UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y ANALISIS DE PROTECCION Y AMENAZAS DE SEGURIDAD EN REDES DE COMUNICACIÓN

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

ROMMEL NILO RÍOS ALCÁNTARA

PROMOCIÓN

1988 - I

LIMA – PERÚ

2011

ESTUDIO Y ANALISIS DE PROTECCION Y AMENZAS DE SEGURIDAD EN REDES DE COMUNICACIÓN

Dedico este trabajo a mis padres,

Y mis hijos, que son mi razón.

SUMARIO

En este trabajo se pone de manifiesto el problema de la seguridad en los procesos de intercambio de información en redes de comunicación, planteando una serie de metodologías usadas y un conjunto de parámetros a tener en consideración cuando se diseñen sistemas de información que deben transportar datos importantes.

En el capítulo I se resume brevemente algunos conceptos y definiciones de uso común, como protocolos, conceptos sobre redes, y equipos de uso cotidiano sin entrar en detalles.

El capítulo II enfoca conceptualmente la seguridad en redes de comunicación, para tener una idea clara del tema. Cubre de manera descriptiva algunas metodologías usadas como protección de información en redes de comunicación.

El capítulo III trata de metodologías para el análisis de amenazas de seguridad presenta una metodología ordenada para analizar amenazas de seguridad de redes de comunicaciones mencionando un modelo desarrollado para tal fin.

El capítulo IV trata de soluciones a las amenazas mediante un Firewall, que pueden ser implementados con Hardware y Software.

El Capítulo V trata de la implementación de un Firewall mediante un servidor ISA usando Windows 2003 Server como Sistema Operativo.

INDICE

INTRODUCCION

El presente trabajo no pretende dar una explicación completa al análisis y estudio riguroso del problema de la seguridad de información en redes de comunicación, que es basta, si no permitir que este tema tenga la relevancia suficiente como para ser considerado dentro de los mecanismos necesarios del procesos de tratamiento de la información, más aun cuando ésta reviste importancia por el tipo de data que se manipula, donde la seguridad es un elemento de crucial importancia y por lo tanto, deberán tomarse todas las medidas de control y seguridad necesarias.

Adicionalmente, en conjunción con los sistemas que deben servir para tales fines, el hardware también cumple un rol de vital importancia, por ello la correcta y adecuada selección de los equipos contribuirá a que las metodologías para el control y la seguridad en redes de comunicación tengan el éxito necesario.

Existen muchos modelos para estudiar el problema de la seguridad y amenazas de la información, más a fin de que permitan poder ahondar aún más sobre otros procedimientos.

Finalmente, quiero expresar mi gratitud por esta institución que permitió lograrme como profesional, así mismo a todos mis profesores que durante largos años me brindaron todo lo necesario y que hoy puedo decir sirvió de mucho.

CAPÍTULO I

CONCEPTOS INTRODUCTORIOS

1.1. PROTOCOLOS

Un protocolo de comunicaciones es el conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación. Estas reglas y normas permitirán que en las comunicaciones se use un mismo lenguaje y de esta manera los sistemas funcionen adecuadamente.

1.1.1. TCP/IP

Se denomina así al protocolo que actualmente usamos para obtener los servicios de Internet (E-Mail, FTP, Comunicación instantánea, etc.) entre ordenadores que no pertenecen a la misma red.

TCP/IP indican dos protocolos:

El Protocolo de Control de Transmisión (TCP) que permite a dos anfitriones establecer una conexión e intercambiar datos. El TCP garantiza la entrega de datos, es decir, que los datos no se pierdan durante la transmisión y también garantiza que los paquetes sean entregados en el mismo orden en el cual fueron enviados.

El Protocolo de Internet (IP) utiliza direcciones que son series de cuatro números que representan a octetos (byte) con un formato de punto decimal, por ejemplo: 192.168.1.59

Actualmente existen dos versiones el **IPV4** y el **IPV6**, este último aparece a raíz de que IPV4 ya tiene agotado las direcciones a nivel mundial. IPV4 proporciona 2^{32} direcciones, mientras que IPV6 proporciona 2^{128} direcciones con los cuales cubriría por mucho tiempo una dirección por habitante en la tierra.

Los Protocolos de Aplicación como HTTP y FTP se basan y utilizan TCP/IP.

1.1.2. SNMP (Simple Network Management Protocol)

Es un protocolo simple de administración de red, se ejecuta en la capa de aplicación, es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

1.1.3. FTP (File Transfer Protocol)

Protocolo de Transferencia de Archivos en español, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmision Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

1.1.4. APPC

Protocolo de transporte de IBM desarrollado como parte de su arquitectura de redes de sistemas (SNA). Se diseña para permitir que los programas de aplicación que se ejecutan en equipos distintos puedan comunicarse e intercambiar datos directamente.

1.1.5. NETBEUI

Es una interface de usuario NetBIOS y extendida, originalmente ambos estaban muy relacionados, y se consideraban un protocolo de nivel de sesión, de forma que se pudiera usar con otros protocolos enrutable de transporte.

NetBIOS (interface de entrada y salida de red) es una interfaz de LAN del nivel de sesión de IBM que funciona como una interfaz de aplicación para la red.

Proporciona las herramientas para que un programa establezca una sesión con otro programa a través de la red. Es muy popular porque muchas aplicaciones lo admiten.

1.1.6. WAP (Wireless Aplication Protocol)

Es un protocolo a la aplicación inalámbrica que se utiliza para comunicar computadoras de mano y celulares para Internet Móvil.

1.2. REDES POR DIFUSIÓN

Tiene un solo canal de comunicaciones compartidas por las máquinas de la red, los mensajes cortos (llamados paquetes en cierto contexto) que envía una maquina son recibidos por todos los demás. Un campo de dirección está dentro

del paquete específico a quien se dirige, al recibir un paquete una maquina verifica el campo de dirección, si el paquete está dirigido a ella lo procesa, si no lo ignora.

La difusión ofrece la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección.

1.3. REDES BASADAS EN SERVIDOR

Cuando una red se expande a más de 10 ó 12 usuarios se recomiendan implementar una red basada en servicios dedicados, debido a que están optimizados para dar un servicio rápido a las peticiones de los clientes y para organizar la seguridad de los archivos y de los directorios.

Distribuir las tareas entre varios servidores, asegura que cada tarea se realizará de forma más eficiente posible.

Ventajas de las redes basadas en servidor:

Compartir recursos: los recursos están ubicados normalmente de manera centralizada y resulta más fácil de ubicar y de administrar que los recursos de os equipos descentralizado.

Seguridad: se puede administrar la seguridad mediante un administrador que configure las normas del sistema que aplique a todo los usuarios de la red.

Copias de seguridad: como todo está centralizado es más fácil asegurarse que se realicen copias de los datos que servirán como respaldo.

Número de usuario: soporta miles de usuarios

Redundancia: permite mantener datos como respaldo que luego se puede recuperar.

1.4. DSL (Digital Subscriber Line)

Línea de abonado digital en español, tecnología que permite el uso de la línea de cobre (la que conecta nuestro domicilio con la central telefónica) para transmisión de datos de alta velocidad y a la vez, para el uso normal como línea telefónica. Se llama XDSL ya que los acrónimos de estas tecnologías acaban en DSL, que está por “Digital Subscribir Line” (línea de abandono digital): IDSL, HDSL, SDSL, ADSL, VDSL. Cada una de estas tecnologías tiene distintas características en cuanto a presentaciones (velocidad de la transmisión de datos) y distancia de la central (ya que el cable de cobre no esta no estaba pensada para

eso, cuanta más distancias peores prestaciones). Una línea telefónica típica, utiliza solo una pequeña parte de su capacidad de transmisión DSL usa el resto, permitiendo conexiones más rápidas que las proporcionadas por un MODEM convencional. De esta forma solo se aprovecha el ancho de banda sobrante, sino que además es posible utilizar el teléfono al mismo tiempo que se recibe o transmite datos.

Para usar DSL se necesita:

Una línea telefónica acondicionada para funcionar con DSL. (Longitud menor de 3.5 km. y central DSL).

Un **MODEM** que soporta DSL.

En algunos casos un spliter (división) para separar la línea de voz de la línea de datos.

Un proveedor de servicios de internet.

1.5. FRAME RELAY

Frame Relay es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones.

El concepto de red Frame Relay es similar a la de X-25, pero al reducir el procesamiento de protocolos en cada modo de la red se disminuye el retardo global de extremo. Todos los acuses de recibo y recuperación de error quedan a cargo del equipo de usuario; asimismo; el control de flujo se realiza en los puntos extremos (aunque la red si genera indicaciones de congestión, cuando ello se hace necesario).

El manejo de red simplificado de Frame Relay conlleva una utilización más eficiente de la línea aumentando el throghput de la red. Frame Relay utiliza solo las dos primeras capas del modelo OSI.

1.6. INTERLAN

La conmutación de paquetes es una técnica de comunicación de paquetes de área extendida, según la cual los datos son empaquetados para su envío por una red de datos compartida en lugar de por líneas alquiladas.

La conmutación de paquetes difiere de la conmutación de circuitos en que utilizan circuitos virtuales, o sea, consta de ancho de banda asignada según demanda desde una red de circuitos compartidos.

En las redes de paquetes no hay conexión física directa entre los dos usuarios que intercambian información; la conexión es lógica. En los circuiros virtuales se establece una ruta específica para cada llamada; todo los paquetes de llamada siguen esta ruta a través de la red. En el destino se vuelven a armar los paquetes para reconstruir el formato original.

- Mayor rendimiento de la línea, ya que los enlaces de largo distancia son compartidos dinámicamente por numerosas llamadas y usuarios.
- Manejo de carga – la red brinda acoplas para sobreponerse a incrementos temporales de la carga sin que se produzca bloqueo.
- Conversión de velocidad de datos – usuarios a distintas velocidades pueden intercambiar información.
- Costos más bajos como resultado de compartir los recursos de la red con numerosos usuarios.

  La red interLAN soporta los productos que puedan ser encapsulados en Frame Relay, los más frecuentes son IP e IPX.

1.7. FIREWALLS

Un sistema de firewall (cortafuego) es un conjunto de componentes Hardware y Software Destinados a establecer controles de seguridad en el punto a punto de entradas de nuestra red a Internet.

Una característica importante de estos sistemas es que permiten llegar hasta los mecanismos de seguridad de sistemas operativos los tipos de firewall son:

1.7.1. Packet Filter (Filtrado de Paquetes)

Se basa en el tratamiento de paquetes IP a los que se aplican unas reglas de filtro que permite discriminar el tráfico según nuestras indicaciones. Normalmente se implementa mediante un router con dos interfaces de red, uno de cara al exterior y otro al interior, aunque podría utilizarse cualquier maquina con dos placas de red o software adecuado para filtrado de los paquetes IP.

Al tratar paquetes IP, los filtros que podremos establecer serán a nivel de direcciones IP, tanto fuente como destino. Normalmente, se establece una lista de filtros por interfaces que se aplican a cada paquete independiente de los anteriores, o de cierto servicio. Algunos filtrados de paquetes permiten establecer filtros también a nivel de puertos TCP, con lo que podremos filtrar que servicios dejamos pasar o no.

1.7.2. Pasarelas a nivel de aplicación.

Es el externo opuesto a los filtros de paquetes. En lugar de basarse en el filtrado del flujo de paquetes, trata los servicios por separado, utiliza el código adecuado para cada uno.

Las pasarelas a nivel aplicación son prácticamente la única solución efectiva para el tratamiento seguro de aquellos servicios que requieren permitir conexiones iníciales desde el exterior (servicios como FTP, Telnet, correo electrónico).

1.7.3. Pasarelas a nivel de Circuito

Se basan en el control de las conexiones TCP y actúan como si fuesen en cable de red, por un lado reciben las peticiones de conexión a un puerto TCP y por otro, establecen la conexión con el destinatario deseado si se han cumplido con las restricciones establecidas, copiando los octetos de un puerto a otro.

1.7.4. Cortafuegos basados en certificados digitales.

Este tipo de cortafuegos basados en certificados digitales son exactamente seguros con una gran funcionalidad.

Cuando se realiza un sistema de Firewall, suelen emplearse varios o todos los tipos antes vistos, se hace así desde los paquetes de red, pasando por los puertos de conexión hasta el servicio propiamente dicho.

1.8. GATEWAY

Es un dispositivo que alcanza una LAND a una red de área amplia usualmente la Internet y a veces incluye un modem de banda ancha.

1.9. ROUTER

Es un dispositivo que recibe el tránsito de Internet y lo encamina a una o más computadoras, lo que permite, por ejemplo compartir una conexión a la web.

1.10. CONCENTRADOR O HUB

Es un dispositivo que suele estar provisto de varios puertos Ethernet a los que se pueden conectar varios componentes de la red para comunicarse.

1.11. REDES INALÁMBRICAS

Están basadas en el estándar IEEE 802.11 el cual tiene dos subgrupos denominados:

1. El estándar IEEE 802.11b
2. El estándar IEEE 802.11g

Existen tres áreas:

Red de área personal

La nueva tecnología inalámbrica Bluetooth permite estar conectado automáticamente a sus periféricos Bluetooth tan pronto y cuando entre dentro del rango de 1 a 10 metros.

Bluetooth es un chip capaz de trasmitir y recibir información desde cualquier dispositivo sin necesidad de utilizar ningún cable y es una manera simple de conectarse de conectarse y comunicarse entre dispositivos sin necesidad de utilizar ningún cable y es una manera simple de conectarse y comunicarse entre dispositivos de mano, teléfonos portátiles, dispositivos de acceso a red y periféricos inalámbricos o con cables. Es una tecnología actual que se utiliza en teléfonos portátiles. Tiene la característica de ser una tecnología de bajo costo que se requiere mucha energía. Esto lo capacita para uso ideal en amplia variedad en el mercado de dispositivo de batería.

Bluetooth es de corto alcance, hasta 10 metros o aproximadamente 30 pies, punto a punto o enlace de radio multipunto. Un dispositivo puede comunicarse con solo un dispositivo u otros múltiples (hasta 7).

Dispositivos Bluetooth en lo que se refiere a un piconet. Esto es muy importante en un ambiente de oficina.

La otra habilidad del Bluetooth es su capacidad de formar un "scatternet". Un scatternet se forma habiendo un enlace de multiplespiconets. Conectando multplespiconets con su scatternet Bluetooth puede dar soporte a un número mayor de dispositivos.

Los dispositivos Bluetooth usan la tecnología spreadspectrum, frequency-hopping la cual provee una buena conexión y evade y evade la interferencia de otros dispositivos de radio.

Cuando nos referimos a Bluetooth, hablamos de una nueva tecnología para comunicaciones inalámbricas que permite conexiones de banda estrecha entre dispositivos, ya sean computadoras, PDA, telefonía móvil o cualquier tipo de periféricos, de tal manera que pueden comunicarse entre ellas sin hilos.

Los sistemas Bluetooth, utilizan una señal que opera en la banda de 2,4GHZ y que hace múltiples saltos de espectro para reducir las posibles interferencias con otros dispositivos. La señal cambia mil 600 veces cada segundo sobre 79 frecuencia distintas. Además, no necesita licencia y está disponible en casi todo el mundo. Su radio de acción es de 10 metros, es decir, se trata de un sistema de corto alcance, aunque su cobertura puede llegar a 100 metros con repetidores.

Llamada en Ingles Cellular Digital Packet Data (Información en pequeña paquetes digitales celulares) que utiliza una red de teléfonos celulares y transmite a una velocidad máxima de 19.2 kbps, pero la tasa convencional de transmisión de información es de 9.6 kbps.

Red de área local

Una vez que haya salido de los confines de una oficina se podrá mantener una conexión al servidor de su compañía utilizado la tecnología IEEE de LAN inalámbrico 802.11b la tecnología de LAN inalámbrico 802.11b le permite rondar (hasta 100 metros o alrededor de 300 pies) en la universidad, en su ambiente de oficina, hogar, escuela, aeropuerto o habitación de hotel, mientras se mantiene conectado a sus datos a una velocidad hasta 11Mbps.

Tecnología IEEE de LAN inalámbrica 802.11b. Una LAN inalámbrica puede simplificar la manera de conectarse o extender de red de área local para negocios. El tipo de LAN inalámbrica que se está introduciendo comúnmente se le llama el “802.1b” WI-FI. Este nombre – número proviene de las especificaciones de industria del IEEE cuya organización define las características de este tipo de LAN inalámbrica.

Así que en vez de estar atado a una conexión de cable de red en su oficina u hogar, se puede fácilmente llevar una portátil (Laptop) a cualquier parte del

edificio y permanecer conectado constantemente por vía una conexión inalámbrica.

IEEE 802.11b es el estándar mundial para LAN inalámbricos en el espectro de 2.4 GHz. Este especifica una tasa alta que opera a 11Mbps comparando a los estándares anteriores, como el 802.11 y el Home RF los cuales se limitan a solo 2Mbps.

Red de área amplia

Combinando la tecnología inalámbrica Bluetooth con un teléfono portátil Bluetooth se puede llegar a extender la capacidad de conexión hacia ambiente fuera de los recintos de la compañía. El teléfono portátil Bluetooth se convierte en un punto de acceso a red para una portátil. Se podría estar sentando literalmente en un banco en el parque, o en cualquier parte del mundo, y aun así conectarse a la red de su compañía por medio de un teléfono portátil.

1.12. TEORÍA FUNDAMENTAL SOBRE REDES INALÁMBRICAS

A pesar del rendimiento y productividad de las modernas redes de aérea local (LAN) razonablemente aceptables, la alta movilidad y disponibilidad de las nuevas formas de negocio precisan nuevas sistemas que mejoran los actuales métodos de conexión. Para muchos profesionales, la telefonía móvil ha supuesto una valiosa ayuda a sus necesidades de conectividad y movilidad. Igualmente, la informática portátil permite extender la funcionalidad de los ordenadores donde vayamos. La unión de ambas herramientas ha hecho posible el intercambio de pequeñas cantidades de información o, incluso, el uso de internet, sin necesidad de tener que usar las tradicionales líneas telefónicas. Para ciertas empresas modernas, PYMES en su mayoría, que precisan comunicar sus diferentes dispositivos sin las limitaciones que acarrea el uso del cable en sus entornos de trabajo; existen desde hace tiempo ciertas tecnologías que tratan de satisfacer las necesidades de conectividad de este tipo de empresas, pero no han tenido el éxito esperado por diferentes motivos, ya sea por los elevados condicionalmente a la hora de efectuar la transmisión libre de errores o la fragilidad de enlace debido a los agentes meteorológicos.

Las Redes inalámbricas jamás reemplazaran a la red cableada.

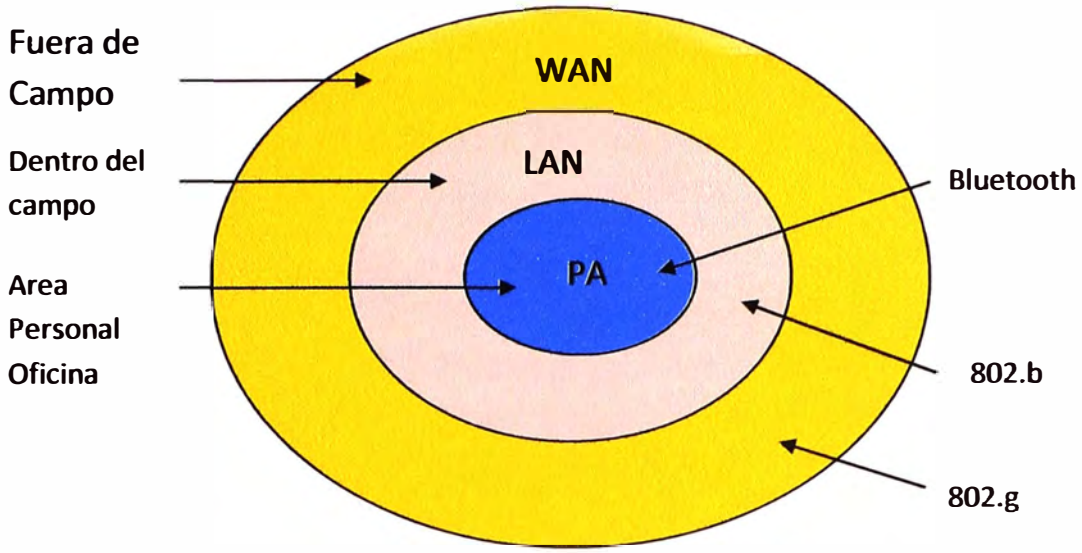


Figura 1.1 Cobertura de las redes inalámbricas

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, principalmente porque las velocidades de transmisión logrados con la tecnología inalámbrica no son comparables con las que actualmente puedan alcanzarse con los diferentes medios físicos de transmisión que utilizan cable o fibra óptica. Mientas que redes inalámbricas actuales ofrecen velocidades de hasta 10Mbps. Las redes cableadas de mayor uso y estandarización ofrecen como mínimo esta misma velocidad, pero alcanzan los 100Mbps, sin mayores complicaciones. Sin embargo, una acertada solución puede pasar por mezclar las redes cableadas y las inalámbricas, y de esta manera generar una red hibridad para resolver los segmentos o puntos más problemáticas de la red. Se puede considerar que el sistema de cableado sea la parte principal y la inalámbrica proporcione la movilidad adicional al equipo o segmento de red para que los posibles usuarios puedan desplazarse con facilidad dentro y fuera del entorno de operaciones.

1.12.1. WLAN, redes inalámbricas de aérea local.

El concepto de WLAN, acrónimo de las siglas en ingles de wireless local área Network no es otra cosa que el sistema de comunicación de datos flexibles utilizando como alternativa a la LAN cableada o como una extensión de esta. Hay

grandes avances en tecnologías inalámbricas de interconexión, así como la presentación de dispositivos personales para informática móvil. El medio de transmisión para comunicaciones inalámbricas utiliza ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico.

Existen básicamente, dos opciones de transmisión en la WLAN; de acuerdo al ángulo de apertura con que emite la información en el trasmisor.

Las ondas de radio son normalmente referidas a portadoras de radio, ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo puedan ser extraídas en el receptor final. Varias ondas portadoras puedan existir en el mismo tiempo y espacio sin interferir entre ellas, siempre que estas ondas sean trasmitidas a distintas frecuencias de radio. Se clasifiquen en:

Sistemas de banda ancha (narrow band) de frecuencia dedicada.

El sistema de banda ancha se transmite y recibe en una banda específica de frecuencia para el paso de información. Los usuarios tienen distintas frecuencias de comunicación para evitar las interferencias. Asimismo, un filtro en el receptor se encarga de dejar pasar únicamente la señal esperando en la frecuencia asignada.

Sistema basado en espectro disperso o extendido (spread spectrum)

Independientemente del sistema empleado, según la banda que utilicen para la emisión y recepción de la información, necesitaran o no, permisos de las autoridades competentes en el asunto, se transmiten la información en bandas del espectro que no quiere autorización para su uso, las llamadas bandas para aplicaciones industriales, científicas y medidas (ICM). Algunas de estas frecuencias están siendo extensamente utilizadas por otros dispositivos como teléfonos inalámbricos, puertos de garaje inalámbrico que operan estas bandas y deben ser diseñados para trabajar bajo interferencia considerables. Por ello, buena parte de estas redes utilizan una tecnología desarrollada en los años de 40 para proveer comunicaciones militares, llamada técnica de espectro disperso.

Para las aplicaciones comerciales, existen dos técnicas de modulación en espectro disperso:

Salto de frecuencia (FHSS – Frecuencia – Hopping Spreed Spectrum)

En la primera, la información se transmite a saltos de manera pseudo aleatoria en intervalos de tiempos fijos, llamados chips, de un canal de frecuencia a otro dentro de la banda, que cambia según un patrón conocido por trasmisor y receptor.

Conveniente sincronizado, es como tener un único canal lógico. Únicamente legal receptor sincronizado en el trasmisor, y que tenga exactamente el mismo código de salto, podría acceder a las frecuencia correspondiente y extraer la información. En cambio, para un receptor no sincronizar FHSS es como un ruido de impulso de corto duración.

Secuencia directa (DSSS – Direct – Sequence Spread Spectrum)

Se genera un bit redundante por cada bit trasmitido. Estos bits redundantes son llamados chippingcode. Cuando mayor sea esta secuencia, mayor es la posibilidad de reconstruir los datos originales. En otras palabras, la información se mezcla con un patrón seudo aleatorio de bist con una frecuencia mayor que la información a transmitir. Al igual que con el asalto de frecuencia, solamente aquel receptor que tenga el mismo código de extensión, será capaz de generar información original, incluso uno o más bits pueden reconstruir los datos originales sin necesidad de retransmitir, mientras que para un receptor, cualquiera emisión DSSS es un ruido de baja potencia que resulta ignorado.

Aunque como referencia sirva decir que la tasa de trasferencia datos de la capa física para sistemas FHSS es de 1Mbps, mientras que para DSSS soporta tasa de 1 o 2 Mbps. La mayor parte de las WLANs pueden configurarse de dos formas diferentes.

Redes ad-hoc

En las primeras, también llamadas redes entre pares, varios dispositivos conforman una red intercambiar información sin contar con el apoyo de elementos auxiliares. Este tipo de red resultado ideal para conformar grupos grupos de trabajo temporales en reuniones, o conferencias.

Redes Basados en infraestructura

Es la más implantada en la actualidad, las **WLAN** se utilizan como una extensión a la infraestructura de red basada en cable. En este modelo, es frecuente que los

modos inalámbricos, a los cuales se les suele denominar estaciones remotas, actúen como cliente que solicitan servicios e información a servidores generalmente conectados a esa estructura cableada de red, a través de puntos de acceso llamados estaciones base.

Los diversos mecanismos de acceso que se han propuesto e implementado para WLAN se agrupan en dos categorías.

1.12.2. Protocolo con arbitraje (FDMA, TDMA)

Es mecanismo de múltiplex eje en frecuencia, FDMA, divide todo el ancho de banda asignado en distintos canales individuales. Este es un mecanismo simple que permite el acceso inmediato al canal, pero poco eficiente para utilización en sistema que presenta un comportamiento típico de trasmisión de información por breves periodos de tiempo (ráfagas). Una alternativa algo más factible seria asignar todo el ancho de banda disponible a cada modo durante un breve intervalo de tiempo de manera cíclica. Este sistema, llamado múltiplex por acción en el tiempo (TDMA), requiere mecanismo muy preciso de sincronización entre los nodos participantes para evitar interferencias, este último esquema ha sido utilizado con cierto éxito, sobre todo las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

1.12.3. Protocolos por contención (CDMA/CD, CDMA/CA)

Por el contrario, el protocolo de acceso múltiple por división de código (CDMA), es el mecanismo de acceso por excelencia para que puedan coexistir diferentes redes. Las WLAN que emplean mecanismo de contención como acceso al medio, están basadas en el modelo utilizado por la tecnología en red local más difundida en la actualidad, Ethernet IEEE 802.3 varias de las primeras redes utilizan el algoritmo de acceso al medio CSMA/CD. El cual se caracteriza por comprobar previamente que el medio de comunicación estaba libre, antes de iniciar la trasmisión. Si se daba esta condición, entonces se trasmitía la información y si no, esperaba a que se liberarse al medio. Como existía que a pesar de iniciar la trasmisión se debería continuar con la vigilancia del canal para detectar posibles colisiones. Cuando éste ocurría, la trasmisión era suspendida y las estaciones involucradas en el conflicto debían esperar un tiempo aleatorio

antes de repetir nuevamente al algoritmo. El protocolo 802.11 utiliza un tipo de protocolo conocido como CSMA/CA (Corrier – Sense, Multiple de Access, CollisionAvoindance). Este protocolo introduce una variante en el algoritmo anterior que evita las colisiones en la transmisión en lugar de descubrir una colisión, fundamentado en el hecho que la probabilidad de que se produzca una colisión en CSMA/CD se da, precisamente, al terminar una trasmisión. Es decir, al haber más de una estación esperando que una trasmisión en curso termine para que ellas puedan comenzar a transmitir, si no se adoptan las medidas oportunas estas estaciones comenzaran, toda a la vez, a enviar información provocando una colisión en el medio.

La capa física para la trasmisión inalámbrica y la capa de control de acceso al medio MAC, representa el primer estándar para los productos WLAN, la capa de acceso al medio se divide en dos subcapas. En el nivel más bajo se define la llamada función de coordinación Distribuida (DCF), que proporciona una comunicación asíncrona entre estaciones que utilizan el protocolo CSMA/CA. Los servicios de trasferencia de datos sin restricciones de tiempo, utilizan directamente este protocolo para intercambiar información.

A pesar del buen comportamiento general de este sistema, presenta una deficiencia cuando un dispositivo inalámbrico transmite con la potencia justa para que sea escuchado por un nodo receptor, pero no con la suficiente como para que esta trasmitido. Para resolver este conflicto, se ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con recomendación positivo. A grandes rasgos, este proceso hace que cuando una estación esta lista para trasmitir, primero envía una solicitud al punto de acceso (RTS- Request to Send) quien, si no encuentra problema, responde con una autorización (CTS – Clear to send) que permite al solicitante enviar sus daros. Cuando el punto de acceso ha recibido correctamente la información, envía una trama de reconocimiento (ACK-Acknow ledgment packet) notificando al trasmisor el éxito de la trasmisión.

Independientemente de los protocolos de acceso al medio y para dar soporte a las medidas de seguridad tan necesarias en este tipo de redes los sistemas inalámbricos, como complemento adicional y característica optativa para evitar las

escuchas indiscretas, disponen de una herramienta de codificación de la información. La seguridad de los datos se realiza mediante una compleja técnica de codificación conocida como WEP (Wired Equivalent Privacy Algorithm) o WAP. Se basa en proteger los datos trasmitidos en el medio RF, usando una clave generada por un número seudo aleatorio y el algoritmo de encriptación del paquete de datos y no protege el encabezamiento de la capa física para que las demás estaciones puedan escuchar el control de datos necesarios para la adecuada gestión de la red.

El estándar WI-FI proporciona el soporte necesario para la transferencia de archivos, conversaciones de voz y control de procesos e tiempo real. Una típica configuración hibrida LAN-WLAN con una estructura medianamente productiva, el primer componente es un punto de acceso que, conectado a la red cableada en un lugar fijo mediante cableado normalizado, trasporta la información hasta una antena encargada de distribuirla a los diferentes equipos dotados con sistemas inalámbricas complementarios de acceso a la red. El punto de acceso recibe la información, la almacena y trasmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango desde treinta metros hasta varios cientos de kilómetros con repetidores.

Este punto de acceso, o la antena conectado al punto de acceso, se coloca normalmente en un lugar en el lugar en el cual se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores proporcionan la interfaz necesaria entre el sistema del cliente.

En estos sistemas las antenas puedan ser de dos clases:

Omnidireccionales, Que toman y envían señales hacia todos lados, se usan para cubrir zonas con un radio variable.

Unidireccionales, Dirigidas a un punto específico, o sea para enlazar dos puntos distanciados varios centenares de metros.

1.12.4. Configuraciones WLAN.

Las redes inalámbricas pueden ser configuradas de distantes formas para cubrir la mayor parte de las necesidades que permiten su especial fisonomía. La forma más elemental se presenta al conectar dos ordenadores equipadas para

WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto se llama red de igual a igual. Cada cliente tiene únicamente acceso a los recursos del otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o pre-configuración. Esta configuración se puede mejorar sustancialmente instalando un punto de Acceso (AP) que permita, no solo doblar el rango entre el cual los dispositivos puedan comunicarse, pues actúan como repetidores, sino que además, desde el punto de acceso, se pueda conectar a la red cableada cualquier cliente para que tenga acceso a los recursos del servidor y actúen como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso pueda servir a varios clientes, según las naturales y número de trasmisiones que tienen lugar, puesto que la tecnología inalámbrica se ha desarrollado en aplicaciones militares, la seguridad ha sido uno de los criterios de diseño para los dispositivos inalámbricos. Normalmente, se suministran elementos de seguridad dentro de la LAN inalámbrica, haciendo que éstas sean más seguras que la mayor parte de redes cableadas. Es muy complicado que receptores ajenos a la infraestructura de la red puedan escuchar el tráfico que se da en la LAN, ya que se utilizan complejas técnicas de encriptado (WEP) haciendo casi imposible para todos, incluso para los sistemas más sofisticados, que no puedan acceder de forma no autorizada al tráfico de la red.

CAPÍTULO II

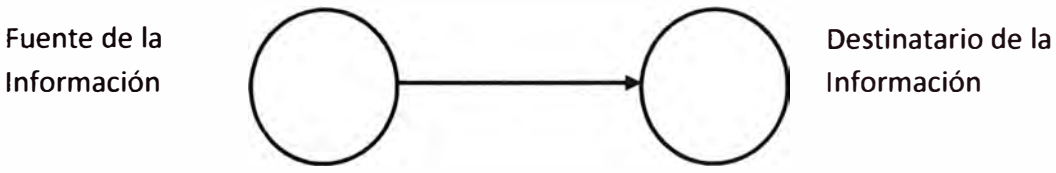
ENFOQUE CONCEPTUAL DE LA SEGURIDAD DE INFORMACIÓN EN LAS REDES DE COMUNICACIÓN

2.1. AMENAZAS

Se entiende por amenaza a un sistema de información (PC Usuario, PC Servidor) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

La política de seguridad y el análisis de riesgos deben identificar las amenazas que han de ser contrarrestadas mediante un diseño del sistema de seguridad, especificando los servicios y mecanismos de seguridad.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente a un usuario, esta puede ser mediante la solicitud del usuario para tener acceso por ejemplo a un archivo o una región de la memoria principal. ***Un ataque no es más que la realización de una amenaza***.

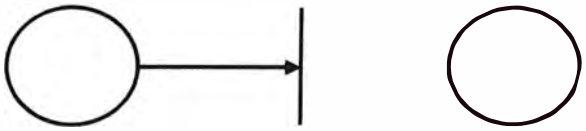


2.1 Flujo Normal de Información

Las amenazas o ataques podríamos distinguirlos en cuatro categorías:

2.1.1. Interrupción

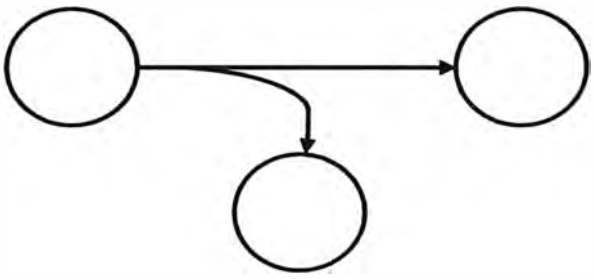
Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplo de este ataque es la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.



2.2 Interrupción

2.1.2. Intercepción

Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para obtener datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

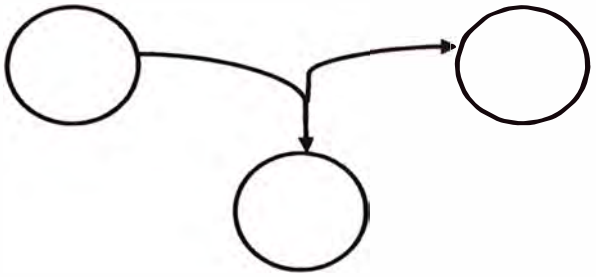


2.2 Intercepción

2.1.3 Modificación

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para

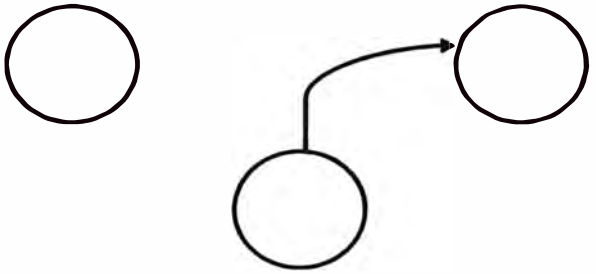
que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.



2.4 Modificación

2.1.4 Fabricación

Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.



2.5 Fabricación

2.2. TIPOS DE ATAQUE

Efectivizada una amenaza se convierte en un ataque y éstas pueden clasificarse de forma útil en términos de ataques pasivos y ataques activos.

2.2.1. ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación puede ser:

- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

2.2.2 ATAQUES ACTIVOS

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad: El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Reactuación: Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes: Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de soles en la cuenta A” podría ser modificado para decir “Ingresa un millón de soles en la cuenta B”.

Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se

encuentran los de **denegación de servicio**, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

2.3 SERVICIOS DE SEGURIDAD

Para hacer frente a las amenazas, a la seguridad de un sistema, se definen una serie de servicios. Estos servicios hacen uso de uno o varios mecanismos de seguridad, una clasificación útil de los servicios de seguridad es la siguiente:

Confidencialidad: requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, esta se puede realizar por ejemplo mediante cifrado.

La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, esta se puede realizar por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, del mismo modo variando el volumen y el momento de tráfico, otra forma podría ser produciendo una cantidad de tráfico espurio constante añadido al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda.

Autenticación: requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa y también del destino. Se puede realizar mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido. Ejemplo acceso a Internet.

Integridad: requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que al recibirlos no han sido modificados, esto se podría determinar por ejemplo un hash criptográfico con firma, mientras que la integridad de secuencia

de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas, por ejemplo mediante time-stamps.

No repudio: ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor del emisor. Mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

Control de acceso: requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.

Disponibilidad: requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

2.4. MECANISMOS DE SEGURIDAD

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

Intercambio de autenticación: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

Cifrado: garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto mediante un proceso de cifrado de texto, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el cripto-sistema es simétrico. Estos sistemas son

mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. El cifrado pueden dividirse en dos categorías: Cifradores de Bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y Cifradores en Flujo, que trabajan sobre flujos continuos de bits. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el cripto-sistema es asimétrico o de clave pública. Una clave privada se mantiene secreta, mientras que la segunda clave pública puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los cripto-sistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

Integridad de datos: Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

Firma digital: Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.

Control de acceso: Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

Tráfico de relleno: Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

Control de encaminamiento: Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras

rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

Unicidad: Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.

Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.

Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.

La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

La información sobre cristología y seguridad es basta que pende de la mano de expertos nacionales en el tema.

CAPÍTULO III

METODOLOGÍA SISTEMÁTICA PARA ANÁLISIS DE AMENZAS DE SEGURIDAD

3.1. INTRODUCCIÓN

Los trabajos más recientes en seguridad en redes de computadoras se han enfocado en la clasificación de las amenazas que pueden montarse contra interproceso de comunicación en sistemas distribuidos. En general, la clasificación ha sido tan comprensiva como ha sido posible. Esto es, todas las amenazas que deben ocurrir contra interprocesos de comunicación han sido incluidas en el modelo de amenaza y consecuentemente usada para formular contadores, medidores aplicadas para la protección contra estas amenazas.
Desde que las amenazas a los interprocesos de comunicación son efectuadas a través de accesos no autorizados a los sistemas distribuidos han surgido gran variedad de propuestas para su análisis y esto es comprensible debido a que cada día aparecen nuevas formas de amenazas y ataques, a una sola máquina, a una red, a un sistema distribuido, etc.

Debe quedar claro que el análisis debe considerar la parte física como también la lógica o programas que usan los sistemas. La existencia de tales amenazas implica que la configuración física de los sistemas distribuidos contiene puntos donde los accesos no autorizados puedan tomar lugar. Así, un análisis de amenazas a interprocesos de comunicación puede ser conducido por los análisis de las características físicas de seguridad de un sistema distribuido.

El termino configuración de seguridad denota una caracterización que describe la seguridad física de un sistema distribuido e identifica los procesos cuyas intercomunicaciones serán analizadas para las amenazas.

La configuración se realizara de acuerdo a las conclusiones llegadas. Un modelo primitivo de seguridad física de un sistema distribuido es desarrollado y usado para elaborar un modelo de configuración de seguridad. Una modificación del modelo propuesto por Kent es usado para describir la amenaza e interprocesos de comunicación.

3.2 AMENAZA CONTRA INTERPROCESOS DE COMUNICACIÓN

3.2.1 ARQUITECTURA DE UN SISTEMA DISTRIBUIDO

3.2.1.1 ARQUITECTURA FÍSICA.

Se asume una vista homogénea de las partes componentes de un sistema distribuido, esto es, un sistema de computadoras distinguidos físicamente sin considerar su función (por ejemplo, modo de almacenamiento y conducción sistema multiprogramación multinivel, concentrador terminal o multiplexor) serán considerados como unidades de cálculo independiente en el mismo grupo como todos los otros sistemas. Cada sistema será llamado un componente del sistema distribuido (Figura 3.1). La estructura del componente se asume para conformar los modelos siguientes.

La unidad mayor de cálculo en un componente es un proceso. Los procesos interactúan por medio de interprocesos basados en mensajes de comunicación. Los mensajes son unidades de datos que se mueven entre procesos, en particular, los procesos poseen uno o más puertos desde los cuales los mensajes emanan y para los cuales los mensajes son solicitados. Un puerto se identifica por una dirección valida del sistema distribuido.

Acceder a un mensaje permitirá identificar el puerto desde el cual llega (dirección origen) e identificar el puerto desde el cual ha sido solicitado (dirección destino). Los mensajes normalmente son divididos en un flujo de paquetes y cada paquete puede ser movido por una ruta diferente a través del sistema distribuido desde el puerto de origen al puerto destino.

El único tipo de comunicación permitida entre procesos el flujo de mensajes; esto es, memoria compartida entre procesos que no está incluida en el modelo arquitectural. Cada componente posee un Kernel que satisface los siguientes criterios:

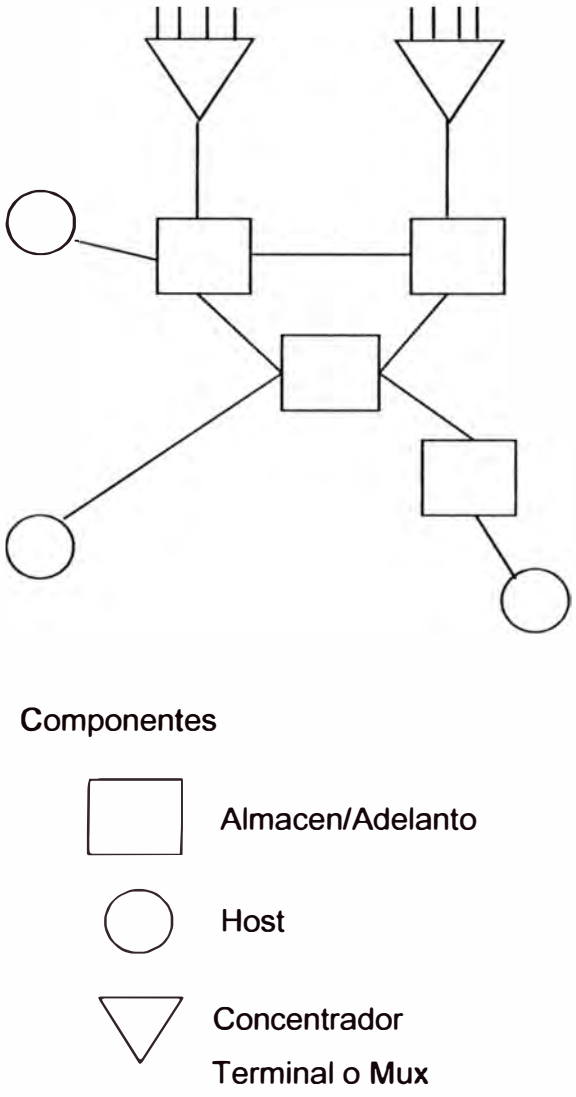


Figura 3.1 vista homogénea de un sistema distribuido

Todos los equipos periféricos (por ejemplo, discos terminales o canales de comunicación) de los componentes es controlado por el Kernel toda data transferida a y desde periféricos es intermediada por el Kernel.

La dirección del proceso fundamental es ejecutada únicamente por el Kernel. En particular, el Kernel controla todos los componentes de hardware que permite procesos independientes de mantenimiento de espacios de memoria, la creación

y distribución de procesos y las funciones de contexto-conmutación de procesos son ubicados en el Kernel.

Todos los interprocesos de comunicación son afectados por el Kernel, incluyendo el manejo de todos los niveles superiores del protocolo e incluyendo el nivel de transporte. Así, todos las rutinas, la detección y corrección de mensaje de error sincronización de mensajes (por ejemplo, reaccionando para duplicar, perder y mensajes fuera de secuencias) son manejados por el Kernel.

Los criterios concernientes a interprocesos de comunicación son motivados por las siguientes observaciones:

La mayoría de maneras de combatir amenazas de repetición, inserción y reordenamiento de un flujo de mensajes son para colocar un servicio de encriptación en el Kernel. Los mensajes empaquetados serán secuenciados y la información de detección y corrección de error será agregado a ellos antes de ser encriptados. El contador medidor provee no solo protección contra re ejecución, inserción y reordenamiento de mensajes, sino también las propiedades de seguridad de un protocolo de nivel de transporte. Para proveer servicios de nivel de trasporte en una capa de protocolo fuera del Kernel duplicarán servicios ya previstos por el servicio de encriptación y así serán usos sobrantes de recursos.

Los módulos de software que implementan funciones rutinarias son los puntos de mayor confluencia de amenazas enmascaradas, retardo y negativa de amenaza de mensajes solicitados pueden ser introducidas; colocando estas funciones en el Kernel, protegerán de procesos no confiables y así permiten que los nodos en los cuales el Kernel es probado, pero que corre procesos no confiables serán usados como punto de almacén y avance.

Notar que el concepto de arriba para un kernel puede no conformar para otras definiciones. Por ejemplo, no todo de un código de programa que implementa una función kernel necesita estar residente permanentemente en memoria. El concepto de kernel usado aquí está principalmente afectado con la identificación de estas funciones protegidas bajo aplicación de control de procesos, los cuales son considerados fundamentales para la corrección y operación segura del sistema operativo.

Los componentes son interconectados vía canales de comunicación. Cualquier software necesario para manejar estos canales será parte del componente kernel. Los canales de comunicación están basados en un número de posibles medios físicos (por ejemplo, par trenzado, enlace microondas, satélite geosíncrono, etc.)

3.2.1.2 Arquitectura Lógica

Es preferible usar una abstracción de la arquitectura física del sistema distribuido cuando se está diseñando, manteniendo o usando los servicios computacionales del sistema distribuido (figura 3.2)

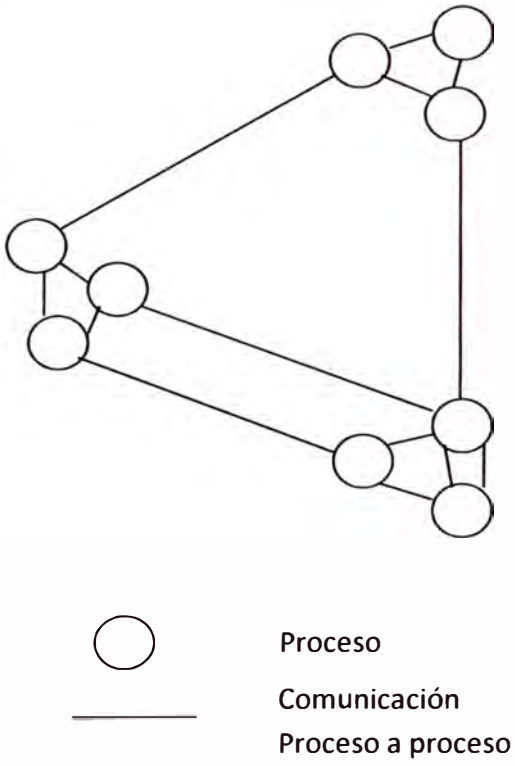


Figura 3.2 Vista lógica de la arquitectura de un sistema distribuido

Esta abstracción observa el sistema distribuido como una gran colección de procesos. Potencialmente, cualquier proceso puede comunicarse con algún otro proceso en la colección; esto es, no hay nada en la arquitectura que prevenga tal comunicación. La intercomunicación de procesos del mismo componente es

lógicamente idéntico a la comunicación entre procesos en diferentes componentes.

Cuando dos procesos en diferentes componentes se comunican, sus mensajes viajan sobre uno o más canales de comunicación. Desde el punto de vista de los procesos involucrados, no obstante, esto no es visible excepto tal vez en términos de la eficiencia de sus intercomunicaciones.

3.2.2. El modelo de amenaza de Kent.

Kent presenta cinco categorías de amenazas en un entorno de comunicaciones interactivo terminal-host. Esta amenaza puede ser visualizada comprendiendo un modelo de amenaza de interproceso de comunicación:

Liberación de contenido de mensaje.

Análisis de tráfico.

Modificación de flujo de mensaje.

Rechazo de servicio de mensaje.

Inicio de conexión espuria.

Las amenazas existen en dos categorías (por ejemplo, liberación de contenido de mensaje y análisis de tráfico) cuando los sistemas distribuidos están sujetos sólo a conexión pasiva (por ejemplo, la observación de mensajes moviéndose a través del sistema distribuido). Las amenazas en todas las cinco categorías existen cuando los sistemas distribuidos están sujetos a conexión activa y pasiva (por ejemplo, la observación, modificación, borrado, inserción, retardo, reordenamiento, redirección duplicación o reenvío de mensajes moviéndose a través del sistema distribuido).

La liberación de contenidos de mensajes ocurre cuando la información contenida en un mensaje es filtrada o hurtada por algún agente no autorizado o intruso.

El análisis de tráfico es una transferencia de información no autorizada por un observador intruso cuando y donde fluyen los mensajes de interprocesos en el sistema distribuido. Por ejemplo, un intruso debe observar un gran número de mensajes que fluyen entre los componentes de dos corporaciones diferentes y supone que algún arreglo de negociación ha tomado un lugar entre ellos. El

análisis de tráfico casi siempre requiere información adicional (del ejemplo, el intruso probablemente necesitará conocer que las corporaciones deben estar negociando, antes de que el análisis de tráfico llegue a tomar mucho valor).

Las modificaciones del flujo del mensaje es el cambio de contenido del mensaje como un flujo de mensaje entre dos procesos. Esto también abarca la repetición, reordenamiento, borrado e inserción de mensajes dentro de un flujo de mensajes entre dos proceso así como el re-direccionamiento de mensajes (es decir, la modificación de la dirección de un mensaje destino).

La negación del servicio de mensaje ocurre cuando un intruso bloquea un flujo de mensajes entre dos procesos. Una conexión es la existencia simultánea de estados sincronizados grabados en los dos puertos que están siendo usados por interprocesos de comunicación (en la mayoría de los casos cada puerto es proceso diferente como se muestra en la figura 3.3a). Estos archivos de estados son llamados conexión de archivos y son usados para el manejo de los recursos de procesos (control de flujo) así como para asegurar la integridad del flujo de mensaje que está transitando entre dos puertos ; esto es, para detectar y corregir duplicados, pérdidas, daños y mensajes perdidos. Un inicio de conexión es la actividad de establecer una conexión (figura 3.3b). Esto usualmente consiste de uno o más mensajes entre dos puertos. Un inicio de conexión espuria es la actividad de un intruso que causa una conexión a ser establecida entre dos procesos en la cual uno o ambos procesos aceptan mensajes como si estuvieran llegando desde un tercer proceso (figura 3.3c). Usualmente un inicio de conexión espuria requiere que cualquier repetición de un flujo de mensaje o la modificación de una dirección origen en la conexión de un mensaje de inicio así como en los mensajes que subsecuentemente fluyen sobre la conexión espuria.

El modelo de Kent es usual para especificar los requerimientos generales funcionales de seguridad de interprocesos de comunicación en un sistema distribuido. Se observa que el modelo está basado en una estructura lógica de arquitectura de sistemas distribuidos, más no la estructura física. De modo que, como las amenazas ocurren actualmente en un sistema distribuido y es

directamente relacionado a la seguridad física de las partes constitutivas del sistema. Ciertas configuraciones de seguridad pueden no admitir todas las amenazas posibles de interprocesos de comunicación son más simples que otras en el sentido que ellas pueden ser desbaratadas por simples, procedimientos más eficientes que estos se necesitan para contar amenazas fuertes.

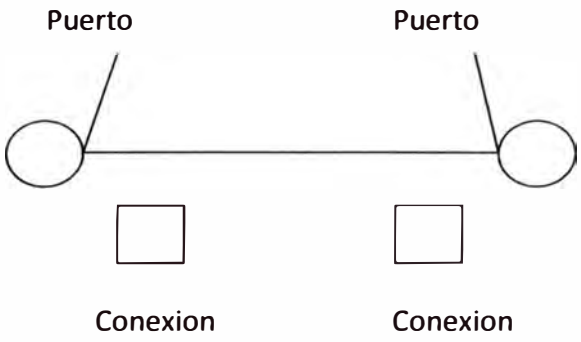
Así, esto es usual para habilitar o mapear una configuración de seguridad para las amenazas de interprocesos de comunicación, esto es necesario para seguir en detalle como la amenaza aparece como resultado de la configuración específica de las características físicas de seguridad. Antes de proceder a la descripción de un modelo primitivo de seguridad física, el modelo de amenaza de kent será modificado ligeramente para ponerlo en una forma aceptable para mapear una configuración de seguridad para amenazas de interprocesos de comunicación. Estas modificaciones no son sustanciales, si no ligeramente cambiadas de la forma en la cual algunas de la amenazas son expresadas.

3.2.3. El modelo de Kent reformulado.

Un principio fundamental de seguridad en un entorno de interprocesos de comunicación es la garantía de identificación de los procesos enviados a los procesos recibidos. La falta de tal garantía de identificación lleva al enmascaramiento de la amenaza. Así, si un intruso puede manipular los subsistemas de comunicaciones de modo que un mensaje que llega de un intruso es identificado como que llega de un tercer proceso (por ejemplo, por la modificación directa o indirecta de la dirección origen), el intruso tiene la máscara exitosa como que es el tercer proceso.

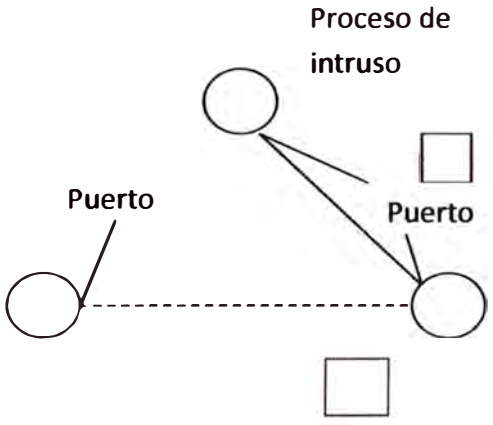
Notar que la máscara está comprometida en el inicio de una conexión espuria, repetición de mensaje (el mensaje repetido debe aparecer para llegar desde la dirección origen del flujo del mensaje y no desde la inserción). La naturaleza fundamental del enmascaramiento motiva su inclusión como una categoría de amenaza en el modelo reformulado.

Desde que el modelo de Kent está completo (todas las amenazas están contenidas en sus categorías de amenazas), se introduce redundancia en el modelo, esta redundancia está asociada con la categoría de amenaza de inicio de conexiones espurias y las amenazas de inserción y repetidas.



(a)

(b)



(c)

Figura 3.3 Inicio de conexiones espurias (a) conexión.(b). Inicio de conexión. (c) Inicio de conexión espuria.

El inicio de conexiones espurias requiere ciertos mensajes de inserción (por ejemplo, los mensajes que causan las conexiones espurias a ser establecidas son insertadas en el flujo de mensajes) o repetidas como en una conexión anterior la secuencia de mensajes establecidos es repetida. Sumando máscaras como una categoría de amenaza y empleando inserción y repetición como el inicio de una conexión espuria de amenaza obvia como una categoría de amenaza.

¿Qué hacer con la inserción y repetición de amenazas de mensaje una vez que la categoría de amenaza enmascarada se agrega al modelo de amenaza?, se plantea una mayor dificultad y problema sutil. En el modelo de Kent, la modificación del flujo de mensajes incluye modificación de mensajes, repetición, reordenamiento, borrado e inserción de amenazas específicas. Tres de estas amenazas (modificación, reordenamiento y borrado) quedan afectadas por un intruso sin la inyección de un mensaje en un flujo de mensajes. Por ejemplo, un intruso puede modificar un mensaje que viaja sobre un canal de comunicación modificado los bits del mensaje (a través de medios apropiados al medio sobre el cual el canal está implementado) como se mueve a través del canal en el cual una vía que el checksum del mensaje quede correcto. Similarmente, un intruso puede causar reordenamiento de mensajes por influencia en las rutinas de almacén-avance y puede causar el borrado de mensajes modificando un mensaje que viaja a través del canal en el cual una manera que este checksum sea correcto.

Las otras dos amenazas (repetición e inserción) por otro lado, quieren que el intruso coloque un mensaje (como una repetición o un nuevo mensaje) en el flujo de mensajes de tal manera que aparezca que viene de alguna otra dirección que la del intruso. Esta actividad es la esencia de que es llamada máscara. Por esta razón, repetición e inserción son movidos desde la modificación del flujo de mensaje en la categoría de amenaza enmascarada.

La negación de servicio de mensajes será separada en dos casos:
Interrupción debido a que un intruso bloquea solicitud de mensajes.
Interrupción debido a que un intruso borra mensajes solicitados.

El modelo modificado de amenaza es así caracterizado por las siguientes seis categorías de amenaza:
Liberación de contenido de mensaje.

Análisis de tráfico.
Modificación de flujo de mensaje.
Negación de solicitud de mensaje
Retardo de solicitud de mensaje.
Máscara.

3.3. SEGURIDAD FÍSICA Y AMENAZA CONTRA INTERPROCESOS DE COMUNICACIÓN.

3.3.1. DESCRIPCIÓN DE SEGURIDAD FÍSICA

Uno de los requerimientos fundamentales en describir una configuración de seguridad en un sistema distribuido, es la identificación de la partes del sistema distribuido que pueden ser confiables. En particular, componentes principales, canales y procesos serán identificados como confiables o no confiables. Tratar los procesos como confiables o no confiables tiene dos implicancias. Primero, se puede asumir que un intruso no tiene acceso a algún proceso confiable y no puede ganar acceso a interprocesos de comunicación de origen o destino. Esto también permite el análisis para ignorar alguna amenaza potencial tal como una invasión de mensajes que debe ser afectado a través de un proceso confiable. Sin esta suposición, la mayoría de amenazas de seguridad serían posibles en alguna configuración de seguridad y no tiene importancia que el medidor de cuentas se instale.

Segundo, las amenazas de seguridad de canales secretos (algunas veces llamadas temporales) no pueden ser detectadas por la metodología de análisis presentada, desde que se asume que los procesos seleccionados no son intencionalmente liberados de contenido de mensaje.

Los componentes principales y canales serán clasificados como confiables o no confiables, ya sea que sean accesibles por intrusos o no. Un canal confiable se asume que está sin explotar. Por ejemplo, un canal de comunicación implementado por un enlace de microondas para público hispano hablante probablemente será accesado por un intruso, esto es, el intruso podrá interceptar, prohibir o interferir con las señales que están siendo emitidas, y tal canal será considerado no confiable.

Claramente, esta técnica de clasificación resulta de una descripción sobre simplificada de las características de seguridad física de un sistema distribuido. En la práctica, no es posible estar no equivocado que un canal o componente principal no puede ser accesado por un intruso. Esto es usualmente sólo es posible para estados, tal vez vagamente, debido a que serán muy costosos para un intruso ganar acceso a una parte especificada de un sistema distribuido, o alternativamente muy improbable que tal acceso pueda ocurrir. Esto redefine la visión de llevar la seguridad física a una gama teórica con una aproximación a la seguridad de sistemas distribuidos en los cuales varias amenazas tienen probabilidades asociadas con ellas. La evaluación de cuan costoso o cuan diferente debe ser el acceso por un intruso a un componente principal o canal, es muy problemático. Desde que un acceso no autorizado no descubierto puede ser usado en la formulación de tal modelo, una cantidad desconocida de datos críticos, está disponible para este propósito. Más aún, esto es muy difícil, sino imposible, para destinar un valor monetario el éxito de ciertas amenazas. Finalmente, en la mayoría de casos el número de compromisos que han sido detectados es tan pequeño que construir un modelo de probabilidad robusto acerca de amenazas es muy difícil. Así, la descripción de seguridad física es un problema complejo, por lo que el enfoque adoptado requiere un juicio subjetivo acerca de cuáles partes de un sistema distribuido serán protegidas como para marcar accesos a ellos por un intruso ligeramente desconocido.

3.3.2. Seleccionando un conjunto de procesos

El primer paso para analizar amenazas en interprocesos de comunicación es seleccionar un subconjunto de amenazas de procesos. Las amenazas catalogadas por el análisis estarán contra las comunicaciones entre procesos en el conjunto, y en general, estas amenazas serán un subconjunto de las amenazas a comunicaciones entre todos los procesos confiables en el sistema distribuido. Así, el análisis revelará diferentes categorías de amenazas para diferentes conjuntos de procesos que dan la misma configuración física (por ejemplo, para diferentes configuraciones de seguridad).

La motivación para llevar el análisis con un subconjunto del conjunto de todos los procesos confiables está relacionada al costo de establecer mediciones

de estas amenazas. Ciertos subconjuntos pueden estar sujetos a más amenazas que otros subconjuntos y así, pueden requerir más mediciones costosas. Si el proceso confiable puede ser dividido en un subconjunto disjunto tal que la comunicación entre miembros en uno requiera menos mediciones costosas que las comunicaciones entre miembros de otra, las mediciones más costosas necesitan sólo ser implementadas para comunicaciones entre procesos en el subconjunto más amenazado.

Por ejemplo, suponemos que el proceso en un sistema distribuido puede ser dividido en estas partes, que conciernen con funciones de almacén-avance y que éstas son afectadas con aplicaciones de usuarios. Si los procesos en los componentes que implementan funciones almacén-avance (tal como tablas actualizadas rotativas y control de congestión) no se comunican con procesos de aplicaciones de usuarios, las amenazas a comunicaciones entre procesos que involucran la función almacén-avance pueden ser desbaratadas por mediciones independientes de las amenazas de comunicación entre procesos de aplicaciones de usuarios. En muchos casos esto puede llevar a un sistema de medición más económico.

Otro ejemplo surge cuando los procesos en un cierto conjunto están involucrados con cálculos que son más sensibles que otros cálculos que están siendo ejecutados en el sistema distribuido. Si el proceso involucra cálculos sensibles para las comunicaciones sólo entre ellos mismos, entonces pueden agrupados en subconjuntos, y así las amenazas a las comunicaciones entre procesos en el subconjunto pueden ser desbaratadas por mediciones independientes de las amenazas de comunicación entre otros procesos de aplicaciones de usuarios.

3.3.3. Análisis del procedimiento

El análisis procede determinando las amenazas de cada componente no confiable (por ejemplo, canal, componente principal, proceso) que representa la comunicación entre cada par de procesos seleccionados. La unión de tales amenazas comprende las amenazas para el conjunto seleccionado como un todo, debido a que las comunicaciones entre ciertos procesos confiables en un conjunto seleccionado puede no ser un subconjunto de todas las amenazas catalogadas.

Sin embargo, cada amenaza catalogada se aplica en la comunicación entre al menos dos procesos en el conjunto seleccionado, y así el mismo conjunto se puede decir que es el rostro de todas las amenazas catalogadas. En detalle, el análisis opera como sigue. Un componente particular no confiable es identificado y entonces se escoge un par de procesos de comunicación.

Dadas estas dos selecciones, una configuración de seguridad primitiva se identifica, la cual conforma las características del componente no confiable y el par de procesos, y las amenazas contra esta configuración de seguridad son catalogadas. Interactuando este procedimiento primero sobre todos los posibles pares de procesos seleccionados y luego sobre todos los componentes no confiables resulta el catálogo de amenazas deseado.

3.3.4. Las amenazas contra configuraciones de seguridad primitivas.

Se presentarán las cuatro configuraciones básicas de seguridad y las posibles amenazas a las comunicaciones entre dos procesos serán catalogadas. Cada configuración, llamada configuración de seguridad primitiva, es definida por la relación entre componentes no confiables en el sistema distribuido y las comunicaciones entre un par de procesos.

Las configuraciones de seguridad primitivas están organizadas en dos clases. El término componente confiable se refiere a componentes que poseen Kernel confiable y que corren sólo procesos confiables. Las clases son:

Un único componente en el cual el Kernel y algún otro, pero no todos, del proceso en ejecución en que los componentes son confiables (el caso de un Kernel confiable con proceso no confiable se incluye en esta clase).

Dos componentes confiables, cada uno conteniendo un par de procesos de comunicación a través de un subsistema de comunicación de almacén-avance en el cual cada uno interconecta canales que no son confiables o algún componente intermedio no confiable.

Las amenazas para comunicaciones entre procesos asociados con cada configuración de seguridad primitiva se presentan de forma desarrollada.

Cada etapa en el desarrollo describirá una configuración de seguridad primitiva específica y entonces analiza la amenaza a la comunicación entre dos

procesos. Quizás la configuración de seguridad más débil que debe ser pensada, de existir, será una en la cual el kernel del componente es no confiable, pero algunos subconjuntos de procesos en los componentes son confiables. Desde que en la práctica no está claro cómo un proceso podría ser confiable sin el kernel confiable que lo implemente, y esta situación no será considerada como una configuración de seguridad legítima.

1. Configuración de seguridad primitiva. Un Kernel confiable y algún proceso pero no todos confiables. La primera configuración de seguridad primitiva enfoca sobre un único componente el cual posee un kernel confiable pero que corre procesos no confiables (figura 3.3.a). La única amenaza por este componente para la comunicación entre un par de procesos en el sistema distribuido es un retardo de mensaje deseado debido a la invasión de mensajes por el proceso no confiable. El desborde de mensajes ocurre cuando uno o más procesos sobre cargan las facilidades de interprocesos de comunicación con mensajes.
2. Configuración de seguridad primitiva. Una red almacén-avance con componentes de almacén-avance no confiables.

   Considere una configuración de seguridad que consiste de dos componentes confiables (círculos grandes, figura 4.4 b y c), cada uno conteniendo uno o dos procesos de comunicación y conectados uno a otro por un subsistema de comunicación, hay componentes no confiables (Canales 2, 3 y 4, figura 4.4 b) y canales no confiables (canales 2,3 y 4, figura 4.4 c).

   Ambos componentes y canales no confiables serán llamados componentes no confiables.

   Esta configuración de seguridad general es usada para definir tres configuraciones de seguridad primitivas. La extensión para el cual un componente no confiable mantiene tráfico entre dos procesos define cual configuración de seguridad primitiva es definida. En la descripción que sigue, se asume que el algoritmo usado en el sistema distribuido es tal que ciertos componentes nunca puede ser usados para mover mensajes entre dos procesos confiables seleccionados, algunos componentes pueden ser usados sólo para mover una fracción de los mensajes entre estos dos procesos, y

algunos componentes pueden ser usados para mover cada mensaje entre estos procesos. Tal identificación puede ser difícil o imposible hacer para ciertos sistemas distribuidos. Por ejemplo, si el sistema distribuido posee un subsistema de comunicación el cual usa un algoritmo dinámico adaptivo, puede ser imposible para identificar componentes los cuales mantengan sólo una fracción del mensaje moviéndose entre dos procesos. En tales casos la distinción entre configuraciones de seguridad de seguridad primitiva 3 y 4 desaparece. De modo que, otros sistemas distribuidos pueden poseer algoritmos los cuales permitan tales distinciones se den. En la práctica, el análisis debe ser consciente de cómo el sistema distribuido trabaja el algoritmo para determinar si la distinción jamás obtenida es necesaria o no.

Manteniendo en un componente no confiable sin tráfico entre los dos procesos (configuración de seguridad primitiva). En esta configuración de seguridad un componente intermedio no confiable no mantiene ningún mensaje entre los dos procesos (por ejemplo, nodo 2, figura 3.4 b y canal 2, figura 3.4 c) En este caso la amenaza es como sigue:

Retardo de mensajes solicitados por avalancha de mensajes. Esto es, muchos mensajes pueden ser insertados en el subsistema de almacén-avance a través de componentes no confiables, por un intruso que llega a convertirse en cuestión.

Máscara para un componente no confiable (por ejemplo, nodo2, figura 3.3 b) que pretende llevar un mensaje que está marcado como si fuera desde un de los dos procesos, o por un intruso insertando mensajes en un canal no confiable (por ejemplo, canal 2, figura 3.3 c) con direcciones de origen olvidadas.

Manteniendo en un componente no confiable algún tráfico entre los dos procesos (configuración de seguridad primitiva 3). En la próxima configuración de seguridad primitiva un componente no confiable mantiene algunos pero no todos de los mensajes que pasan entre los dos procesos (por ejemplo, nodo 3, figura 3.4 b y canal 3, figura 3.4 c). En este caso hay las siguientes amenazas:

Todas las amenazas de configuración de seguridad primitiva 2.

Revisión de algunos contenidos de mensajes, es decir, un componente o canal no confiable puede revisar los contenidos de mensajes que pasan a través de él.

Análisis de tráfico parcial; es decir, un intruso que ha acezado a un componente no confiable puede juntar y analizar la información de tráfico acerca de los mensajes que pasan a través de él.

El rechazo de solicitud de algunos mensajes.

Modificación de algunos de los flujos de mensajes.

Como se expuso anteriormente, las amenazas parciales necesitan ser más analizadas con respecto al algoritmo usado en el subsistema de comunicación. Por ejemplo, si el algoritmo siempre está dirigiendo tráfico entre los dos procesos a través de modo 3 en la figura 3.3 b o canal 3 en la figura 3.3 c, entonces estas amenazas parciales están de hecho; es decir, todos los mensajes están sujetos a las amenazas dadas. Más aún, se puede dar el caso de que cada mensaje entre los dos procesos esté enrutado a través de al menos un componente no confiable. En este caso nuevamente las amenazas parciales son totales.

Manteniendo en un componente no confiable todo el tráfico entre dos procesos (configuración de seguridad primitiva 4). Finalmente, un componente no confiable puede mantener todos los mensajes que pasan entre dos procesos (por ejemplo, nodo 4, figura 3.4 b y canal 4, figura 3.4 c). Las amenazas son:

Todas las amenazas de configuración de seguridad primitiva 2 Revisión de los contenidos de todos los mensajes.

Análisis completo del tráfico.

Rechazo de todas las solicitudes de mensajes.

Retardo de todas las solicitudes de mensajes.

Modificación del flujo completo de mensajes.

3.4. CONSIDERACIONES PRÁCTICAS:

La metodología descrita está diseñada para el análisis de amenazas de interprocesos de comunicaciones en una clase muy general de sistemas distribuidos. De modo que, la experiencia muestra que el trabajo de sistemas distribuidos posee topologías comunes y con características operacionales que impactan el uso práctico de la metodología.

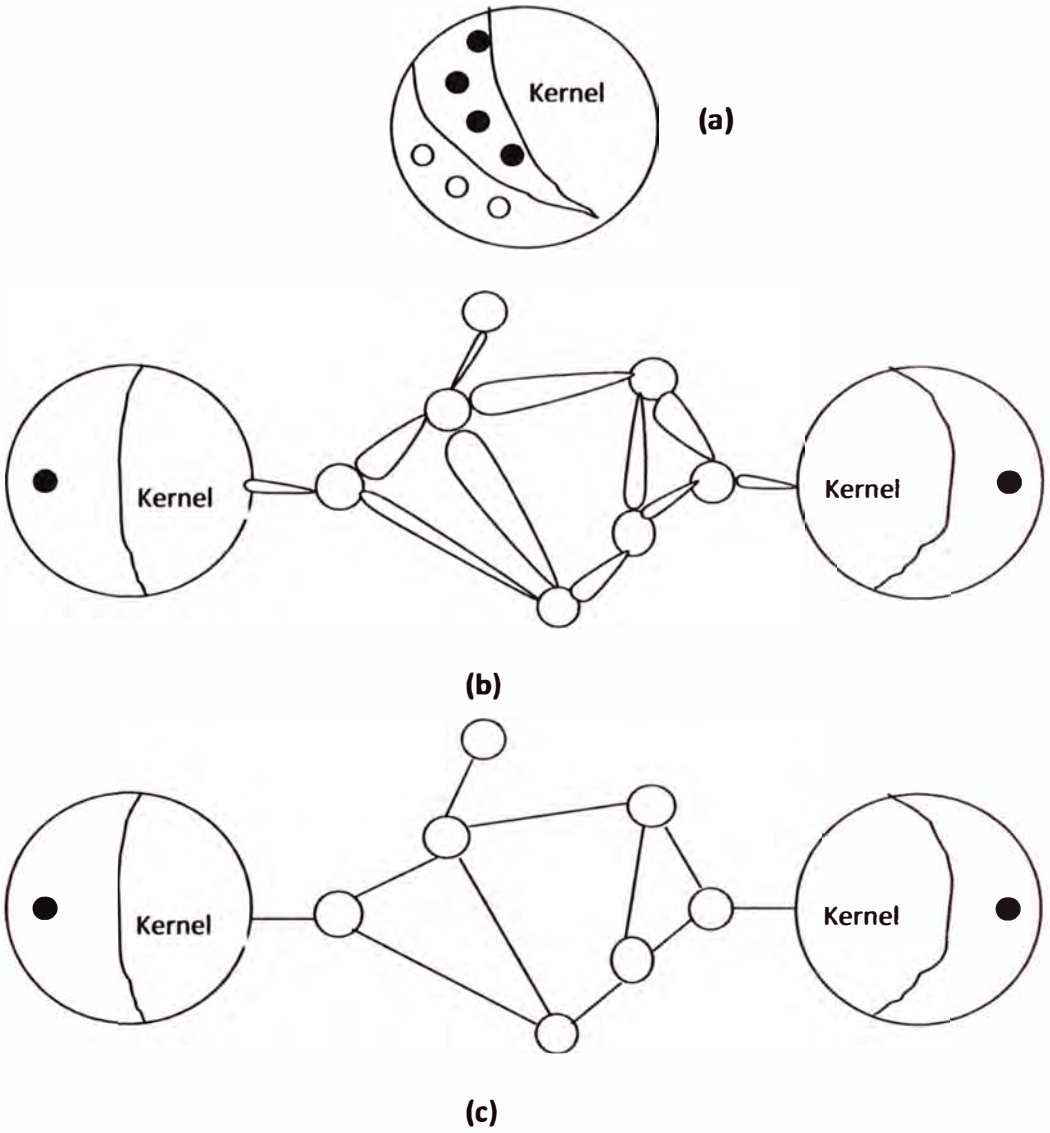


Figura 3.4 Componentes no confiables. (a) Proceso no confiable corriendo en un kernel confiable. (b) Componentes no confiables. (b) Componentes no confiables. (c) Canales no confiables.

Algunas consideraciones prácticas conciernen a la aplicación de la metodología como sigue:

Algunas topologías son más comunes que otras, implicando que algunas amenazas catalogadas son también más comunes. Otras topologías influyen dos

redes locales confiables interconectadas por una red semiconfiable de gran extensión y dos redes locales confiables interconectadas por una red semiconfiable de gran extensión y dos redes locales confiables interconectadas por medio de un enlace no confiable (por ejemplo, canal satelital).

Los catálogos de amenazas son muy sensibles al conjunto de procesos seleccionados. Por la misma topología, amenazas bastante diferentes serán obtenidas por diferentes conjuntos de selección de procesos.

La metodología puede ser bastante sensible a los cambios en la topología de los sistemas distribuidos. Si ocurren cambios frecuentes, puede ser mejor asumir el peor caso; es decir, se sume que las amenazas contienen todas las amenazas, y se instala los medidores necesarios. De otro modo, cada cambio topológico teóricamente requiere un nuevo análisis el cual puede ser muy costoso, dependiendo de la frecuencia de los cambios, en lugar de instalar todos los posibles medidores. Por otro lado, si ciertas características generales topológicas de los sistemas distribuidos esperan para quedar estables por un largo periodo de tiempo, puede no ser necesario reanalizar la red para cada cambio topológico.

Ciertos sistemas distribuidos pueden ser vulnerables para efectos de amenazas secundarias, no estudiadas aquí. Por ejemplo, en un sistema distribuido que utilice un subsistema de comunicación el cual descarga mensajes cuando ocurre una congestión, el flujo de mensajes puede no sólo causar retardos de solicitud de mensajes, sino también rechazo de solicitud de mensajes; es decir, los mensajes que se mueven entre dos procesos confiables seleccionados pueden ser descargados para propósitos de control de congestión.

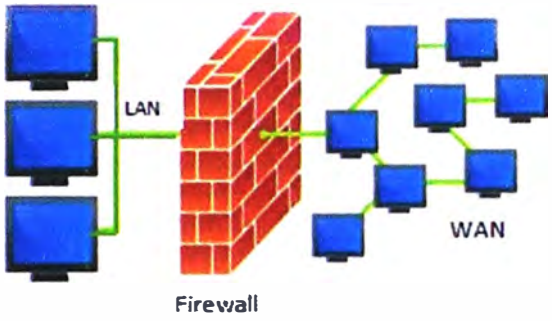
Una metodología para analizar las amenazas contra comunicaciones entre un conjunto seleccionado de procesos confiables en un sistema distribuido es el estudiado en el presente trabajo, que trata de cubrir la metodología a fin de catalogar las amenazas de interprocesos de comunicación que incluyen revisión de contenidos de mensajes, modificación de flujo de mensajes, análisis de tráfico, rechazo de solicitud de mensajes, retardo de solicitud de mensajes y enmascaramiento.

CAPÍTULO IV

SEGURIDAD EN REDES DE COMUNICACIÓN

4.1. Redes Firewall

Una red Firewall se puede definir de una forma simple como aquel sistema o conjunto combinado de sistemas que crea una barrera segura entre 2 redes. Para ilustrar esta definición podemos observar las figuras.



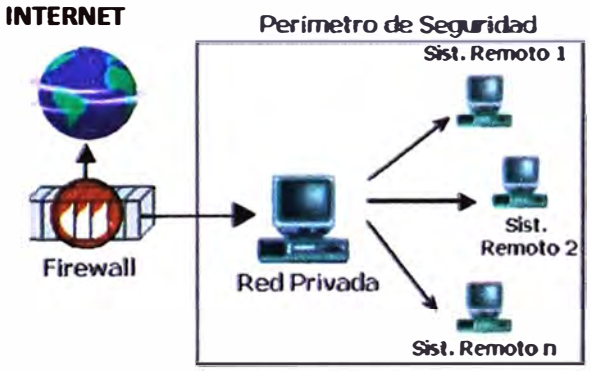


Figura 4.1 Red firewall

El propósito de las redes firewall es mantener a los intrusos fuera del alcance de los trabajos que son propiedad de uno. Frecuentemente una red

firewall puede actuar como una empresa embajadora de internet. Muchas empresas usan subsistemas firewall como un lugar donde poder almacenar información pública acerca de los productos de la empresa, tales como ficheros que pueden ser recuperados por personal de empresa y otra información de interés para los miembros de la misma. Muchos de estos sistemas han llegado a ser partes importantes de la estructura de servicios de internet (entre los ejemplos encontrados tenemos: UU.net, whithouse.gov, gatekeeper.dec.com).

Algunas firewall solamente permiten tráfico de correo a través de ellas, de modo que protegen de cualquier ataque sobre la red distinto de un servicio de correo electrónico. Otra firewall proporciona menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión.

Generalmente, las firewalls están configuradas para proteger contra ¨logins¨ interactivos sin autorización expresa, desde cualquier parte del mundo; esto ayuda principalmente a prevenir actos de vandalismo en máquinas y software de nuestra red. Redes firewalls más elaboradas bloquean el tráfico de fuera a dentro, permitiendo a los usuarios del interior comunicarse libremente con los usuarios del exterior. Las redes firewall, pueden protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello. Las redes firewall son también un buen sistema de seguridad a la hora de controlar estadísticas de usuarios que intentaron conectarse y no lo consiguieron, tráfico que atraviesa la misma, etc. Esto proporciona un sistema muy cómodo de auditar la red.

Las redes firewall no pueden proteger de ataques que se producen por causas distintos de la red firewall instalada. Muchas organizaciones que están aterradas con las conexiones que se pueden producir a través de internet no tienen coherencia política a la hora de protegerse de invasiones a través de módems con acceso vía telefónica. Es absurdo poner una puerta de acero de 6 pulgadas de espesor si se vive en una casa de madera, pero por desgracia, algunas empresas se gastan mucho dinero en comprar redes firewall caras, descuidando después las numerosas aberturas por lo que se puede colocar un intruso (lo que se llaman “back-doors” o “puertas traseras”). Para que una firewall tenga una afectividad completa, debe ser una parte consistente con la arquitectura de seguridad de la empresa. Por ejemplo, una organización que

posea datos clasificados o de alto secreto, no necesita una red firewall: en primer lugar, ellos no deberían engancharse a internet, o los sistemas con los datos realmente secretos deberían estar aislados del resto corporativo.

Otra cosa contra la que las firewall no pueden luchar, son contra los traidores y estúpidos que hayan en la propia organización. Es evidente, que de nada sirve que se instale una firewall para proteger nuestra red, si existen personas dentro de la misma que se dedican a pasar información a través de discos. Las redes firewall no pueden protegernos muy bien contar los virus. Hay demasiados modos de codificación binaria de ficheros para transmitirlos a través de la red y también son demasiados las diferentes arquitecturas y virus que intentan introducirse en ellas. En el tema de los virus, la mayor responsabilidad recae siempre en los usuarios de la red, los cuales deberían tener un gran control sobre los programas que ejecutan y donde se ejecutan.

Hay una serie de asuntos que hay que tratar en el momento que una persona toma la responsabilidad (o se la asignan), de diseñar, especificar, implementar o supervisar la instalación de una firewall.

El primero y más importante, es reflejar la política con la que la compañía u organización quiere trabajar con el sistema: ¿Se desina la firewall para denegar todos los servicios excepto críticos para la misión de conectarse a la red? O ¿Se destina la firewall para proporcionar un método de medición y auditoría de los accesos no autorizados a la red?

El segundo es: ¿Qué nivel de vigilancia, redundancia y control queremos? Hay que establecer un nivel de riesgo aceptable para resolver el primer asunto tratado, para ello se pueden establecer una lista de comprobación de lo que debería ser vigilado, permitido y denegado. En otras palabras, se empieza buscando una serie de objetivos, entonces se combina un análisis de necesidades con una estimación para llegar a una lista en la que se especifique lo que realmente se puede implementar.

El tercero es financiero. Es importante intentar cuantificar y proponer en términos de cuánto cuesta comprar o implementar tal cosa o tal otra. Por ejemplo, un producto completo de red firewall puede costar 100.000 dólares. Pero este precio corresponde a una firewall de alta resolución final. Si no se busca tanta

resolución final, existen otras alternativas mucho más baratas. A veces lo realmente necesario no es gastarse mucho dinero en una firewall muy potente, sino perder tiempo en evaluar las necesidades y encontrar una firewall que se adapte a ellas.

En cuanto al asunto técnico, se debe tomar la decisión de colocar una máquina desprotegida en el exterior de la red para correr servicios proxy tales como telnet, ftp, etc. O bien colocar un router cribador a modo de filtro que permita comunicaciones con una o más maquinas internas. Hay ventajas e inconvenientes en ambas opciones, con una maquina proxy se proporciona un gran nivel de servicios que puedan proporcionar.

4.2. Tipos básicos de redes firewall

Conceptualmente, hay dos tipos de firewall:

Nivel de red

Nivel de aplicación

No hay tantas diferencias entre los dos tipos como se podría pensar. Además las últimas tecnologías no aportan claridad para distinguirlas hasta el punto que no está claro cuál es mejor y cual es peor. Pero en cualquier caso, se deberá prestar atención y poner mucho cuidado a la hora de instalar la que realmente se necesita en nuestra organización.

La firewalls a nivel de red generalmente, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un sistema router es un “tradicional” firewall a nivel de red particularmente, desde el momento que no puede tomar decisiones sofisticados en relación con que esta un paquete ahora o desde donde está llegando en este momento. Las modernas firewall a nivel de red se han sofisticado ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellas, los contenidos de alguna datagrama y más cosas. Un espacio importante que distingue a las firewall a nivel de red es que ellas enrutan el trafico directamente a través de ellas, de forma que un usuario cualquiera necesita tener un bloque valido de dirección IP asignado. Las firewalls a nivel de red tienden a ser más veloces y más transparentes a los usuarios.

Screened Host Firewall:

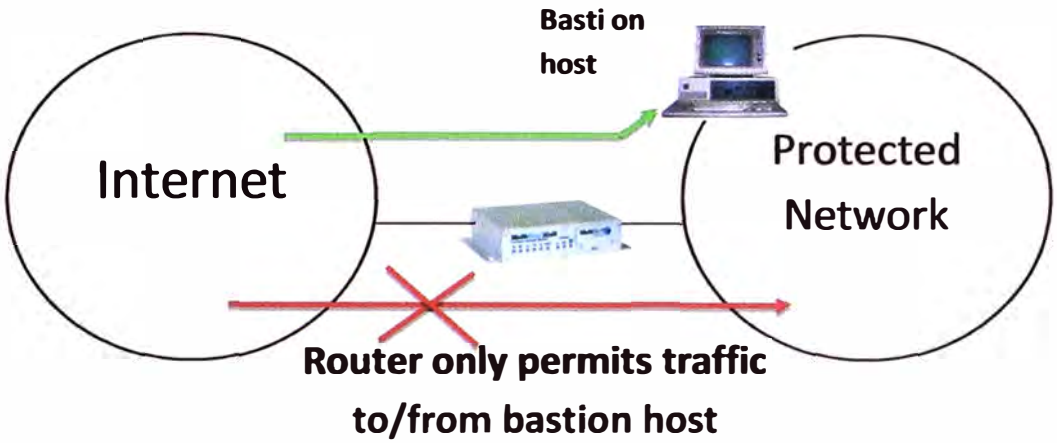


Figura 4.2 Router que solo permite tráfico a/desde Host

Un Ejemplo de una firewall a nivel de red se muestra en la figura:

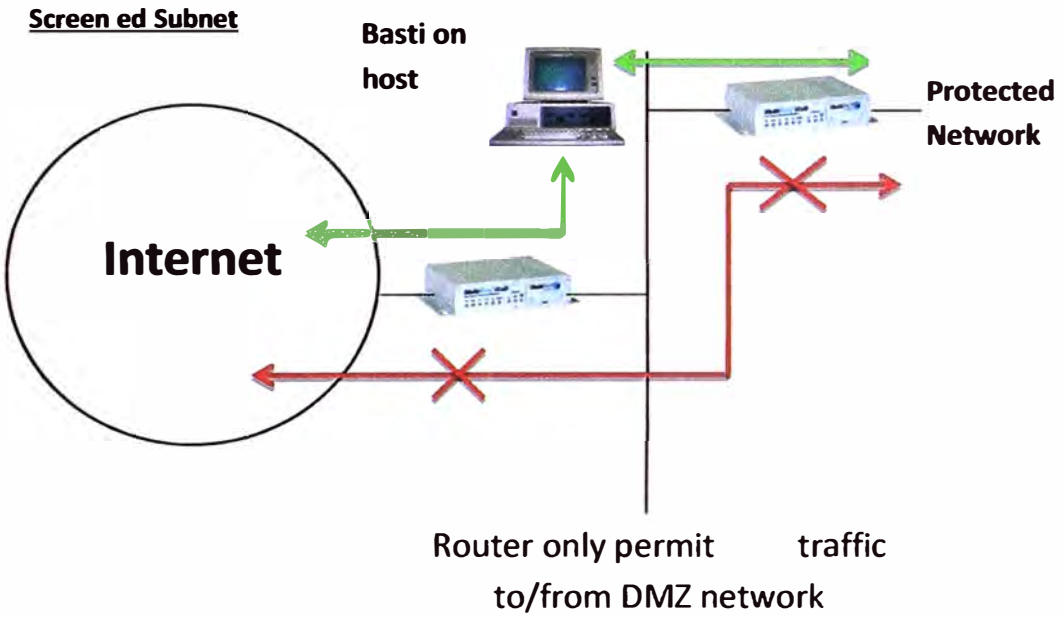


Figura 4.3 Router que solo permite tráfico a/desde red DMZ

En este ejemplo se representa una firewall a nivel de red llamada "screend Host Firewall". En dicha firewall, se accede a y desde un único host el cual es controlado por un router operando a nivel de red. El host es como un bastión, dado que está muy definido y es punto seguro para refugiarse contra los ataques.

Otro ejemplo sobre una firewall a nivel de red es el mostrado en la figura 3.3 en este ejemplo se representa una firewall a nivel de red llamada "screened subnet firewall" en dicha firewall se accede a y desde el conjunto de la red, la cual es controlada por un router operativo a nivel de red. Es similar al firewall indicada en el ejemplo anterior salvo que esta si es una red efectiva de hosts protegidos.

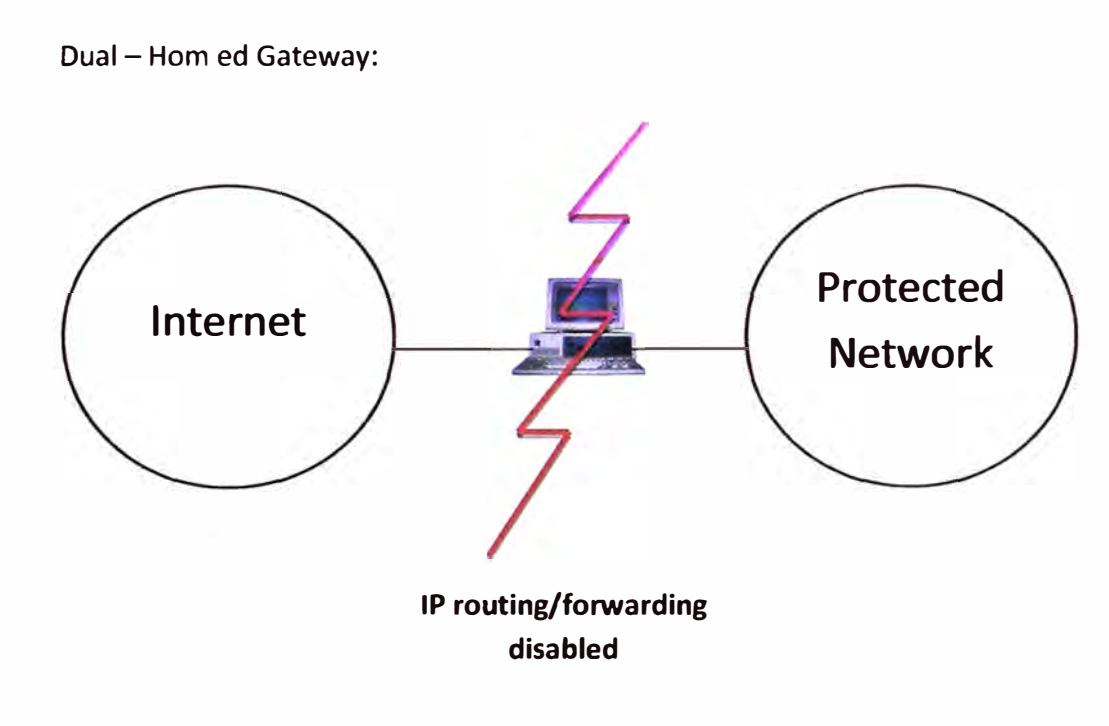


Figura 4.4 Enrute y avance de IP desabilitado

Las firewalls a nivel de aplicación son generalmente, hosts que corren bajo servidores proxy, que no permite tráfico directo entre redes y que realizan logins elaborados y auditan el tráfico que pasa a través de ellas.

Las firewall a nivel de aplicación se pueden usar como traductor de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el

otro. Las primeras firewall a nivel de aplicación eran poco transparentes a los usuarios finales, pero las modernas firewall a nivel de aplicación son bastante transparentes. Las firewall a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto las hace diferenciar de las firewalls a nivel de red.

Un ejemplo de una firewall a nivel de aplicación representa una firewall a nivel de aplicación llamada "dual home d Gateway". Una firewall de este tipo es un host de alta seguridad que corre bajo software proxy. Consta de 2 interfaces de red (uno a cada red) los cuales bloquean todo el tráfico que pasa a través del host.

El futuro de las firewalls se encuentra a medio camino entre las firewalls a nivel de aplicación. El resultado final de los estudios que se hagan será un sistema rápido de protección de paquetes que conecte y audite datos que pasan a través de él cada vez más las firewalls con encriptación extremo –a-extremo (end-to-end), se puede usar en organización con múltiples puntos de conexión a internet, para conseguir utilizar internet como una "central privada" donde no sea necesario preocuparse de que los datos o contraseña pueden ser capturados.

4.3. Servidores Proxy.

Un servidor proxy (algunas veces se hace referencia a él con el nombre de "Gateway" – puerta de comunicación – o "forwarder" – agente de transporte), es una aplicación que media en el tráfico que se produce entre una red protegida e internet. Los proxies se utilizan a menudo, como sustitutos de router, controladores de tráfico para prevenir el tráfico que pasa directamente en las redes; muchas proxis contienen logines auxiliares y soportan la autentificación de usuarios. Un proxy debe entender el protocolo de la aplicación que está siendo usado, aunque también pueden implementar protocolos específicos de seguridad (por ejemplos: un proxy FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente). Los servidores proxy, son aplicaciones específicos. Un conjunto muy conocido de servidores proxy son los TIS Internet Firewall Toolkit "FWTK", que incluyen proxies para Telnet, Rlogin, FTP, x-windows, http/Web, y NNTP/Usentnews. SOCKS en un sistema proxy genérico que puede ser compilado en una aplicación cliente para hacerla trabajar a través de una firewall.

Hay 3 formas de conseguir que trabajen la Web/http con la firewall:
Permitir establecer conexiones vía un router, si se están usando routers protegidos.
Usar un cliente Web que soporte SOCKS, y correr SOCKS en la firewall.
Ejecutar alguna clase de servidor Web proxy en la firewall. El TIS firewall tolkit incluye un proxy llamado http-gw, el cual permite proxy Web, gopher/gopher+ y FTP. Además, muchos clientes Web, tienen servidores proxy construidos directamente en ellos, que soportan: Netscape, Mosaic, Spy, Chamaleon, etc…

Para trabajar la FTP a través de una firewall generalmente, se consigue usando un servidor proxy, tal como el "firewall toolkits ftp-gw" o bien realizando alguna de las dos operaciones siguientes:
Permitiendo conexiones entrantes a la red en un rango de puerto restringido.
Restringiendo las conexiones entrantes usando alguna clase de reglas de protección, preestablecidas.

Para trabajar Telnet a través de una firewall, esta se soporta habitualmente usando una aplicación proxy tal como "firewall toolkitstn-gw, o simplemente configurando un router que permita las conexiones salientes usando alguna clase de reglas de protección preestablecidos.

La denegación del servicio se produce cuando alguien decide hacer inútil su red o firewall por desestabilización, colisión, atasco o colapso en la misma. El problema con la denegación de servicio en Internet es que es imposible prevenir la razón, viene por la distribución natural de la red: cada nodo está conectado vía otra red, la cual está conectado a otra red, etc.… un administrador de firewall o ISP solo tiene control sobre unos pocos elementos locales dentro de la radio de acción.

Las típicas firewall, requieren alrededor de 1 hora a la semana de mantenimiento. Esto es, sin contar el tiempo relativo a internet que el administrador de una firewall gastara. La conectividad con Internet trae consigo la necesidad de que alguien actúe como administrador de correo electrónico para Email, Web máster, gestor de FTP y gestor de noticias USENET. Estas tareas requieren tiempo llegar a ser un trabajo a tiempo completo para una única persona.

Hay numerosas herramientas disponibles para construir tu propia firewall, “TrustedInformationSystemas”, “inc`s Internet Firewall Toolkit”, son un ejemplo de implementación con un conjunto de aplicaciones proxies. Si estas construyendo la firewall usando un router o un router y su herramienta de desarrollo, se puede tener ventajas frente a los ya elaborados. Los libros de Brent Chapman y Elizabeth Zwichy´s describen algunos métodos sobre configuración de un router protegido en una firewall. Una Firewall construida a pedido proporcionar un soporte técnico para el futuro.

En años anteriores, había una gran variedad de firewalls comerciales disponibles, y muchas compañías contrataban a consultores para que les construyeran las firewalls. Hoy en día, no es una buena opción seguir realizando esto, si tenemos en cuenta que el costo de contratar un consultor eventualmente que nos construya la firewall es superior al de comprar una firewall comercial terminada.

Como saber si una firewall es segura? Es muy difícil saberlo, dado que no hay pruebas formales que puedan ser fácilmente aplicados a algo tan flexible como un firewall. Una moraleja dice que cuanto mayor tráfico de entrada y salida permite una firewall, menor será su resistencia contra los ataques externos, la única firewall que es absolutamente segura es aquella que está apagada.

Si usted está preocupado sobre la calidad de una firewall de un vendedor particular, use el sentido común y hágale preguntas del tipo siguiente:
¿Cuánto tiempo ha estado en los negocios dicho producto?
El tamaño de la institución base.
¿Han tenido expertos independientes revisando el diseño y la implementación de la aplicación en cuestión?

Un vendedor deberá claramente explicarle como se diseñó la firewall en concepto de seguridad. No acepte insinuaciones acerca de que los productos de la competencia son inseguros sin habernos explicado la seguridad de producto en cuestión.

Un error común en las firewall es pensar que pagando más en una firewall cara se consigue más seguridad en la misma. Hay que pensar que si el costo de

una firewall es 2 veces superior al de otra, el vendedor tendría que ser capaz de explicarnos porque uno de dichos productos es 2 veces mejor que el otro.

La mayoría de la firewall solía ser vendida como paquetes de consulta. Cuando una firewall era vendida, parte de su costo se destinaba a instalación y soporte, generalmente, involucrando a un consultor que proporcionaba el vendedor, para ayudar en la instalación. En los "malos días" muchas de las empresas que estaban conectadas a Internet, no tenían expertos en TCP/IP local, a veces por deficiencias propias de la evolución de la tecnología de Internet o la vulnerabilidad de los equipos que comprometían a menudo tiempos a configurar los router y correo electrónico (tareas que eran realizadas por el administrador interno de DNS). Si el diseño de la Firewall es realizado a pedido entonces son ellos que se encargaran del servicio Post Venta.

Típicamente, cuando se instala una firewall, la conexión a Internet debe estar realizando, pero no tiene que estar conectado a la red protegida. Para instalar una firewall debe planificarse las funciones que debe realizar, esto se puede obtener con las respuestas a las preguntas que se plantean:

¿Cuál será la política de acceso que se va a poner en práctica?

¿A dónde se va dirigir el correo electrónico?

¿Dónde se deberá buscar la información de login?

Y otros temas….

Una vez instalada tiene una buena base para la configuración de la firewall, entonces se conecta a Internet y se prueba que las operaciones con la red sean correctas. En ese momento se instalan y chequean las reglas para el control de acceso a la firewall y se conectan a la red protegida. Además se realizan, generalmente, algunas operaciones típicas como acceso a Web recepción y envió de correo electrónico, etc. Cuando todos los controles son correcto entonces ya se puede decir que uno está, en Internet.

Actualmente las empresas vendedoras proporcionan soporte periódico para y para clientes que se encuentran en lugares lejanos usan el servicio VPN para obtener el control de sus redes a distancia.

También algunos proveedores de servicios Internet ofrecen un soporte de firewall como parte del servicio de conexión a Internet.

La mayoría de empresas prestadoras de servicios por Internet (Correo electrónico, FTP, comunicación instantánea) "que son gratuitas" ofrecen este servicio incluyendo servicios de protección a la información compartida con los usuarios, incluso se ha convertido en una competencia cuyo único ganador son los usuarios.

Algo muy importante que debe brindar un vendedor con respecto a las firewalls es su conocimiento para poder brindar el Firewall adecuado y preciso para su cliente, de esto dependerá la satisfacción de realizar la inversión en la Firewall.

Los vendedores, típicamente, no configuran sistemas de herencia interna para trabajar con las firewall. Por ejemplos muchas firewall asumen que hay que hablar de Internet por un lado y a la red TCP/IP por el otro. Generalmente, es responsabilidad del cliente tener sistemas TCP/IP aptos para interactuar con firewall. Para email, la mayoría de las firewalls soportan solamente SMTP (Simple Mail Transfer Protocol) y es afán del cliente tener un sistema compatible con SMTP en algún lugar de la red. A menos que se esté comprobando una firewall desde un proveedor de servicios de Internet, es responsabilidad del cliente tener una clase de direcciones de red TCP/IP y un nombre de dominio localizado.

4.4. Redes privados virtuales

Las redes privados virtuales crean un túnel o comando dedicado de un sitio a otro. Las firewalls o ambos sitios permiten la conexión segura a través de internet. Las VPNs son una alternativa de costo útil, para usar líneas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión, protegido a la información y el password.

La tecnología de VPN proporciona un medio para usar el canal público de internet como una canal apropiada para comunicar los datos privados, con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de internet. Instalado VPNs, se consigue reducir las responsabilidades de gestión de una red local.

La tecnología de VPN proporciona un medio para usar el canal público de internet como una canal apropiada para comunicar los datos privados.

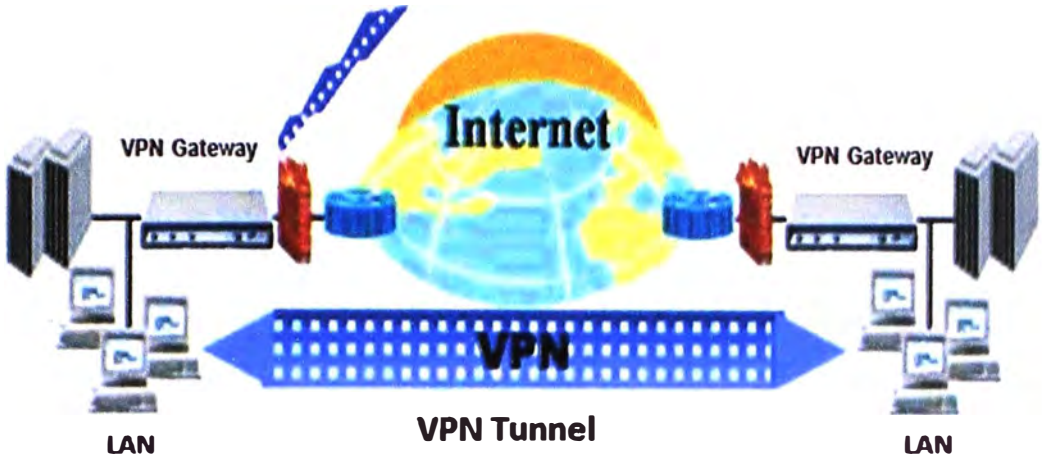


Figura 4.4 VPN túnel de comunicación

Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de internet. Instalado VPNs, se consigue reducir las responsabilidades de gestión de una red local.

4.4.1. Tecnología De Túneles De Una Red Privada Virtual

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos. La tecnología de túneles es un modo de transferir datos entre 2 redes similares sobre una red interna. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado – encapsulación, ya que los paquetes están encriptados de forma de los datos ilegibles para los extraños. Los paquetes encapsulados viajan atreves de Internet hasta que alcanzan su destino, entonces, los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autentificación se emplea para asegurar que el cliente tiene autorización para conectar con el servidor.

Los proveedores de varias firewall incluyen redes privados virtuales como una característica segura en sus productos.

4.4.2. REDES PRIVADAS VIRTUALES DINÁMICAS NETWORKS (DVP)

Basada en la tecnología de Intranets, las Intranets, han llegado a ser una parte esencial de los sistemas de información corporativos de hoy en día. Sin embargo, Internet no fue diseñada, originalmente para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios: ¿Cómo establecer y mantener la confianza en un entorno, el cual fue diseñado desde el comienzo para permitir un acceso libre a la información? Para decidirlo de otro modo: ¿Cómo conseguir seguridad en una Intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperabilidad y facilidad de uso?

La compañía Trade Wade cree que la respuesta apropiada y satisfactoria a esta disyuntiva, se encuentra en la utilización de **VPNs** dinámicas basadas en los servicios y aplicaciones Trade VPI de dicha compañía. A diferencia de una VPN tradicional que ofrece seguridad limitada e inflexible, una VPN dinámica proporciona ambos extremos, con altos niveles de seguridad, e igualmente importante que proporcionan la flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs dinámicas, pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura así como pueden proporcionar otras ventajas, una VPN dinámica es una habilitadora de internet. Habilita que una intranet ofrezca y más recursos y servicios que de otra forma es una aplicación, sino que puede trabajar con otras aplicaciones Internet, así como con aplicaciones corporativas específicas.

Anteriormente, al usar una VPN, un usuario o servicio en primer lugar, debe funcionar (join) la VPN, registrándola con el certificado de autenticidad (CA). Los fuertes procesos de seguridad, aseguran que solamente los usuarios nominados, están registrados y reciban la certificación. La CA, asegura que los criticados revocados son enviados por correo y se denegaba el servicio cuando se intentan usar.

Figura 4.5 Red Privada Virtual Dinámica

Los usuarios y servicios, reciben continuamente, información dentro de la VPN. Sin embargo, los pasos básicos de cada intercambio son los mismos siguiendo los pasos ilustrados en la figura 3.5, un usuario realiza una petición de información a un servidor, pulsando con su ratón en un hipervínculo, los pasos seguidos se pueden describir en los siguientes puntos:

1. Un usuario solicita información usando una aplicación tal como un browser Internet, desde un ordenador. El intercambio de información comienza cuando un usuario envía información a otro usuario o solicita información al servidor. La VPN, puede incorporar aplicaciones propietarios sin embargo, también debe ofrecer aplicaciones propietarios, sin embargo también debe de ofrecer aplicaciones que se benefician de Internet, particularmente de la WWW. en el supuesto de que un usuario ha accedió a un hipervínculo desde dentro de algún documento Web, dicho hipervínculo es seguro y solamente puede ser accedido por usuarios autorizados.
2. La aplicación envía y asegura el mensaje. Cuando un cliente y un servidor detectan que se necesitan seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectan en un mutuo protocolo de autentificación, pero antes de que la aplicación envié la petición, se asegura el mensaje encriptándolo. Adicionalmente, se puede atribuir un certificado o firma electrónica al usuario encriptado la información se protege la confidencia y la integridad. Si se envía la firma, se podrá usar para auditorias. Para

habilitar la interoperabilidad entre múltiples mecanismo de seguridad, las funciones de seguridad se deben basar en estándares bien definidos, tal como el estándar de Internet GSSAPI (Generic Security Services Aplication Programming Interface).

3. El mensaje de se transmite a través de Internet. Para que la petición alcance el servidor, debe dejar la LAN y viajar a través de Internet, lo cual permitirá alcanzar al servidor en algún punto de la misma durante este viaje, puede darse el caso de que atraviese 1 o más firewalls antes de alcanzar su objetivo. Una vez atravesada la firewall, la petición circula a lo largo de pasillo Internet hasta alcanzar el destino.
4. El mensaje recibido debe pasar controles de seguridad. Cuando el mensaje alcanza su destino, puede ser que tenga atravesar otra firewall. Esta Firewall protegerá cuidadosamente el tráfico entrante asegurado que se ciña a la política corporativa, antes de dejarlo atravesar la red interna. El mensaje se transfiere al servidor. Como consecuencia de la autentificación mutua que se produjo entre el cliente y el servidor, el servidor reconoce la identidad del usuario cliente cuando recibe la petición.
5. Durante la petición, se verifican los derechos de acceso de los usuarios. Al igual que en todas las redes corporativas, todos los usuarios no pueden acceder la totalidad de la información corporativa. En una VPN dinámica, el sistema debe poder restringir que usuarios pueden y no pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de informaron. Esto lo hace usando un mecanismo de control, Imposibilitaría al mundo de los negocios a hacer mayor uso de los recursos de información.

4.4.3. Potencial de una red privada Virtual Dinámica.

Tarde VPI es un conjunto de aplicaciones u servicios relacionados. El potencial de esta solución es el siguiente.

Proporciona una seguridad importante para la empresa.

Se ajusta dinámicamente al colectivo dispar de usuarios.

Permite la posibilidad de intercambio de información en diversos formatos (Páginas WEB, Ficheros, etc.)

El ajunte fue hace para cada usuario lo consigue gracias a los diferentes browsers, aplicaciones, sistemas operativos, etc.

Permite a los usuarios unirse a distintos grupos, así como a los administradores pueden asignar identidades en un entorno simple pero controlado.

Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

4.4.4. Trabajo de las Redes Privadas Virtuales Dinámicas.

La VPN dinámica de TradeWare consta de una plataforma se seguridad de red y un conjunto de aplicaciones para usar en la plataforma de seguridad. El diagrama de bajo, muestra cómo se engranan las piezas de esta plataforma para conseguir una solución de tipo VPN dinámica. El siguiente ejemplo va pasando a través de las partes de una VPN dinámica suponiendo una comunicación segura http (Web). Sin embrago, no preferiblemente un servidor separado. El servidor de control de acceso, restringe a la información en niveles de documento. De modo que, si incluso un usuario presenta un certificado válido, puede ser que se las rechace el acceso basándose con otros criterios (por ejemplo: políticas de información corporativa).

La petición de información es devuelta por internet, previamente asegurada. Si el usuario tiene derecho de acceso a la petición de información, el servidor de información encripta la misma y opcionalmente la certifica. Las claves establecimiento durante los pasos de autenticación mutua se usan para encriptar y desencriptar el mensaje. Ahora, un usuario tiene su documento asegurado.

4.5. EQUIVALENCIA A LAS VPN DINÁMICAS: IDENTIFICADO DE EMPLEADO Y UN SISTEMA DE IDENTIFICACIÓN.

Para entender la solución propuesta por tradeWare para las VPN podemos considerar un equivalente consiste en identificar de empleado corporativo y un sistema de identificación. Del mismo modo que los departamentos de Recursos Humanos o Seguridad pueden verificar la identidad de un empleado y asignar un número de empleado único, una VPN verifica la identidad del usuario y emite un único “nombre distintivo” el cual se usa para todos los accesos y movimientos dentro del sistema. Del mismo modo que una compañía también lleva el control

de quienes tienen una clave de seguridad y donde ir con ella, las VPN tienen controlada la gestión y poner a disposición claves y certificados. Al igual que muchas tarjetas de seguridad pueden ser utilizados por una compañía, muchas claves se pueden convertir, mediante el certificado de Autorización. Además del mismo modo que los accesos a construcciones y áreas de seguridad, se controlan por varis niveles de seguridad, las VPN validan las listas de Control de Acceso contra los nombres de usuario y passwords, para autorizar el acceso a redes a ciertos documentos y ficheros. Por último, las VPN mantienen una lista de usuarios revocados y deniegan los futuros accesos al sistema a dichos usuarios, al igual que se produce en una empresa cuando un usuario se marcha, debe devolver todos los sistemas de identificación de seguridad para no poder volver a entrar en la compañía.

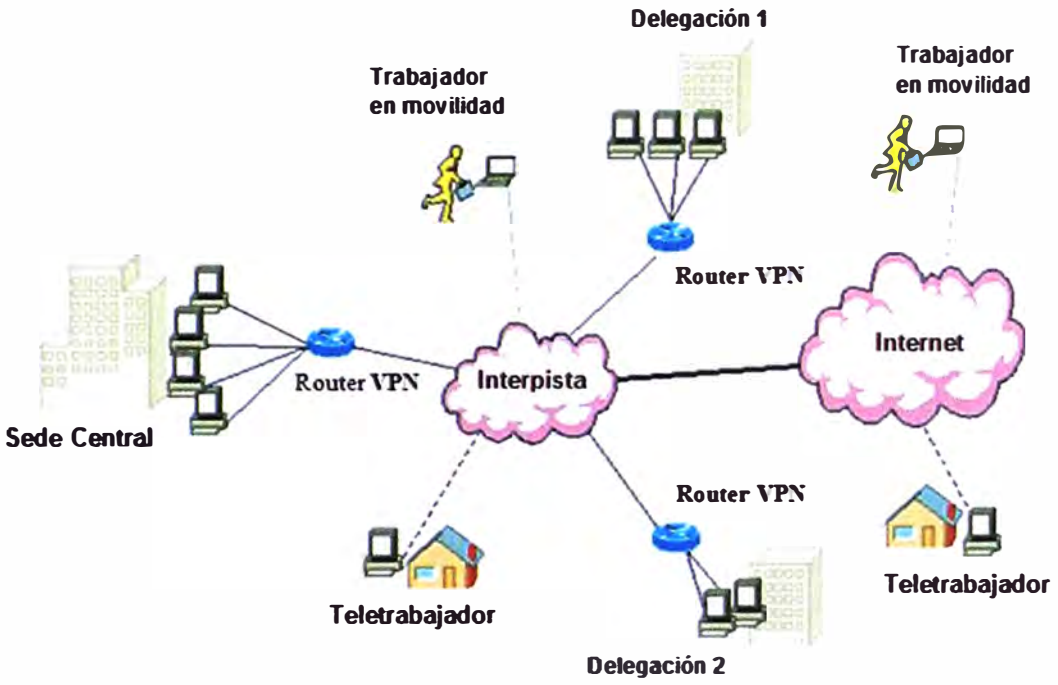
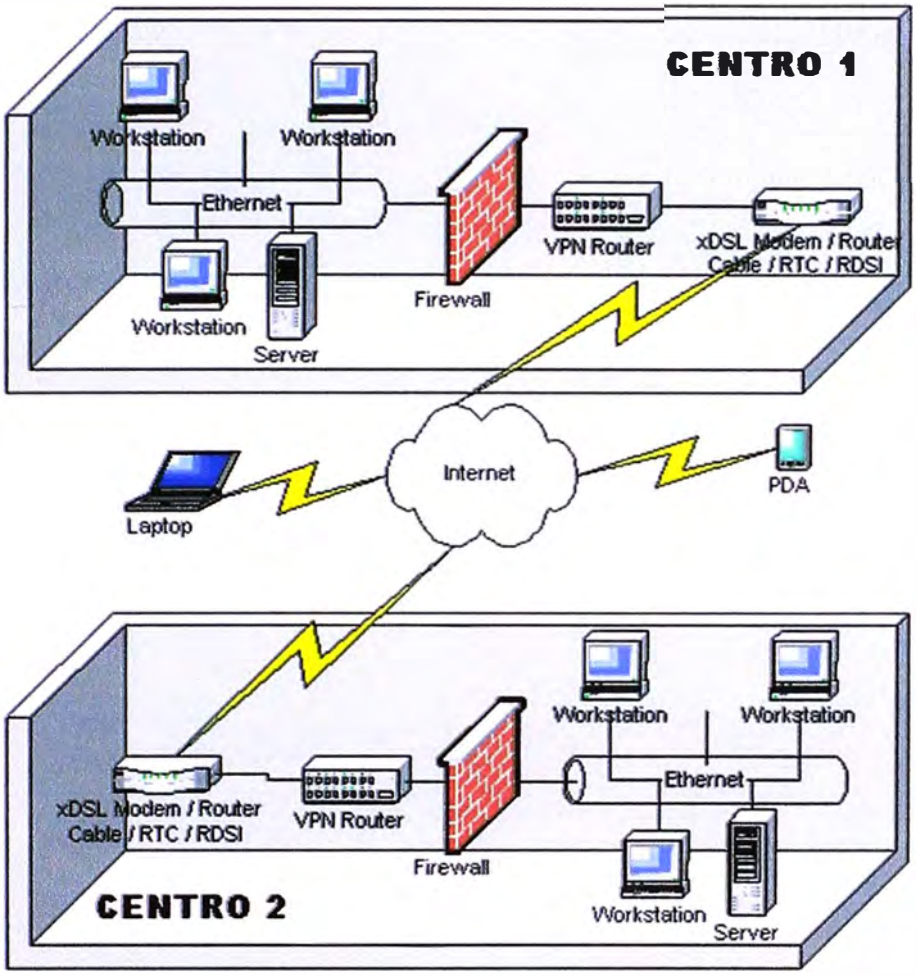


Figura 4.6 equivalencia constatada en el párrafo.

Un aspecto critico en las VPN de TradeWave en su arquitectura basada en agentes. Los agentes TradeWave son módulos o entidad Software que se

comunican vía protocolos entandar. Como consecuencia de ello, TradeWave ha "desacoplado" arquitectónicamente sus agentes de otras aplicaciones, de forma que un negocio puede cambiar o expandir su intranet – incluyendo expansión de plataforma – sin tener que rediseñar su sistema internet. Más específicamente, esta arquitectura permite que un negocio seleccione y use cualquier browser, cualquier servicio y cualquier aplicación con su VPN dinámica. La siguiente figura la arquitectura basada en agentes.



Figuera 4.7 arquitectura basada en agentes

Los agentes TradeWave Pueden:

Ser insertado fácilmente, en streams de comunicaciones existentes con un mínimo de alteración en el sistema

Contener habilidades que no posee el sistema existente.
Ser actualizado rápidamente.
Incorporar múltiples protocolos de seguridad.

Además, la arquitectura basada en agentes, proporciona una solución al problema tradicional en los sistemas de información corporativos: el conflicto entre los estándares de empresa por un lado y la adopción local de tecnologías para necesidades específicos en el otro. Una arquitectura basada en agentes permite, por ejemplo, departamentos que usen los browsers que ellos quieran sin perturbar los estándares de seguridad empresarial.

Un beneficio adicional a la arquitectura basada en agentes en la posibilidad de usar una variedad de módulos, software llamadas TradeAttaches. Estos módulos se pueden añadir al sistema TradeVPI también para incrementar su funcionalidad e interpretativo por ejemplo, TradeAttaches permite que la VPN se puede extender para incluir diferentes protocolos de seguridad sin perturbar a los browsers o servidores. Con este sistema, están inmediatamente disponible, las nuevas funciones de seguridad. TradeVPNtambién puede gestionar simultáneamente, varios TradeAttachés de seguridad, de modo que la VPN pueda soportar múltiples plataformas de seguridad al mismo tiempo.

4.6. ACCESO REMOTO SEGURO

4.6.1. PROPÓSITO DE LOS ACCESOS REMOTOS SEGUROS

Con los accesos remoto seguros, las conexiones vía modem telefónico pueden transferir datos seguros vía un proveedor de servicios Internet o vía una red corporativa. Los datos se encriptan en el cliente antes de que sean transmitidos y se desencriptan en la puerta de la firewall. El software proporcionado, habilita a los usuarios remotos a que puedan conectar a la red corporativa como si ellos estuvieran detrás de la firewall. La tecnología de VPN proporciona un medio para usar el canal público de internet como un canal apropiado para comunicar los datos privados. Con tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de internet. Instalando VPNS, se consigue reducir las responsabilidades de gestión de la red local.

4.6.2. RED SEGURA, PRIVADA Y VIRTUAL

Una red privada virtual es una red donde todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicos) de distancia. Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas. Primero, deben poder pasar paquetes IP a través de un túnel en la red pública, segunda, la solución debe agregar encriptación, tal que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado. Finalmente, la solución tiene que ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de manera que un adversario no pueda acceder a los recursos del sistema.

4.6.3. RED PRIVADA A TRAVÉS DE UN PAQUETE DE SOFTWARE

La serie InfoCrypt de Isolation Systems crea una red privada segura de la siguiente manera. Primero, los paquetes IP que tienen como destino una zona protegida son encapsulados en un nuevo paquete que contiene solo las direcciones IP de los encriptores origen y destino. Este le permite a los clientes a conectar redes IP sin router y redes IP routeadas, creando un túnel efectivo a través de la red pública por donde pasar los paquetes.

La encriptación es lograda usando triple Pass DES con llaves de doble o triple longitud para encriptar paquetes destinados a redes remotas. Como la encriptación es una función matemática que requieres significativos recursos del sistema, los InfoCrypt Enterprise Encrytors de IsolationSystems incorporan un procesador ASIC (ApplicationSpecificIntegratedCircuit) dedicado exclusivamente a los procesos de encriptación y desencriptación esto provee a los clientes con una performance de red en tiempo de real.

Los productos InfoCrypt de IsolationSystems, encriptan el paquete entero, incluyendo el encabezado original, antes de encapsular la información en un nuevo , paquete además de proteger los datos que se están transmitiendo, esto esconde completamente la topología interna de los dos redes remotas y también protege otra información de encabezado valioso, tal como el tipo de hackers y adversarios.

Para conseguir seguridad en las redes privadas virtuales, F-Secure VPN en una solución flexible y de coste aprovechable para obtener los beneficios de internet comprometiéndose a mantener la seguridad en la misma. Dota a la gestión de la red de túneles entre los puntos de empresa mantenimiento el acceso a puntos externos si se quiere. Es mejor usar este paquete en unión a una firewall para conseguir un control total sobre el tráfico de datos toda la organización.

F-Secure VPN es un nuevo producto de la compañía Data Fellows que se encuentra dentro de la línea de producto enfocado a la seguridad de Internet. La compañía Data FellowsLtd, es la primera vendedora de productos de seguridad usa los mecanismos de encriptación disponibles, más sofisticado y además es compatible con las arquitecturas modernas Cliente-Servidor y por supuesto Internet.

El modo tradicional de conectar puntos empresariales próximos es usar servicios tradicionales de "Telco", tales como x.25 en líneas alquiladas o FrameRelay. Sin embargo, esos servicios tendieron a ser difíciles de obtener o eran muy caros, principalmente, en el entorno internacional. Como resultado de esto, muchos usuarios están pensando seriamente en usar internet como su nexo de unión empresarial. Un gran número de análisis creen que pronto Internet reemplaza a la mayoría de las comunicaciones entre puntos empresariales internacionales, y también penetrara en las redes empresariales nacionales.

F-Secure VPN es un encaminador – router – de encriptación que te posibilita construir una VPN sobre la red con una seguridad criptográfica similar a la utilizada en el ejército. Para un gestor de red comparativa, ayudará a recortar el coste de las líneas sin perder seguridad. Para un proveedor de servicios, dará la oportunidad de competir y rebasar a la competencia, dado que F-Secure VPN proporciona nuevos servicios con respecto a la seguridad.
Las características principales son las siguientes:

Fácil **de instalar**. Requiere muy pocos parámetros de instalación para el administrador, durante la instalación inicial.
Fácil de configurar. F-Secure VPN 1.1 destaca por un editor de red grafico que permite configurar la totalidad de red VPN desde una simple estación de trabajo.

Configurable para asegurar las conexiones Extranet. Con el editar de red de F-Secure VPN, se puede definir la seguridad en las conexiones Extranet con los clientes habituales.

Rápido. En la actualidad, las redes privadas virtuales pueden aumentar la velocidad en las conexiones entre puntos empresariales gracias a que comprimen todo el tráfico, añadiéndoles encriptación.

Seguro. Usa una Extensa variedad de algoritmos de selección de usuarios, incluyendo 3DES, Blowfish, RSA, etc.

Basado en una tecnología ampliamente probada y usada. F-SecureVPN está basando en la tecnología F-Secure SSH, el estándar de hecho para conexiones entre terminales encriptados usando Internet. Es usada por la **NASA.**

Asequible. Una pequeña red privada virtual de 2 puntos puede instalarse por 5000 dólares más el precio de los PC's dedicados.

Disponible a nivel global con una fuerte encriptación. Data Fellows puede enviar el software encriptado a todo el mundo, sin ningún compromiso, desde las oficinas situados en Europa o en USA. Como compañía Europea que es no se encuentran bajo las restricciones de exportaciones de americanas referentes a la encriptación.

CAPITULO V

IMPLEMENTACION DE UN FIREWALL CON ISA SERVER

5.1. ¿QUÉ ES ISA SERVER 2006?

Es un servidor de seguridad de nivel empresarial que permite proteger las Tecnologías de la Información del entorno de su red frente a las amenazas de Internet, además de proporcionar a los usuarios un acceso remoto seguro a las aplicaciones y datos corporativos.

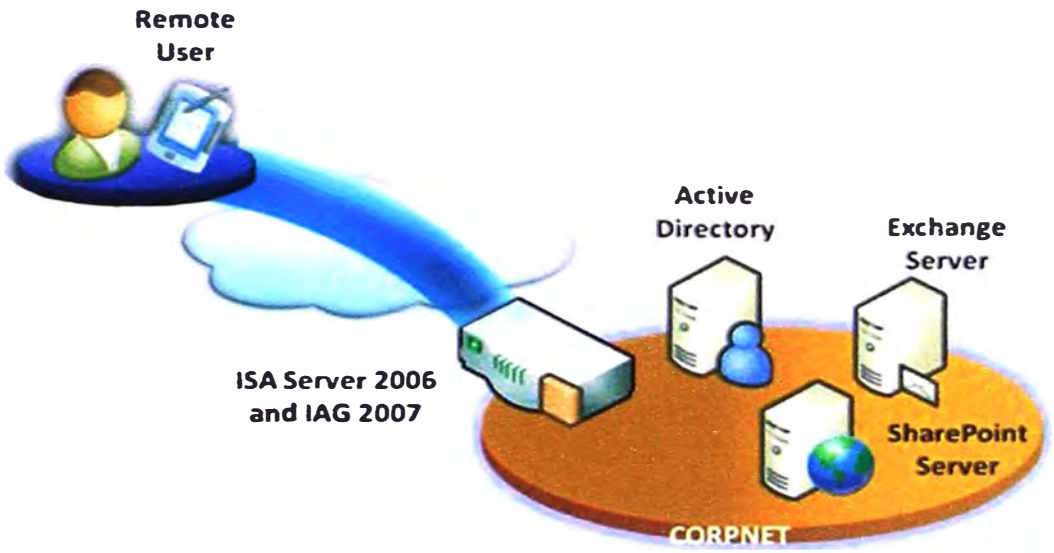


Figura 5.1 Una Red es protegida de internet, pero puede ser accedida remotamente por un administrador

En función a otros conceptos podríamos decir también que un servidor ISA es un Firewall por la protección de acceso a Internet.

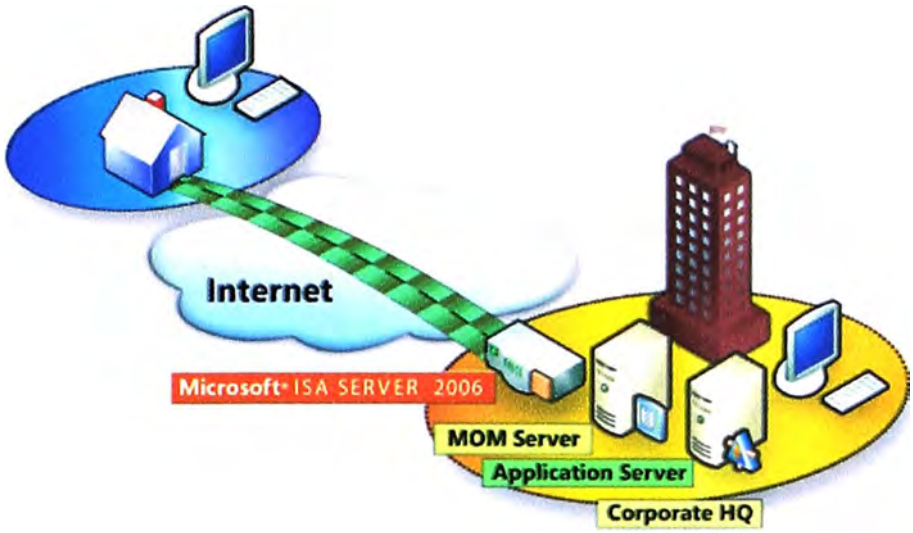


Figura 5.2 ISA defiende su entorno frente a la amenaza procedentes de Internet

Las empresas necesitan evitar los dañinos efectos que provocan los ataques y el código malintencionado, mediante herramientas integrales capaces de analizar y bloquear contenidos, archivos y sitios Web potencialmente peligrosos. La protección que ofrece ISA Server 2006 para el acceso a Internet permite a las organizaciones proteger sus entornos frente a amenazas basadas en tecnologías Web que pueden proceder de Internet, pero también desde dentro de la propia red corporativa. Con una arquitectura híbrida firewall-proxy, capacidad para la inspección en profundidad de los contenidos de los paquetes de red, políticas de alta granularidad y un sistema completo de alertas y funciones de monitorización, ISA Server facilita la gestión y hace posible la protección de toda su red.

ISA Server puede extender sus servicios a subredes para cumplir su función de manera extendida.

5.2. CONFIGURACION DEL ISA SERVER

Para creara un Servidor ISA mediante máquinas virtuales debemos considerar que este servidor debe tener dos tarjetas de Red una denominada interna y la otra externa. La configuración de estas tarjetas de red se muestra en el gráfico de la figura 5.4.

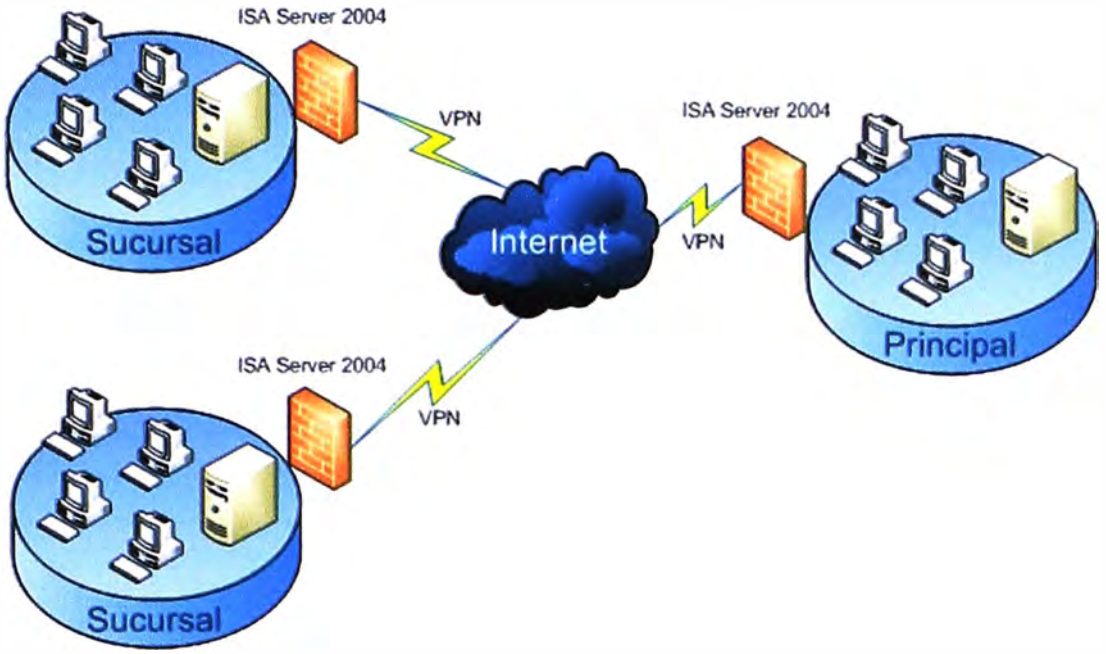


Figura 5.3 ISA extendido para varias subredes

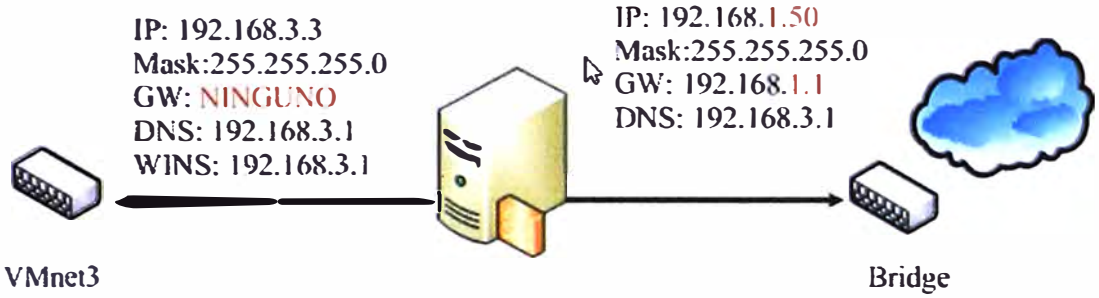


Figura 5.4 Configuración de las tarjetas Interna y Externa del Servidor ISA

Observe que la tarjeta interna está conectada al VMnet3 (Swich de la máquina virtual) y la externa al **swich Bridge** (Swich de la máquina virtual conectada a la tarjeta de la PC conectada a Internet).

Levantamos la máquina virtual que puede ser clonando o instalando una nueva.

Una vez instalada debemos configurar el Hardware y ejecutar lo que manifestamos, es decir debe tener dos tarjetas de red. Por defecto nos instala una, la otra debemos adicionarla (Fig 5.5).

En la ventana respectiva Clic en Next.

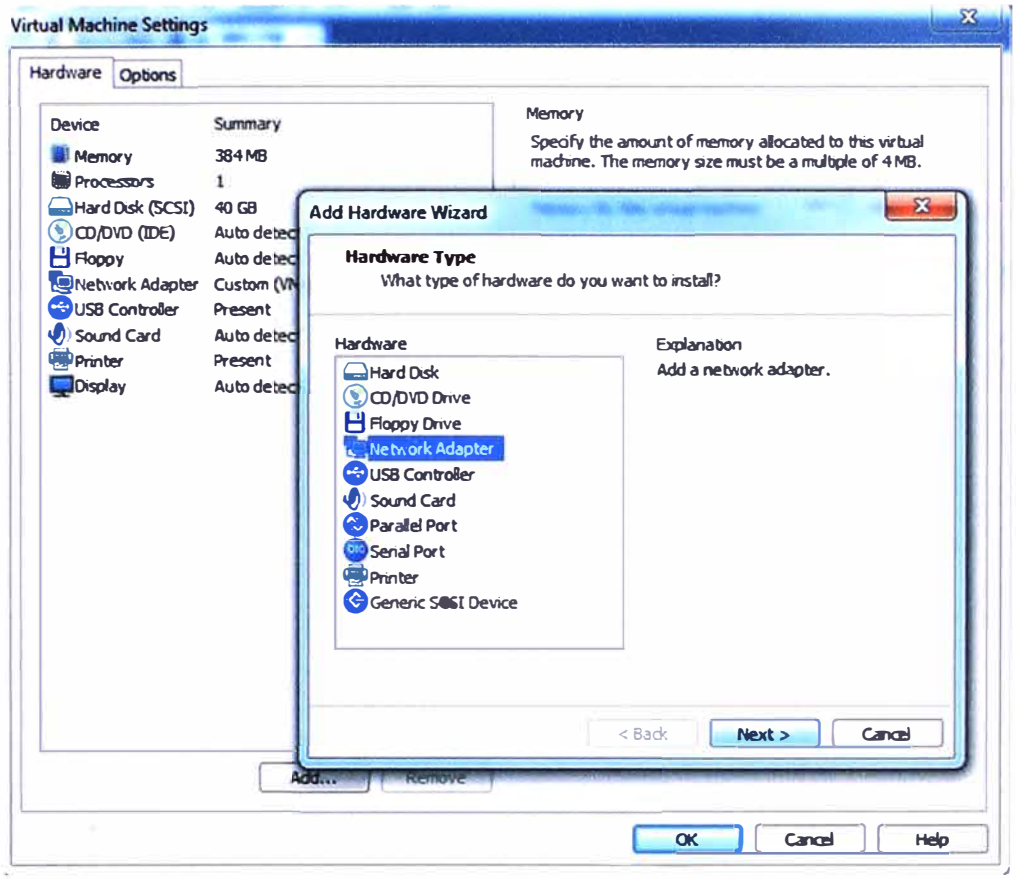


Figura 5.5

En la ventana que se muestra check en bridge porque es allí donde conectaremos esta segunda tarjeta de red. Clic en Finish (Fig. 5.6).

Durante la instalación del sistema operativo el sistema configurado es muy vulnerable, así que por precaución a que ingresen virus al momento de las actualizaciones, optaremos por algo que trae buenos resultados y es conectar la segunda tarjeta de red al swich VMnet3.

Una vez instalado y configurado el Servidor ISA, podremos abrirlo hacia Internet porque ya empezara a cumplir su función, es decir de controlar la información que quiere pasar de Internet.

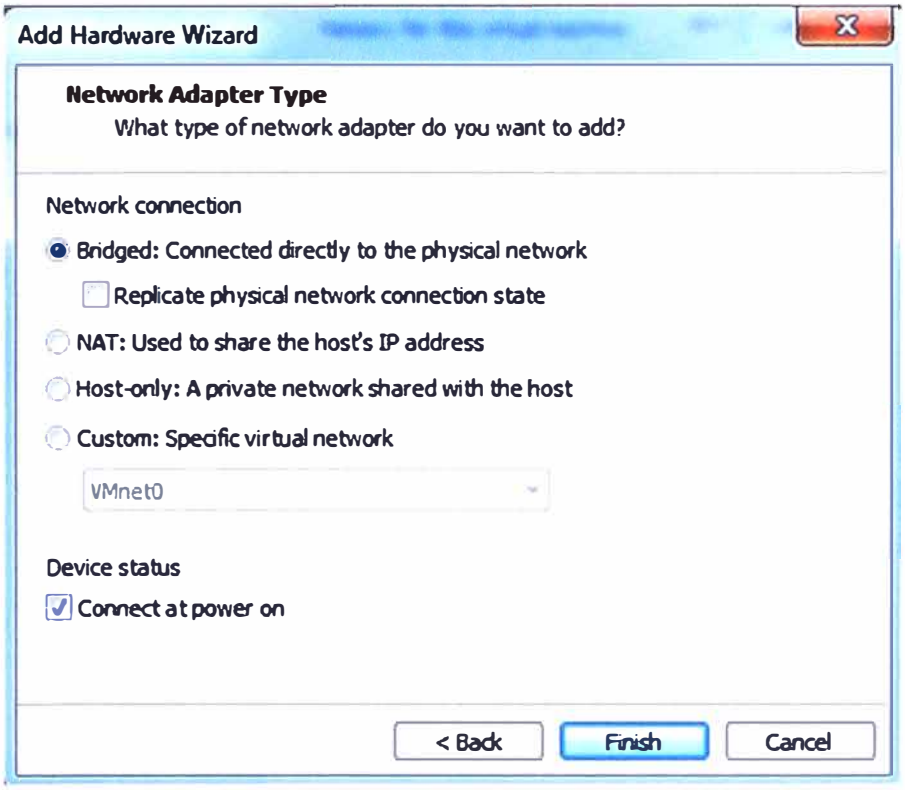


Figura 5.6

5.3. CONFIGURACION DE LAS TARJETAS DE RED

Primero.- Abrimos Mis sitios en Red y ubicamos los adaptadores configurados por Hardware (Fig. 5.7).

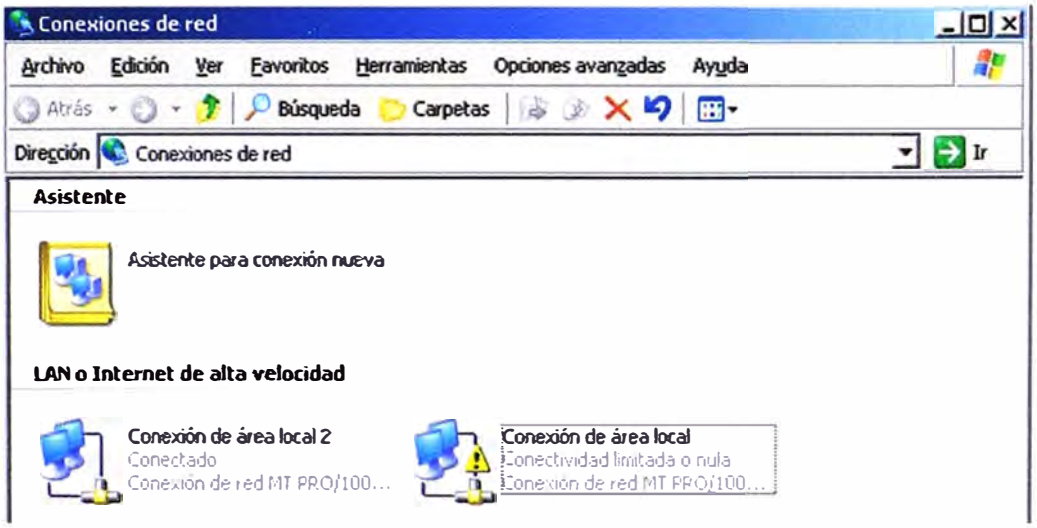


Figura 5.7

Segundo.- Procedemos a la configuración del adaptador interno, Clic con el botón derecho en el adaptador y configuramos la IP y resto de los parámetros tal como muestra la figura 5.8. Tenga claro que estamos configurando la tarjeta interna donde solo el Gateway no debe contener nada, el DNS y el Wins deben ser los mismos que del controlador de Dominio. Con estas consideraciones queda:

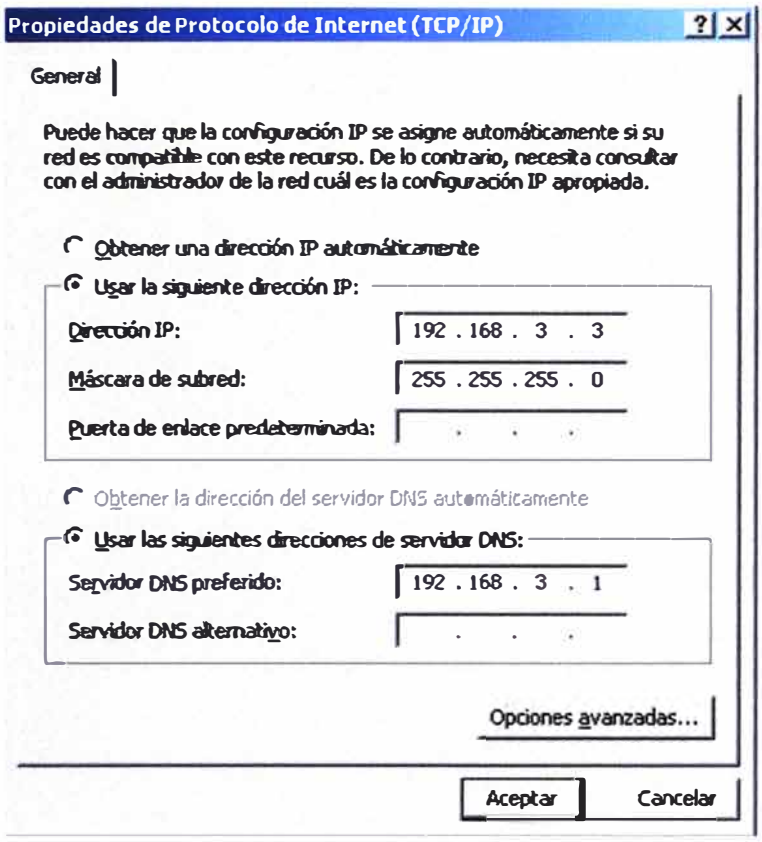


Figura 5.8

Tercero.- En opciones avanzadas dejamos el DNS por defecto pero incluimos el Wins de manera similar al DC (Figs. 5.9 y 5.10).

Cuarto.- Aceptamos y Cerramos.

Quinto.- Luego le cambiamos el nombre al adaptador con la denominación INTERNO.

Sexto.- Configuramos el adaptador externo, en la primera ventana consideramos: (Fig. 5.11)

Séptimo.- Luego clic en Propiedades. Para configurar los parámetros que se indican (Fig. 5.12):

Octavo.- En Opciones Avanzadas en la pestaña de DNS configuramos como se indica (Fig. 5.13). Quitamos el check en registrar estas direcciones de conexiones en DNS, Las maquinas lo identificaran a este servidor mediante la tarjeta interna.

Noveno.- En Wins configuramos como se indica (Fig. 5.14). En esta se deshabilita NetBios sobre TCP/IP. Clic en Aceptar.

Decimo.- Aceptamos las ventanas y cerramos. Luego cambiamos el nombre del adaptador por EXTERNO y nos quedara como se muestra la figura 5.15.

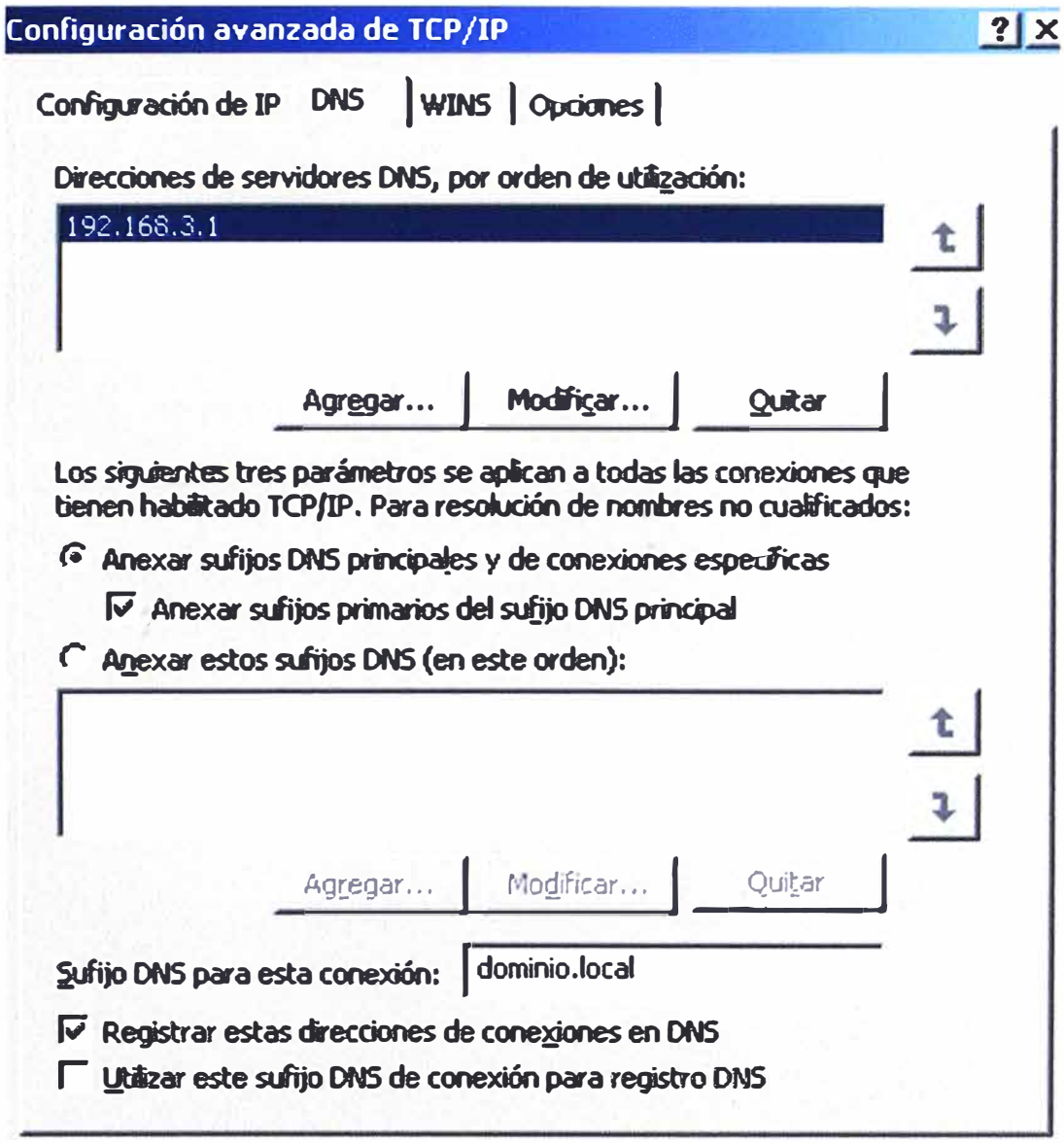


Figura 5.9

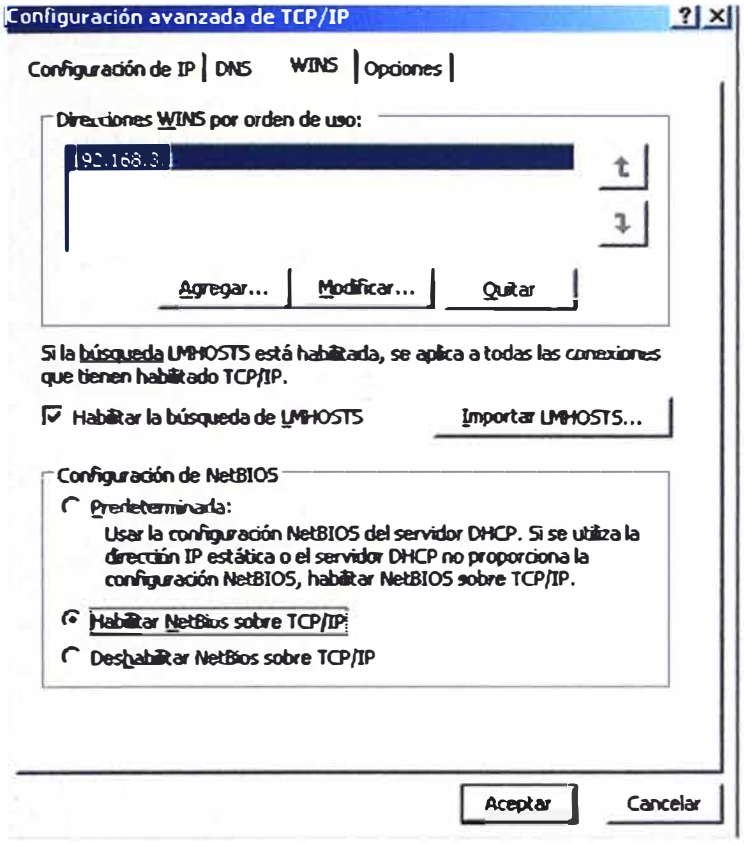


Figura 5.10

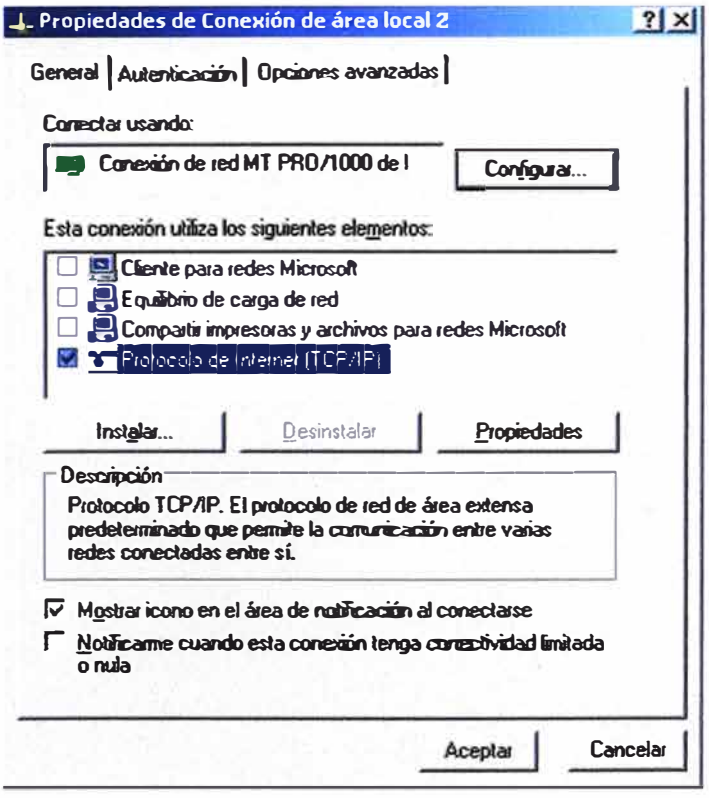


Figura 5.11

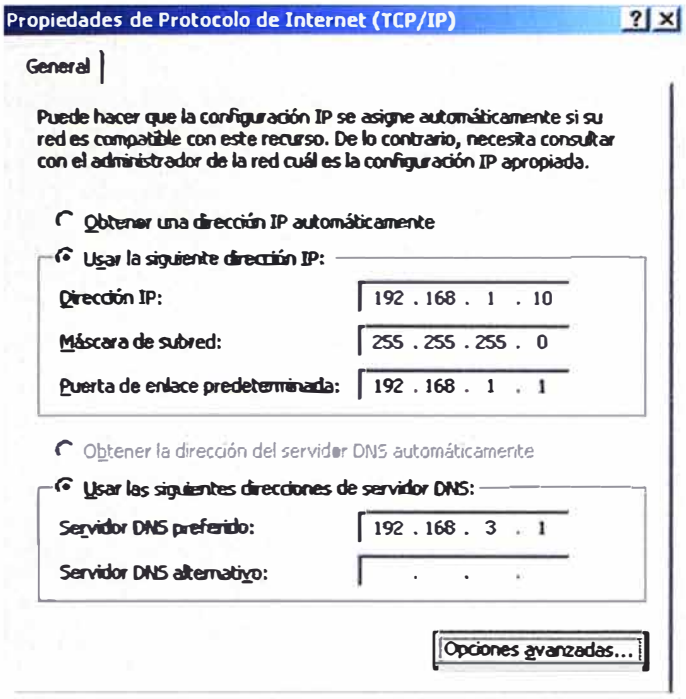


Figura 5.12

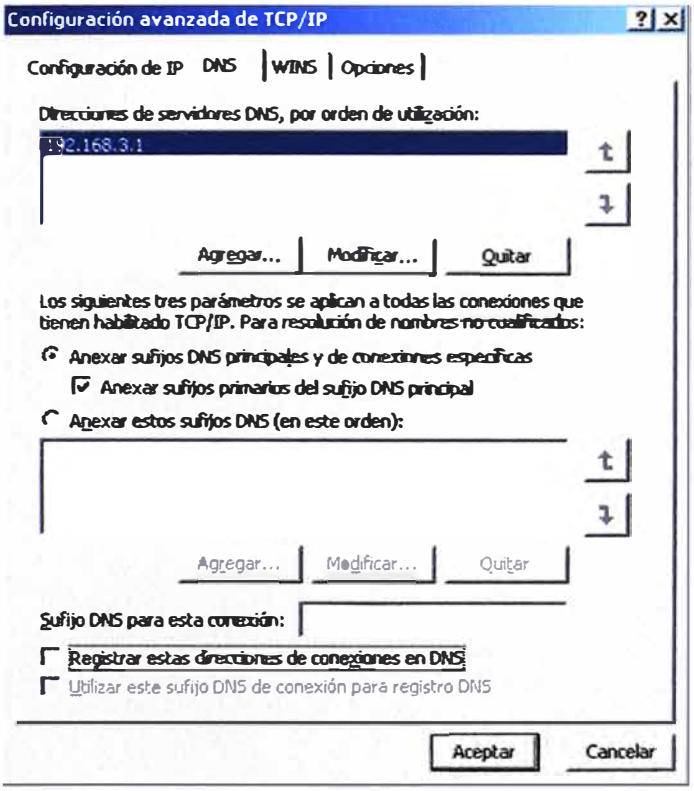


Figura 5.13

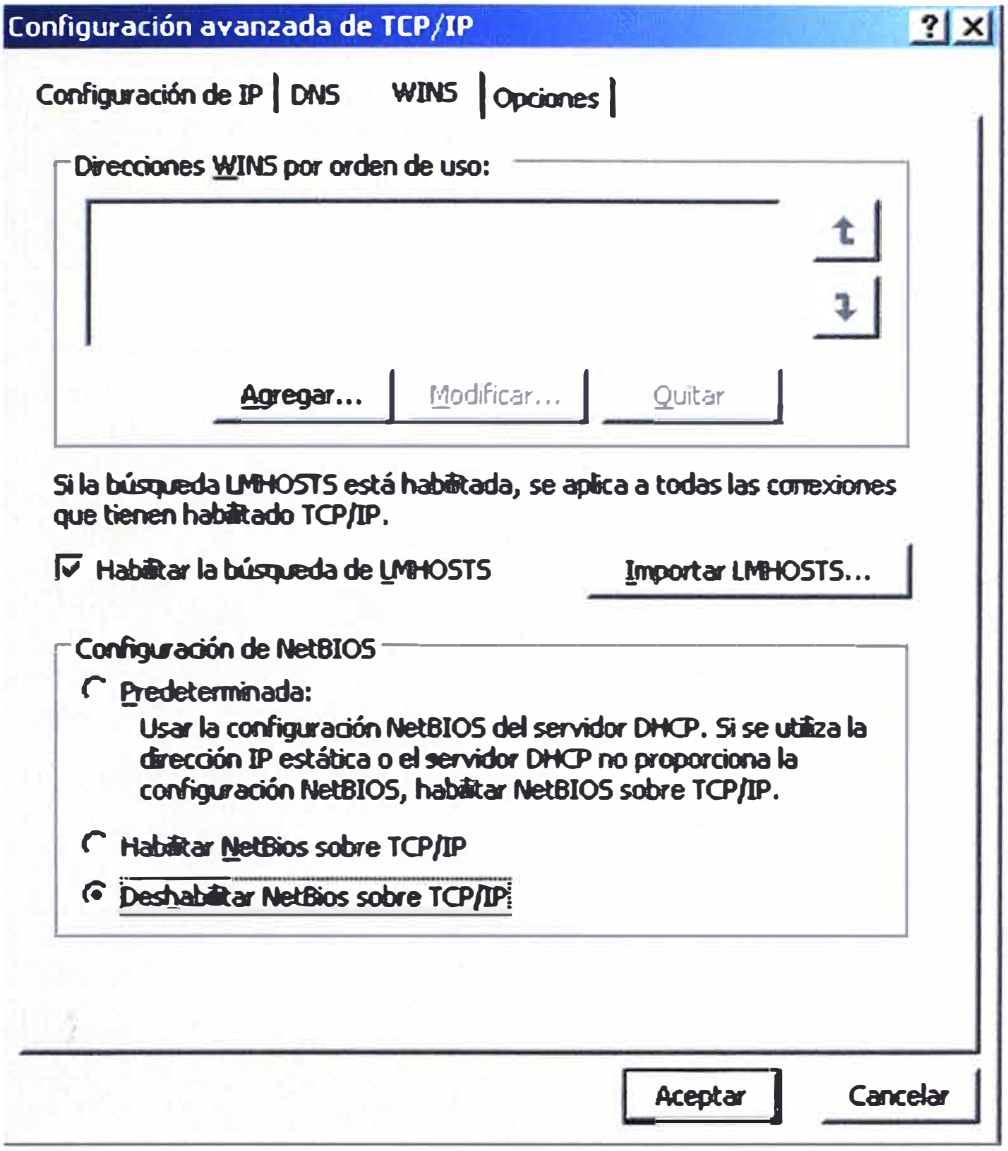


Figura 5.14

Figura 5.15

5.3.1. ORDEN EN LAS TARJETAS DE RED

Es importante saber que cuando se tienen varias tarjetas de Red el sistema trabaja según un orden, es decir las tarjetas deben estar identificadas, quien es la primera la segunda y así sucesivamente para ello podemos ordenarlas de la siguiente manera:

1. Estando en la ventana anterior, hacemos clic en Opciones avanzadas del menú, y en esta seleccionamos y clic en configuración Avanzada, tal como muestra la figura 5.16.

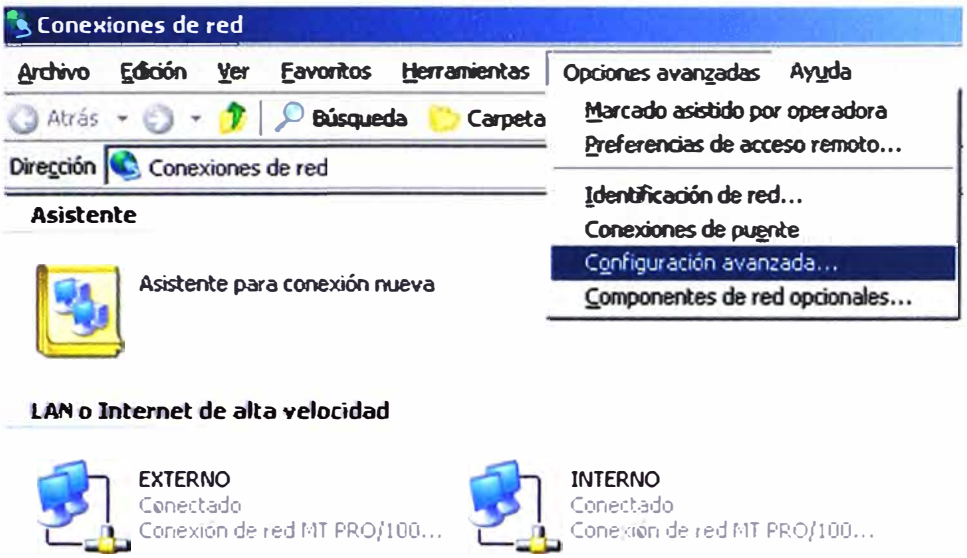


Figura 5.16

2. En la nueva ventana que se muestra seleccionamos interno y lo ubicamos primero haciendo clic en las flechitas que se muestran a la derecha para subir su ubicación (Fig. 5.17).

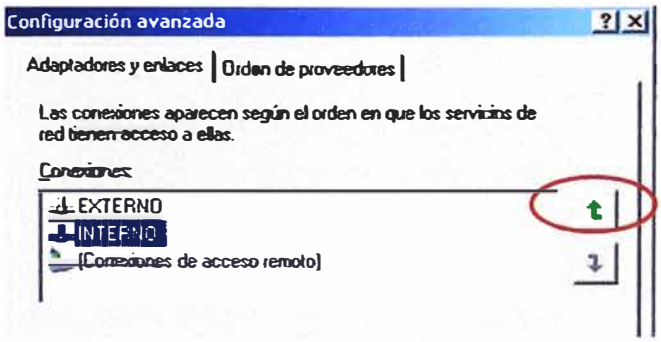


Figura 5.17

3. Una vez ejecutado queda como se muestra en la figura 5.18. Clic en Aceptar.

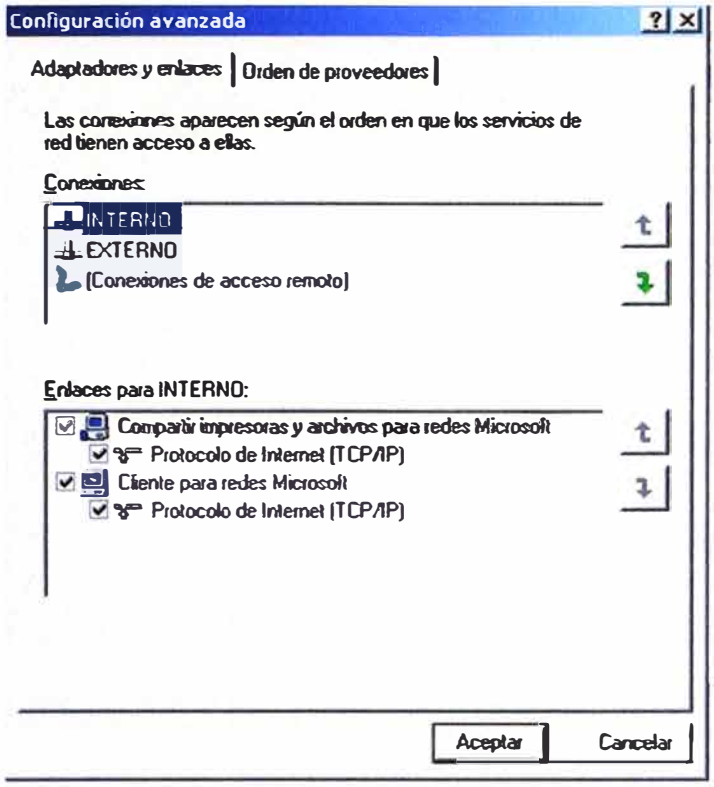


Figura 5.18

5.4. UNION DEL SERVIDOR ISA AL CONTROLADOR DE DOMINIO

Una de las razones para pegar el ISA al DC, es que algunos grupos requieren tener autenticación. Para realizar esta acción procedemos de la siguiente manera:

1. Clic con el botón derecho en MiPc.
2. Activar la pestaña Nombre de equipo.
3. Clic en cambiar.
4. Check en Dominio y ponemos el nombre del dominio, en este caso dominio.local, luego Clic en aceptar.
5. Llenamos la ventanita con los siguientes datos (Fig. 5.19).

La contraseña no se pone porque no pusimos contraseña en el Servidor ISA. Clic en Aceptar y luego reiniciamos el equipo.

Cuando reinicia la maquina debemos ingresar no al ISA si no al Dominio como Administrador la como muestra la figura 5.20. Clic en Aceptar.

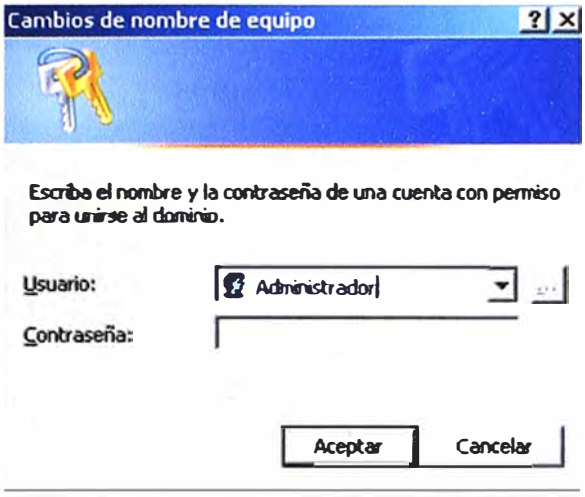


Figura 5.19

Figura 5.20

Una vez que se ingresó al dominio como administrador del ISA debemos cambiar la contraseña para el administrador local.

5.5. CAMBIO DE CONTRASEÑA

1. Clic con el botón derecho sobre MiPc.
2. Seleccionar y luego clic en Administrar.
3. En la ventana de administración de equipos despliegue usuarios y grupos locales.
4. Clic en Usuarios, y en la parte derecha seleccione administrador.

5. Clic derecho en Administrador, luego clic en establecer contraseña (Fig. 5.21).

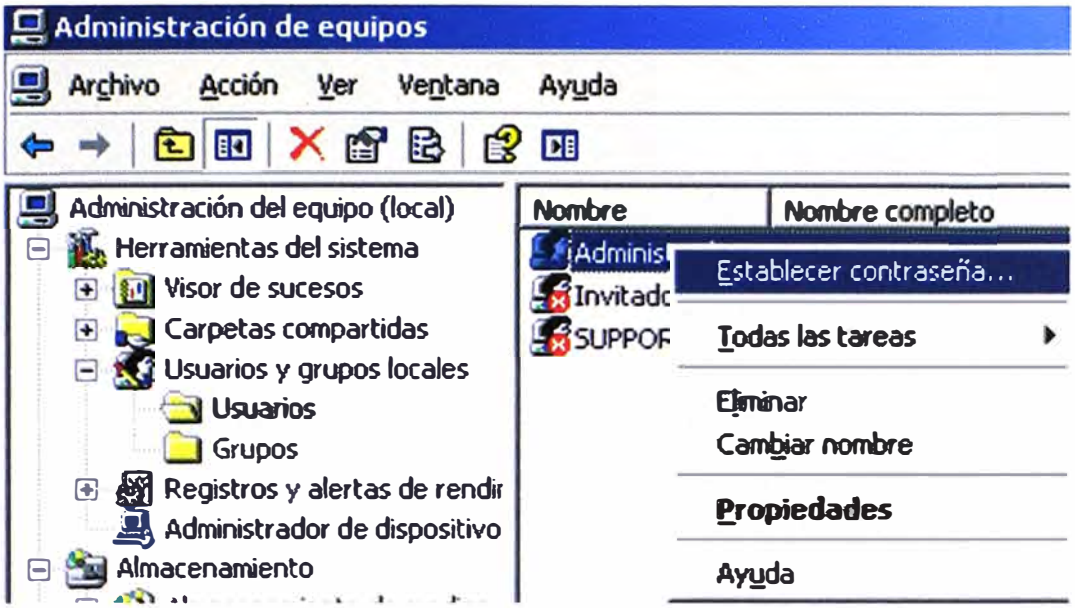


Figura 5.21

6. Clic en continuar.
7. En la nueva ventana escribir la nueva contraseña en ambos recuadros, luego clic en aceptar.

5.6. INSTALACION DEL ISA SERVER

Ya está configurado y en esta máquina debemos instalar ahora el ISA Server 2006 Estándar. Para su instalación realice:

1. Ejecute el programa de instalación y se abrirá la siguiente ventana (Fig. 5.22).
2. Clic en instalar ISA 2006
3. Empieza la instalación y en la pantalla que se queda estática Clic en Siguiente.
4. Aceptamos los términos del contrato y clic en siguiente.
5. Llenamos el cuadro de Organización puede ser INFOTRONIC, y clic en siguiente.
6. En la ventana que se muestra nos pide señalar si la instalación será Típica o Personalizada (Fig. 5.23). Chequeamos personalizada y clic en siguiente.

Figura 5.22

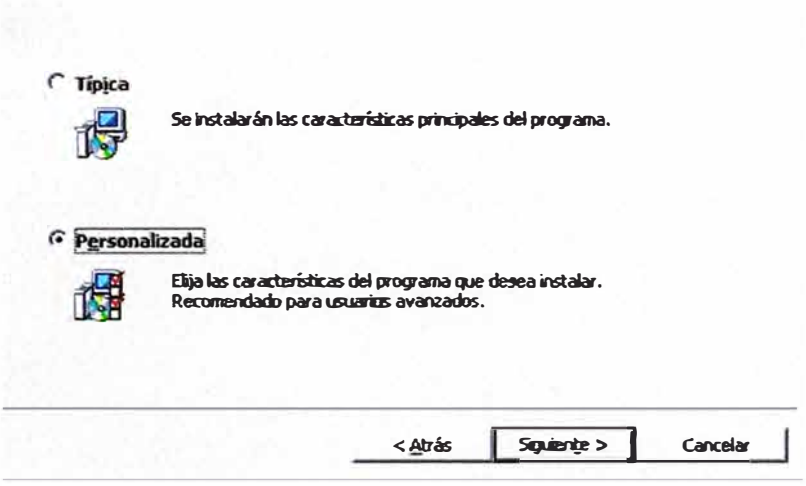


Figura 5.23

7. En la nueva ventana que se muestra no configuramos nada solo clic en siguiente.
8. En esta ventana nos solicita definir cuáles serán las direcciones que considerara ISA Server como internas. Clic en Agregar.

9. En la ventana que se muestra, es una práctica Hacer Clic en Agregar adaptador (Fig. 5.24).

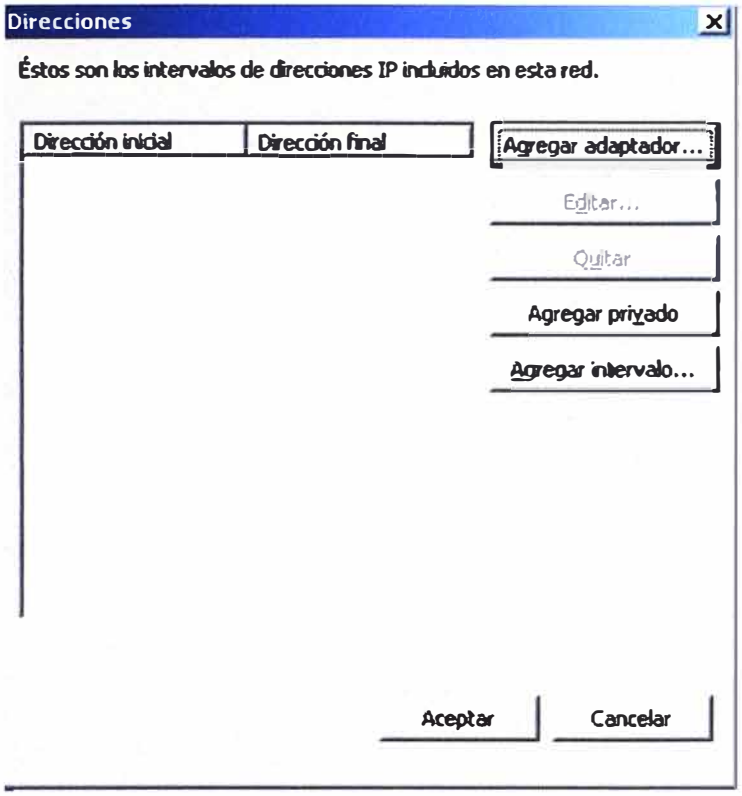


Figura 5.24

10. En esta ventana Chequeamos Interno luego clic en aceptar y las direcciones se agregaran automáticamente (Fig. 5.25).

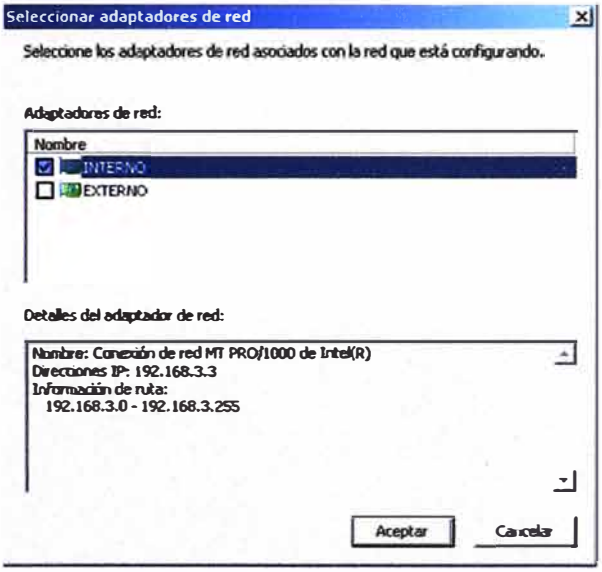


Figura 5.25

11. Clic en aceptar (Fig. 5.26).

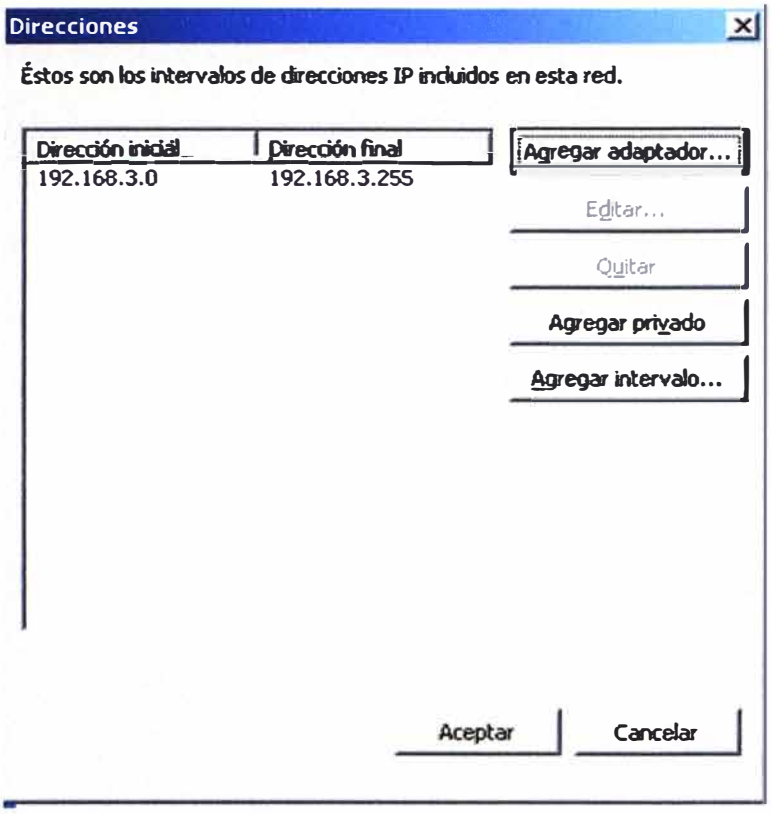


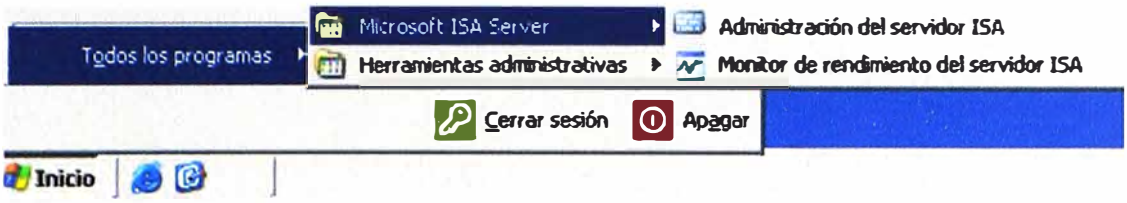
Figura 5.26

12. En la siguiente pantalla te da la posibilidad de editar los rangos de direcciones es decir puedes aumentar o quitar, si no hay nada que cambiar Clic en siguiente.
13. Seguidamente me pide chequear la compatibilidad con otras versiones para otras máquinas de la Red, clic en siguiente.
14. En la siguiente ventana también siguiente.
15. En la próxima ventana también siguiente y empezara a instalarse, dura algunos minutos. Al final se Abre una pantalla para chequear una opción. No chequear y clic en siguiente de esta manera finaliza la instalación dando unas sugerencias.
16. ISA server no pide reiniciar la maquina pero es recomendable hacerlo.

5.7. CONSOLA DEL ISA SERVER

Para ingresar a la consola del ISA Server seguimos la siguiente ruta:

Inicio / Microsoft ISA Server / Administración del servidor ISA



Al ejecutar la ruta anterior ISA nos muestra la consola conformada por 3 cuerpos tal como muestra la figura (Fig. 5.27).

En la parte central hay basta información sobre ISA, configuración y otros que usaremos cuando lo requiramos.

Si hacemos clic en el servidor la consola nos muestra información para las diferentes tareas que podemos realizar en ella.

Figura 5.27

5.8. CREACION DE DIRECTIVAS PARA EL ACCESO A INTERNET

Para crear esta directiva procedemos de la siguiente manera:

1. Abrir la consola del ISA Server.
2. Clic derecho sobre Directiva de Firewall / seleccionar Nuevo / Clic en regla de acceso (Fig. 5.28).

3. En la ventana que se muestra ponga el nombre de la directiva que en este caso será "Permite DNS desde DNS Interno hacia Internet", tal como se muestra en la imagen. Luego clic en siguiente (Fig. 5.29).
4. Check en Permitir y luego clic en siguiente.
5. En la ventana que se muestra en la figura 5.30, seleccionar "Protocolos Seleccionados" y clic en agregar, aparece una ventana en el cual despliega Infraestructura y selecciona DNS. Luego clic en agregar y siguiente en la primera ventana.

Figura 5.28

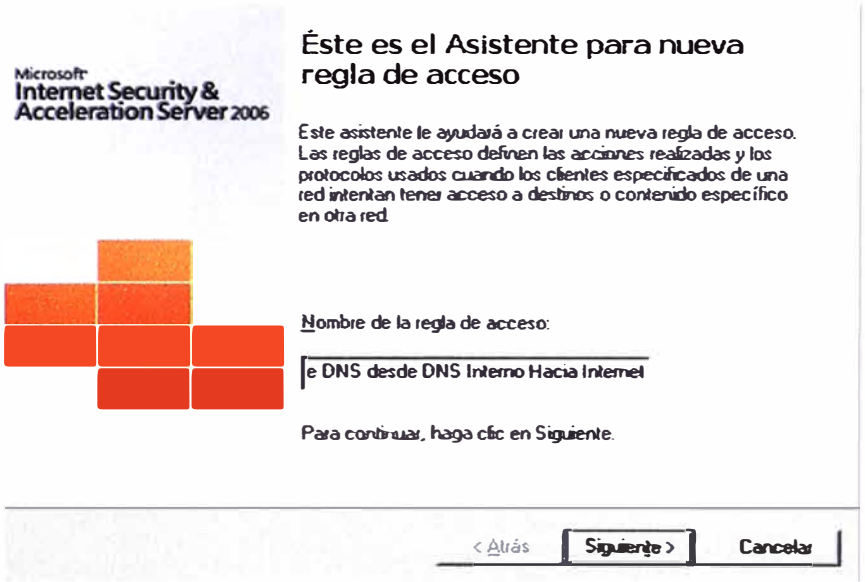


Figura 5.29

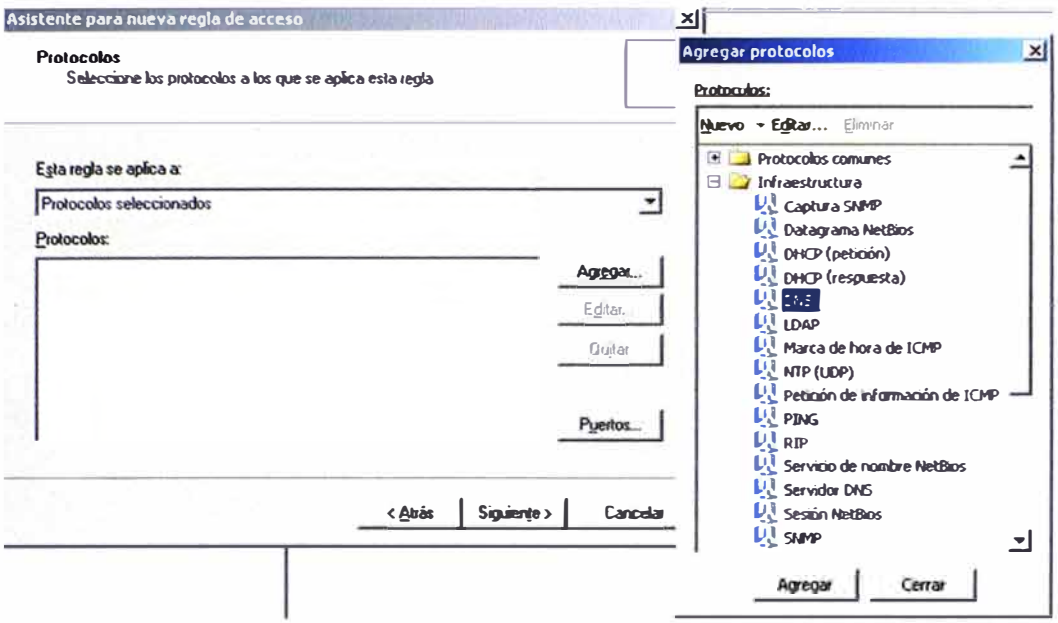


Figura 5.30

6. Ahora debemos indicar desde donde vamos a permitir el trafico DNS, lo mejor es que el trafico sea desde el servidor controlador de dominio. Para ello creamos una computadora con el nombre del servidor y la IP será encontrado automáticamente. En la ventana que se muestra clic en agregar y se abre una nueva ventana, en esta clic en nuevo y luego seleccionar equipo y hacer click en ella, al ejecutar se abrirá una ventanita en la cual debes poner el nombre del servidor y luego clic en examinar, en la nueva ventana clic en buscar y la IP llegara automáticamente. Clic en aceptar, en descripción poner DENS interno y otra vez aceptar. En esta ventana inicial dentro de equipo, ya está el equipo creado, marcarlo y clic en agregar. Aparecerá la ventana que se muestra (Fig. 5.31). Clic en siguiente.
7. Ahora indicamos el destino, para ello en la ventana que se muestra clic en agregar, se abre una nueva ventana en esta desplegamos Redes y allí seleccionamos externa para luego hacer clic en agregar, luego cerramos y obtenemos la imagen que se muestra (Fig. 5.32). Clic en siguiente.
8. Marcamos todos los usuarios y clic en siguiente.
9. En la ventana que se muestra clic en finalizar.
10. Para concluir debemos todavía aplicar la nueva directiva para ello clic en Aplicar (Fig. 5.33).

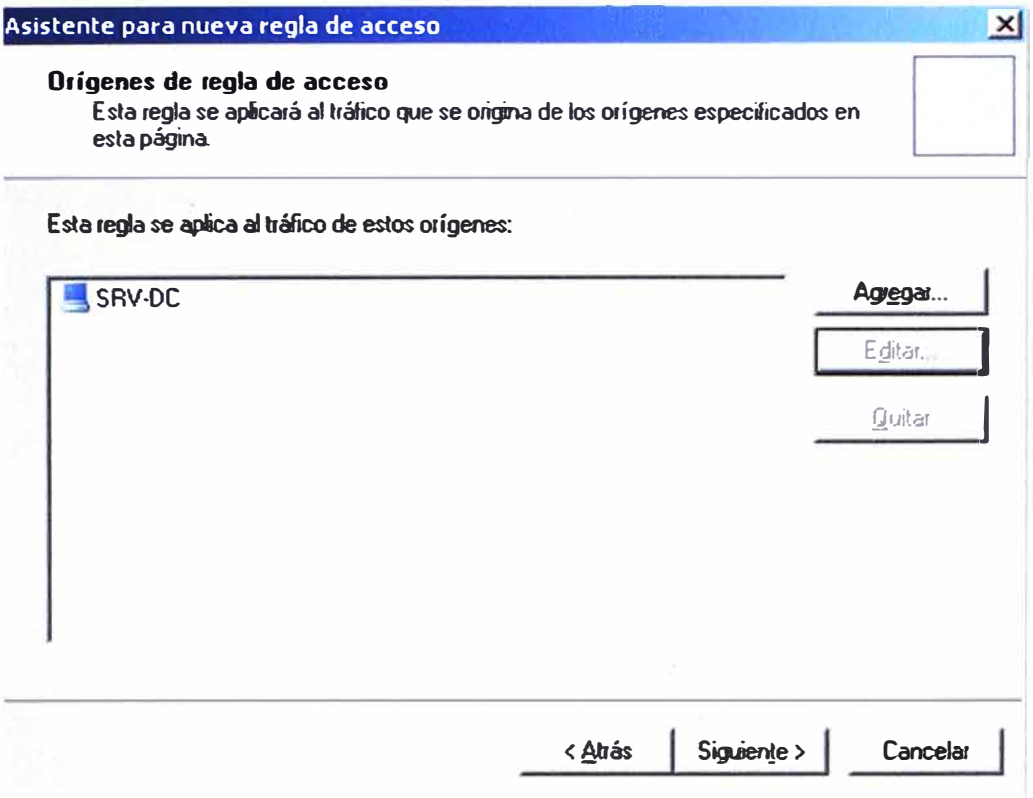


Figura 5.31

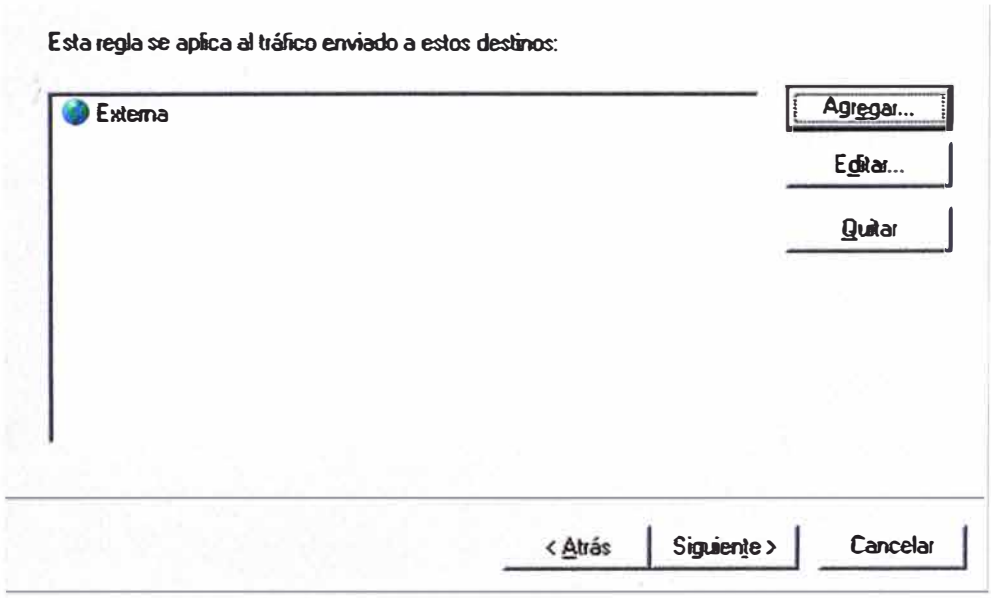


Figura 5.32

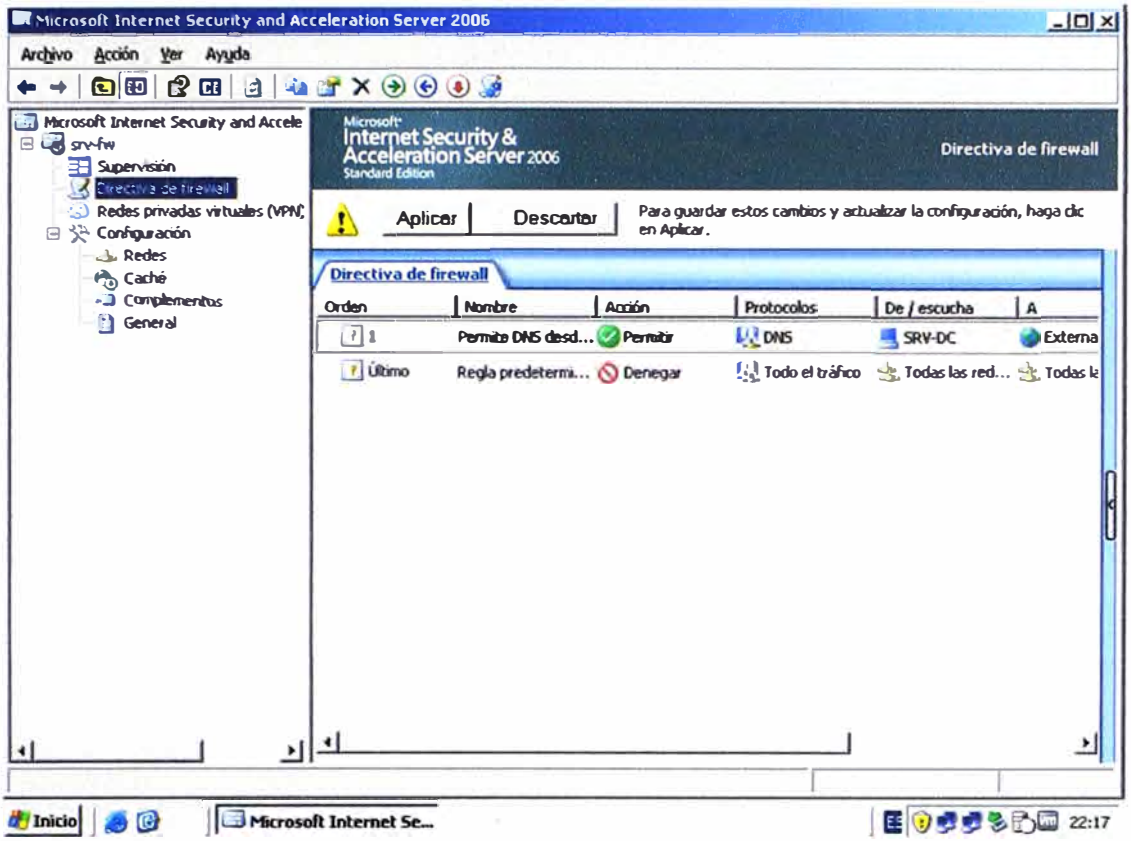
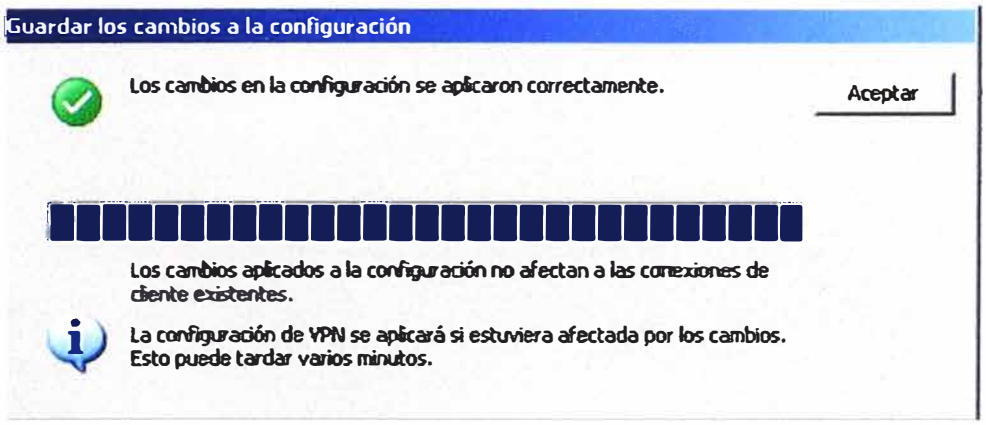


Figura 5.33

Aparecerá:



Si intentamos ingresar a Internet desde una PC usuario, no se podrá porque el ISA no está autorizado para permitir el tráfico de http.

5.9 CREACION DE LA REGLA QUE PERMITA LA NAVEGACION DE USUARIOS

1. Abrimos la consola del ISA y procedemos de manera similar al caso anterior, en la ventana para poner el nombre de la nueva regla, ponemos: "Permite navegación de usuarios http, https" y luego clic en siguiente (Fig. 5.34).

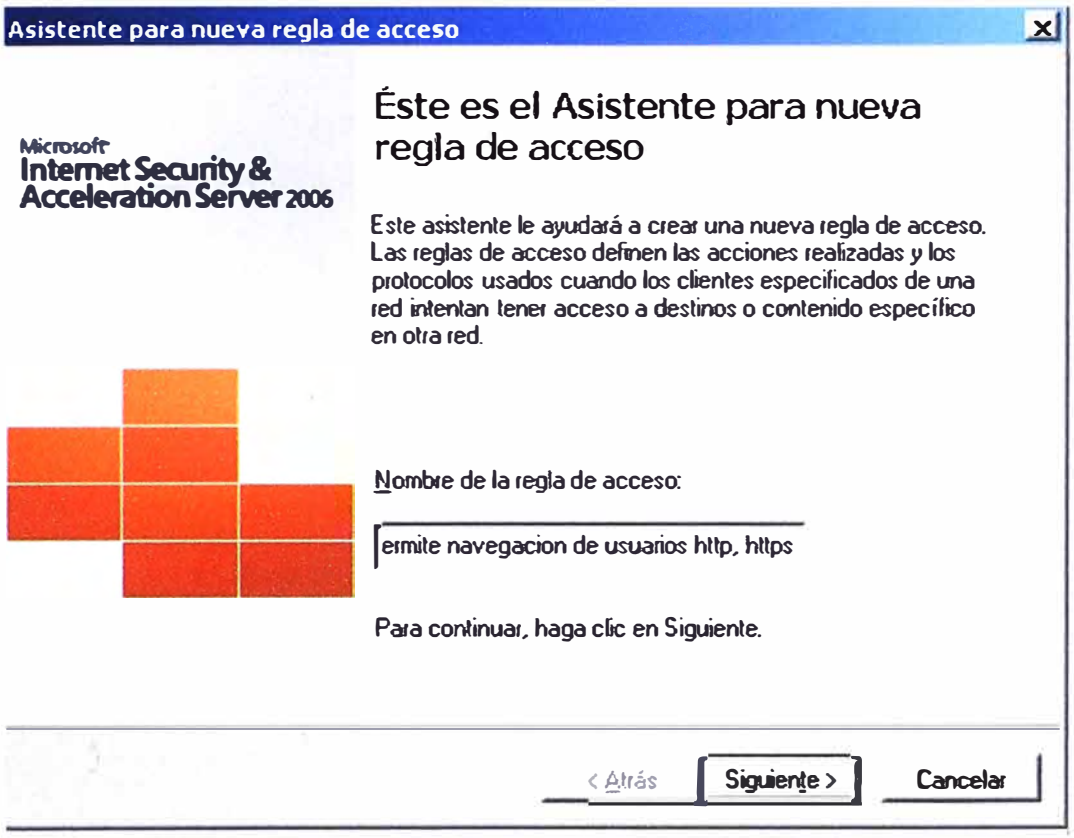


Figura 5.34

2. Check en permitir y clic en siguiente.
3. En la ventana que se abre hay que indicarle el protocolo que debe manejar, en este caso será http, https, al seleccionar cada uno debemos agregar para que se muestre en la primera ventana. Clic en siguiente (Fig. 5.35).
4. Luego nos pide indicar el origen, en este caso será Interno.
5. Indicar el destino, en este caso Externo.
6. Indicamos todos los usuarios y clic en siguiente.
7. Clic en finalizar.
8. Aplicamos la regla.

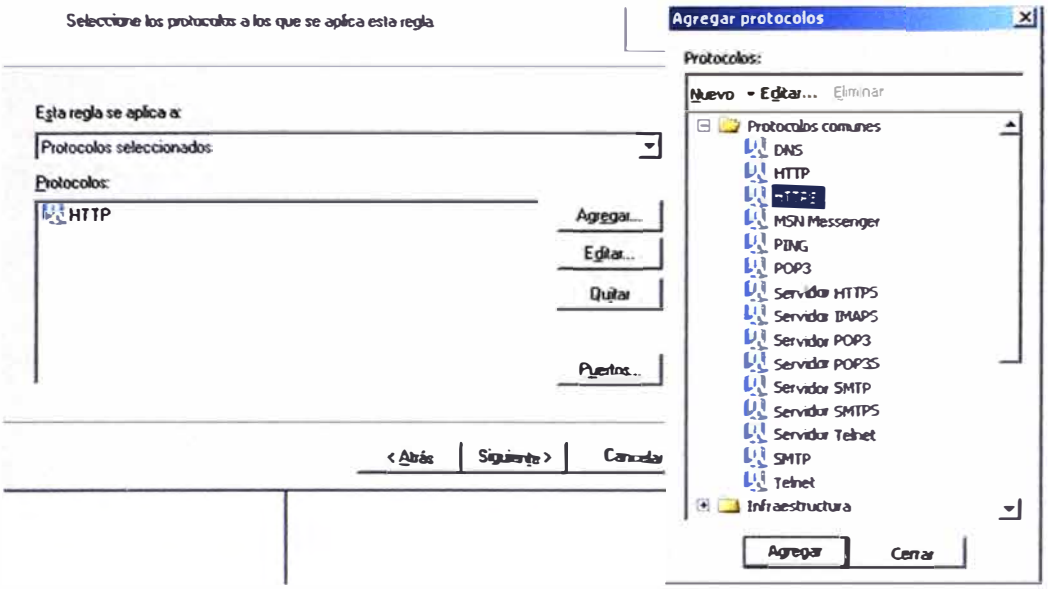


Figura 5.35

Ubíquese en la maquina usuario y ahora ingrese a Internet.

CONCLUSIONES Y RECOMENDACIONES

1. Es importante tener en cuenta que la seguridad y los mecanismos de supervisión y control de tráfico de información deben ser considerados fundamentales, especialmente cuando la data que se intercambie sea muy importante.
2. Existen una serie de estudios sobre protección de los sistemas de información, lo que hay que hacer es poner a prueba cada uno de ellos, para así conocer su robustez y seguridad.
3. Aún se tenga un sistema muy cercano al 100% seguro, es claro que siempre puede ser susceptible de caer bajo la influencia de algún hacker especialista, por ello también las metodologías de protección deben ir cambiando de estrategias cada cierto tiempo.
4. Al proteger la información con algún sistema, es necesario tener presente que también hay hardware que tiene mecanismos de protección que trabajan en conjunción con los sistemas, por ello es importante la correcta selección de tales dispositivos, que debe ser realizado por profesionales, ya que de ello dependerá que los sistemas trabajen de forma óptima.
5. No hay que pasar por alto también, lo que las empresas proveedoras ofrezcan, ya que por ese lado también hay un complemento importante para el tratamiento de nuestra información.
6. Una recomendación importante es considerar la infraestructura de la red antes de diseñar su seguridad.
7. Debemos mentalizar que toda red es insegura y por lo tanto debe tener su sistema de seguridad.

8. En el mercado existen sistemas costosos para la seguridad de redes, puede con un sistema operativo como el Windows 2003, o el Windows 2008 resolver problemas de seguridad y la inversión es menor.
9. Es recomendable usar máquinas virtuales para poner a prueba la seguridad de una red, trae buenos resultados y sobre todo es práctico.

ANEXO

GLOSARIO DE TÉRMINO

Cifrado:

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. El cifrado se usa cuando desee un alto nivel de protección de la información.

Criptografía:

Criptografía es la ciencia y arte de escribir mensajes en forma cifrada o en código. Es parte de un campo de estudios que trata las comunicaciones secretas, con finalidades entre otras, para autentificar la identidad de usuarios, autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias; Proteger la integridad de transferencias electrónicas de fondos.

Hash criptográfico:

En informática, **hash** se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc. Las funciones de hash criptográfico se usan en varios contextos, en especial para computar el compendio del mensaje al hacer una firma digital.

Time-stamps:

Es una secuencia de caracteres, que denotan la hora y fecha (o alguna de ellas) en la cual ocurrió determinado evento. Esta información es comúnmente presentada en un formato consistente, lo que permite la fácil comparación entre dos diferentes registros y seguimiento de progresos a través del tiempo; la práctica de grabar timestamps de forma consistente a lo largo de la información actual, se llama timestamping.

Sistemas distribuidos:

Un sistema distribuido es un conjunto de computadoras independientes; es decir autónomas, que aparecen ante los usuarios del sistema como una única computadora. Por ejemplo una red de estaciones de trabajo en un departamento de una universidad o compañía, donde además de cada estación personal, podría existir una pila de procesadores en el cuarto de máquinas, que no estén asignados a usuarios específicos sino que se utilicen de manera dinámica cuando sea necesario.

Kernel:

Es un software que constituye la parte más importante del sistema operativo.

Checksum:

Denominada también suma de verificación, es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corruptos. Es empleado para comunicaciones (internet, comunicación de dispositivos, etc.) tanto como para datos almacenados (archivos comprimidos, discos portátiles, etc.).

Abuso de privilegio:

Cuando un usuario realiza una acción que no tiene asignada de acuerdo a la política organizativa o a la ley.

Ataque Interior

Un ataque originado desde dentro de la red protegida.

Autentificación:

El proceso para determinar la identificación de un usuario que está intentando acceder a un sistema.

Autorización:

Proceso destinado a determinar qué tipos de actividades se permiten normalmente; la autorización, está en el contexto de la autentificación: una vez autentificado el usuario en cuestión, se les puede autorizar realizar diferentes tipos de acceso o actividad.

Bastión Host:

Un sistema que ha sido configurado para resistir los ataques y que se encuentran instalado en una red en la que se prevé que habrá ataques. Frecuentemente, los bastión hosts son componentes de las firewalls, o puede ser servidores Web “exteriores” o sistemas de acceso público. Normalmente, un bastion hosts está ejecutando alguna aplicación o sistema operativo de propósito general (por ejemplo: UNIX, VMS, WNT, ETC…) más que un sistema operativo de firewall.

Detección de intrusión:

Detección de rupturas o intentos de rupturas bien sea manual o vía sistema, expertos en software que atentan contra la red o contra la información.

Dual Homed Gateway:

Un "Dual Homed Gateway" es un sistema que tiene 2 o más interfaces de red, cada uno de los cuales está conectado a una red diferente. En las configuraciones firewall, un "dual homed Gateway" actúa generalmente, como bloqueo o filtrador de parte o del total tráfico que intenta pasar entre las redes.

Firewall:

Un sistema o combinación de sistemas que implementan una frontera entre 2 o más redes.

Firewall a nivel de aplicación:

Un sistema firewall en el que el servicio se proporciona por procesos que mantienen estados de conexión completos con TCP y secuencia miento las firewall a nivel de aplicación, a menudo redirigen el tráfico, de modo que el tráfico saliente, es como si se hubiera originado desde la firewall y no desde el host interno.

Host – based Security:

La técnica para asegurar de los ataques, a un sistema individual.

Logging:

El Proceso de almacenamiento de información sobre eventos que ocurren en la firewall en la red.

Perimeter-based Security:

La técnica de seguridad de una red, para controlar los accesos a todos los puntos de entrada y salida de la red.

Política:

Reglas de gobierno a nivel empresarial / organizativo que afectan a los recursos informáticos, prácticas de seguridad y procedimiento operativos.

Proxy

Un agente software que actúa que beneficio de un usuario, los proxies típicos aceptan una conexión de un usuario, toman una decisión al respecto de si el usuario o cliente IP es o no un usuario de proxy, quizás realicen procesos de autentificación adicionales y entonces completan una conexión el usuario y el destino remoto.

Router – Encaminador:

Dispositivo destinado a conectar 2 o más redes de área local y que se utiliza para encaminar la información que atraviesa dicho dispositivo.

Screened Host:

Un host – ordenador servidor – en red, detrás de un router protegido el grado en le host puede ser accesible depende de las reglas de protección del router.

ScreenedSubnet:

Una subred, detrás de un router protegido el grado en que en que la subred puede ser accesible depende de las reglas de protección del router.

TurnnelingRouter:

Un router o sistema capaz de dirigir el tráfico, encriptado y encapsulando para trasmitir a través de una red y que también es capaz de des encapsular y descifrar lo encriptado.