UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACION DE SEGURIDAD EN CONEXIONES REMOTAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

RICARDO REATEGUI SORIA

PROMOCIÓN
1986- I

LIMA – PERÚ
2007

DISEÑO E IMPLEMENTACION DE SEGURIDAD EN CONEXIONES REMOTAS

Dedico este trabajo a:

Mi Padre que en paz descanse

a

Mi Madre y esposa que están en el extranjero

y a

Mis hijos por su aliento en esta etapa.

SUMARIO

El siguiente informe de suficiencia profesional es un estudio referente al diseño e implementación de seguridad en las conexiones remotas. Afrontamos este estudio, primero con una descripción de los diferentes conceptos y componentes que conforman una infraestructura de red para soporte de las conexiones remotas. Luego, realizamos un resumen de los diferentes mecanismos que se emplean para proporcionar seguridad en redes y se detallan dos productos de software: el RRAS y el ISA Server 2004 de la familia Microsoft, que se emplean para la implementación de estos mecanismos de seguridad. En la tercera parte del informe describimos y analizamos el caso una red real perteneciente a la empresa Vega Upaca S.A. - Relima, se definen sus componentes físicos y sus componentes lógicos, se detallan los requerimientos planteados por la empresa Relima y sobre la base de estas definiciones y requerimientos planteamos una solución de seguridad para su red. En la parte final del informe especificamos y definimos las configuraciones del arreglo de redes y servidores que participan en la implementación de la seguridad de la red de Vega Upaca S.A., la propuesta contempla una solución a los requerimientos específicos de implementación de una red VPN, la creación de una red perimétrica (DMZ), así como la selección, ubicación y publicación de servidores en la zona DMZ.

INDICE

PRÓLOGO

El estudio tratado en el presente informe de suficiencia profesional tiene como propósito servir como fuente resumida de conceptos, habilidades y herramientas de software a tener en cuenta cuando nos enfrentemos en el campo laboral a un reto de diseñar e implementar un problema real de seguridad de una red especialmente en el campo de las transmisiones remotas. En el estudio, tratamos un conjunto de requerimientos del caso de una red real, realizamos el análisis, transformamos o diseñamos su infraestructura y proponemos una solución alternativa al problema de seguridad y sobre todo al acceso de información para los requerimientos remotos.

El método empleado para realizar este estudio se centra en la primera parte en detallar todos los componentes que debe poseer una infraestructura de red segura para que de esta manera se pueda tener la destreza y conocimientos necesarios para entender todo lo involucrado en el contexto de las conexiones remotas. En el capítulo II describimos algunos mecanismos comunes para implementar seguridad en redes tales como el control de tráfico a través de servidores Firewalls, el control de acceso a Internet mediante NAT y servidores Proxy y el control de acceso a una red mediante servidores VPN y también describimos los certificados digitales como medio de autenticación y realizamos una descripción del protocolo IPSec como medio para realizar VPN.

En el capítulo III presento el caso de una red real de la empresa Vega Upaca S.A.-Relima y se plantea implementar algunos requerimientos como la implementación de una zona DMZ, la publicación de sus servidores e implementación de una VPN para sus usuarios remotos.

En la parte de la implementación correspondiente al capítulo IV, partimos de un esquema impuesta por una herramienta avanzada de seguridad denominada ISA Server 2004 (Internet Security and Acceleration Server 2004) de Microsoft, para satisfacer los requerimientos de la red Vega Upaca, y especifico los diferentes pasos y configuraciones a realizar en la solución propuesta empleando dos servidores ISA en una configuración back-to-back.

Finalmente expresar mi agradecimiento y gratitud para la empresa Vega Upaca-Relima por permitirme acceder a la información de su red especialmente a los señores Marlon Brandes jefe del sección tecnológica de esta empresa, al Ing. Miguel Garro, gerente de administración y finanzas y al Ing. José Fachín jefe de costos de la empresa, sin la cual se habría tenido que simular un caso ficticio de este trabajo

CAPITULO I
CONCEPTOS VARIOS CONEXIONES REMOTAS

1.1 Introducción

En este primer capítulo del informe tratamos cuatro aspectos relacionados con el acceso a una red: los métodos de acceso hacia una red, la infraestructura de acceso remoto, las conexiones dial-up y las conexiones VPN. Describimos las diferentes formas posibles en que los usuarios puede conectarse a una red y los componentes necesarios que conforman una infraestructura de acceso remoto. Indicamos como configurar una conexión VPN (red privada virtual) y una conexión Dial-up, y hacemos una indicación general sobre las conexiones inalámbricas. En el capítulo también indicamos lo necesario para controlar el acceso de los usuarios remotos a una red mediante la autenticación, introducimos el concepto de centralizar la autenticación y la administración de políticas de acceso de red mediante la implementación del IAS (servicio de autenticación por Internet-Internet Autentication Service) y hacemos una referencia al servicio de directorio del directorio activo como medio importante de almacenamiento y búsqueda en los dominios de una red Microsoft.

1.2 Métodos de acceso hacia una RED

Hay varias formas posibles de acceso a los diversos recursos y servicios de una red. Se puede acceder a una red mediante conexiones tipo LANs, conexiones inalámbricas y mediante las conexiones tipo VPN o dial-up comúnmente conocidas como conexiones remotas. La Figura 1.1 nos muestra los diferentes escenarios en que se pueden encontrar los usuarios y cada escenario define un método de acceso a los recursos y a los servicios en una red.

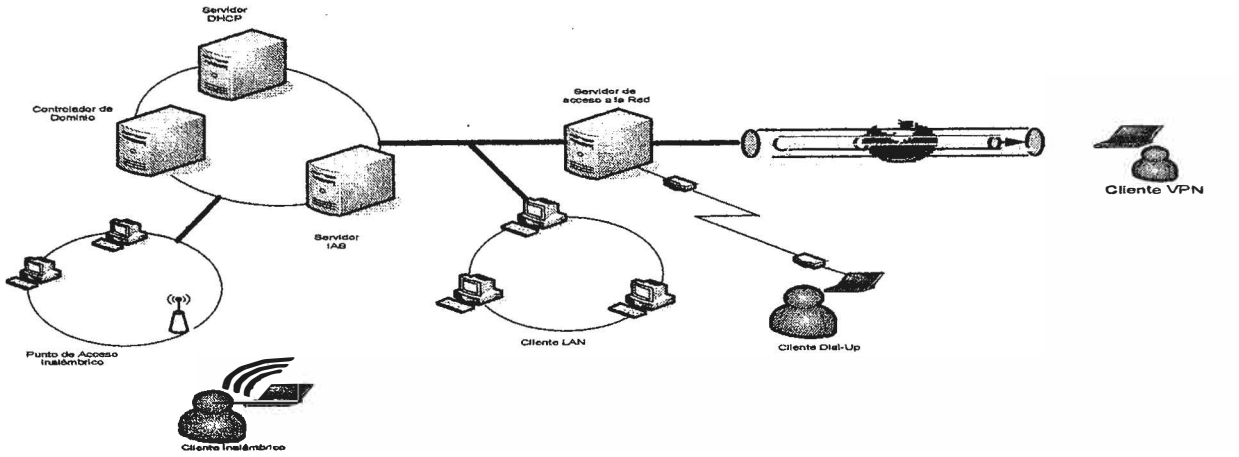

Figura 1.1 Métodos de acceso a una red

1.2.1 Conexiones de red

Para realizar una comunicación entre un equipo y una red debemos establecer una conexión física (conectividad) entre ellos y estas conexiones pueden ser realizadas a través de cables, señales de radio, o de otros métodos; las conexiones son creadas y configuradas en los equipos mediante los protocolos a nivel de enlace de datos.

- **Conexiones locales (Wired LAN)**

Estas conexiones permiten acceder a los recursos de red localmente, son típicamente alámbricas, emplean tecnologías tipo ethernet o token ring a nivel físico y de enlace de datos con velocidades desde 10 mps hasta 1000 mbps y en algunos casos pueden utilizar full duplex.

- **Conexiones inalámbricas (Wireless LAN)**

Podemos acceder a una red utilizando luz infrarroja o señales en las frecuencias de radio y son óptimas para distancias cortas. Las velocidades típicas son 11 mbps a 54 mbps. Los dispositivos que comúnmente se usan en las redes inalámbricas son las computadoras portátiles, asistentes digitales personales (PDAs) y teléfonos celulares.

- **Conexiones tipo Dial-up**

Usan equipos como los MODEM o dispositivos ISDN para conectar dos equipos sobre redes telefónicas públicas (PSTN), estas conexiones pueden ser de cliente a servidor o de Router

a Router. Se pueden tener conexiones no persistentes de acuerdo a necesidades como el caso de una conexión cliente-servidor, o se pueden tener conexiones persistentes como el caso de una conexión router–router, las velocidades pueden ser desde 128 kbps para ISDN o de 56 kbps para un MODEM tradicional.

- **Conexiones tipo VPN**

Se utilizan para enviar datos haciendo túnel sobre una red existente ya sea la propia intranet o una red pública tal como Internet, utilizan protocolos tales como el protocolo túnel punto a punto (PPTP) o el protocolo túnel de capa2 (L2TP). Las opciones de comunicación pueden ser un cliente que se comunica a un servidor o dos Routers que usan el túnel para unir dos redes constituyendo una WAN. Las velocidades de la conexión dependen del medio utilizado por el túnel. Este medio puede ser una LAN, una línea DSL, una ISDN, cable o una línea telefónica de 56 kbps.

1.2.2 Acceso mediante conexiones remotas

Los usuarios que se conectan a una red desde un sitio no local utilizan las conexiones remotas. Los dos métodos básicos para acceso remoto son el de llamada directa o telefónica un equipo de red y las redes privadas virtuales (VPN); existen protocolos especiales para poder establecer estas conexiones a nivel de enlace de datos. Además de estos protocolos de establecimiento de conexión se requieren protocolos de autenticación y de encriptación de usuario o de equipo y se pueden forzar la aplicación de condiciones de conectividad, permisos y profiles a los equipos o usuarios.

Para el acceso mediante llamada telefónica, se necesita configurar un servidor para que además de responder a las llamadas entrantes deba poder autenticar, proporcionar los permisos de acceso y los requisitos de encriptación/cifrado. Los VPN permiten que las conexiones privadas utilicen una red pública como Internet, estas conexiones requieren un conjunto diferente de procedimientos de configuración para la autenticación, cifrado y seguridad.

1.3 Infraestructura de acceso Remoto

Como se ve en la figura 1.2 hay usuarios que conectan a una red usando una topología de red de área local (LAN) y usuarios que se conectan usando otros métodos de acceso. Para soportar usuarios que no usan una topología LAN se les debe proporcionar una

infraestructura de acceso remoto para que puedan conectarse a la red. En esta infraestructura intervienen los siguientes componentes:

- Clientes de acceso de Red
- Servidor de acceso de Red
- Servicio de autenticación (IAS)
- Servicio de Directorio Activo-Controlador de dominio
- Políticas de acceso remoto

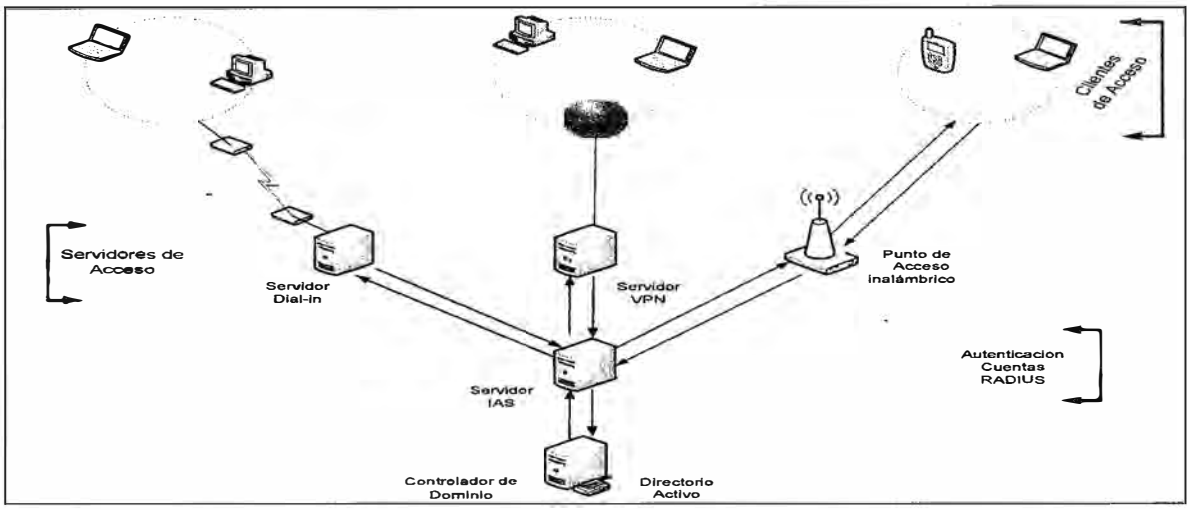

Figura 1.2 Infraestructura de acceso remoto

Podemos describir el rol que cumple cada componente de la siguiente manera:
El cliente de acceso de red usa una conexión dial-up, una red privada virtual o conexión VPN, o una conexión inalámbrica para conectarse a un servidor de acceso (Dial-up/VPN) o a un punto de acceso inalámbrico situados en red interna. El servidor de acceso o el punto de acceso inalámbrico se conecta al servidor que proporciona el servicio de autenticación de Internet denominado servidor IAS usando un servicio de autenticación para usuarios remotos denominado RADIUS. El servidor IAS es un servidor que ejecuta el Windows Server 2003 que proporciona el servicio de autenticación tipo RADIUS; adicionalmente al servicio de autenticación el IAS se comporta como una fuente centralizada de políticas de acceso remoto para controlar el nivel de acceso a la red para los clientes de acceso remoto y aplica las políticas a los clientes. El servidor IAS se conecta a los servicios de directorio para verificar la información de las cuentas de los usuarios remotos.

El proceso por el cual un usuario remoto se conecta a la red interna podemos describirlo de la siguiente manera: supongamos que un usuario XX remoto que esta trabajando en casa y que está conectada a Internet inicia una conexión a la red interna usando una conexión VPN. La computadora de XX, y la Red cliente de acceso se conectan entonces al servidor VPN a través de Internet. El servidor VPN envía la solicitud de conexión de XX hacia el servidor IAS para autenticación. El servidor IAS verifica la cuenta de usuario y la cuenta de computador que está configurado y alojado en el servicio de directorio del directorio activo. Si el servidor IAS autentica a XX, entonces el servidor IAS aplica las condiciones y restricciones contenidas en las políticas de acceso remoto. Las políticas de acceso remoto pueden dictar que redes de cliente de acceso están restringidas o cuales son los requerimientos de encriptación para transmitir hacia o desde la red. Después de que se aplica las condiciones y restricciones de las políticas, el usuario XX tiene acceso a la red como si estuviera conectado localmente a la LAN.

1.3.1 Clientes de acceso de RED

Los clientes acceden a la red a través de conexiones Dial-up, Internet, o conexiones inalámbricas. Los clientes de acceso pueden ser de diversa naturaleza (empleados, contratistas, socios, proveedores etc.).

- **Clientes Dial-up**

Un cliente Dial-up se conecta a la red usando una red de comunicación tal como la red de telefonía publica conmutada (PSTN), para crear una conexión física a un puerto del servidor de acceso remoto ubicado en una red privada. Esta conexión puede ser echa empleando varias tecnologías incluyendo un módem o una red de digital de servicios integrados (ISDN).

- **Clientes VPN**

Un cliente VPN se conecta a la red a través de una red compartida o red pública como Internet, de tal manera que emula enlace punto a punto sobre una red privada.

- **Clientes inalámbricos (Wireless Clients)**

Se conectan a la red utilizando frecuencias de radio y equipos denominados puntos de acceso inalámbrico que se encuentra conectado a la red mediante una tarjeta de red y

cable. Los dispositivos más comunes que se utilizan en las conexiones inalámbricas son las computadoras portátiles, asistentes digitales personales (PADs), teléfonos celulares, etc.

1.3.2 Servidor de acceso de RED

El servidor de acceso para los clientes puede ser: un servidor de acceso VPN, Servidor de acceso Dial-up y puntos de acceso inalámbricos (Wíreless access Point).

El servidor de acceso que actúa como una puerta de acceso **(Gateway)** a la red para los clientes remotos. Este servidor utiliza un servicio de acceso para soportar usuarios remotos y autentica las sesiones de estos usuarios para que puedan trabajar en la red como si estuvieran físicamente conectados a ella.

En la redes Microsoft con el Windows Server 2003 se utiliza la herramienta o servicio RRAS (Rounting and Remote Access Server) instalado en el servidor de acceso para realizar todas las tareas involucradas con el acceso remoto, es decir: autenticación, autorización, VPN, dial-up y también puede ser utilizado como una versión básica de firewall (ver sec. 2.6.1 pag. 47).

1.3.3 Servicio de autenticación

Para las conexiones VPN, Dial-up, y conexiones inalámbricas el servicio de autenticación comprende dos procesos: **la autenticación y la autorización**, ambos de estos procesos se deben completar exitosamente para que un usuario acceda a los recursos de la red.

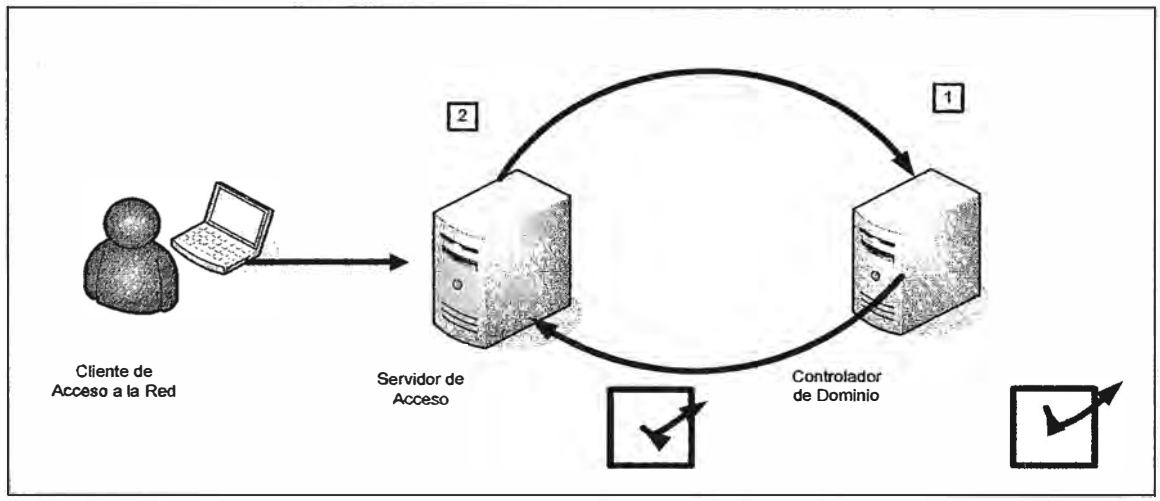

Fig. 1.3 Autenticación y autorización con solo un servidor de acceso

1.3.3.a Autenticación con solo un servidor de acceso remoto

En un escenario simple el servidor de acceso remoto maneja la autenticación entre el cliente remoto y el controlador de dominio. La distinción entre autenticación y autorización es importante para entender cómo los intentos de conexión son aceptados o rechazados.

- **Autenticación**

Es la validación de las credenciales durante un intento de conexión. El proceso de autenticación consiste en el envío de credenciales desde un cliente de acceso de red a un servidor de acceso de red en texto plano (plaintext) o en forma encriptada usando un protocolo de autenticación. La autenticación lo realiza el controlador de dominio.

- **Autorización**

Es la verificación de si el usuario esta permitido acceder al recurso (tal como a un servidor de acceso remoto). Después que el cliente es autenticado, el acceso es permitido o denegado basado en las credenciales de la cuenta y en las políticas de acceso remoto. La autorización puede ocurrir solamente después de un exitoso intento de autenticación. Si la autenticación falla, el acceso al usuario es denegado. La autorización lo realiza el servidor de acceso remoto.

En resumen la autenticación lo realiza el controlador de dominio basado en las credenciales (cuenta de usuario y password) del cliente almacenados el active directory y la autorización lo realiza el controlador de acceso remoto basado en la propiedades dial-in de la cuenta de usuario en el active directory del controlador de dominio y las políticas de acceso remoto almacenados en el servidor de acceso. Entonces para que una conexión sea válida, ésta debe ser autenticada por el controlador de dominio y autorizada por el servidor de acceso remoto.

1.3.3.b Autenticación con Múltiples servidores de acceso remoto

Cuando tenemos múltiples servidores de acceso distribuido en una corporación que están cada uno como servidores RRAS por ejemplo para diferentes tipos de clientes podemos considerar emplear una estructura centralizada de autenticación en un solo servidor al que se le denomina servidor RADIUS, que en el Windows Server 2003 lo ejecuta el complemento IAS (Internet Autentication Service). En este caso se pueden dar 2 situaciones:

Caso de un solo servidor RADIUS

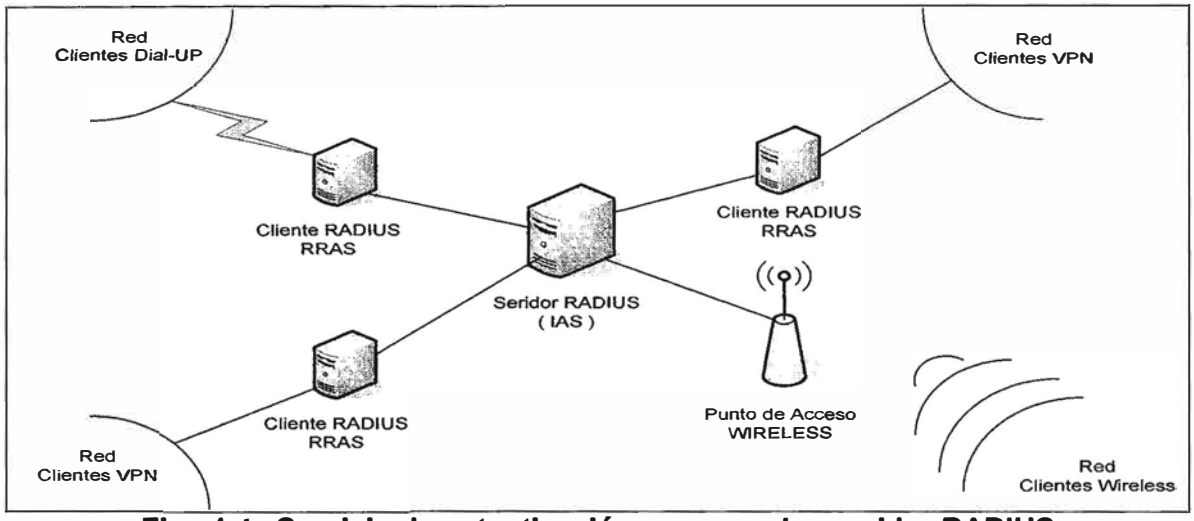

Fig. 1.4. Servicio de autenticación con un solo servidor RADIUS

Esta infraestructura de autenticación requiere de las siguientes configuraciones:

Lado servidor RADIUS (IAS)

- Instalamos el IAS en este servidor
- Registramos este servidor en el Active Directory
- Especificamos los nuevos clientes RADIUS que serán los servidores RRAS
- Indicamos los nombres o las direcciones IP de los RRAS
- Especificamos los passwords preshared de la máquinas RRAS

Configuramos los RRAS (Radius Client)

- Configuramos los RRAS como cliente RADIUS seleccionando el protocolo RADIUS como protocolo de autenticación
- Indicamos el nombre del servidor IAS o su IP
- Especificamos la misma clave preshared del paso anterior para cada servidor RRAS.

Creamos una política de acceso en el IAS

- Indicamos el nombre de la política
- Seleccionamos los usuarios o grupos VPN
- Escogemos el método de autenticación de los usuarios (MS-CHAP, MS-CHAP V2...)

Caso de múltiples servidores RADIUS

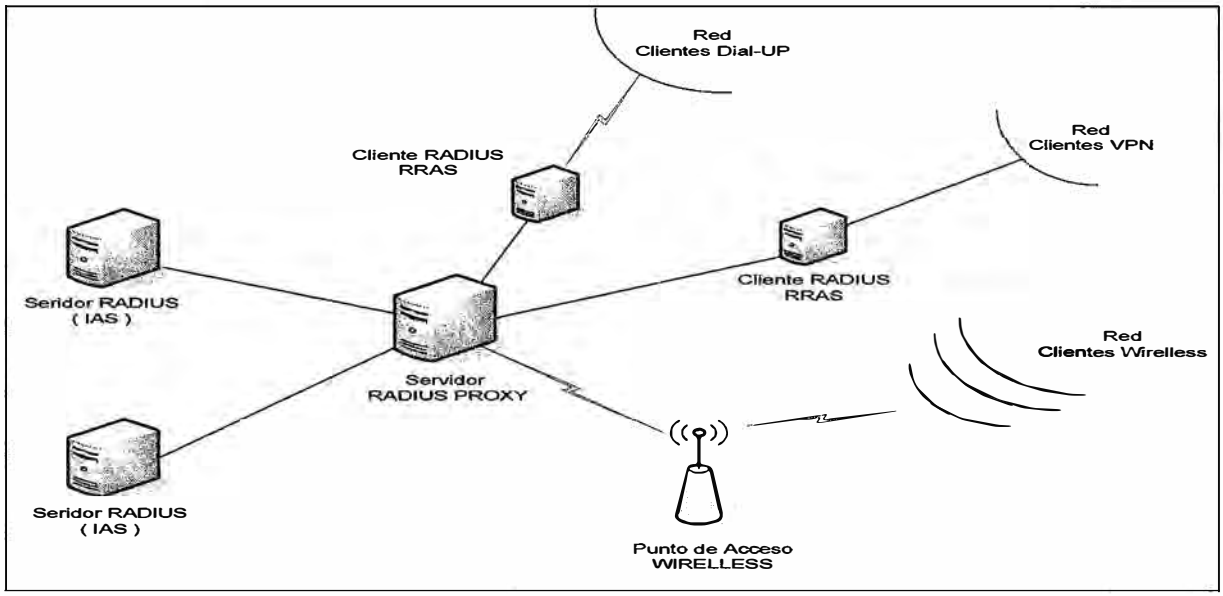

Fig. 1.5. Autenticación con múltiples servidores RADIUS

En este caso se emplea un servidor Radius Proxy para distribuir la autenticación entre los diferentes servidores RADIUS (IAS).

1.3.4 El servicio de directorio de directorio activo

Los controladores de dominio contienen una base de datos (Active Directory) con las cuentas, passwords y las propiedades de Dial-up y de VPN que son requeridas para autenticar las credenciales de los usuarios y para evaluar tanto la autorización y las restricciones de conexión. Después que los usuarios se han conectado a la red podemos controlar el acceso a los recursos mediante varios controles administrativos tanto en el cliente como en el servidor de acceso. Los controles administrativos incluyen compartir archivos e impresoras (file and printer sharing), políticas de grupo locales (local Group Policy), y políticas de grupo a través del servicio de directorio activo. Los conceptos de políticas de grupo locales y políticas de grupo también denominados políticas de dominio se tratan en cursos de administración de servidores, aquí sólo menciono que son herramientas o medios de distribuir en forma automática las configuraciones de máquina o de usuario a través de la red.

1.3.5. Políticas de acceso remoto

Para realizar una conexión de acceso remoto siempre debe existir una política de acceso remoto. Una política de acceso remoto es un conjunto ordenado de reglas que determinan como las conexiones son aceptadas o rechazadas. Cada regla consiste de uno o más condiciones, una configuración de permiso de acceso remoto y configuraciones de un profile de usuario. Las políticas de acceso remoto son configuradas para especificar los diferentes tipos de restricciones de conexión. Una política de acceso remoto consta de los siguientes componentes:

- **Condiciones.**

Son una lista de parámetros (hora del día, grupos de usuarios, direcciones IP) que son comparados con los parámetros de los clientes que se están conectando al servidor. Para que una política se aplique a un intento de conexión todas las condiciones de la política deben cumplirse. Si todas las condiciones de la política no se cumplen el servidor evaluará las condiciones de la próxima política de acceso remoto.

- **Permisos de acceso remoto**.

Las conexiones de acceso remoto son permitidas basados en una combinación de las propiedades dial-in de una cuenta de usuario y de las políticas de acceso remoto.

El del permiso se configura en las propiedades Dial-in de la cuenta en el controlador de dominio, los permisos en la propiedades Dial-in de la cuenta son permitir, denegar o usar lo permisos de una política de acceso remoto.

Los permisos en la política de acceso remoto son permitir o denegar, pero pueden ser sobrescritos u omitidos por el permiso configurado en las propiedades Dial-in de la cuenta en el Active Directory.

Se puede configurar las propiedades Dial-in de la cuenta para que utilice el permiso especificado en la política de acceso remoto. Esta característica es la configuración por default en el Windows Server 2003.

Profile.

Cada política incluye una configuración de Profile, que especifica por ejemplo la autenticación y la encriptación que se aplica a la conexión. Puede causar que la conexión sea denegada. Por ejemplo si el Profile para una conexión especifica que el usuario no

puede permanecer conectado más de 30 minutos cada vez, el usuario será desconectado del servidor de acceso remoto después de los 30 minutos.

Proceso de evaluación de una política de acceso remoto

1. El servidor de acceso remoto chequea la primera política de acceso remoto para determinar si el intento de conexión cumple todas las condiciones de la política., si se cumplen todas las condiciones, la política es aplicada a la conexión.
   - Si las condiciones de la primera política no se cumplen, el servidor de acceso remoto evalúa la próxima política para ver si se cumplen todas las condiciones de esta política. El proceso continuará hasta que el intento de conexión cumpla todas las condiciones de una política de acceso remoto.
   - Si no se encuentra ninguna política que se cumpla, la conexión es denegada.
   - Si no existe políticas de acceso remoto, todos los intentos de conexión serán denegadas.
2. El servidor de acceso remoto chequea los permisos Dial-in de la cuenta
   - Si el permiso en la cuenta de usuario es denegar acceso, se deniega el acceso al usuario.
   - Si el permiso en la cuenta de usuario es permitir acceso, se asigna el acceso al usuario y se aplica el profile de la política.
   - Si el permiso es Controlar el Acceso a Través de una Política de Acceso Remoto, el permiso configurado en la política determina el acceso del usuario.
3. El servidor de acceso remoto aplica las configuraciones del profile de la política de acceso remoto.

1.4 Acceso mediante una conexión Dial-up

En una red Dial-up (Figura 1.6) un cliente de acceso remoto realiza una conexión no permanente a un puerto (PORT) físico de un servidor de acceso remoto usando los servicios de un proveedor de telecomunicaciones y un tipo de conexión: tal como una línea de teléfono análoga y un módem, la red digital de servicios integrados (ISDN) o una red X.25.

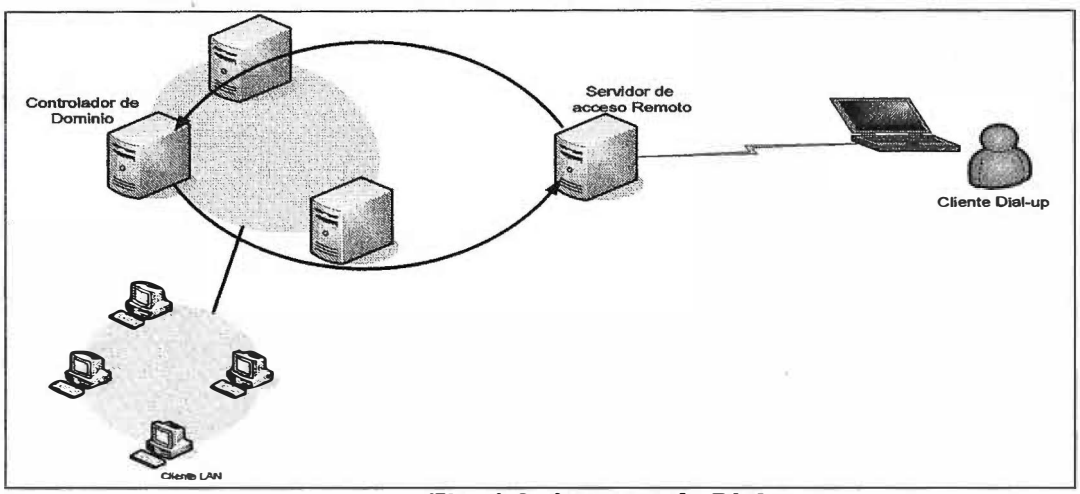

Fig. 1.6 Acceso vía Dial-up

1.4.1 Proceso de acceso Dial-up:

1. Un cliente realiza una llamada Dial-up al servidor de acceso remoto
2. El equipo Dial-up instalado en el servidor de acceso remoto contesta las solicitudes de conexión que están llegando desde los cliente Dial-up
3. El servidor de acceso remoto autentica contactando con el controlador de dominio y autoriza la llamada
4. El servidor de acceso remoto transfiere la data desde el cliente Dial-up hacia la red interna. El servidor de acceso remoto actúa como gateway y proporciona acceso a toda la red a la cual está conectada.

1.4.2 Ventajas

- Proporciona conectividad Dial Up directa a la red para usuarios móviles
- Potencia la seguridad del camino de la DATA sobre una conexión basado en conmutación de circuitos. El camino o la ruta es segura solamente si se usa encriptación.
- Las líneas Dial-UP son soluciones inherentemente más privadas que las soluciones que usan redes públicas tales como Internet.

1.4.3 Desventajas

- Las conexiones están sujetas al límite de la máxima velocidad suportada por el medio de conexión, lo cual es usualmente de 56 Kbps.
- Gran inversión en módems y otros hardware de comunicaciones, hardware de servidores e instalación de líneas.

1.4.4 Componentes de una conexión Dial-up

Una conexión Dial-up comprende varios componentes: servidores de acceso remoto, clientes dial-up, protocolos de acceso remoto, y métodos de autenticación.

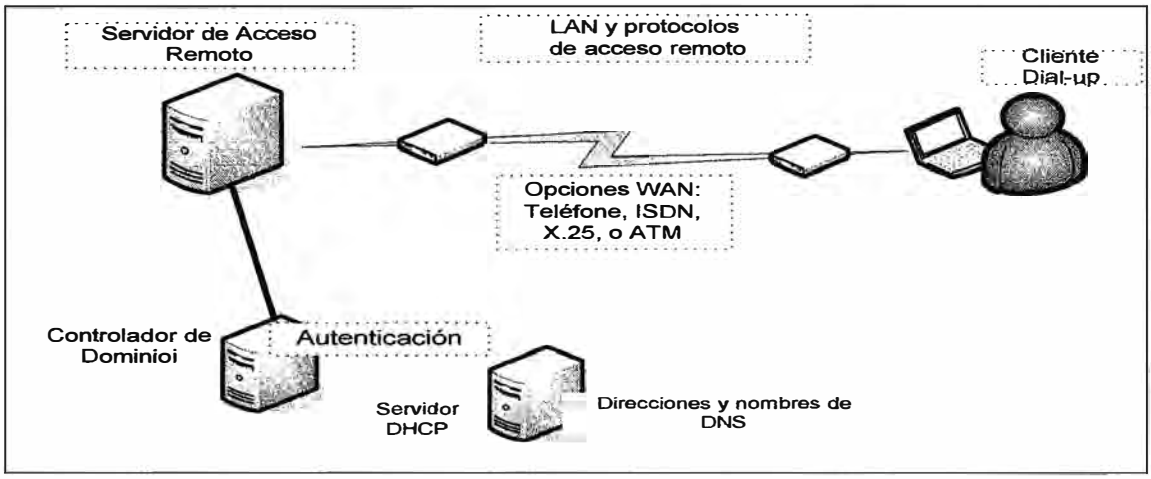

Figura 1.7 Acceso via dial-up

- **Servidor de acceso remoto.** Una computadora que acepta conexiones dial-up desde los clientes dial-up y puede ser un servidor ejecutando el RRAS.
- **Cliente Dial-up.** Un cliente que inicia una conexión dial-up al servidor de acceso remoto.
- **Protocolos de acceso remoto.** Los programas de aplicaciones utilizan protocolos LAN para transportar la información y los protocolos de acceso remoto son utilizados para negociar las conexiones y proporcionar el empaquetamiento (framing) para los protocolos LAN que se envían sobre los enlaces de red WAN.
- **Opciones Wan.** Las conexiones dial-up se pueden realizar usando líneas telefónicas mediante un módem o un banco de módems. Las conexiones más veloces emplean redes ISDN, X.25 o ATM. También se pueden usar conexiones directas a través de módem de cable Nulo RS-232C o de una conexión de puerto paralelo o de una conexión inalámbrica infrarroja.
- **Autenticación.** La autenticación de las conexiones es a nivel de computadoras y de usuarios. Las computadoras clientes y servidores pueden usar certificados como medios de autenticación y los usuarios pueden usar smart cards.

- **Direcciones y ubicación de servidores de nombres.** El servidor de acceso asigna direcciones IP usando por default un DHCP. También asigna a los clientes remotos las direcciones de los servidores DNS y WINS.

1.4.5 Métodos de autenticación en una conexión Dial-up

Existen los siguientes métodos de autenticación para las conexiones Dial-up que se detallan el anexo C del informe.

CHAP	MS CHAP v2
PAP	PEAP
SPAP	EAP-TLS
MSCHAP	EAP-MD5 Challenge

El método de autenticación más fuerte para las computadoras es el EAP-TLS que emplea certificados para una mutua autenticación de las computadoras cliente y servidor y los usuarios pueden usar certificados o smart cards con EAP-TLS para autenticarse.

1.5 Red Privada Virtual (VPN)

Una red privada virtual (VPN) es una extensión de una red interna localizado detrás de un computador o dispositivo configurado como un servidor VPN. La VPN habilita la comunicación entre un servidor de acceso remoto y las computadoras de la red interna o entre dos sitios remotos, sin importar que las computadoras estén en diferentes localizaciones y separados por una red pública tal como Internet.

La red privada virtual-VPN es una red lógica que cruza físicamente Internet. Con la VPN, los paquetes privados primero se cifran (encriptan) y luego se encapsulan dentro de un paquete público dirigido a un servidor VPN remoto. Esta información de enrutamiento permite a la carga cifrada de datos privados "abrir un túnel" en la red pública para alcanzar su destino. Al recibir los datos encapsulados mediante un túnel VPN, el servidor VPN destino elimina la cabecera pública y descifra el paquete privado. La figura 1.8 ilustra este concepto.

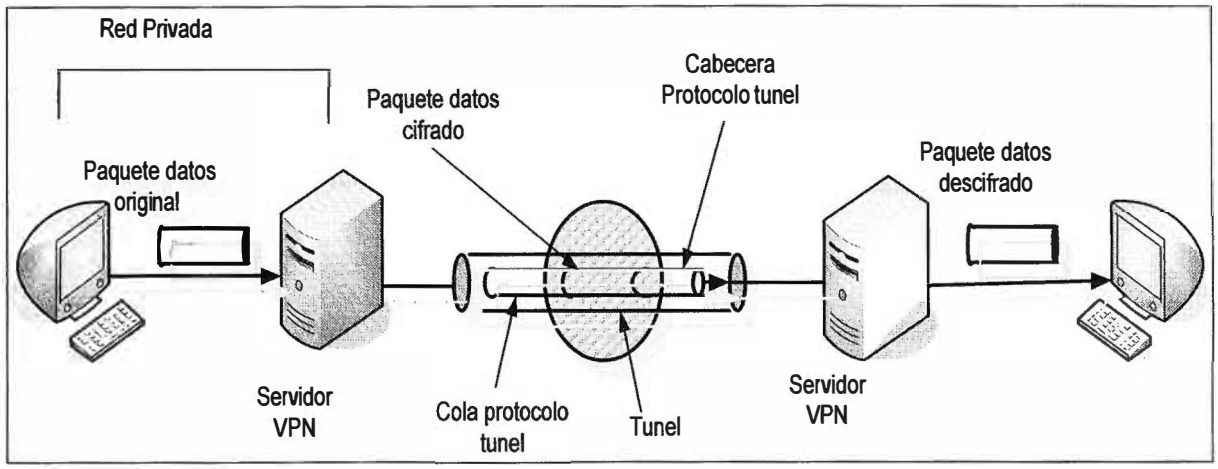

Fig. 1.8 Acceso vía VPN

Una característica importante de la VPN es que la red física pública por la que se envían los datos privados se vuelve transparente a los extremos de la comunicación, como se ilustra en el figura 1.9. Dos equipos, Equipo 1 y Equipo 2, están conectados solo a través de Internet. La transparencia de este enlace físico es revelado en que hay varios saltos que separan los dos equipos, sin embargo, cada uno se muestra al otro como si solo hubiese un salto a través de la conexión VPN. La comunicación ocurre entre las dos direcciones IP privadas, cada uno dentro de la subred 192.168.10.0, como si ambos equipos estuviesen situados en un segmento de red aislado.

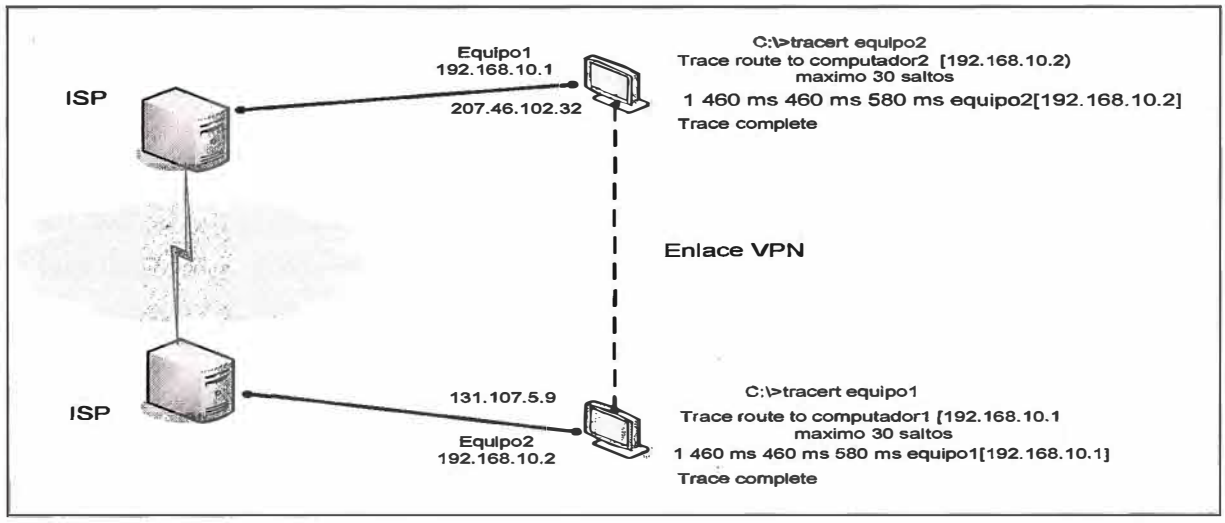

Fig. 1.9 Conexión punto a punto con VPN

Como se ve en la Figura 1.9, con el enlace VPN, se crea una conexión "**punto a punto**" seguro a través de una red privada o pública.
El cliente VPN usa protocolos especiales basados en TCP/IP llamados protocolos túnel para conectarse a un puerto de conexión virtual de un servidor VPN.

1.5.1 Protocolos Túnel

Los dos protocolos más comunes usados por los servidores VPN para realizar túnel son:

- El Protocolo túnel punto a punto (PPTP: Point to Point Tunnelling Protocolo)
- Y el Protocolo túnel capa 2 (L2TP: Layer 2 Tunnelling Protocol)

Ambos protocolos crean una directa conexión "virtual" (por que la conexión fisíca no existe) entre un cliente VPN y el servidor de acceso remoto o entre dos puertas de enlace VPN (VPN gateways). Esta conexión de red virtual permite a las computadoras conectadas a través de la red virtual enviar y recibir mensajes TCP/IP de la misma manera como si estuvieran conectados directamente es decir sobre la misma red LAN. La conexión virtual es transparente de las aplicaciones que se están ejecutando en el computador cliente.
Los protocolos PPTP y L2TP usan protocolos de encriptación para asegurar que la conexión sea privada o segura, encriptando toda la data que está siendo enviada a través de la red pública. El protocolo VPN PPTP usa el protocolo de encriptación MPPE de Microsoft para proteger la data a que se mueve a través de la conexión virtual PPTP y el protocolo VPN L2TP utiliza el protocolo IPSec para encriptar la data que se está moviendo a través de la red virtual L2TP.

1.5.2 Ventajas de una conexión VPN

- En vez de estar limitado a la velocidades de los módems, un usuario puede conectarse a una línea de Internet de alta velocidad usando una banda ancha y establecer una VPN sobre esta conexión
- **Costos reducidos**: al usar Internet como medio de conexión se ahorra largas distancias de líneas de teléfono y se requiere menos hardware que una solución dial-up.
- **Suficiente Seguridad:** la autenticación evita la conexión de usuarios no autorizados. Un robusto/ fuerte método de encriptación hace extremadamente difícil para un hacker poder interpretar la data enviada a través de la conexión VPN.

- **Flexibilidad:** Cuando usamos Internet como medio de transporte, el soporte para las re-configuraciones de los clientes remotos es más simple que mover líneas telefónicas dedicadas.
- **Transparencia para las aplicaciones:** una de las ventajas de una conexión VPN en relación a una conexión tipo cliente servidor tal como un aplicación Web, es que los usuarios VPN pueden usar todos los protocolos y servicios dentro la red. Los usuarios remotos no necesitan software especial para conectarse a los servicios de la red.

1.5.3 Componentes de una conexión VPN

La Figura 1.10 muestra los distintos componentes para realizar una conexión VPN tales como Clientes VPN, protocolos túnel y métodos de autenticación a utilizar.

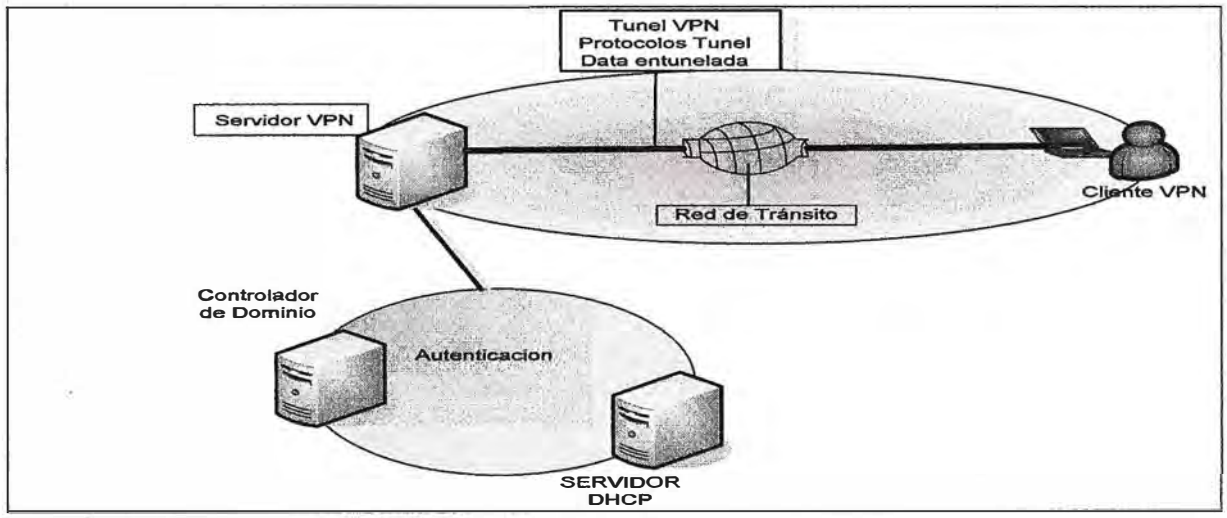

Figura 1.10 Componentes de una conexión VPN

- **Servidor VPN:** es un computador que acepta conexiones VPN desde clientes VPNs.
- **Ciente VPN:** un computador que realiza conexión VPN a un servidor VPN
- **Red de tránsito:** una red compartida o red publica que encapsula la data que cruza la red de tránsito. La red mas comui utiilzada para implementar VPN es la red pública de Internet.
- **Conexión VPN o Túnel**: es la poción de conexión en la cual se encripta y encapsula la data.
- **Protocolos Túnel:** protocolos que se usan para administrar el túnel y encapsular la data.
- **Data entunelada :** la data que se envía a través de un enlace punto a punto.

- **autenticación (controlador de dominio DC)**: los clientes y servidores deben autenticarse en una conexión VPN. También se autentica la data enviada para asegurar que esta no ha sido interceptado y sufrido cambios. El servidor VPN utiliza el directorio activo como una base de datos.
- **Servidor de Direcciones y Servidor de nombres (DNS/WINS):** se puede tener un servidor que preste los servicios de asignación de direcciones IP usando el protocol DHCP o mediante un pool de direcciones estáticas, puede también realizar el servicio de resolución de nombres mediante el servicio DNS o WINS.

1.5.4 Como trabaja una conexión vpn

En la figura 1.11 podemos mostrar los pasos del proceso de realizar una conexión VPN

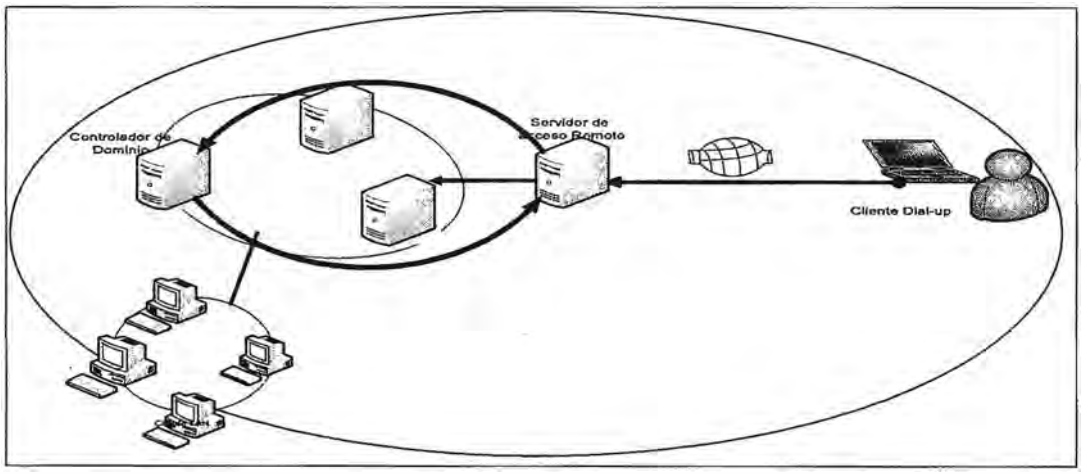

Fig. 1.11 Proceso de una conexión VPN

1. Un cliente VPN realiza una conexión a un servidor VPN que esta conectado a Internet. El servidor VPN actúa como un gateway y es configurado comunmente para proporcionar acceso a la red entera a la cual el servidor está atachada.
2. El servidor VPN responde a esta llamada virtual.
3. El servidor VPN autentica al cliente a través o contactando a un controlador de dominio y verifica la autorización de los clientes.
4. El servidor VPN transfiere la data entre el cliente VPN y la red corporativa.

1.5.5 Escenarios VPN

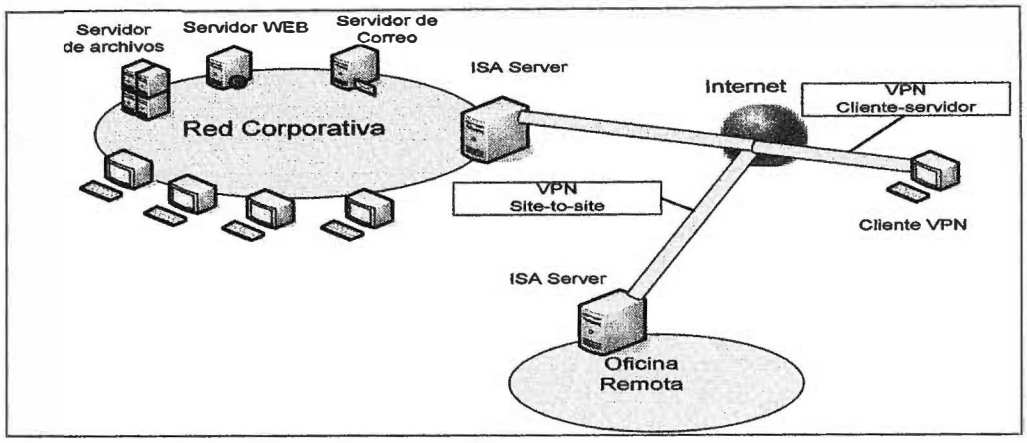

Fig. 1.12 Escenarios VPN

1.5.6 Aplicaciones comunes de VPN

Existen escenarios comunes para aplicar conexiones tipo VPNs. Por ejemplo podemos implementar y utilizar VPN para:

- **Realizar una comunicación segura entre un cliente remoto y la red de una empresa a través de Internet.**
  En este escenario el cliente remoto realiza la conexión VPN a un servidor VPN de la red de la empresa, establecida la conexión el cliente puede acceder a los recursos de la red como si estuviera conectado directamente a la red.

- **Realizar una comunicaciones seguras entre oficinas sucursales**
  En esta implementación, se establece una conexión entre un servidor VPN de una oficina con otro servidor VPN de la otra oficina empleando Internet. Una vez que se establece la conexión ambas oficinas pueden conectarse una con otra, los datos enviados a través de las LAN solo se encriptan cuando pasen por el túnel VPN. En este caso no es necesario configurar autenticación en lado del cliente.

1.6 Redes inalámbricas

Las redes inalámbricas se han convertido en un medio adecuado de implementar redes. Antiguamente eran lentas y poco fiables. La IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) ha publicado un nuevo estándar denominado 802.11b que ha elevado la

velocidad de transmisión de las LAN inalámbricas hasta 11Mbps que es mas rápido que las redes Ethernet cableadas de forma estándar y también se ha conseguido mejorar su fiabilidad. Pueden funcionar utilizando dos topologías distintas: la topología ad hoc y la topología de infraestructura que se muestran en las figuras 1.13 y 1.14 respectivamente.

Topología ad hoc

Una red inalámbrica ad hoc son dos o más computadoras que utilizan tarjetas de red inalámbricas que se pueden comunicar entre si.

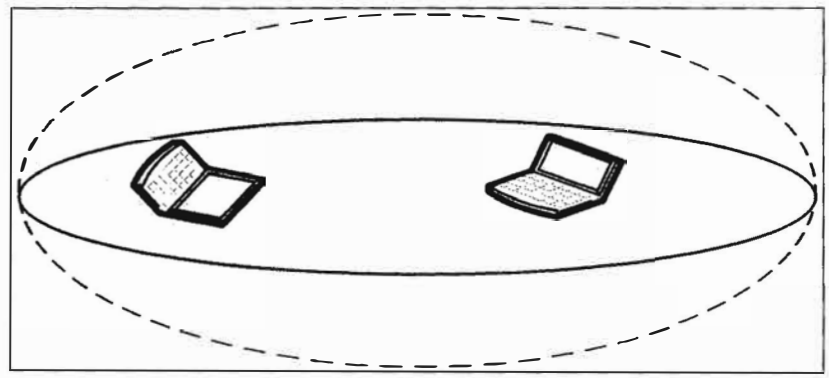

Figura 1.13 red inalámbrica topología ad hoc

Topología de infraestructura

Esta topología permite a los equipos inalámbricos interactuar con una red cableada. Se utiliza un transceptor inalámbrico denominado punto de acceso (access point) que se conecta a la red cableada.

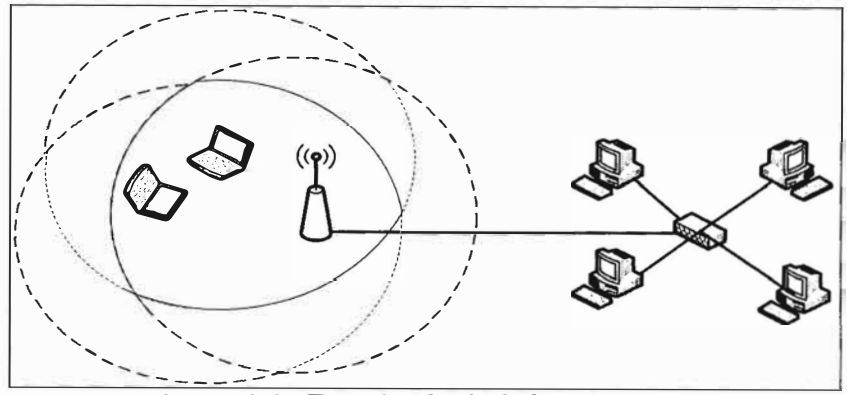

Figura 1.14 Topología de infraestructura

CAPITULO II
CONCEPTOS DE SEGURIDAD EN TRANSMISIONES REMOTAS

2.1 Introducción

En este capítulo del informe describimos los mecanismos de seguridad que se pueden implementan en una transmisión remota. El problema de implementar seguridad en redes es amplio, para atacar la seguridad en las transmisiones remotas hay que tener en cuenta algunos conceptos relacionados con el control del tráfico que se permite entrar o salir hacia o desde una red, la interacción con Internet, y la protección de la data que se trasmite. En un escenario real de implementar seguridad de una red, además de enfocar estas tareas es necesario tener otras consideraciones relacionadas con la seguridad de la data que se quiere proteger dentro la red, los mecanismos de protección de esta data no está en el alcance de nuestro informe, por lo que centramos nuestro estudio en la seguridad de la data que se mueve desde y hacia la red y en la protección de la red contra ataques desde fuera de la red.

2.2 Mecanismos de Seguridad en transmisión remota

La seguridad en el contexto que tratamos podemos dividirlo en tres partes: seguridad de acceso a Internet, seguridad concerniente al control del tráfico desde o hacia una red y la seguridad concerniente a la data que se transmite.

2.3 Mecanismos de seguridad de acceso a Internet

Cuando se interactúa con Internet, existen algunos mecanismos que nos permiten el acceso seguro a cualquier recurso ubicado en Internet y que podemos escoger según nuestros requerimientos de diseño. Los mecanismos que se pueden implementar son: la seguridad mediante traslación de direcciones IP (NAT), seguridad con servidores Proxy.

2.3.1 Seguridad mediante traslación de direcciones NAT

Es bien conocido que para que un equipo interno de una red pueda ser visto o accedido desde Internet el equipo interno debe tener asignado una dirección pública registrada y

asignada por el IANA (organismo que distribuye las direcciones públicas). En cambio los usuarios de la red que deseen acceder a los servicios de Internet no necesitan utilizar direcciones registradas; ya que se existen métodos para acceder a Internet sin tener una dirección pública asignada. Esto es así por que no conviene que los equipos internos de una red tengan direcciones públicas asignadas por dos motivos:

- Reduce el espacio de direcciones IP. Si cada uno de lo equipos que tiene asignada una dirección IP tuviera una dirección IP registrada, el grupo de direcciones disponibles en el IANA habría acabado por desaparecer. Incluso ahora, está en marcha un programa para aumentar el espacio de direcciones IP disponibles desde 32 bits (denominado Protocolo Internet Versión 4 o IPv4) a 128 bits, denominado IPv6, y eliminar así la posibilidad de agotar completamente todo el espacio de direcciones IP en el futuro.
- El empleo de direcciones IP registradas en una red privada presenta un serio riesgo de seguridad. Los equipos que cuenten con una dirección IP pública registrada no solo pueden acceder a Internet, sino que los demás equipos conectados a Internet podrán acceder también a los primeros.

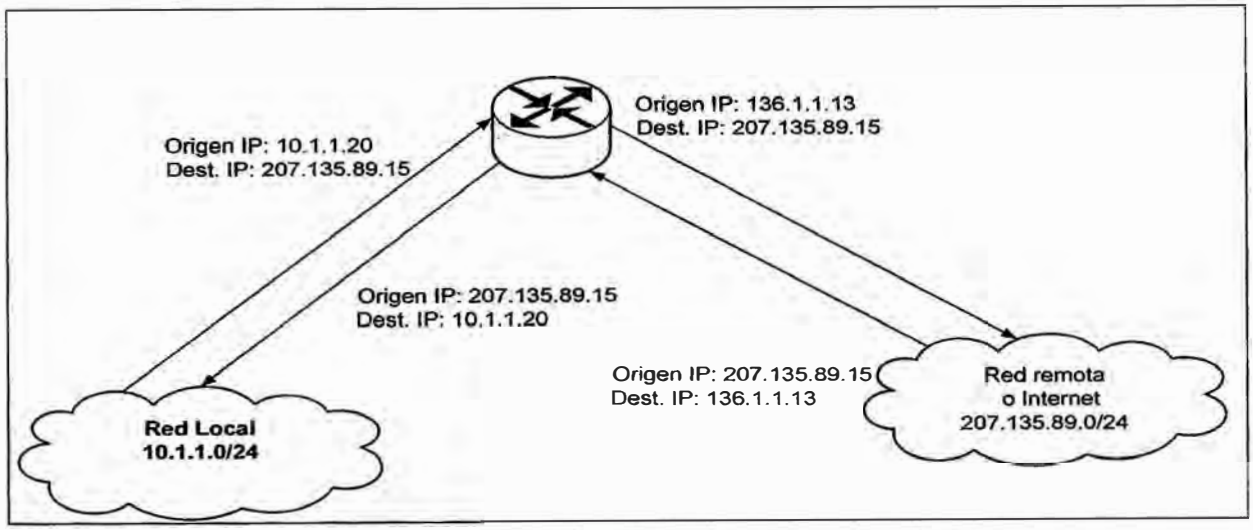

Fig. 2.1 Traslación de direcciones de red

La mayor parte de las redes TCP/IP utilizan direcciones IP no registradas denominadas direcciones IP privadas, para los servidores y estaciones de trabajo que solo tengan que ser accedidos por los usuarios internos. Estas direcciones no están registradas en la IANA y, como resultado, son invisibles para Internet y por lo tanto los delincuentes de Internet no

podrán especificarlas para efectuar cualquier tipo de ataque como la distribución de virus por ejemplo. La IANA ha definido tres rangos de direcciones IP para el empleo en redes privadas, estas direcciones no se encuentran asociados con ninguna red en particular, por lo que se pueden utilizarlas para las equipos dentro de una red, estos tres rangos son los siguientes:

- 10.0.0.0 a 10.25.255.255
- 172.16.0.0 a 172.31.255.255
- 192.168.0.0 a 192.168.255.255

Entonces para que los clientes con direcciones IP no registrados puedan acceder a los servicios de Internet, se implementa mecanismos a acceso tales como NAT y los servidores Proxy.

La traducción de direcciones de red (NAT) es un servicio integrado en un enrutador que modifica la información del encabezado de los datagramas IP modificando la dirección IP del remitente antes de enviarlos a sus destinos. Cuando un equipo interno envía un mensaje de petición dentro de un datagrama a un enrutador NAT, este sustituye la dirección no registrada por la suya propia, que sí está registrada y luego enviará el datagrama a su destino ya sea directamente o a través de varios enrutadores.

Cuando el servicio de Internet recibe la petición, la procesará y generará su datagrama de respuesta. , pero dirigirá el datagrama respuesta al enrutador NAT, Cuando el enrutador NAT reciba la respuesta desde el servidor de Internet, volverá a modificar el datagrama, incluyendo de nuevo la dirección no registrada del cliente en el datagrama. Finalmente, envía el paquete al equipo interno de la red privada.

Todo lo que se ejecuta el NAT resultan invisibles para el cliente interno y el servidor de Internet. El cliente genera una petición y la envía al servidor, y termina recibiendo una respuesta de dicho servidor. El servidor recibe una petición desde el enrutador NAT y transmitirá su respuesta al mismo enrutador. Tanto el cliente como el servidor habrán funcionando normalmente, sin ser conscientes de la intervención enrutador NAT. Lo más importante aquí es que el equipo cliente permanece invisible para Internet y que se encuentra protegido de cualquier acceso no autorizado.

En resumen el NAT tiene tres principales propósitos:

- Permite compartir una simple conexión a Internet
- Incrementa la seguridad ocultando las direcciones IP internas
- Permite a una empresa solicitar pocas direcciones IP públicas

Tipos de NAT

- **NAT estático:** Traduce un número de direcciones IP no registradas en un número igual de direcciones registradas de tal forma que cada cliente siempre utiliza la misma dirección registrada. Es decir utiliza el mismo número de direcciones registradas como no registradas lo que significa que no minimiza desgaste del espacio de direcciones IP registradas. Los NAT estáticos no son tan seguros ya que un intruso de Internet puede utilizar una dirección IP registrada para llegar hasta un determinado equipo de a red por que cada equipo se encuentra permanentemente asociado con una dirección registrada.

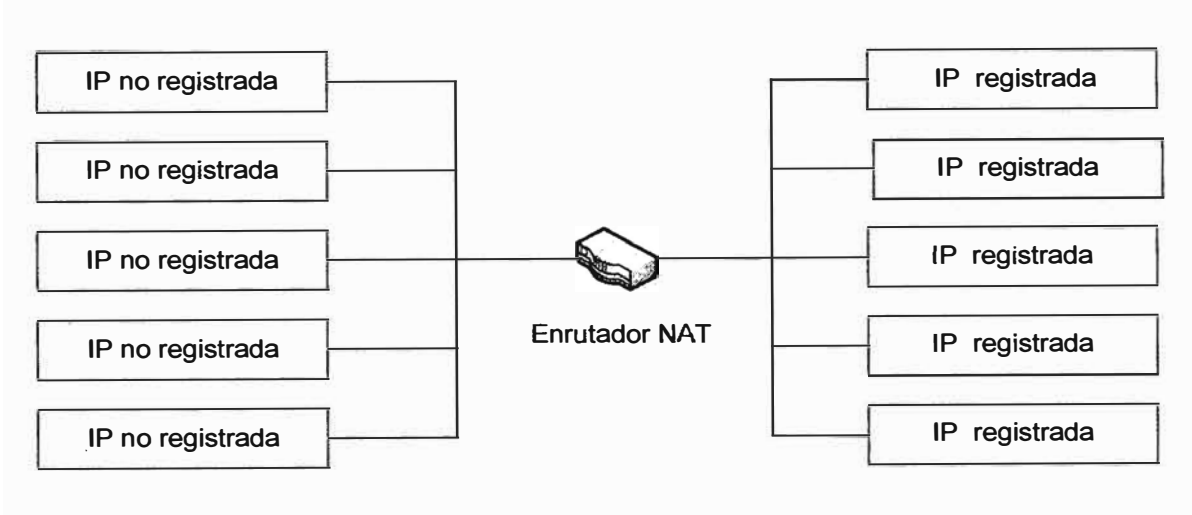

Fig. 2.2 NAT estático

- **NAT dinámico** Los NAT dinámicos resultan adecuados en aquellas circunstancias en las que se disponga de menos direcciones IP registradas que de equipos no registrados. Traducen cada equipo no registrado en una de las direcciones registradas. Se tiene más seguridad que en los NAT estáticos, por que la dirección registrada asignada a cada cliente cambiará con frecuencia. El inconveniente es que aquí solo se puede atender de forma simultánea a un número de usuarios que equivalga a las direcciones IP que se tiene

registradas. Si todas las direcciones registradas se están utilizando en un determinado momento cualquier cliente que intente acceder a Internet recibirá un mensaje de error.

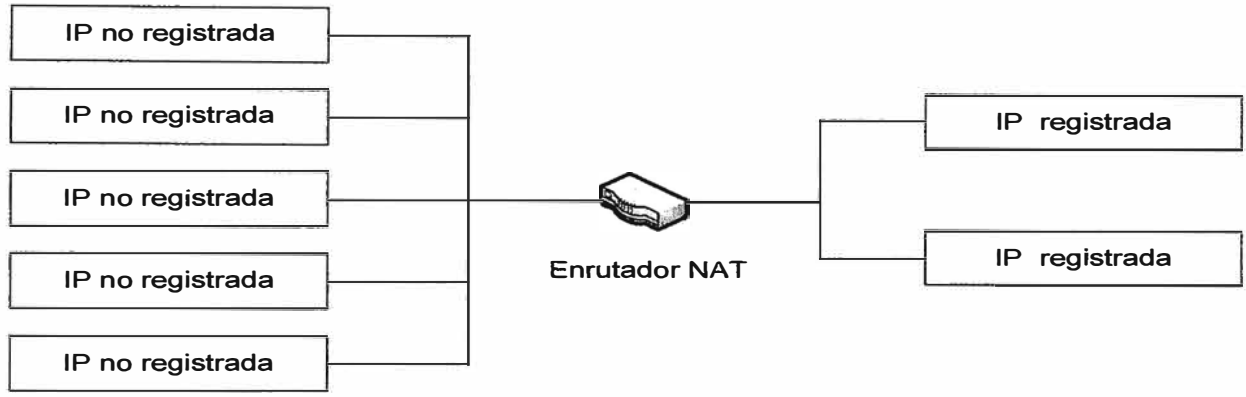

Fig. 2.3. NAT dinámico

- **NAT enmascaramiento:** el enmascaramiento traduce todas las direcciones IP no registradas que hay en la red utilizando una única dirección IP registrada. Para permitir que varios clientes puedan acceder a Internet de forma simultánea, el enrutador NAT utiliza números de puertos para distinguir los paquetes generados (y destinados a) por los distintos equipos. El enmascaramiento proporciona la mejor seguridad de todos los NAT, por que la asociación entre el cliente no registrado y la combinación de dirección IP registrada/número de puerto en el enrutador NAT dura únicamente lo que dura la conexión.

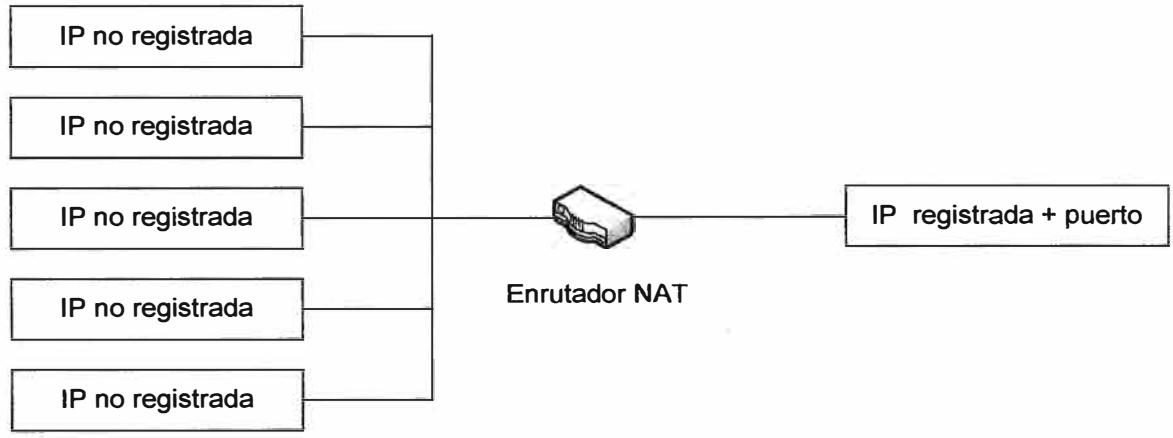

Fig. 2.4 NAT enmascarado

2.3.2 Seguridad usando un servidor Proxy

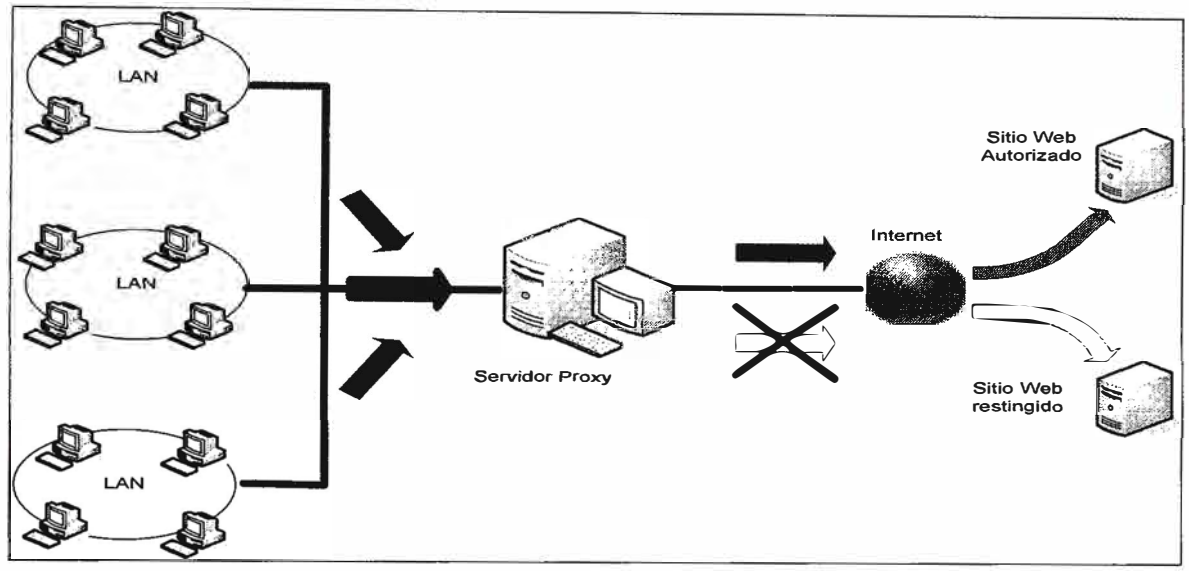

Fig. 2.5 Servidor Proxy

Un servidor Proxy es similar a un enrutador NAT en el sentido de que actúa como un intermedio entre los equipos cliente de una red privada y los servidores de Internet. A diferencia de NAT, un servidor Proxy es un producto de software independiente que se ejecuta en el nivel de aplicación y no está incorporado en un enrutador. Los clientes no registrados envían sus peticiones de acceso a Internet al servidor Proxy, que genera sus propias peticiones y las envía al servidor de Internet. Cuando el servidor Proxy recibe una respuesta, reenvía la información al cliente perteneciente a la red no registrada.

A diferencia de los NAT, los servidores Proxy no procesan todo el tráfico TCP/IP. Los servidores Proxy solo funcionan con determinadas aplicaciones clientes, y debemos configurar los clientes para que envíen sus mensajes al servidor Proxy en lugar de que los envíen al destino real. Esto significa que no hay una directa conexión entre el cliente interno y el Servidor de Internet, es decir que la información interna del cliente no es enviada a través de Internet, cumpliendo de esta manera un mecanismo de seguridad para los clientes internos de la red.

Los servidores Proxy permiten una mejor administración y control sobre el acceso de los usuarios a Internet. Mediante esta función se puede restringir que usuarios y que tipo de información pueden acceder y que aplicaciones pueden usar para acceder a esa información.

Por qué se usa Proxy Server

Mejorar la seguridad de las conexiones a Internet

La razón más importante para usar Proxy Server es hacer más segura las conexiones a Internet.

- Autenticación de los Usuarios: el Proxy Server puede negar o permitir el acceso a los recursos de Internet mediante la autenticación de los usuarios bien usando nombres y passwords o credenciales almacenados en el caché de la computadora cliente.
- Filtrado de solicitudes/peticiones: se puede usar múltiples criterios de filtrado, basado en direcciones IP, el protocolo o aplicación que se usa para acceder a Internet, la hora del día, la página Web o el URL que el usuario está usando.
- Inspección de contenido: el servidor Proxy puede inspeccionar todo el tráfico que esta fluyendo hacia y desde Internet y determinar si algún tipo de tráfico es denegado. Esto puede ser inspeccionar palabras inapropiadas, extensiones de archivos, virus.
- Registro de acceso de los usuarios: El servidor Proxy puede registrar todo lo que hace un usuario. Por ejemplo para una solicitud HTTP se puede registrar cada URL visitada por el usuario, se puede configurar para tener un detallado reporte de las actividades del usuario que pueden ser usados para mejorar el cumplimiento de las políticas internas de la organización.
- Oculta detalles de la red interna

Mejorar la performance del acceso a Internet

Otro beneficio de usar un servidor Proxy es acelerar el rendimiento del acceso a Internet mediante el almacenamiento en caché de las páginas descargadas de Internet en el servidor Web. Las visitas repetidas de los clientes al mismo sitio Web se satisfacen utilizando archivos almacenados en el servidor Proxy, en lugar de repetir la descarga desde Internet. Como el servidor Proxy está ubicado en la red de la empresa, el tiempo de respuesta en la ubicación de la información almacenada en la caché es bastante mas corto que el correspondiente al tiempo de descarga desde el servidor de Internet.

2.4 Mecanismo de seguridad para control de tráfico

La regulación del tráfico hacia o desde una red se realiza mediante filtros que se implementan en los servidores Firewalls, o en los routers. Vamos a tratar el tema de firewall en forma detallada ya que es el elemento más usado y versátil como control de tráfico.

2.4.1 Seguridad con Servidor Firewall

El propósito principal de un Firewall es asegurar que ningún tráfico proveniente de una red pública como Internet pueda entrar a la red interna. El único tráfico permitido entrar a la red interna será el tráfico que explícitamente se permite. Por ejemplo se puede tener un servidor Web interno que se necesita sea asequible por los usuarios de Internet, entonces el Firewall puede ser configurado para permitir solo el tráfico de Internet a ese servidor Web, al mismo tiempo el Firewall puede permitir a los usuarios internos de la red acceder a los recursos y servicios en Internet.

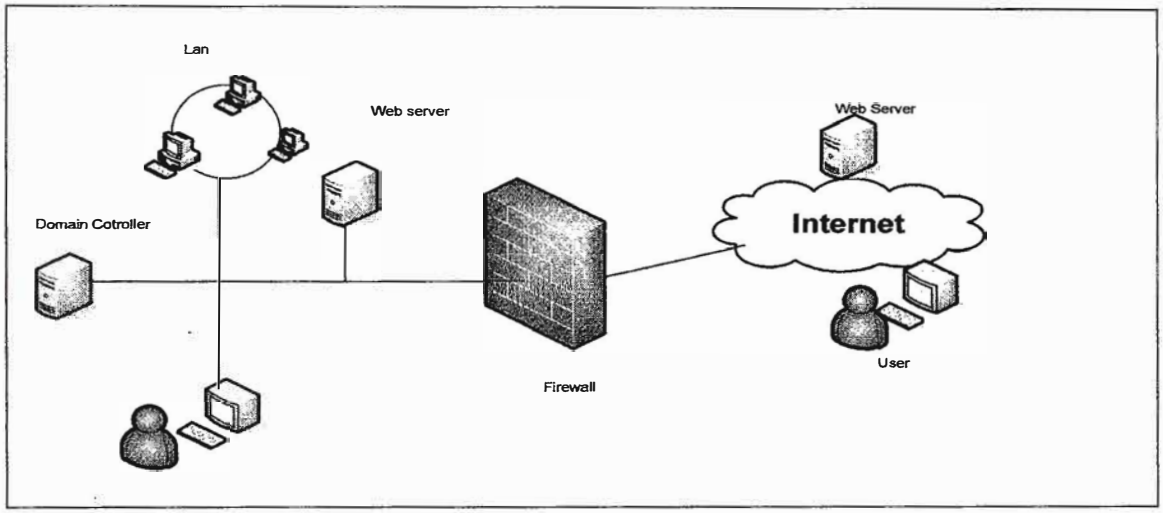

Fig. 2.6 Esquema básico de seguridad con Firewall

Un buen servidor Firewall puede realizar tres tipos de filtrado:

- Filtrado de paquetes (Packet Filtering)
- Inspección de estado completo (Stateful Filtering)
- Filtro a nivel de capa de aplicación (Aplication Layer Filtering)

Filtrado de Paquetes (Packet Filtering)

El filtrado de paquetes evita que cierto tipo de paquetes que están siendo enviados o recibidos crucen a través del router.

Filtros

Los filtros de paquetes se especifican en cada interfase y se configuran para realizar uno de las siguientes acciones:

- Permitir todo el tráfico excepto paquetes que el filtro prohíbe
- Descartar todo el tráfico excepto paquetes que el filtro permite.

Cuando configuramos un filtro de paquetes primero debemos especificar si es un filtro de entrada o un filtro de salida y luego seleccionar la acción del filtro, ya sea para aceptar todos los paquetes o para rechazar todos los paquetes que el filtro especifica.

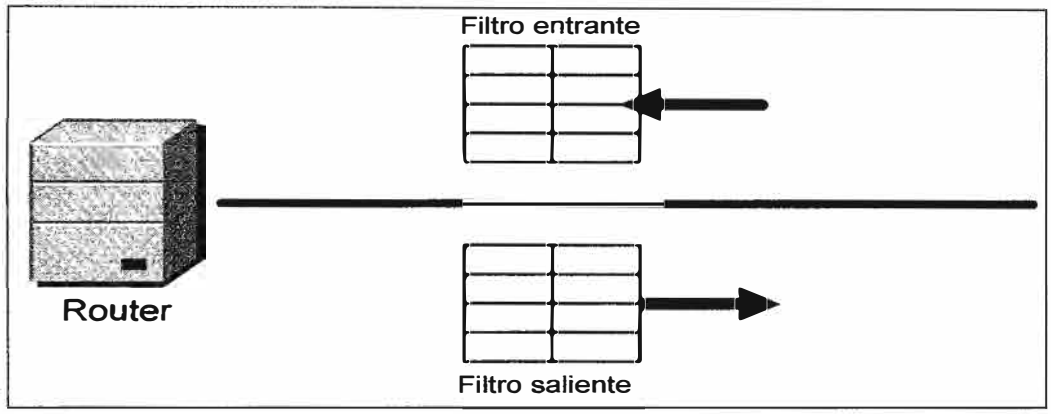

Figura 2.7 Filtros entrante y saliente en router

Los filtros de paquetes se utilizan para:

- Evitar que los usuarios accedan a determinadas computadoras usando direcciones IP, o identificadores (ID) de red.
- Prevenir el acceso a los recursos usando específicos puertos TCP o UDP (User Datagram Protocolo), número de protocolo, y protocolo ICMP (Internet Control Message Protocolo).
- Mejorar la performance de la red previniendo que viajen innecesarios paquetes sobre una conexión de baja velocidad.

El sistema que implementa el filtro examina cada paquete cuando éste llega y determina si satisface los criterios para su admisión. Los paquetes que cumplan los criterios de admisión

serán procesados por el sistema en la manera habitual, mientras que aquellos que no lo hagan serán descartados. Por ejemplo, los servidores de correo electrónico de Internet utilizan normalmente el protocolo de transferencia de correo (SMTP, Simple Mail Transfer Protocol) y el Protocolo de Oficina de Correo 3 (POP3, Post Office Protocol). Estos protocolos utilizan los puertos 25 y 110, respectivamente. Podemos crear un filtro de paquetes que permita únicamente la entrada de los paquetes que vayan dirigidos a los puertos 25 y 110.

Cada filtro puede tener múltiples parámetros, dentro de cada filtro los parámetros son comparados con una relación lógica AND cuando se aplica el filtro al paquete.
En cada interfase se pueden crear múltiples filtros que indican al router el tipo de tráfico que va a permitir o denegar, los filtros pueden ser a su vez de entrada o salida.
Los múltiples filtros ya sea de entrada o salida se aplican mediante una relación lógica OR.

Filtro No 1

Componente	Ejemplo
Red origen	192.168.0.48
Red destino	192.168.0.32
Protocolo	UDP

Filtro No 2

Componente	Ejemplo
Red origen	Any
Red destino	192.168.0.32
Protocolo	UDP

Acción: rechazo

Por ejemplo si los dos filtros mostrados se aplican a un paquete entrante o saliente, primero se evalúan los parámetros de cada filtro aplicando la relación AND y luego se aplican a ambos filtros la relación OR para decidir la aceptación o rechazo. En el caso de arriba el filtro No 2 es el que se aplica con la acción de rechazo.

El filtrado de paquetes se utiliza principalmente en los enrutadores y servidores de seguridad que conectan una red privada con Internet. Sin embargo, se pueden emplear también dentro de las redes privadas para aislar una parte de la red de los demás usuarios.

Criterios de filtrado de paquetes

Los filtros de paquetes se crean seleccionando criterios específicos que se desea que el sistema examine y especificando los valores cuyo paso se desea permitir o denegar. Los filtros pueden ser **inclusivos y exclusivos**.

Los **filtros inclusivos** comienzan con una conexión completamente bloqueada y se utilizan filtros para especificar que tráfico puede pasar.

Los filtros exclusivos comienzan con una conexión completamente abierta y se especifica los tipos de tráfico que se desea bloquear.

Los criterios que se emplean con mayor frecuencia en el filtrado de paquetes son los siguientes: Números de puerto, Identificadores de protocolo, Direcciones IP y Direcciones Hardware.

- **Filtrado de paquete basados en Números de puerto:** También conocido como **filtrado dependiente del servicio,** es el más frecuente y más flexible. Como los números de puertos están unidos a determinadas aplicaciones, se pueden utilizar para impedir que el tráfico generado por otras aplicaciones llegue a la red. Un ejemplo muy conocido es la protección de los servidores Web que se encuentran en una red perimétrica creando filtros que permitan únicamente las entradas desde Internet el tráfico dirigido al puerto 80. El puerto 80 es el asignado al servicio World Wide Web HTTP que es el principal protocolo de nivel de aplicación utilizado por los servidores Web.

- **Filtrado de paquetes basados en Identificadores de protocolo:** En las cabeceras IP de cada paquete hay un campo **Protocolo** que contiene un código que identifica al protocolo que deberá recibir a continuación el paquete. En la mayoría de los casos, el código representa un protocolo de nivel de transporte tal como el TCP o el UDP.

- **Filtrado de paquetes basados en Direcciones IP:** este tipo de criterio permite limitar el acceso a la red a los equipos que se define expresamente. Por ejemplo podemos crear un filtro que permita que los paquetes que vienen de Internet solo puedan entrar a la red si van dirigidos a un determinado servidor Web.

- **Filtrado de paquetes basados en Direcciones Hardware (MAC)**

  Funcionan de la misma manera que los filtros basados en direcciones IP, solo que se emplean las direcciones físicas de las tarjetas de red codificada e impresa en fábrica. Resultan más seguras ya que son más difíciles de suplantar. No se suele emplear en los enrutadores o en los servidores de seguridad de Internet por que los equipos que no pertenezcan a la red no tienen forma de saber la MAC de los equipos, en cambio se puede utilizar en filtrados internos.

Stateful Filtering (inspección de paquetes de estado completo): mediante este filtro se examina no solamente la información de la cabecera del paquete, sino también el estado del paquete. Se examina las cabeceras de los IP y TCP para determinar el estado de los paquetes dentro del contexto de otros paquetes o dentro del contexto de otra sesión TCP, es decir todo los paquetes que llegan desde la red externa son examinados para ver si son consecuencia de algunas solicitudes anteriores desde la red interna o de una sesión actual, si corresponden a un a petición anterior o a alguna sesión actual son direccionadas hacia la red interna en caso contrario son rechazados.

Aplication Layer Filtering (filtrado a nivel de aplicaciones): con este tipo de filtro el firewall examina el contenido actual de un paquete de red para determinar si el paquete será dirigido a través del firewall. El filtro de aplicación abre el paquete entero y examina la data en el paquete antes de realizar una decisión de envío. Por ejemplo un usuario de Internet puede solicitar una página ubicada en un servidor de la red interna usando el comando GET HTTP, cuando el paquete llega al firewall, el filtro de aplicaciones inspecciona el paquete y nota el comando GET, el filtro de aplicación chequea su política para determinar si el comando GET es permitido, como este comando es de lectura normalmente se permite y el paquete es direccionado al servidor Web interno.

2.4.2 Seguridad mediante redes Perimétricas

Cuando se quiere hacer pública alguna información a los usuarios externos de una red, esta información se coloca en servidores públicos de información que pueden ser servidores de páginas Web, servidores de correo, servidores de aplicaciones etc. a los cuales se les puede asignar direcciones IP registradas denominadas también direcciones públicas para que puedan ser vistas desde Internet. Sin embargo, la publicación de los servidores hace

insegura a la red interna, por lo que se la protege ubicando los servidores de acceso público en lo que se conoce como redes DMZ, zonas desmilitarizadas o también en su forma mas conocida de redes perimétricas que son separadas de la red mediante firewalls o routers, que de acuerdo al modo en que se ubiquen definen una serie de características relacionadas con el perímetro de una red.

Configuraciones conocidas de los Firewalls

Los servidores firewalls pueden ser configuradas para cumplir específicas funciones conocidas que podemos escoger de acuerdo a las consideraciones de diseño con que nos afrontemos, detallamos tres de estas configuraciones.

Configuración Bastion host

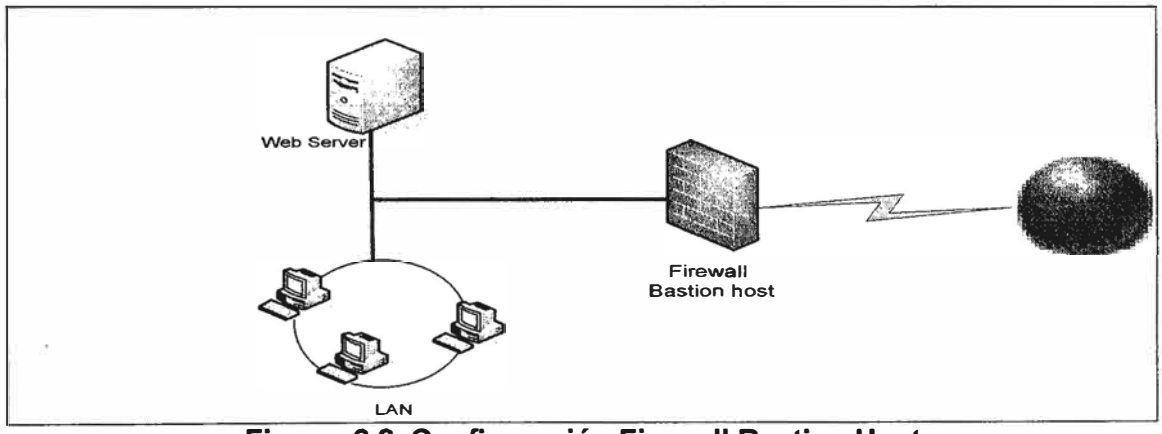

Figura 2.8 Configuración Firewall Bastion Host

- Actúa como el principal punto de conexión para las computadoras de la red interna que están accediendo a Internet.
- Es usado por redes pequeñas
- Utiliza un firewall con 02 tarjetas de red, una conectada hacia la red y la otra hacia Internet.
- Solamente es una simple línea de defensa entre Internet y la red interna.

Configuración three-pronged

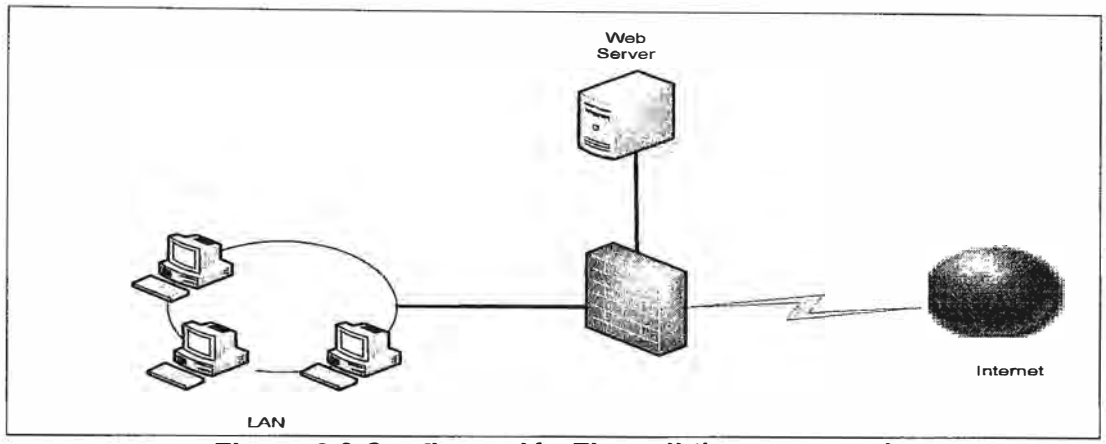

Figura 2.9 Configuración Firewall three-pronged

- Usa tres tarjetas de red, cada una conectada a la red interna, a la red perimétrica y a la red Internet respectivamente.
- Generalmente el tráfico desde Internet hacia la red perimétrica es a través de enrutamiento o empleando NAT.
- El Firewall es configurado para no permitir tráfico directo hacia la red Interna.
- La ventaja de esta configuración es que nos permite tener un simple punto de administración para la configuración de la red perimétrica y la red interna.
- La desventaja de esta configuración es que tienen un simple punto de acceso a las redes. Si el Firewall es comprometido, tanto la red perimétrica y la red interna pueden ser comprometidas.

Configuración Firewall back- to-back

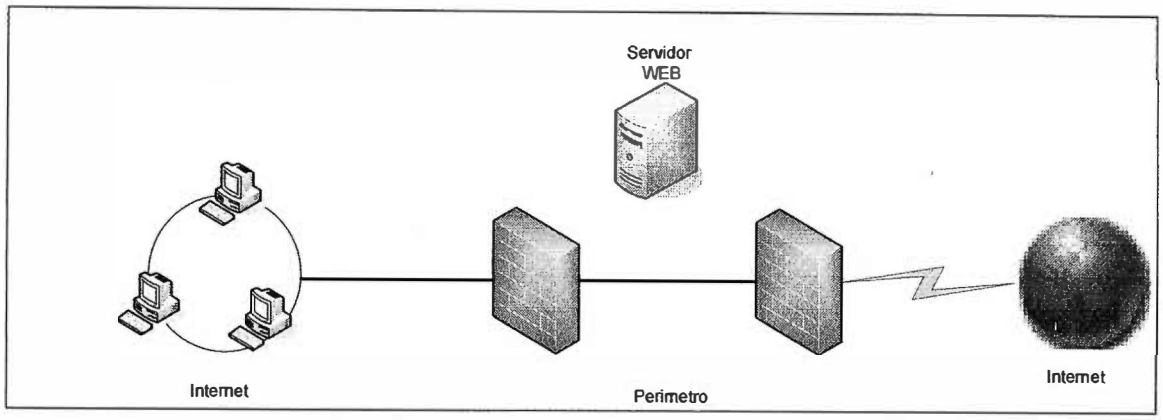

Fig. 2.10 Configuración Firewall back-to-back

- Coloca la red DMZ entre 02 Firewalls
- Los 02 fierwall son conectados a la zona DMZ.
- Un firewall es conectado a Internet y el otro firewall es conectado a la red interna.
- En esta configuración no hay un simple punto de acceso desde Internet a la Lan.
- Para alcanzar o penetrar a la red el atacador debe pasar ambos firewalls.

2.5 Mecanismos de Seguridad en la transmisión

Existe una variedad de amenazas en las transacciones digitales dentro de una misma empresa como entre empresas. Entre estas amenazas podemos tener la interceptación de los mensajes, la suplantación de identidad y el repudio o rechazo de los mensajes. Existen una serie de componentes se pueden utilizar en la protección contra estas amenazas como son la encriptación y los certificados digitales que conforman y los protocolos de encriptación y firmado (IPSec).

2.5.1 Encriptación (Cifrado)

Para proteger los datos que se transmiten, los equipos utilizan diferentes tipos de encriptación o cifrado tanto para codificar los mensajes y para crear firmas digitales que verifiquen la autenticidad. Para que un equipo pueda cifrar un mensaje y otro pueda descifrarlo ambos deben poseer una clave. La encriptación o cifrado puede ser realizada basada en clave secreta o en clave pública.

Encriptación basado en clave secreta

Se basa en la sustitución de un carácter por otro. Por ejemplo se puede crear una clave que especifica que la letra A debe ser sustituida por la Q, la letra B por la O y la letra C por la T y así sucesivamente, sin embargo cualquier mensaje que se codifique de esta manera podrá ser descifrada por cualquier persona que la conozca. A este proceso se le conoce como **cifrado por clave secreta,** por que se deberá proteger la clave de revelado. En este tipo de cifrado no existe una manera práctica de distribuir la clave secreta a todos los participantes, si el objetivo es enviar un mensaje cifrado a un determinado destino a través de la red, no resulta adecuado enviar primero la clave secreta de cifrado utilizando un mensaje no seguro.

Encriptación basado en clave Pública

Para que la encriptación o cifrado de los datos en una red sea posible y práctico, los equipos suelen emplear una forma de cifrado basado en clave pública. El cifrado basado en clave pública cada usuario o equipo utiliza dos claves, una clave pública y una clave privada. La clave pública está disponible para cualquiera y la clave privada se protege y nunca se transmite por la red. Los datos que hayan sido cifrados con la clave pública sólo podrán ser descifrados utilizando la clave privada, mientras que los datos cifrados utilizando la clave privada solo podrán ser descifrados utilizando la clave pública. Las claves privadas nunca se transmiten por la red. Las claves públicas se transmiten mediante certificados digitales.

Se puede emplear encriptación/cifrado para:

Encriptar datos Si un usuario A desea enviar un mensaje a un usuario B y quiere asegurarse que nadie pueda leerlo, el usuario A debe obtener la clave pública de B y utilizarla para encriptar el mensaje para transmitirla a través de la red, con la seguridad de que solo el usuario B que contiene la clave privada podrá descifrarlo. El usuario B recibe el mensaje lo descifra con su clave privada y podrá responder, utilizando la clave pública de A para encriptar la respuesta, para que solo el usuario A pueda descifrar la respuesta utilizando su clave privada.

Firmar digitalmente los datos Si el usuario A desea que el usuario B esté absolutamente seguro de que es el emisor del mensaje, puede firmar digitalmente el mensaje utilizando su clave privada para cifrar todo o parte de los datos. El usuario B podrá descifrar el mensaje utilizando la clave pública de A. El hecho de que la clave pública de A descifre el mensaje probará que es el emisor del mensaje, por que solo su clave privada habrá podido cifrar el mensaje. Este mecanismo proporciona no solo una protección contra suplantación de identidad sino permite al destinatario B la prueba de que el usuario A ha enviado el mensaje, por lo que no podrá repudiarlo o rechazarlo.

Verificar datos El usuario A para asegurarse de que el mensaje que envía no sea modificado en el camino, utiliza un algoritmo hash para crear **un resumen** del mensaje y a continuación encripta tanto el mensaje como el hash utilizando su clave privada. Cuando el mensaje llegue al destino B, éste descifrará el mensaje utilizando la clave pública de A, a continuación B utiliza el mismo algoritmo de hash para crear un hash del mensaje que le ha llegado. Si el hash que lo ha llegado coincide con el hash calculado, se habrá verificado el mensaje y comprobado que le mensaje no ha sido modificado en el camino.
Un hash es un resumen digital de un mensaje que se crea eliminando los bits redundantes de acuerdo a un determinado algoritmo de hash.

2.5.2 Certificados digitales

Los certificados se emplean para la distribución de las claves públicas en forma confiable. Un certificado digital es un documento que asocia una clave pública a una determinada persona o empresa. Existe un estándar publicado por la ITU-T denominado X.509 (the Directory: Public-key and Attribute Certificate Framework) que define el formato de los certificados que utilizan la mayoría de los sistemas que soportan PKI (Infraestructura de clave pública), es decir un certificado además de la **clave pública** tiene la siguiente información:

- **Versión** Identifica la versión X.509 utilizado para dar formato al certificado
- **Número de serie** Identifica de forma única al certificado
- **Identificador del algoritmo de firma** Tipo de algoritmo que se ha utilizado para calcular la firma digital del certificado.
- **Nombre del emisor** Nombre de la entidad que emitió el certificado
- **Periodo de validez** especifica el periodo durante el cual es valido el certificado

- **Nombre del sujeto** especifica el nombre del sujeto para el que se ha emitido el certificado.

Autoridad de certificación

Para utilizar encriptación basado en clave pública se debe obtener un certificado de una autoridad de certificación (AC), que puede ser una empresa que cuenta con la confianza necesaria para verificar las identidades de todas las partes involucradas en una transacción digital, o puede ser un elemento de software de un equipo basado en el sistema operativo. Para transacciones internas se emplean las AC basados en los sistemas operativos internos, para las transacciones externas se emplea certificados de terceras empresas como por ejemplo Thawte y VeriSing, Inc., los certificados se obtienen de forma manual en el caso de que el usuario lo solicite de manera expresa a una AC que le emita un certificado, o automático en caso de sea una aplicación la que solicite y obtenga un certificado en segundo plano como parte de su funcionamiento normal. En ambos casos la AC emitirá una clave privada y una clave pública como un par. La clave privada se almacenará en el equipo del usuario en forma cifrada y la clave pública se emitirá como parte del certificado.

Aplicaciones de los certificados

Los certificados se pueden emplear en las siguientes aplicaciones:

• **Firmas digitales** Para confirmar que la persona que ha enviado el mensaje, archivo o los datos es, en realidad quien dice ser. Las firmas digitales no protegen los datos de los ataques, solo verifican la identidad del remitente.

• **Autenticación en Internet** Para autenticar clientes y servidores en conexiones a través de Internet.

• **Seguridad IP** Permite cifrar y firmar digitalmente las comunicaciones para evitar que sean comprometidas al ser transmitidas por la red.

• **Correo electrónico seguro** Los protocolos de correo electrónico de Internet transmiten los mensajes en texto plano, lo que hace sencillo su interceptación y lectura de su contenido. Se puede enviar correo electrónico seguro cifrando los mensajes con la clave pública del destinatario y firmándolos con la clave privada del remitente.

• **Inicio de sesión con tarjeta inteligente** Una tarjeta inteligente es un dispositivo electrónico del tamaño de una tarjeta de crédito que contiene memoria y un circuito

integrado. Se utiliza para autenticar la identidad de un usuario que inicia una sesión. Contiene el certificado del usuario y la clave privada lo que permite al usuario iniciar sesión en cualquier equipo de la empresa con total seguridad.

- **Firma del código de software** Se utilizan para confirmar que el software que se descargan e instalan provienen realmente del fabricante y que no se han modificado.
- **Autenticación de red inalámbrica** Para proteger una red inalámbrica, identificando y autenticando a los usuarios antes de que sean garantizados el acceso a la red.

2.5.3 Seguridad con IPSec

Los datos almacenados se pueden proteger mediante varios mecanismos, por ejemplo podemos utilizar una aplicación para proteger la data mediante una contraseña, o podemos almacenar los archivos en forma encriptada utilizando alguna propiedad de los sistemas operativos avanzados como el sistema de encriptación de archivos (EFS, Encrypting File System) del Windows Server 2003. Pero, cuando se acceda a los archivos a través de la red o cuando se envíen a otras personas, estas siempre serán desincriptadas primero.

El IPSec ha sido diseñado para justamente proteger la data que se transmite, evitando una serie de amenazas muy comunes en la transmisión tales como: la captura de claves de encriptación, suplantación de persona (spoofing), modificación de datos, y el ataque de aplicaciones.

El IPSec tiene dos objetivos: proteger los paquetes IP, y proporcionar una defensa contra ataques a la red. La configuración de IPSec en la computadora de envío y en la computadora de recepción habilita a las computadoras a enviarse datos entre ellos en forma segura. El protocolo IPSec asegura el tráfico de la red utilizando encriptación, desincriptación y firmando la data.

La aplicación que transmite la data define si se va ha utilizar IPSec, si se utiliza IPSec primero se establece una negociación de seguridad y como consecuencia de esta negociación se genera una clave compartida de encriptación y desincriptación, luego una política (directiva) IPSec define el tipo de tráfico que IPSec examina, como es asegurado y encriptado y como las computadoras se autentican.

Protocolos IPSec

Existen dos protocolos IPSec que proporcionan diferentes tipos de seguridad para las comunicaciones de red

- **Encabezado de Autenticación IP (AH)**

Este protocolo no encripta la data. La data es leíble pero no puede ser modificado. Es decir este protocolo proporciona autenticación, integridad y protección contra reemplazo de información pero no proporciona confidencialidad.

Cuando un equipo utiliza AH para proteger sus transmisiones, el sistema inserta una cabecera AH en el datagrama IP, inmediatamente detrás de la cabecera IP y antes de la carga de pago del datagrama como se ve en la figura 2.11.

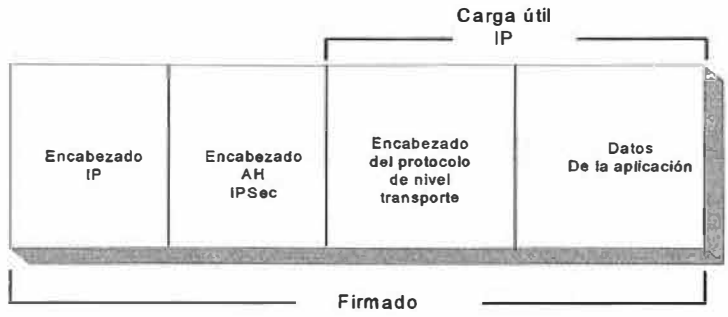

Figura 2.11 Ubicación del encabezado AH

- **Carga de seguridad encapsuladora de IP (ESP)**

El protocolo ESP (Encapsulating Security Payload) cifra los datos contenidos en un datagrama IP, impidiendo que se pueda leer la información contenida en los paquetes que puedan ser capturados. También proporciona autenticación, integridad, y antirreproducción. ESP inserta un encabezado y una cola que encierran a la carga de pago del datagrama como se ve en la figura 2.12

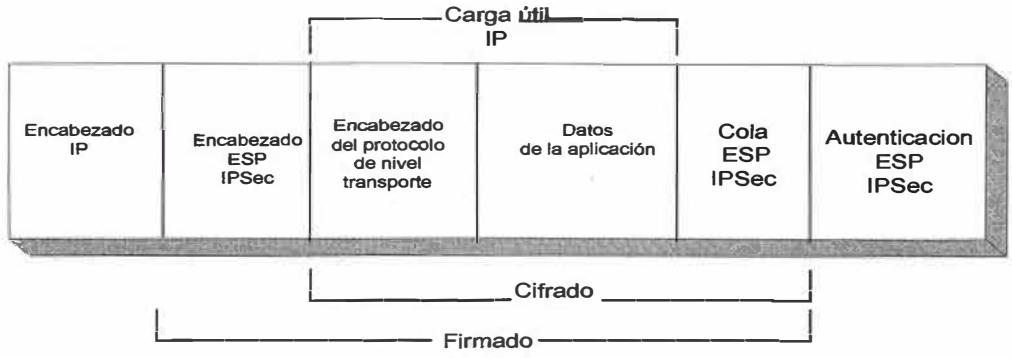

Figura 2.12 Ubicación del encabezado y de la cola ESP

Modos de trabajo del IPSec

- **Modo transporte**

En el modo transporte los dos equipos terminales (extremos) deben soportar IPSec y los equipos intermedios como los enrutadores no lo necesitan.

- **Modo túnel**

El modo túnel ha sido diseñado para proteger las conexiones de red de área extensa (WAN, Wide Area Network) y, en particular, las conexiones de red privada virtual (VPN, Virtual Private Network), que utilizan Internet como un medio de comunicación. En una conexión modo túnel, los sistemas extremos no soportan ni implementan los protocolos IPSec; los enrutadores situados en los extremos de la conexión WAN si lo hacen.

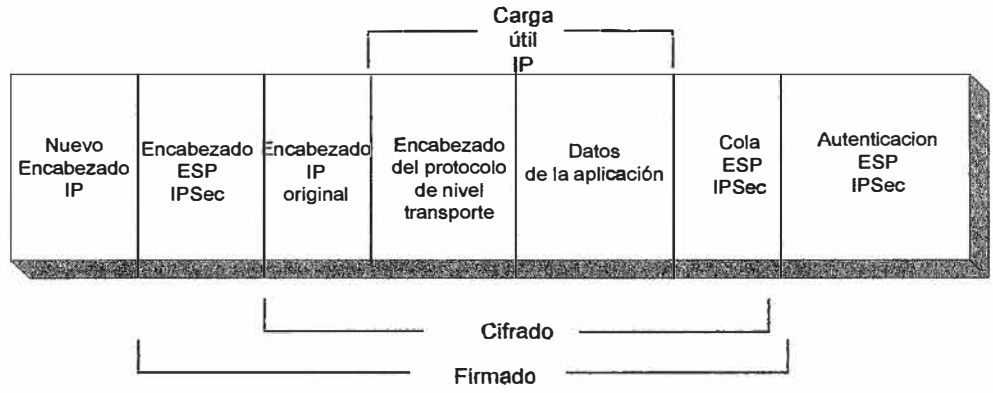

Figura 2.13 Paquete en modo túnel de IPSec

El modo túnel emplea una estructura de paquete distinta, se crea un datagrama completamente diferente como se ve en la figura 2.13. y agrega un nuevo encabezado al datagrama, el datagrama original contenido dentro del nuevo datagrama, no cambia.

Directivas IPSec. (Políticas IPSec)

Una directiva IPSec define el tipo de tráfico que IPSec examina, como el tráfico es asegurado y encriptado y como se autentifican las computadoras. Las directivas IPSec se pueden crear o se pueden emplear directivas preconfiguradas y también se pueden modificar estas directivas preconfiguradas.

Para implementar una comunicación IPSec entre dos computadoras, ambas deben tener una directiva IPSec asignada y además esta directiva debe permitir negociar un método de autenticación común.

Elementos de una directiva IPSec

Se puede implementar IPSec asignando una misma directiva IPSec a ambas computadaras. Cada directiva puede contener varias reglas, también referenciadas como lista de filtros, pero solo podemos asignar solamente una sola directiva a un computador. Se deben combinar todas las reglas deseadas dentro de una simple política. Cada regla está compuesta de:

- **Un filtro** La directiva utiliza el filtro para determinar a que tipo de tráfico se le aplicará la acción, por ejemplo el filtro puede especificar tráfico HTTP o tráfico FTP.

- **Una acción de filtro** La directiva usa una acción de filtrado para determinar que hacer si se cumplen o concinden las condiciones de filtrado. Las acciones de filtrado pueden especificar bloqueo de cierto tráfico tráfico, o especificar si IPSec deberá utilizar AH, ESP o ambos, así como qué algoritmos de integridad de datos y de cifrado utilizará el sistema.

- **Un método de autenticación** Se pueden emplear tres posibles métodos de autenticación: certificados, kerberos y clave compartida (preshared key). Cada regla puede especificar múltiples métodos de autenticación y son tratados en el orden listado en el filtro de la directiva IPSec.

Directivas IPSec preconfiguradas

Existen tres políticas que son configuradas por default bajo el sistema operativo W2K3, que son útiles y que en la mayoría de los casos son suficientes para implementar comunicaciones seguras entre dos computadoras.

- **Cliente (sólo responder) [Client (respond only)]**

Configura el equipo para utilizar IPsec sólo cuando otro equipo solicite IPSec. El equipo que utilice esta directiva nunca inicia una negociación IPSec; sólo responde a peticiones desencadenadas desde otros equipos para iniciar una comunicación segura.

- **Servidor (solicitar seguridad) [Server (Request Security)]**

Configura el equipo para que solicite el empleo de IPSec cuando se comunique con otro equipo. Si el otro equipo es compatible con IPSec, comenzará la negociación IPSec. Si el otro equipo no soporta IPSec, los sistemas establecerán una conexión IP estándar y no segura.

- **Servidor seguro (requerir seguridad) [Secure Server (Require Security)]**

Configura el equipo para solicitar seguridad IPSec en todas sus comunicaciones. Si el equipo intenta comunicarse con otro equipo que no puede utilizar IPSec, el equipo que ha iniciado la conexión la finalizará.

2.5.4 Seguridad con servidor VPN

La seguridad VPN está basada en los tipos de protocolos túnel y los métodos de autenticación que usa y en el nivel de encriptación que aplica a las conexiones VPN. Como se trató en el capítulo I, las conexiones VPN se realizan con los protocolos túnel PPTP y L2TP. Cada uno de estos dos protocolos crean una conexión directa entre un cliente VPN y un servidor de acceso remoto o una conexión directa entre dos VPN gateways para el caso de sitios remotos.

- **Seguridad en VPN con PPTP**

La conexión VPN creada mediante PPTP usa métodos de autenticación de usuario del protocolo punto a punto (PPP: Point-to-Point Protocolo) y el protocolo de encriptación MPPE (Microsoft Point-to-Point Protocolo Encryption) para encriptar el tráfico. Para una autenticación basada en **passwords** el PPTP usa el protocolo de autenticación MSCHAP V2 (Microsoft Challenge Handshake Autentication Protocol Version 2). Para una autenticación mas fuerte de conexiones PPPT se puede implementar una infraestructura PKI (public key infrastrucuture) basado en tarjetas inteligentes (smarts cards) o

certificados y el protocolo EAP-TLS (Extensible Autentication Protocol-Transport Level Security).

La conexión VPN PPTP es la más ampliamente utilizada y la más fácilmente implementada, y trabaja mayormente con implementaciones NATs. Si bien no es tan segura como la IPsec, es la menos compleja de administrar y puede reducir los costos asociados en una implementación de una infraestructura de certificados.

- **Seguridad en VPN L2TP/IPSec**
  Es la más segura de las dos conexiones VPN, utiliza los mótodos de autenticación PPP y utiliza el protocolo de encriptación IPSec para encriptar el tráfico. Esta combinación usa métodos de autenticación de computadoras basado en certificados para crear una asociación de seguridad IPSec además de autenticación de usuarios basados en PPP. El L2TP/IPSec proporciona integridad de la data, autenticación del origen de la data, confidencialidad de la data, y protección contra reemplazo de cada paquete.

2.5.5 Control de cuarentena VPN

El servidor de acceso remoto en la mayoría de los casos valida solamente las credenciales de los usuarios de acceso remoto. Si el usuario remoto se autentica exitosamente puede acceder a los recursos de la red interna. Sin embargo los usuarios remotos pueden no cumplir con las políticas de red de la empresa u organización. El control de cuarentena VPN pone en espera o retraza el normal acceso remoto para privar al cliente remoto de la red hasta que un programa (script) en el cliente valide la configuración del cliente de acceso remoto.

El control de cuarentena VPN permite ocultar la máquina cliente VPN antes de permitirle el acceso a la red. Para habilitar la cuarentena VPN se crea un paquete CMAK (Connection Manager Administration Kit) que incluye un profile cliente VPN, y un script en el lado del cliente en cuarentena. El script se ejecuta en el cliente y chequea la configuración de seguridad del cliente de acceso remoto y reporta los resultados al servidor VPN. Si el cliente pasa el chequeo de configuración, se le permite el acceso a la red y el cliente es movido de la red de cuarentena a la red de clientes VPN.

2.6 Herramientas y productos de Microsoft que permiten implementar seguridad

Hay dos poderosas herramientas que se utilizan con el sistema operativo Windows Server 2003 para cuestiones de seguridad, el RRAS que viene como producto integrado al sistema operativo para soluciones simples tales como ambientes de simulación y pruebas o para soluciones de redes pequeñas, y el ISA Server 2004 un producto que viene en forma independiente y que instalado en una computadora con software base W2K3 cumple una serie de funciones integradas especialmente para conformar un potente servidor de seguridad, un medio seguro de publicación de servidores, y un método verdaderamente elegante de implementar VPN tanto para clientes remotos y para establecer conexiones site-to-site entre oficinas remotas.

2.6.1 Servicio de enrutamiento y acceso remoto - RRAS de Microsoft.

Los sistemas operativos Windows 2000 y el Windows Server 2003 tienen un producto denominado RRAS (Routing and Remote Access Service) que puede ser empleado en una variedad de funciones:

- **Enrutamiento (Router),** para unir dos o más segmentos subredes separados físicamente
- **Traslación de direcciones (NAT),** para la conexión de una empresa hacia Internet.
- **Servidor de acceso** para permitir el acceso a una red interna a usuarios externos mediante VPN o dial-up.
- **Filtrado de paquetes**, para proporcionar seguridad, como un Firewall básico.

Una herramienta que se utiliza para la administración del acceso remoto en RRAS son las políticas (directivas) de acceso remoto, que son un conjunto ordenado de reglas que definen como las conexiones remotas son aceptadas o rechazadas. Una política de acceso remoto esta formado por los siguientes tres componentes:

- ***Condiciones***: son una lista de parámetros, tales como la hora del día, grupos de usuarios, IDs de llamadas, o direcciones IP, que son confrontados con los parámetros del cliente que se esta conectando al servidor, si los parámetros de la políticas coinciden con los parámetros comprados se acepta el acceso., de otra manera el intento de acceso es rechazado.

- **Permiso de acceso remoto**: la conexiones de acceso remoto son permitidos basados en las propiedades dial-in de una cuenta de usuario en el active directory y de las políticas de acceso remoto.
- **Profile**: cada política incluye un profile (perfil) de configuraciones, tales como los protocolos de autenticación y encriptación que se aplican a la conexión.

RRAS soporta el protocolo de autenticación RADIUS (Remote Autenticación Dial-In User Service) para configuración de autenticación y de políticas de acceso remoto. Se configura el RRAS como un cliente RADIUS para direccionar las peticiones de autenticación a un RADIUS.

RRAS soporta el uso de filtros PPTP y L2TP/IPSec de entrada y salida en la entrada que esta conectado a Internet para solo permitir el tráfico de estos protocolos VPN. Cuando configuramos un servidor VPN, se habilita el enrutamiento IP entre la red interna e Internet, esto es una vulnerabilidad que puede ser aprovechada por los atacadores desde Internet, por lo que se debe bloquear todos los paquetes de red excepto el tráfico PPTP o L2TP/IPSec en la interfase con Internet

RRAS también soporta el control de cuarentena, usa filtros IP para limitar los recursos que pueden acceder los clientes remotos mientras están en cuarentena y les da un tiempo de espera para desconexión si no cumplen los requerimientos de seguridad.

Enrutamiento con RRAS

El enrutamiento es el proceso de transferir datos en una interconexión de redes desde una red de área local a otra. En la redes IP el enrutamiento se lleva a cabo mediante dispositivos denominados enrutadores (routers) que pueden ser equipos hardware o computadoras con software. El enrutamiento se realiza en función de tablas de enrutamiento.

Propósito de los enrutadores (routers). Los routers permiten:

- el crecimiento o escalamiento de una red y mantienen el ancho de banda mediante la segmentación de la red.
- se configuran para hacer decisiones inteligentes para determinar como serán direccionados los paquetes entre los segmentos de red. Esto asegura que los

segmentos de red no sean inundados por tráfico destinado a hosts de otros segmentos de red.

- Los enrutadores previenen ciertos tipos de tráfico, tales como los Brodcast que pueden saturar la red.

Tipos de routers. Los dos tipos de routers que son utilizados en el mundo de las redes son:

- **Hardware routers.** Son equipos hardware que ejecutan software especializado dedicado exclusivamente para propósitos de enrutamiento. Proporcionan buena performance, sin embargo son caros y proporcionan poca funcionalidad para otras tareas distintas de su propósito. Algunos routers pueden realizar VPN y filtrado de paquetes. Se utilizan en ambientes de alta carga de trabajo entre redes.

- **Software routers.** Son equipos que no están dedicados al enrutamiento solamente, realizan enrutamiento como una de sus múltiples procesos que se ejecutan dentro del computador router. Por ejemplo el RRAS de Windows Server 2003 cuando está trabajando como router puede ofrecer servicios como WINS, DNS y DHCP.

Componentes de un esquema de Enrutamiento (Ruteo)

- **Interfase de ruteo.** Es una interfase física o lógica hacia la cual se direccionan los paquetes.

- **Protocolo de ruteo**. Es un conjunto de mensajes que intercambian los routers para compartir tablas y determinar las rutas por donde direccionar la data.

- **Tabla de ruteo.** Es una base de datos que contiene una serie de entradas llamadas rutas que contiene información que determina el camino hacia varios segmentos de red, basados en los ID de los segmentos.

2.6.2 Internet Security and Acceleration Server 2004 (ISA Server 2004)

El ISA Server 2004 es un producto de Windows que nos permite implementar seguridad de una manera integral. El ISA Server puede trabajar como Firewall, como servidor VPN y como servidor Proxy and Caching.

Características:

2.6.2.a Soporte de múltiples redes

El ISA Server 2004 utiliza redes para definir bloques de direcciones IP que pueden ser directamente conectadas al equipo servidor ISA o direcciones IP que pueden estar en redes remotas. Significa que podemos configurar múltiples redes en el servidor ISA, y podemos configurar reglas de red y reglas de acceso para inspeccionar y filtrar todo el tráfico entre todas las redes.

Una configuración bien conocida es como Firewall three-legged que se muestra en la figura 2.14

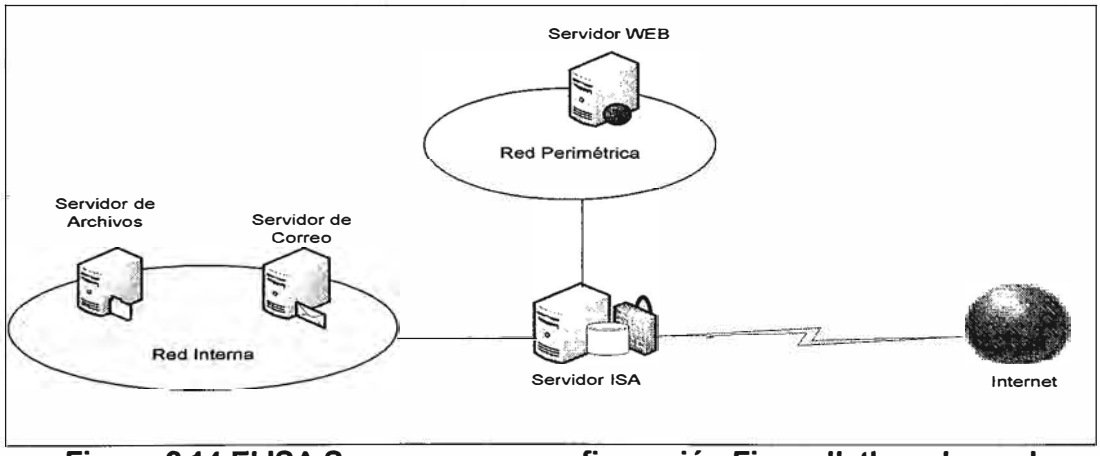

Figura 2.14 El ISA Server en una configuración Firewall three-legged

En esta configuración, podemos crear tres redes:

- Los servidores que son asequibles desde Internet, son aislados en una red propia, tal como la red perimétrica.
- Las computadoras clientes y servidores internos que no son asequibles desde Internet son colocados en una red interna.
- La tercera red es la red Internet

Otra configuración más complicada es la que se muestra en la figura 2.15 en este escenario tenemos lo siguiente:

- **Dos redes perimétricas:** una para servidores que son servidores miembros y otra red perimétrica para servidores stand-alone. En este escenario los servidores miembros podrán comunicarse con los controladores de dominio de la red interna.
- **Dos rede internas:** podemos tener clientes que acceden a Internet con diferentes aplicaciones y reglas de seguridad. Es decir podemos crear diferentes redes internas y configurar reglas especificas de acceso a Internet para cada una.
- **Red de cliente VPN y red VPN Site-to-Site:** el ISA define una regla para los clientes VPN y podemos definir una red para cada sitio remoto conectado con una conexión VPN site-to-site.

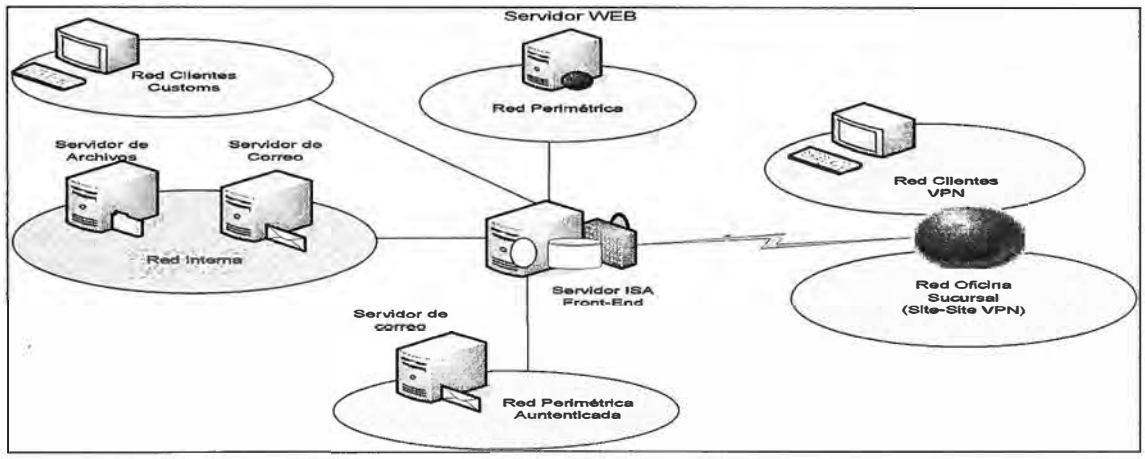

Figura 2.15 El ISA Server soporta ilimitado número de redes

2.6.2.b Comunicaciones entre redes basadas en reglas de Red

Las reglas de red definen las relaciones de comunicación entre dos redes y el tipo de relación que existe entre ellas, si no existen reglas de red entre dos redes el ISA rechazará todo tráfico entre ellas y no habrá comunicación entre ellas, las relaciones son NAT y enrutamiento.

- **Relación de Enrutamiento (Routing):** en este tipo de relación las peticiones de una red origen son directamente enrutados hacia la red destino basado en direcciones IP.

- **Relación NAT:** bajo esta relación las direcciones desde la red origen siempre son trasladadas al pasar por el ISA Server hacia Internet.

2.6.2.c Comunicación con Internet basado reglas de acceso

El acceso a Internet se controla mediante reglas de políticas de acceso, estas reglas emplean lo que se llama los elementos de reglas de acceso: protocolos, users, tipo de contenido, schedules, network objects.

Una regla de acceso nos define las condiciones para que el tráfico entre dos redes sea permitido o denegado, y los elementos de las reglas de acceso son las opciones de configuración de estas reglas.

Las reglas de acceso en el ISA tienen una estructura definida que consta de:

- **Una acción:** que puede ser permitir o denegar
- **Tráfico:** basado en específicos protocolos o números de puertos.
- **Origen:** usuarios, computadoras o redes.
- **Destino:** Computadoras basados en dirección IP, network ID, sitios.
- **Condiciones:** las condiciones pueden ser Tipo de contenido,

Elementos de reglas de acceso

Protocolos

Este elemento de regla contiene protocolos que se usa para definir el protocolo que es usado en una regla de acceso es decir podemos permitir o denegar uno o más protocolos.

Conjunto Usuarios

Este elemento incluye usuarios o grupos. Estos elementos se pueden crear con usuarios y grupos del directorio activo, grupos de un servidor RADIUS, o grupos SecureID.

Tipos de contenido

Mediante este elemento se puede permitir o denegar basado en el tipo de contenido del tráfico por ejemplo prohibir descargas de archivos con extensiones tipo .exe, vbs.. etc.

Schedules

Este elemento permite diseñar horas de la semana en que la regla se aplica. Así permitiremos acceso a Internet solamente durante específicas horas.

Objetos Red

Permite crear un conjunto de computadoras a las cuales se aplicará o se excluirá la regla.

Podemos configurar objetos URL y objetos Domain para permitir o denegar acceso a específicos URLs o dominios.

2.6.2.d Publicación de Servidores de Red

ISA Server 2004 usa reglas de publicación de servidores Web y reglas de publicación de servidores para poner los recursos internos de una red a disposición de Internet, esto es lo que se llama publicar servidores. Las reglas de publicación de servidores Web determinan como el ISA Server 2004 trata las solicitudes HTTP y HTTPS desde Internet dirigidas hacia los servidores Web internos. Por otro lado las reglas de publicación de servidores definen como el ISA Server 2004 responde a las solicitudes desde Internet por otros recursos de red en la red interna. Con el ISA Server se puede implementar tres tipos de reglas de publicación de servidores:

Web publishing rules. Para uso de tráfico HTTP y tiene los siguientes elementos:

Action

Name (or IP address):

Users: define los usuarios que podrán acceder al web site

Traffic source: define los objetos red que pueden acceder al web site

Public name: define el URL o el IP address con el que se accede al web..

Web listener: define el IP address y el número de Port en el cual el ISA server escuchará las conexiones de los clientes. Si el ISA Server tiene varias tarjetas de red o varios IP address se puede implementar la misma configuración Listener para todas las IP address o podemos tener diferentes listeners configuraciones para las diferentes IP addresses.

Path mappings: es una característica de ISA Server que redirecciona una solicitud hacia múltiples servidores Web internos o hacia a múltiples localizaciones en el mismo servidor web.

Bridging: define como las solicitudes HTTP son direccionados hacia el servidor publicado.

- **Secure Web publishing rules.** Es lo mismo que una regla de publicación de servidores WEB pero utiliza además el protocolo SSL para encriptación para usar con HTTPS .

- **Server publishing rules.** Para publicación se servidores con tráfico diferente de HTTP y HTTPS, servidores de aplicaciones, de base de datos etc.

Además de estas reglas, el ISA Server 2004 también proporciona las siguientes opciones para habilitar el acceso a servidores internos:

2.6.2.e Mail Server publishing rules. Son especializadas reglas de publicación de servidores Web o de servidores que son usados para proporcionar acceso a servidores SMTP y a computadoras que están ejecutando el Microsoft Exchange Server.

2.6.2.f Virtual private networking. El ISA Server puede también ser usado como un servidor VPN para proporcionar acceso a usuarios o localizaciones remotas a una red interna.

2.6.3 El ISA Server 2004 como herramienta de seguridad

2.6.3.a El ISA Server como Control de Tráfico (Firewall):

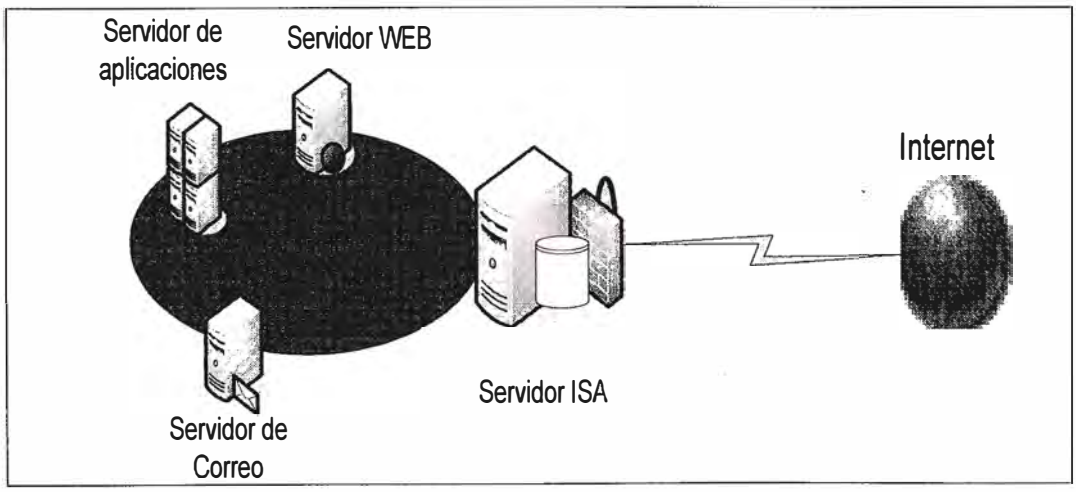

Figura 2.16 Servidor ISA como Firewall Bastion Host

- como Firewall el ISA Server realiza filtrado de paquetes, stateful filter, filtrado a nivel de capa de aplicaciones, características que ya hemos descrito.
- El ISA Server se puede implementar para trabajar como Firewall Bastion Host, Firewall Three-legged y Firewall back-to-back.

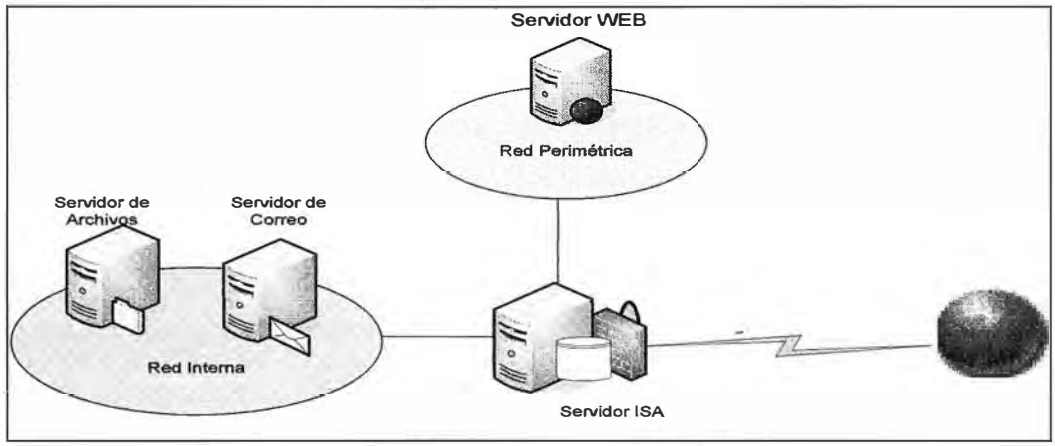

Figura 2.17 Servidor ISA como Firewall three-legged

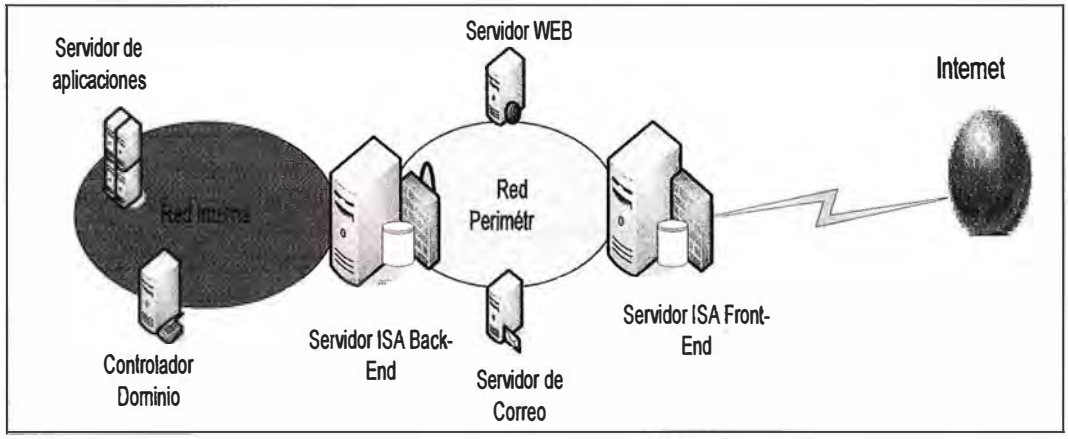

Fig. 2.18 Servidores ISA como Firewalls back-to-back

2.6.3.b El ISA Server como control de Acceso a Internet

Para que los usuarios internos puedan acceder a Internet a través del ISA este puede trabajar haciendo las funciones de **Servidor Proxy y servidor de caché.**

Proxy Server: Para el acceso de los clientes desde la red interna hacia Internet el ISA Server actúa como un Proxy Server lo que significa

- que no hay una directa conexión entre el cliente y el servidor Web de Internet .
- la información interna del cliente no es enviada a través de Internet
- se puede filtrar las peticiones de acceso basados en los nombres de usuarios, direcciones IP de los clientes, protocolos, y contenido de las peticiones.

Es decir que podemos limitar cual usuarios pueden acceder a Internet, que aplicaciones pueden utilizar para acceder a la información y a que tipo de información pueden acceder.

2.6.3.c El ISA Server como un servidor VPN

El ISA Server puede operar como servidor VPN para los usuarios remotos o puede operar como un gateway VPN en una VPN site-to-site.

El ISA integra esta funcionalidad dentro del Firewall.

Los clientes conectados usando VPN son parte de una red denominada **red de clientes VPN.**

Se puede implementar el control de la Cuarentena con los clientes VPN que no cumplan con la configuración exigida por el servidor de acceso remoto y retrasar el acceso a estos clientes hasta que sean examinados y validados por un programa en la computadora cliente.

2.6.4 Beneficios de usar ISA Server Respecto al RRAS en implementaciones VPN

- **Control y seguridad de la conexión:** el ISA controla el acceso a través de políticas de acceso de Firewall, así el tráfico después de ser inspeccionado es direccionado o rechazado basado en criterios como quien envía, hacia donde van y en las aplicaciones que están llegando y hacia donde están yendo.
- **Registro y Monitoreo:** el RRAS solamente permite registrar una rudimentaria base de datos basado en texto de las conexiones. El ISA registra además de las conexiones, el

tráfico relacionado a estas conexiones. Esto permite identificar problemas VPN que tiene relación con la comunicación. Este tráfico puede ser almacenado en una archivo texto, base de datos MSDE (Microsoft data engine) o en una base de datos SQL. También se puede ver el estado y las sesiones activas en las conexiones.

- **Protección de los recursos del Servidor VPN:** El ISA Server es protegido por medio de políticas de acceso de Firewall en todas las interfase instaladas en el ISA Server. El RRAS no es capaz de proteger los recursos del servidor VPN de los ataques internos a través de la interfase interna. EL ISA extiende este nivel de protección aplicando políticas de acceso de Firewall a todas las interfases, es decir interfase a la red interna, red perimétrica, y las interfases VPN.

CAPITULO III
DISEÑO DE SEGURIDAD EN LAS CONEXIONES REMOTAS - RED RELIMA

3.1 Escenario

La empresa Vega Upaca S.A - RELIMA cuya red se muestra en la figura 3.1, nos ha planteado estudiar la seguridad en su arquitectura y trazar una estrategia de seguridad para la red mediante la implementación de una zona DMZ para la publicación de sus servidores e implementación de una VPN para sus conexiones remotas.

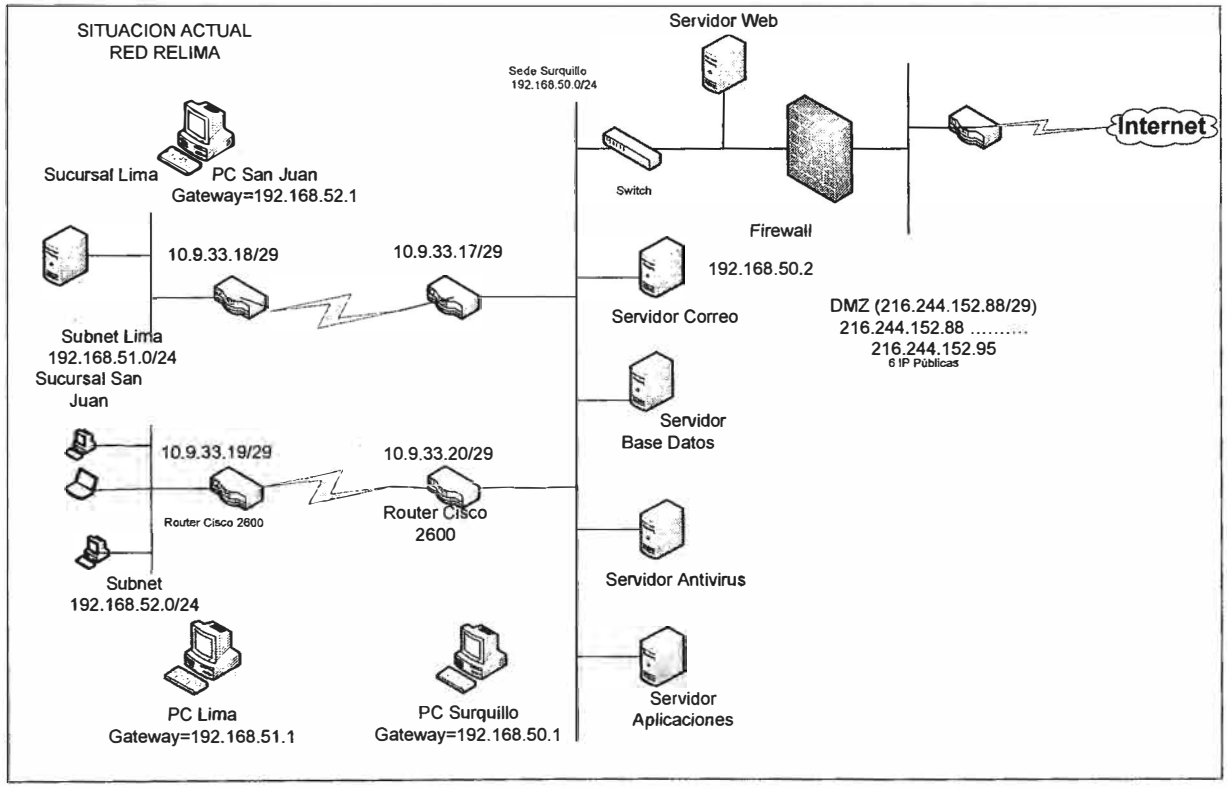

Figura 3.1 Arquitectura topológica actual de la Red Relima

3.2 Requerimientos de implementación

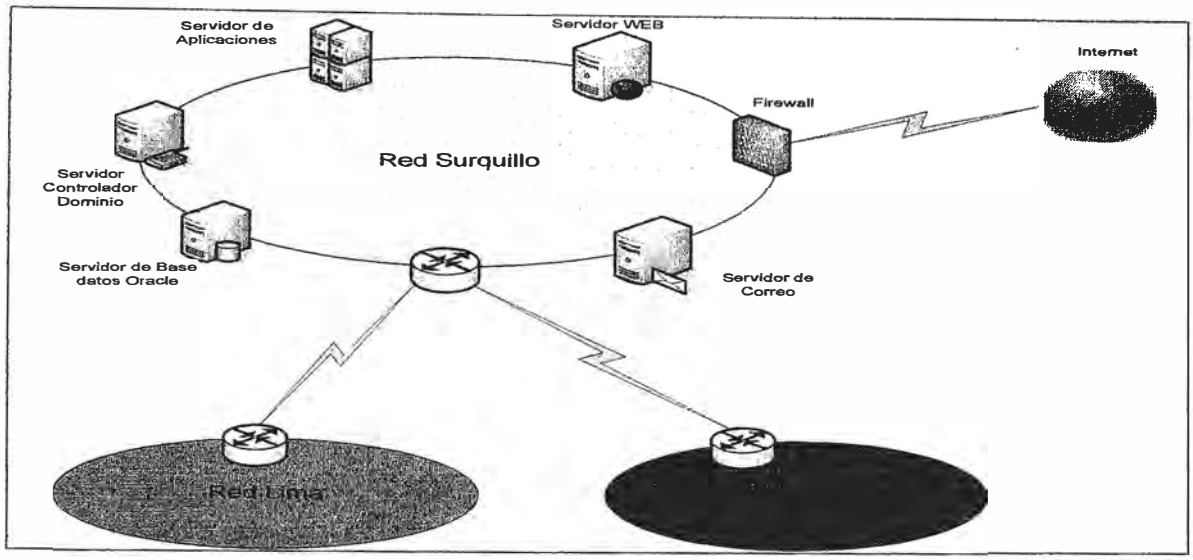

Fig. 3.2 Esquema red actual Relima

- **El Firewall actual debe ser reemplazado**

  Se requiere un Firewall que realice filtrado de paquetes, stateful filtering, filtrado a nivel de aplicaciones, y detección de intrusos. El firewall actual solo tiene abiertos los puertos 80 y 25 para el servidor WEB y correo.

- **Se requiere implementar una DMZ para los servidores públicos**

  Actualmente se tiene una zona perimétrica tipo bastion host, como vemos en la figura 3.2, el Firewall ubicado de esta manera es una simple línea de defensa entre Internet y la red interna, la protección se implementa aplicando filtros de paquete en el puerto 80 para el servidor Web y en el puerto 25 para el servidor de correo.

- **Localizar / Publicar dentro de esta zona DMZ los siguientes servidores:**

  El servidor de páginas Web

  El servidor de correo electrónico

  Y el servidor de aplicaciones

- **Implementar VPN para usuarios remotos y móviles**

  Se requiere que los usuarios móviles y remotos, puedan acceder a las aplicaciones financieras de la empresa, y también que la principal de Brasil pueda intercambiar de forma segura información con la red Relima.

3.3 Descripción de los componentes de la red actual de Relima

La Figura 3.2 es un esquema que muestra la red actual de la empresa Vega Upaca S.A.-Relima. Es una estructura soportada por el sistema operativo Windows Server 2003. Se ha implementado bajo este sistema el servicio de directorio de directorio activo (Active Directory Directory service). La estructura de directorio activo de la red Relima esta conformada por los siguientes componentes:

3.3.1 Componentes físicos de la red Relima

Sitios (Sites)

Se tiene un solo dominio con 3 subredes ubicados en Surquillo, San Juan y Lima.

Subred Principal : Surquillo

Ubicación: Av. Tomas Marzano 432 - Distrito de Surquillo
Número Servidores: 05 servidores W2k3
Clientes Windows XP: 30 clientes
ID de Red: 192.168.50.0
Máscara de Sub Red: /24 = 255.255.255.0
Capacidad: 254 equipos IP
Gateway hacia Lima: 192.68.50.1
Gateway hacia San Juan: 192.168.50.2

Interfase router Surquillo-Lima

ID de interfase: 10.9.33.17
Máscara de interfase /29= 255.255.255.248

Subredes secundarias

Sub Red Lima

Ubicación: Jr. Chota - Distrito Cercado de Lima
Número Servidores: 0 servidores W2K3
Clientes Windows XP: 30 clientes
ID de Red: 192.168.51.0
Máscara de Sub Red: /24 = 255.255.255.0
Capacidad: 254 equipos IP
Gateway hacia Surquillo: 192.68.51.1

Sub Red San Juan

Ubicación: Av. – Distrito de San Juan

Número Servidores: 10 servidores W2K3

Clientes Windows XP: 30 clientes

ID de Red: 192.168.52.0

Máscara de Sub Red: /24 = 255.255.255.0

Capacidad: 254 equipos IP

Gateway hacia Surquillo: 192.68.52.1

Interfase router Surquillo-San Juan

ID de interfase: 10.9.33.20

Máscara de interfase /29= 255.255.255.248

Velocidades de Conexión

Las subnets están interconectadas con líneas dedicadas alquiladas con la siguiente distribución de velocidades/anchos de banda:

- Surquillo – Sanjuán con ancho de banda de 256 kbps
- Surquillo – Lima con ancho de banda de 256 kbps
- Salida hacia Internet: a través del nodo surquillo con 1 mbps.

El proveedor de este servicio es la empresa TELMEX y es a base de fibra óptica

Controlador de Dominio y servidor de correo

Se tiene un solo controlador de dominio, es un equipo que tiene el Windows Server 2003 instalado, el cual también realiza las funciones de DNS interno y de servidor de correo.

- Está ubicado en la sede de Suquillo
- Contiene el directorio activo del dominio Relima.
- Realiza el servicio de **autenticación** de inicio de sesión de cada usuario de cada local del dominio ya sea Surquillo, San Juán ó Lima.
- Otra función importante de este servidor es mantiene las directivas de seguridad del dominio.
- Contiene ó aloja una copia del catálogo global de la empresa, por lo que hace las veces de servidor de catálogo global.
- Este servidor proporciona el servicio de correo electrónico Lotus Domino 7

Servidor de base de datos ORACLE

Este servidor es un servidor con W2K3 y es miembro del dominio Relima en el cual se ha instalado el motor de base de datos ORACLE y contiene la base de datos administrativa financiera soporte para las operaciones diarias de la empresa.

Servidor de Antivirus

Es un servidor con W2k3 Stand Alone, se emplea para bajar desde Internet las actualizaciones antivirus, para luego distribuirla a los equipos de la red. La instalación de estos parches es manual.

Servidor de Aplicaciones ORACLE

Contiene las aplicaciones a medida integradas a un sistema administrativo financiero denominado sistema NAF desarrollado en ORACLE 9i con la cual se gestiona la base de datos. Esta instalado en un servidor miembro con W2k3.

Servidor de desarrollo

Es un servidor de prueba con base datos y aplicaciones para el personal de soporte y desarrollo.

Servidor Web

Es un servidor miembro con W2K3, que esta ubicado en la zona perimétrica tipo bastion host con una dirección pública.

Dirección IP Pública: 216.244.152.88

Zona Perimétrica

La zona perimétrica de Relima es una zona ubicada detrás del filtro y delante del switch que acopla a los demás equipos de la red interna. En esta zona se tiene ubicado el servidor Web de Relima con una dirección pública 216.244.152.88.

3.3.2 Componentes lógicos de la Red Relima

La figura 3.1 muestra la estructura de dominio de la red Vega Upaca y está formado por los siguientes componentes lógicos:

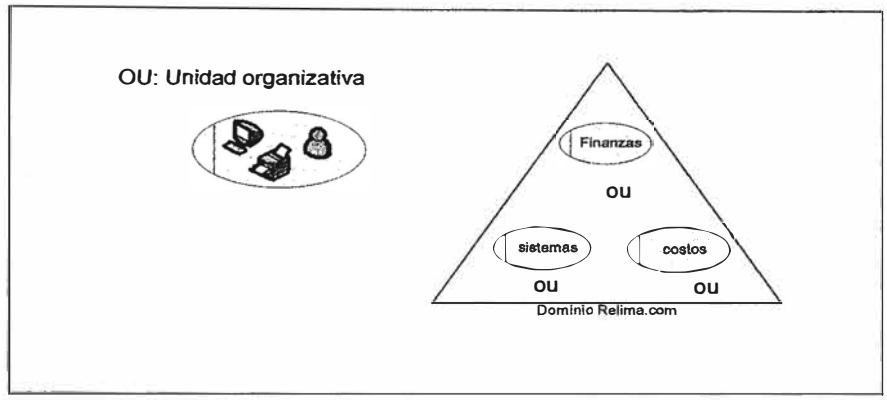

Figura 3.3 Estructura de dominio de la Red Relima

Sistemas operativos

Se emplea el Windows Server 2003 en la Versión Enterprice, el cual es una versión propia para medianas empresas. Su principal característica es su escalabilidad y puede soportar una gran carga de trabajo.

Dominios

Se opera con un solo dominio, denominado Relima.com.pe

Unidades Organizativas (OU)

Esta estructura de un solo dominio se complementa con la implementación de una serie de unidades organizativas (OU). Las principales OUs son:

Unidad organizativa Finanzas : contiene a todos los usuarios y recursos de finanzas

Unidad Organizativa Sistemas: contiene a todos los usuarios y recursos de sistemas

Unidad Organizativa Costos: contiene a todos los usuarios y recursos del área de costos

Arboles

Como la organización consta de un solo dominio se tiene un árbol lógico de un solo dominio principal que refleja la organización de la empresa.

Bosque

Se puede deducir que la estructura lógica consta de un solo bosque constituido por un solo árbol.

3.3.3 Aplicativos a medida

Dentro del sistema administrativo financiero (NAF) se integra los siguientes sistemas modulares:

- Sistema de Planillas
- Sistemas de contabilidad
- Sistemas de cuentas por cobrar
- Sistemas de cuentas por pagar
- Sistemas de administración de cheques
- Sistema de Facturación
- Sistema de costos

CAPITULO IV
IMPLEMENTACION DE SEGURIDAD EN CONEXIONES REMOTAS - RED RELIMA

4.1 Introducción

En este capítulo del informe proponemos una solución a los requerimientos planteados para la red Vega Upaca-Relima. Consideramos en esta solución la implementación de los siguientes componentes: implementación de seguridad utilizando un Firewall ISA, la publicación de servidores y la implementación de VPN. Nuestra solución considera la utilización del ISA Server 2004 como herramienta de seguridad, mas aún consideramos la utilización de dos servidores ISA en una situación back-to-back para efectos de implementar una DMZ para el acceso a sus servidores públicos de los usuarios desde Internet y desde la red interna.

4.2 Esquema de solución propuesta

En forma conceptual una solución de seguridad con el ISA Server como la propuesta puede aparecerse al esquema de la figura 4.1, se puede imaginar dos dispositivos como cajas a la cual se pueden conectar diferentes redes posibles de implementación (red interna, red perimétrica, red VPN, red de cuarentena, y la red Internet), soportando varias tarjetas de red cuya cantidad está limitada por el hardware del equipo servidor. Sin embargo nuestra solución se simplifica más abajo en la figura 4.2 con la utilización de dos tarjetas de red para cada servidor ISA, esta simplificación es posible debido a nuestra reagrupación de nuestras redes atacando a cada interfase de red. A esta distribución de los equipos se conoce como una configuración back-to-back de servidores como vimos en el capitulo II referente a configuraciones de redes perimétricas con servidores Firewall.

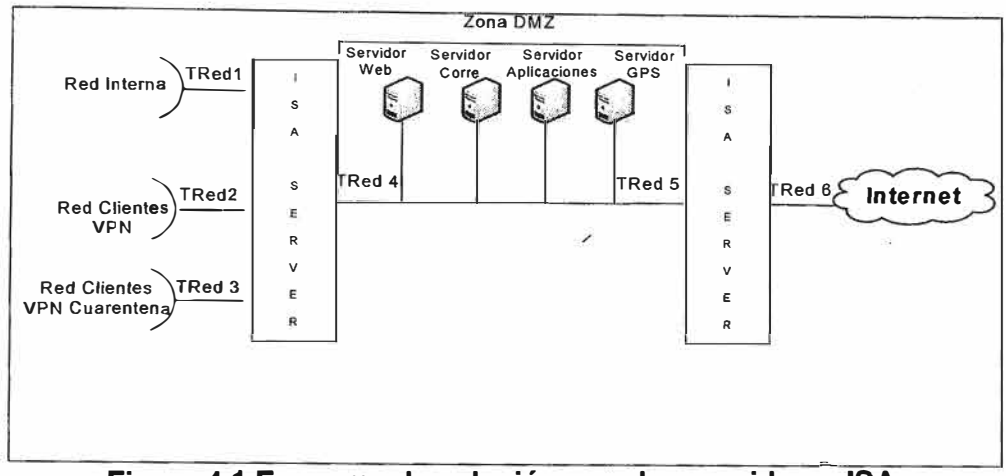

Figura 4.1 Esquema de solución con dos servidores ISA

4.3 Justificación de la solución back-to-back

- La exigencia de Relima impone reemplazar el Firewall actual por otro Firewall, ya que este tiene una configuración estática y dependiente del proveedor.
- El Firewall actual es un equipo que realiza filtrado de paquetes, y algunas funciones integradas de restricción de contenido como la detección de contenido de virus a nivel de páginas Web y de correo electrónico. Una ventaja importante del ISA respecto a los Firewalls tradicionales es su habilidad para filtrar la data de aplicación en los paquetes que entran y salen de la red. Esta característica es importante, la solución propuesta además de estas funciones nos proporcionará, filtrado a nivel de aplicaciones con lo que tendremos la capacidad de limitar el acceso a Internet teniendo en cuenta el tipo de página, el URL empleado y la detección de intrusos.
- Actualmente la publicación de recursos está limitada a mostrar la página Web de Relima como propósitos publicitarios de los servicios que ofrece la empresa.
- La interacción de información con la principal de Brasil no se da en línea, mediante la configuración propuesta se podrá acceder a otros recursos distintos del servidor Web, como el servidor de aplicaciones, el servidor de correo o el servidor de GPS.
- Estos accesos de recursos de la red de Relima por parte de la central de Brasil y demás usuarios remotos se realizarán mediante reglas de publicación de servidores que serán administradas a voluntad de Relima.
- Finalmente podremos realizar una **VPN site-to-site** que permitirá transferencia de información segura entre Brasil y Relima, y también una **VPN cliente-servidor** para ser utilizado por los usuarios remotos móviles.

4.4 Definiciones de redes y configuraciones de las interfases de los servidores ISA.

El esquema de la figura 4.2, presenta una distribución de la red Relima acorde a lo que queremos y que nos muestra una clara distinción de los diferentes componentes que intervienen en la solución, tenemos dos servidores ISA conocidos como front-end y back - end, una de las tarjetas de red del servidor front-end está conectado a Internet y un segundo adaptador está conectado a la red perimétrica. El servidor back-end tiene una tarjeta de red que está conectada a la red perimétrica y otra tarjeta de red conectada a la red interna. Todo el tráfico debe fluir a través de ambos servidores y a través de la red perimétrica para pasar desde Internet a la red iterna de Relima.

4.4.1 Definiciones iniciales

- El servidor ISA Back-End para nuestra solución lo implementamos como miembro del dominio Relima, para poder usar autenticación tanto para el administrador y para los clientes.
- El servidor ISA Front-End lo implementamos como miembro de un grupo de trabajo lo que nos permite aislar la red interna de los posibles ataques desde Internet.
- Asignamos los siguientes rangos de direcciones para las redes:

  Red Perimétrica = 172.16.1.0 – 172.16.1.255 Red Lima = 192.168.51.0

  Red Surquillo = 192.168.50.0 Red San Juan = 192.168.52.0

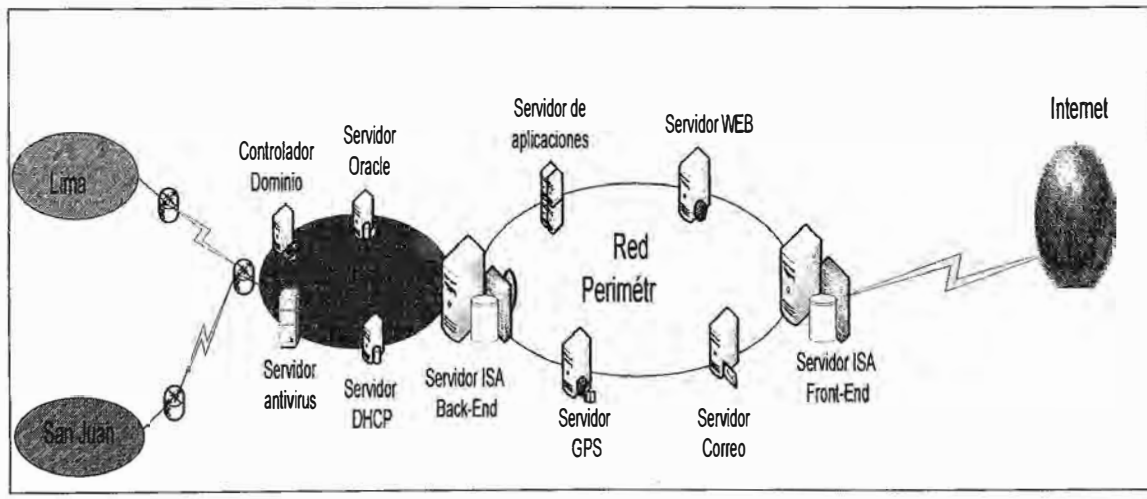

Fig. 4.2 Localización de redes y Servidores red relima

4.4.2 Definición de redes para los servidores ISA Back-End y Front-End

Definición de las redes en el servidor Back-End

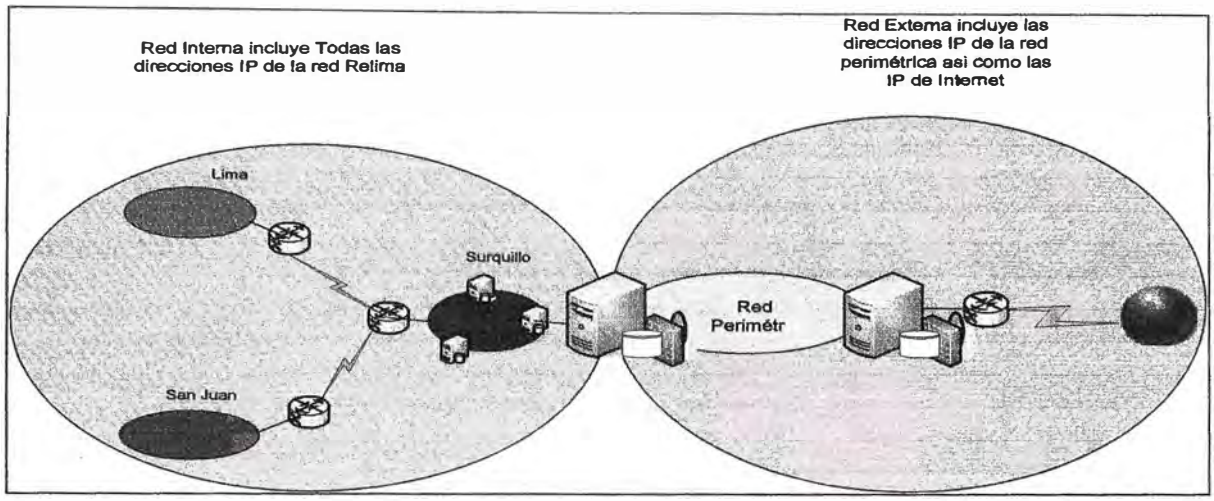

Figura 4.3 Definición de la Red interna y de la Red externa del servidor ISA Back-End

Red Interna: Estará formada por el segmento de Red de San Juan, segmento de Red de Lima y el segmento de Red central de Surquillo. Los componentes más importantes a tener en cuenta son los siguientes servidores localizados en el segmento de red de Surquillo.

Controlador de dominio (DC), el cual debe autenticar a todos los usuarios de la red y ejecuta el servicio de correo

Servidor DNS integrado al directorio activo instalado en el DC.

Servidor DHCP, para la asignación dinámica de IPs. con tres scopes definidos por los rangos de cada local.

Red Externa: La red externa para el servidor Back-End, estará formado por la red perimétrica y la red Internet, consideramos las siguientes direcciones IP:

Para la red perimétrica: 172.16.1.0 -172.16.255

Red Internet: dirección pública de la interfase externa 216.244.152.88

Definición de las redes en el servidor Front-End

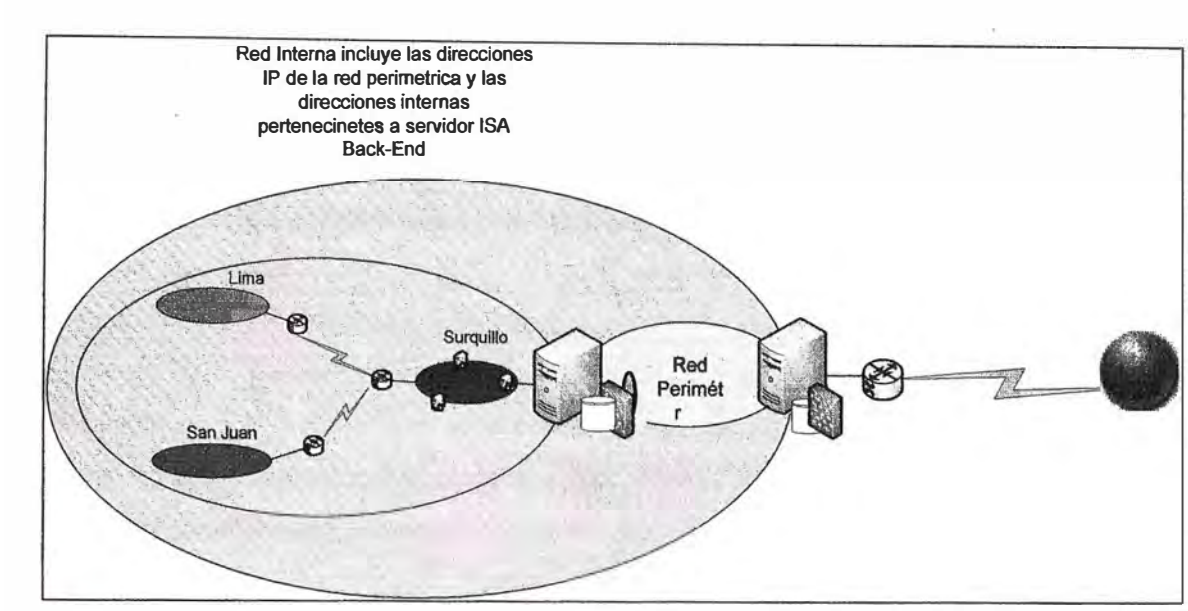

Figura 4.4 Definición de la red interna y de la Red Externa para el servidor Front-End

Red Interna: Para el servidor ISA Front-End la red interna estará formada por la red interna perteneciente al servidor Back-End (segmento de Red de San Juan, segmento de Red de Lima y el segmento de Red central de Surquillo) además de la red perimétrica.

Red Externa: La red externa para el servidor Front-End estará formado solo por las direcciones IP de Internet.

4.4.3 Configuración de interfases del Servidor Back-End.

Interfase interna del servidor Back-End

- Configuramos la interfase interna del ISA Back-End con una dirección IP correspondiente a una dirección privada del rango de direcciones de la red interna
  Para nuestro caso configuramos con la dirección IP= 198. 168.50.2
- Configuramos la interfase interna del ISA Back-End con una dirección del servidor DNS para que pueda resolver nombres de los equipos internos.
  Lo configuramos con la dirección del servidor interno DNS= 192.168.50.1 que es también la dirección del controlador de dominio.
- Configuramos sin default gateway.

Interfase externa del servidor Back-End

- La dirección para esta interfase debe corresponder a una dirección privada del rango de direcciones de la red perimétrica
  Para nuestro caso IP interfase externa= 172.16.1.1
- Tampoco debe tener default gateway

4.4.4 Configuración de interfases del Servidor Front-End

Interfase interna del servidor Front-End

- Usamos una dirección privada correspondiente al rango de direcciones de la red perimétrica.
  Para nuestro caso colocamos una dirección IP=172.16.1.2
- No debe tener default gateway
- Configuramos con la dirección del servidor DNS=192.168.50.1

Interfase externa del servidor Front-End

- Esta interfase debe tener una dirección IP pública provisto por Telnet, quien es el ISP de relima.
  Para nuestro caso considero la IP pública= 216.244.152.88
- Debemos asignarle un default gateway , esta dirección también lo proporciona el proveedor ISP–Telnet
  Para nuestro caso consideramos como default gateway=216.244.152.89
- Vamos a usar Proxy Server para resolver nombres de servidores cuando nos comunicamos a Brasil vía VPN , por lo tanto configuraremos la interfase externa con la dirección del servidor DNS de Brasil

4.5 Configuración del Servidor Front-End

4.5.1 Enrutamiento de tráfico desde el servidor Front-End a la red interna del servidor Back-End.

Creamos una tabla de enrutamiento estática en el servidor Front-End para poder alcanzar la red interna en el servidor Back-End desde el servidor Front-End, las entradas de esta tabla

apuntarán hacia los servidores internos detrás del servidor Back-End, es decir hay que realizar los siguientes pasos:

- Configuramos el servicio de enrutamiento con el RRAS instalado antes de instalar los servicios del ISA en el servidor Front-End.
- Creamos una tabla estática con entradas para cada servidor interno que se quiera acceder desde Internet.

Por ejemplo para acceder al servidor XX, la tabla debe contener la siguiente entrada:
IP Destino: IP de XX
Máscara: 255.255.255.0
Gateway: IP de la interfase externa del servidor Back-End
Interfase de Salida: IP de la interfase interna del servidor Front-End

4.5.2 Relaciones de Red (Reglas de Red):

Como estamos considerando direcciones IP privadas en la perimétrica, definimos una relación de traslación de direcciones entre la red perimétrica y la red Internet.
Red Perimétrica y Red Internet: relación NAT
Red Perimétrica: 172.16.1.0 – 172.16.1.255
Red Externa: Internet

4.5.3 Reglas de Publicación de Servidores para dar acceso a los servidores en la red perimétrica:

Voy a crear como ejemplo solo las reglas de publicación para el servidor web y el servidor de aplicaciones, para los demás servidores si hubiera se aplica el mismo procedimiento.

Como se ha definido una relación NAT entre la red perimétrica e Internet solo configuramos reglas de publicación para acceder a los servidores en la red perimétrica, no es necesario reglas de acceso de Firewall hacia la red perimétrica, para nuestro caso todas las conexiones desde Internet utilizarán la interfase externa del servidor Front-End.

4.5.4 Regla de publicación para el servidor WEB de Relima:

Configuramos una regla de publicación para permitir trafico http:
Acción: *permitir*
Nombre del Servidor Web a publicar : *Rel-Web*

Usuarios: *todos los usuarios de Internet van a acceder al servidor Web de Relima*
Red origen: Internet
Nombre Público del Servidor Web*: www.relima.com.pe*
Web Listener: *escuchamos las solicitudes de acceso en la interfase externa del Front-End usando el puerto 80.*

4.5.5 Regla de publicación para permitir el acceso a la red interna detrás del servidor Back-End.

Esta regla permitirá a los usuarios de Internet el acceso a los recursos internos desde el servidor Front-End.

Accion: Permitir
Destino: IP de la interfase externa del servidor Back-end
Origen: Internet
Tráfico: puede ser cualquier protocolo depende del servidor que se accede

4.5.6 Regla publicación segura para el Servidor de aplicaciones de Relima:

Para este caso vamos a utilizar una regla para el servidor de aplicaciones utilizando el protocolo SSL usando una conexión bridging entre el servidor back-end y el servidor de aplicaciones de relima.
Acción: permitir
Nombre del Servidor Aplicaciones:
Nombre público del servidor de aplicaciones:
Web Listener: creamos un listener en el puerto seguro 443
Usuarios permitidos: todos los usuarios de Internet

4.5.7 Regla publicación segura de acceso a los Servidores ubicados detrás del servidor Back-End dentro la red interna de de Relima:

Por asegurar el tráfico a través del tramo perimétrico vamos a utilizar conexión SSL bridging entre el servidor Front-End y el servidor Back-End para lo cual hacemos lo siguiente:

Habilitamos conexiones SSL en ambos servidores ISA
Instalamos certificados en ambos servidores ISA

4.5.8 Autenticación

Habilitaremos la autenticación de los usuarios en la red perimétrica solo para el servidor de aplicaciones usando RADIUS en el servidor Front-End, para poder hacer uso de las cuentas de usuarios del Active Directory del controlador de dominio de Relima.

4.6 Configuración del servidor ISA Back-End

4.6.1 Implementamos enrutamiento en el servidor Back-End

Considero la interfase interna del servidor Front-End como gateway para el servidor Back-End para efectos de enrutamiento desde este último servidor.

4.6.2 Implementamos la red perimétrica en el servidor Back-End

Para el caso de Relima la red perimétrica estará formado por direcciones privadas por lo tanto definimos una relación de enrutamiento entre la red interna y la red perimétrica. Esta relación de enrutamiento es necesario definirla ya que necesitamos comunicar los servidores de la red perimétrica con la red interna, por ejemplo el servidor de aplicaciones de la red perimétrica se comunica con el servidor de base de datos Oracle en la red interna.

Red Perimétrica: 172.16.1.0 – 172.16.1.255
Red interna: 192.168.50.0 -192.168.50.255
Red interna-Red Perimétrica: Relación de enrutamiento

4.6.3 Implementamos objetos de Red

Para efectos de optimizar la interacción de los servidores de la red perimétrica y la red interna creamos algunos objetos de red para los servidores de la red perimétrica y para la interfase interna del servidor Front-End:

Objeto WebRelima: asociado a la computadora servidor Web de Relima, para poder crear una regla de acceso solo del servidor Web desde el perímetro hacia la red interna.

Objeto ISAFront-End: asociado a la dirección interna del servidor Front-End. , este objeto para ser usado en la creación de reglas de acceso desde el servidor Front-End a los recursos de la red interna.

4.6.4 Acceso a la red perimétrica desde la red Interna

Para permitir el acceso a los servidores de la red perimétrica desde la red interna, creamos una regla de publicación o una regla de acceso para cada servidor que queremos acceder.

Ejemplo: creamos una regla publicación para acceder al servidor Web de relima desde la red interna

Acción: permitir

Tráfico: http

Nombre del Servidor Web: WebRelima

Nombre público del servidor : www.relima.com.pe

Web Listener: creamos un listener para escuchar en el puerto 80

Usuarios permitidos: todos los usuarios de la red interna

4.6.5 Acceso a los recursos de la red Interna desde la red perimétrica

Para acceder a los recursos de la red Interna desde la red perimétrica creamos reglas de acceso: por ejemplo para el servidor DNS interno

Acción: permitir

Tráfico: protocolo DNS

Origen: red perimétrica

Destino:red interna

condición: todo el día lunes a domingo

4.6.6 Acceso a los recursos de la red Interna para los usuarios de Internet desde el servidor Front-End.

Creamos una regla de publicación segura para permitir acceso a los recursos internos a los usuarios de Internet desde el servidor Front-End (ISA-01), esto es para cada servidor que se quiere permitir el acceso, es decir creamos una regla de publicación con la siguiente estructura:

Acción: permitir

Tráfico o protocolo permitido: depende que servidor queremos publicar

Tráfico Origen: para todos los casos será todos los usuarios desde la red Internet

Tráfico Destino: para todos los casos el destino será la interfaz externa del Back-End

Red de escucha: escucharemos todas las solicitudes en la interfase externa del servidor Back-End.

Schedule: para poder restringir los momentos en que se pueda acceder el servidor publicado.

4.6.7 Acceso a los controladores de dominio de la red interna desde los servidores miembros desde la red perimétrica.

Para permitir el acceso a los controladores de dominio ubicados en la red interna desde la red perimétrica configuramos una regla de acceso que permita el tráfico DNS, Kerberos-TCP, Kerberos-UDP, LDAP, LDAP UDP, LDAP GC. desde los servidores miembros hacia los controladores de dominio.

4.7 Implementación de VPN

Se puede realizar VPN de dos maneras: empleando el RRAS del Windows Server 2003 y el ISA Server 2004, especifico las configuraciones empleando el ISA Server 2004.

4.7.1 Implementación VPN usando el ISA Server

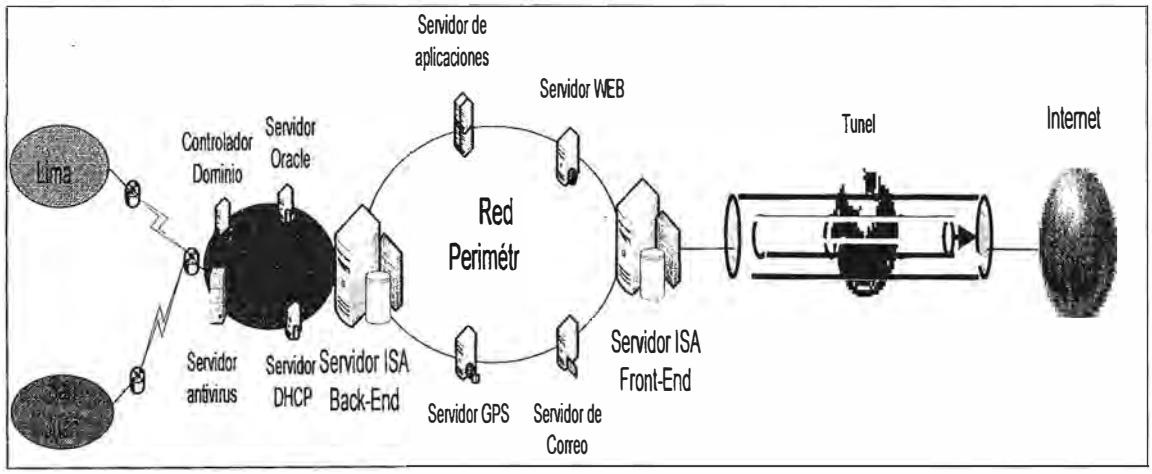

Fig. 4. 5 VPN con el ISA Server

a) Configuración del controlador de DOMINIO (DC)

1. Primero agregamos la cuenta de la computadora del ISA Server como miembro del grupo RRAS and IAS del active directory.

Agregamos la cuenta del **computador** Front End a la cuenta de grupo **RRAS and IAS** en el controlador de dominio de Relima

2. Luego configuramos en el Active Directory las cuentas de usuarios VPN para habilitar los permisos dial-in para estas cuentas. Si no se configuran estas cuentas no se podrá conectar al ISA Server usando VPN. Las opciones de configuración para estas cuentas lo hacemos en las propiedades dial-in de las cuentas para:

- **Denegar el acceso:** si habilitamos esta opción no se podrá realizar conexión remota aun si las políticas de acceso remoto establezcan lo contrario en el ISA Server.
- **Permitir el acceso:** si escogemos esta opción siempre se podrá realizar la conexión despreciando la configuración de permisos en las políticas de acceso remoto. La única manera de sobrescribir esta opción es mediante las configuraciones del profile de la política de acceso remoto.
- **Control de acceso a través de políticas de acceso remoto:** esta opción disponible solo en los dominios en el nivel funcional de Windows 2000 o Windows Server 2003.

Creamos una cuenta de grupo denominado **GVPN_Users_Relima**
Creamos cuentas de usuarios que van a realizar VPN: ejemplo **mbrandes**
Asignamos estas cuentas como miembros del Grupo GVPN_Users_Relima
En la propiedades **Dial_In** de la cuenta **mbrandes** seleccionamos **permitir el acceso**

b) Configuración del servidor ISA

1. **Configurar el ISA para habilitar el acceso para los clientes VPN:** por default el ISA no permite el acceso VPN. Se debe habilitar al ISA Server para utilizar una configuración de acceso por default. Esta configuración lo podemos modificar de acuerdo a nuestros propios requerimientos.

Desde el Isa Server Manager , de la opción **Virtual Private Network,** escogemos **Enable** VPN Client access.

2. **Configurar el acceso de los clientes VPN:**

- especificamos el número de conexiones VPN que permitiremos
- seleccionamos los grupos de usuarios que harán VPN

- Configuramos los tipos protocolos VPN que se va a usar: debemos escoger PPPT o L2TP/IPSec o podemos configurar ambos.

Desde el **Isa Server Manager**, de la opción **Virtual Private Network,** escogemos la opción **Configure** VPN Client Access
En esta pantalla especificamos:
Número de conexiones VPN simultáneas: **escogemos 10 conexiones**
Las cuentas de Grupo que harán VPN: escogemos **GVPN_Users_Relima**
Escogemos el protocolo VPN a usar para la conexión: **escogemos el PPTP**

3. Configurar las propiedades de la conexión VPN:

- debemos indicar desde que red se van aceptar o escuchar las conexiones provenientes de los clientes VPN.
- Escoger el método de asignación de direcciones a los clientes VPN bien DHCP (desde una red interna, perimétrica o externa) o direccionamiento estático proporcionado por el mismo ISA.
- y las opciones de autenticación disponibles para los clientes VPN: MS-CHAP v2, EAP-TLS, etc.
- seleccionar el mecanismo usado en la autenticación ya sea autenticación basado en Windows usando el Active Directory o usando Radius. Para estos últimos usuarios que no soportan autenticación Windows podemos emplear el mapeo.

Desde el **Isa Server Manager**, en las propiedades de la opción **Virtual Private Network** configuramos:
La opción **Red Externa** como la red desde la que se escucharán en el ISA las solicitudes de conexión de los clientes VPN
Escogemos el **método asignación denámica de direcciones IP** (DHCP), desde un servidor interno de Relima.
Escogemos como **método de autenticación el MS-CHAPV2,** y utilizamos el active directory para este fin., no usamos Radius.

4. Configurar reglas de acceso de red:

Configuramos reglas de red para definir las relación de red entre la red clientes VPN y las redes interna o externa.

Por default cuando instalamos el ISA Server se crean 02 reglas de red:

- Una que especifica una relación de ruteo entre la red de clientes VPN y la red interna
- Otra regla que especifica una regla de NAT entre la red de clientes VPN y la red externa o Internet.

5. Configurar las reglas de acceso de Firewall para los clientes VPN:

Si no existe una regla de acceso en el ISA, ningún cliente VPN podrá tener acceso a la red interna, por lo debemos crear una regla de acceso que habilite este acceso o podemos escoger una plantilla de red disponible en el ISA para configurar la regla. Si escogemos una plantilla se crea automáticamente una regla denominada **VPN Clients to Internal Networks.** Escogemos esta regla la cual permite el acceso desde la red de clientes VPN a la red interna usando todos los protocolos.

También esta regla permite el acceso a Internet desde la red de clientes VPN.

6. Política de acceso Remoto:

Por default se crea una política de acceso remoto denominado **ISA Server Default Policy** en el RRAS. Esta política deniega el acceso a todas las conexiones excepto a aquellas explícitamente permitidas por las propiedades de las cuenta en **Dial_in** o por el **profile** de acceso remoto.

Nosotros hemos habilitado de forma explícita el acceso en la cuenta del cliente VPN en el Active Directory por lo que esta política es socreescrita y nuestra conexión VPN será permitida.

c) Configuración de las computadoras Clientes VPN

1. Configurar la la computadora cliente con una dirección estática cualquiera del ámbito del ISA.
2. Crear una conexión VPN nueva mediante el asistente de conexión nueva del Windows.

- Debemos especificar un nombre para la conexión que puede ser el nombre de la compañía a la cual vamos a conectarnos mediante VPN

- Desde el Control Panel-network and Internet conections-create a connection to the network at your workplace escogemos la opción : **Virtual Private Network** y colocamos el nombre de la conexión: **Conexión_VPN Relima.**
- Indicamos el nombre HOST o la dirección IP del servidor de acceso en este caso del ISA Server.

  Colocamos la dirección del ISA Server externo como **216.244.152.88** que es una dirección pública

3. Si vamos a utilizar VPN PPTP debemos proporcionar las credenciales de usuario o sea el user name y el password. Si vamos a utilizar VPN L2TP/IPSec debemos instalar un certificado de cliente en la computadora cliente o configurar una clave preshared.

CONCLUSIONES

- La solución back-to-back es uno de los más complicados escenarios de implementar con el ISA Server, sin embargo, el entendimiento de los pormenores de este escenario proporciona al profesional la ventaja de poder implementar los servidores ISA en cualquier escenario u otras configuraciones exigidas que se le presente en el campo laboral.

- Así de esta manera la solución en el fondo pretende ser una solución flexible, en el sentido de que bajo el mismo esquema back-to-back podemos reemplazar el servidor front-end por el Firewall actual y seguir el mismo procedimiento de implementación.

- Se presenta la solución completa con dos servidores ISA por que de esta manera se obtiene centralización de la administración e independencia del mantenimiento de la red para el futuro. De otra manera, cada modificación a las configuraciones emergentes se tendría que solicitar la apertura de algunos puertos del Firewall actual por el proveedor externo, ya que actualmente solo sólo se tiene disponible el puerto 80 para el acceso a la página Web de relima.

- Estamos considerando el uso de la versión Stándard del ISA Server en la solución, sin embargo todo el procedimiento es también aplicable a la versión Enterprise del ISA Server que es recomendado como prototipo para este tipo de aplicaciones por las literaturas especializadas.

- El costo ni los tiempos de implementación es considerado en el presente trabajo, por que está enfocado a demostrar técnicamente que la solución presentada satisface los requerimientos planteados por Relima. Sin embargo indico que el costo del producto ISA Server 2004 en la versión estándar está alrededor de los 4500 dólares, podría implementarse por etapas. En una primera etapa implementar el servidor front-end para

aprovechar las virtudes del ISA Server como Firewall, y como servidor de acceso en una VPN y gradualmente ir migrando a la solución completa.

- Para las pruebas de este trabajo se puede utilizar el producto Virtual PC de Microsoft, herramienta que permite simular toda una infraestructura de red en una sola PC bajo Windows XP como software base.

- Se indica que para la simulación de esta solución, se necesita una computadora con una RAM mínima de 2 GigaBytes y un disco con un mínimo de 80 GigaBytes, para que las máquinas virtuales que se creen puedan correr simultáneamente en la misma PC. Hay que crear las siguientes máquinas virtuales en la PC:

    - 02 Servidores ISA con Windows Server 2003 instalado
    - 01 Controlador de dominio Windows Server 2003 instalado
    - 01 Servidor DHP Windows Server 2003 instalado
    - 01 Servidor WEB con Windows Server 2003 instalado
    - 01 Servidor aplicaciones Windows Server 2003 instalado
    - 01 servidor de Base datos Windows Server 2003 instalado
    - 01 máquina cliente Windows XP

ANEXO A

IMPLEMENTACIÓN VPN USANDO UN SERVIDOR RRAS

Para implementar una VPN con el RRAS debemos realizar una serie configuraciones en la computadora cliente VPN, computadora controladora de dominio (DC) y el computador servidor de acceso ejecutando el servicio RRAS.

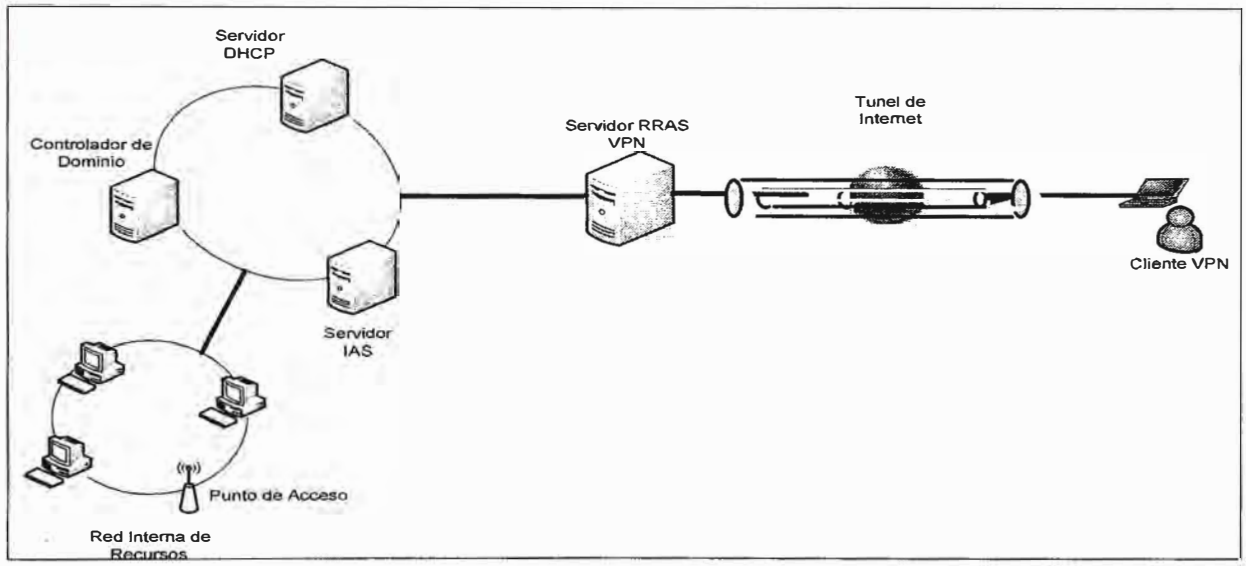

Figura 4. VPN con RRAS

a). Computador Controlador del Dominio (DC)

- Debemos tener instalado en la base de datos del Active Directory la cuenta del cliente a realizar VPN

Creamos una cuenta de grupo denominado **GVPN_Users_Relima**

Creamos cuentas de usuarios que van a realizar VPN: ejemplo **mbrandes**

Asignamos estas cuentas como miembros del Grupo GVPN_Users_Relima

- Configurar las propiedades Dial-in de la cuenta para permitir el acceso remoto.

b). Computador servidor de acceso VPN (RRAS)

- Seleccionamos la tarjeta de red a través del cual nos conectamos a Internet.

- Configuramos el servidor para ser un servidor VPN a través de la tarjeta/conexión seleccionado en el paso anterior.
- Especificamos como se va asignar las direcciones IP a los clientes VPN bien a través de DHCP o a través del mismo servidor VPN mediante direcciones estáticas
- Seleccionamos también las cantidad de conexiones concurrente VPN. En el caso de que se asigne las direcciones en forma estática el núumero de conexiones debe ser la misma que el pool de direcciones estáticas.

c) Computador Cliente VPN

- Componer/crear una conexión VPN, mediante el asistente para crear una nueva conexión del Windows.
- Al crear la conexión nueva debemos especificar:
    - La compañía a la cual vamos a conectarnos mediante la VPN.
    - El nombre o la dirección IP del servidor RRAS de la compañía.

Establecimiento de una VPN con políticas de acceso remoto costomizado

a) Configuramos la base de datos del servidor controlador de dominio

- Creamos cuentas de grupo de dominio para incorporar todas las cuentas de los clientes VPN.

b) Configuramos el RRAS

- Especificamos el grupo al que vamos a aplicar esta política (es decir el grupo creado en el paso anterior)
- Especificamos el método de autenticación de estos usuarios.(MS-HAP, MS-HAP V2)

ANEXO B

PUERTOS Y PROTOCOLOS

La cabecera de los paquetes en cada uno de los niveles del modelo de referencia OSI contienen los identificadores que especifican el protocolo del siguiente nivel que debe recibir el paquete. Por ejemplo, los protocolos del nivel de enlace de datos, tal como Ethernet, incluyen un valor **Ethertype** en su cabecera que especifica qué protocolo del nivel de red deberá procesar el paquete. De la misma forma, a nivel de red, el protocolo de Internet (IP) dispone de un campo denominado **Protocol**, que especifica el protocolo de nivel de transporte que deberá recibir el paquete, y cada protocolo del nivel de transporte dispone de un campo **Port** que especifica la aplicación que va ha ser la destinataria final de los datos contenidos en el paquete.

Los valores de los campos **protocolo y puerto TCP** son asignados por un cuerpo administrativo denominado Internet Assigned Numbers Authority (IANA). Las aplicaciones de servidor más utilizadas suelen tener asignados los números de puertos de forma permanente ; a estas asignaciones se les conoce por **puertos bien conocidos**. Los clientes se suelen conectar a un servidor utilizando un número de puerto elegido de forma aleatoria y utilizando únicamente el tiempo que dura la transacción ; es lo que se denomina **puerto efímero.** La tabla 1 muestra algunos de los puertos utilizados mas frecuentes.

Tabla 1 Números de puertos bien conocidos (especifican la aplicación)

Aplicación	Abreviatura	Protocolo	Número puerto
Protocolo de Transferencia de Archivos (control)	ftp-control	**TCP**	**21**
Protocolo de Transferencia de Archivos (datos predeterminados)	ftp-default data	**TCP**	**20**
Telnet	TCP	**TCP**	**23**
Potocolo Simple de transferencia de Correo	smtp	**TCP**	**25**
Servicio de Nombres de Dominio	DNS	**TCP**	**53**
Protocolo de Configuración Dinámica del Host (server) Bootstrap protocol server (nondynamic)	Dhcps bootps	**UDP**	**67**
Protocolo de Configuración Dinámica del Host (cliente) Bootstrap Protocol Client (nondynamic)	Dhcpc bootpc	**UDP**	**68**
World Wide Web http	http	**TCP**	**80**
Protocolo de Oficina de Correo Version 3	Pop3	**TCP**	**110**
Servicio sesión NetBios	netbios	**TCP**	**139**
Protocolo simple de Administración de Red	snmp	**UDP**	**161**
Trampa de Protocolo Simple de administración de Red	snmptrap	**UDP**	**162**
Secure Sockets Layer	ssl	**aplicación**	**443**
Red Privada Virtual	vpn	**PPTP**	**1723**
Asistencia Remota	rass	**TCP**	**3389**

Tabla 2. Códigos de Protocolo

Protocolo	Código de Protocolo
Protocolo de Internet (IP, Internet protocol)	**0**
Protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol)	**1**
Protocolo de Control de Transmisiones (TCP, Transmisión de Contro, Protocol)	**6**
Protocolo de datagrama de usuario (UDP, User Datagram Protocol)	**17**
Encapsulación de enrutamiento genérico (GRE, Generic Routing Encapsulation)	**47**

Tabla 3. Componentes de paquetes TCP/IP

Network Interface Layer	Destination Address: 0003FFD329B0 Source Address:0003FFFDFFFF	Physical payload
Internet Layer	Destination:192.168.1.1 Source:192.168.1.10 Protocol:TCP	IP payload
Transport Layer	Destination Port: 80 Source: 1159 Secuence: 3337066872 Acknowledgment: 2982470625	TCP payload
Application Layer	HTTP Request Method: Get HTTP Protocol Version:=HTTP/1.1 HTTP Host=www.Relima.com	

ANEXO C

MÉTODOS DE AUTENTICACIÓN

Existen los siguientes métodos de autenticación para las conexiones remotas e inalámbricas:

CHAP. (challenge handshake auntentication protocol)

- Proporciona a three-way handshake en el cual el password del usuario jamás es enviada a través de la red.
- Es usado por varios proveedores de servidores y clientes de acceso remoto.

PAP. (Password Autentication Protocol)

- Utiliza passwords en texto plano y es el protocolo de autenticación menos sofisticado.

SPAP. (Shiva Password Autentication Protocol)

- Es un protocolo simple de autenticación de passsword encriptado

MAS-CHAP. (Microsoft Challemge Handshake Autentication Protocol)

- Usado por las versiones de Windows 95 para adelante
- Soporta solamente clientes Microsoft

MS-CHAP v2. (Microsoft Challemge Handshake Autentication Protocol version 2)

- proporciona autenticación mutua
- Es el método de autenticación por default en el Windows 2000 hacia adelante.
- Proporciona two-way y autenticación mutua

EAP–TLS. (Extensible Autentication Protocol - Transport Layer Security (EAP-TLS)

- proporciona autenticación mutua
- Requiere una infraestructura de certificados smart cards
- Proporciona el más alto nivel de seguridad de autenticación.

PEAP. (Protected Extensible Autenticación Protocol)

- Usado para las conexiones inalámbricas , estándar 802.1x
- El acceso es asignado basado en la identidad del usuario
- Incrementa la seguridad de la redes inalámbricas encriptadas

BIBLIOGRAFIA

1. TEXTOS

- Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
  MCSA/MCSE: GUIA DE ESTUDIO OFICIAL DE CERTIFICACION
  Autores: J.C Mackin, Ian MacLean

- Seguridad en Redes Telemáticas
  Autor: Justo Carracedo Gallardo
  Universidad Politécnica de Madrid

- Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
  MCSE GUIA: DE ESTUDIO OFICIAL DE CERTIFICACION
  Autor: Craig Zacker

2. MANUALES

- Microsoft Official Course 2830: Designing Security for Microsoft Networks.

- Microsoft Official Course 2823B: Implementing and Administering Security in a Microsoft Windows Server 2003 Network

- Microsoft Official Course 2824: Implementing Microsoft Internet Security and Acceleration Server 2004

- Microsoft Official Course 2277: Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure: Network Services