya que las secciones de redundancia y disponibilidad requieren disponer de tecnologías que los ofrezcan y vayan en concordancia con el diseño jerárquico de la red corporativa. Asimismo, el Ingeniero de Seguridad de Red deberá evaluar y cuestionar las características de seguridad que ofrece el carrier o proveedor de multiservicios y el ISP para Internet consultados.
- Se ha demostrado que la mejor disposición para la seguridad de red es un esquema centralizado, el cual concentra la administración y minimiza el esfuerzo a la hora del troubleshooting y respuesta ante incidentes.
- En la seguridad de red siempre se tiene el factor costo/beneficio y más se nota en la encriptación, es por ello que es necesario encriptar estrictamente lo necesario. En general sobre cualquier plataforma la encriptación consume recursos de CPU enormes. Antes de decidir encriptar, realizar un estudio de los servicios a nivel de puertos TCP y UDP. Descartar la encriptación según si el costo por intromisión o modificación de la información es menor al costo en adquirir plataformas adecuadas.

- Tanto en la seguridad a nivel de host como a nivel de red se debe buscar la tecnología que ofrezca la solución más escalable. Resulta penoso pues a la hora de realizar actualizaciones o modificaciones de red operar sobre cada equipo individualmente.
- La sincronización de los equipos de telecomunicaciones de la red corporativa proporciona la referencia crucial a la hora de investigar un ataque de red. La ausencia de ésta significaría desconocer la correlación de los eventos que dispara un problema de seguridad.
- El registro de eventos no sólo debe incluir los de los equipos de telecomunicaciones, a saber, Syslog, sino los eventos por injerencia humana. La contabilidad de comandos de configuración por los administradores de red deberá ser obligatoria y deberá existir accesos de último recurso cuando el servidor de control de acceso se halle indisponible.
- La experiencia demuestra manifiestamente que un hardware dedicado como el PIX de Cisco provee la robustez solicitado a un firewall. El hecho que sea el firewall más vendido en el mundo es una realidad latente. Si bien su interface de usuario es arcaica, la seguridad primo por sobre la flexibilidad.
- Si bien L2TP no es ofrecido en el mercado peruano, éste ofrece un nuevo servicio, ventajoso, flexible y seguro que puede ser explotado por los ISPs locales. Básicamente el costo se reduce al NAS y a las líneas telefónicas adquiridas.
- Un diseño de red y de seguridad de la misma debe afanarse en emplear tecnologías interoperables como IPSec y L2TP, que aseguren que operen bajo

plataformas de diferentes fabricantes. Así el crecimiento de red no se ve restringido o limitado por las características propietarias de un equipo.

- El sistema operativo idóneo para los servidores del NOC de la red corporativa es el UNIX, debido a su gran soporte en aplicaciones y características de seguridad, su gran robustez y performance, flexibilidad y accesibilidad.

BIBLIOGRAFIA

[1] Firewalls and Internet Security, Repelling the Wily Hacker: *William R.. Cheswick & Steven M. Bellovin,* Adisson-Wesley 1994.

[2] Practical UNIX & Internet Security: *Simson Garfinkel & Gene Spafford,* O´Reilly 1996.

[3] Designing Network Security: *Merike Kaeo*, CiscoPress 1999.

[4] CCIE Professional Development: Advanced IP Network Design: *Alvaro Retana, Don Slice & Russ White,* Cisco Press 2000.

[5] CCIE Professional Development: Large-Scale IP Network Solutions: *Khalid Raza, Mark Turner,* CiscoPress 2000.

[6] Building Internet Firewalls: *D. Brent Chapman & Elizabeth D. Zwicky.* O´Reilly 1995.

[7] Solaris Security: *Peter H. Gregory,* Sun Microsystems Press 2000.

[8] Building and Managing Virtual Private Networks: *Dave Kosiur,* John Wiley & Sons, Inc. 1998.

[9] Virtual Private Networks: Turning the Internet Into Your Private Network: *Charlie Scott, Paul Wolfe & Mike Erwin.* O´Reilly 1999.

[10] L2TP, Implementation and Operation: *Richard Shea.* Adisson-Wesley, 2000.

[11] Secure Shell: *Anne Carasik,* McGraw-Hill, 1999.

[12] Cisco IOS Dial Solutions, CiscoPress 1998.