IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES EN LA MEDIANA EMPRESA

IMPLEMENTATION OF VIRTUAL PRIVATE NETWORKS IN THE MEDIUM ENTERPRISES

WINSTON ALBEIRO BARBOSA[1]
DUILIO BUELVAS P.[2]

RECIBIDO: JULIO 2010
APROBADO: OCTUBRE 2010

RESUMEN

en este documento se presenta la información y consideraciones pertinentes para la implementación de redes privadas virtuales en la mediana empresa colombiana, como herramienta de evolución a la medida de las distintas tecnologías de conexión, que posibilitan alcanzar mejores formas de compartir los servicios y recursos disponibles, manteniendo la integridad de la información, y permitiendo de este modo la expansión de las organizaciones al amparo de una perspectiva de bajo costo económico.

Palabras clave
herramienta, implementación, red privada virtual, seguridad, *firewall*

Abstract
This paper presents information and relevant considerations for implementing virtual private networks in employment practices, as a tool to measure progress of the various connection technologies, which allow to achieve better ways of sharing facilities and resources available, maintaining the integrity of the information thus allowing the expansion of organizations under a low economic cost perspective.

Key words
tools, implementation, virtual private network, security, firewall

1. INTRODUCCIÓN

La evolución constante de las tecnologías de conectividad ha traído una rápida propagación de las telecomunicaciones en todos los niveles de la actividad empresarial, y como consecuencia de ello, el desarrollo de nuevos servicios, e incluso nuevas formas de plantear el trabajo habitual. Para la mediana empresa no resulta inmediato ni fácil poder

1. Tecnólogo electrónico de la Universidad Distrital Francisco José de Caldas, Facultad Tecnológica. Lugar de trabajo: Universidad Distrital Correo electrónico: Winston_barbosa@hotmail.com

2. Ingeniero electrónico de la UAC. Especialista en soluciones telemáticas de la UAC. Magíster en Teleinformática de la Universidad Distrital. Lugar de trabajo: Universidad Distrital. Correo electrónico e-mail: dbuelvas10@gmail.com

incorporar a su estructura organizacional nuevas agencias ubicadas en distintas áreas geográficas a la red. El costo de los equipos, el alquiler de canales dedicados, y la administración de los recursos para hacer realidad una infraestructura de esta magnitud, hacen que esta sólo esté al alcance de un pequeño grupo de grandes corporaciones.

Sin embargo, las ventajas competitivas en la actividad empresarial que conllevan las facilidades tecnológicas que se implementen, no se reducen a obtener un mejor rendimiento del trabajo habitual. Además, posibilitan centralizar la información, realizar pedidos, facturar, y consultar inventarios, agilizando con ello los procesos que forzosamente se trasladarán a los clientes, a los que se podrá responder inmediatamente. Al integrar herramientas de comunicación y seguridad como las redes privadas virtuales (VPN) y los *firewall* en el desarrollo y la expansión de la mediana empresa, utilizando Internet como canal de comunicación para todo tipo de propósito, se pretende solucionar un tema de competitividad que debería diluir los problemas técnicos y económicos que limitan la expansión de la mediana empresa, a través de la construcción de nuevas agencias.

1.1. POR QUÉ VPN Y FIREWALL

Aunque Internet es el medio ideal para poder conectar distintos sistemas entre sí con sus usuarios, estén donde estén, de forma económica y con total flexibilidad, su propio planteamiento lleva implícita la característica de "público", sinónimo de inseguro.

Esta circunstancia hace que se deba cambiar el escenario y utilizar herramientas que suplan y complementen de manera eficiente el proceso de transmisión de datos por la red pública. Es de este modo que aparecen las VPN y los *firewall* como canales apropiados para el transporte y el aseguramiento de la información, junto con la protección de la organización del mismo Internet.

Por otra parte, la implementación en la mediana empresa de soluciones que contemplen seguridad tanto de la red de datos como del transporte de estos por la red pública de Internet, reduce notoriamente el costo que implicaría arrendar canales dedicados, provistos por empresas prestadoras de servicios, y solucionar pérdidas de información por violaciones de seguridad de la red interna.

2. ENTORNO DE IMPLEMENTACIÓN

Definir un entorno común para la mediana empresa resultaría desgastante, teniendo en cuenta la cantidad de actividades comerciales existentes, pero el desarrollo de su actividad siempre busca la expansión y el posicionamiento de su marca dentro de un área geográfica, sea esta una ciudad, un departamento, el país y más. Este crecimiento, en la mayoría de las oportunidades se encuentra ligado a la oportunidad, la legislación y los ciclos económicos. En ese punto es cuando la organización inicia el proceso para determinar qué herramientas va a utilizar y determina los costos operativos de esas soluciones. Generalmente, se inicia con un acceso a Internet para efectos de comunicación, y en consecuencia, un *firewall* que asegure la integridad de la red interna frente a ataques externos, administrando de paso este recurso.

Seguido y con base en el tipo de expansión que la mediana empresa busca, se presentan alternativas de comunicación en las cuales se arrienda un servicio (canales dedi-

cados) o se implementa una solución de redes privadas virtuales (VPN). La definición de dicho medio de comunicación se basa en el costo, la eficiencia, la calidad de servicio que estas redes aporten, no sin antes advertir las particularidades propias de ubicación geográfica de las agencias.

2.1 INTERNET SECURITY AND ACCELERATION SERVER - ISA (2004)

Por definición, un cortafuego (*firewall*) es un dispositivo diseñado para bloquear el acceso no autorizado, cifrando el tráfico, permitiendo al mismo tiempo comunicaciones autorizadas, sobre la base de un conjunto de normas y políticas establecida por la organización [1].

La figura 1 presenta la topología de un *firewall* basado en el modelo de solución planteado para la herramienta Microsoft Internet Security and Acceleration Server 2004 de Microsoft® [2], [3].

ISA Server es una de las tantas herramientas que existen en el mercado que se utilizan como *firewall* de seguridad en las empresas. Por pertenecer a la familia de Microsoft es de las más usadas y conocidas.

2.2 . CONFIGURACIÓN

Para controlar el acceso a Internet, el equipo servidor ISA debe actuar como puerta de enlace predeterminada a Internet. De no ser así, los equipos de la red pueden tener acceso a Internet a través de otra puerta de enlace sin necesidad de pasar por el equipo servidor ISA.

ISA Server funciona a través del uso de reglas y elementos de regla, con los cuales se definen las políticas de seguridad a imponer en su operación.

La autenticación en ISA Server afecta a todos los equipos, usuarios y servicios que requieran acceso a Internet. Independientemente del tipo de cliente, cuando el servidor ISA recibe alguna petición HTTP [13], al cliente se lo trata como si fuera un cliente *proxy web* [2], [3].

2.3. ELEMENTO DE REGLA Y REGLAS DE ACCESO

Tanto los elementos de regla como las reglas de acceso hacen parte de las directivas del *firewall*. Los elementos de regla indican o definen protocolos, usuario, tipos de contenido, programaciones y objetos de red. Las reglas de acceso determinan la forma en que

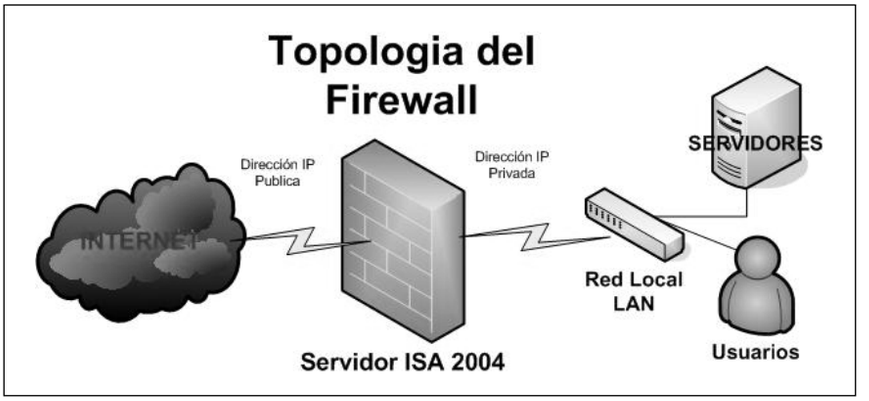

Figura 1. Topología de un firewall

los clientes de una red de origen pueden tener acceso a los recursos de una red de destino. Utilizan los elementos de regla para su operación, y por ende se configuran de modo que se pueda aplicar a todo el tráfico IP a un conjunto determinado de definiciones de protocolo y a protocolos seleccionados.

2.4. CONTROL DE ACCESO CON ISA SERVER 2004

Existen cinco entornos posibles que de forma individual o en conjunto permiten controlar el acceso a Internet por medio del *firewall* [1], [2], [3] :

Control de acceso por programación y conjunto de usuarios.
Acceso controlado por una entidad de red.
Acceso controlado por la autenticación.
Acceso controlado por el tipo de contenido.
Acceso controlado por una programación.

Cada control se caracteriza por una propiedad de análisis para su uso. Es así como se puede utilizar un horario de servicio para ciertos usuario del servicio, un grupo dentro de la red, una autenticación por usuarios, un acceso limitado a cierto contenido, o restricción de cierto contenido, y por último, una programación específica de protocolos y contenidos en función de un servicio.

2.5. DIRECTIVAS DE FIREWALL

De acuerdo con el control de acceso que se quiera ejercer, se definen las políticas de *firewall*; estas deben contar con el aval del departamento administrativo o de tecnología, y son en su mayoría de carácter restrictivo, con el fin de optimizar el uso de los recursos. Como ejemplo, a continuación se listan algunas políticas generales, tanto de acceso como de restricción, creadas para un servidor ISA:

- Permitir acceso a internet utilizando servidor ISA: permite todos los protocolos a las redes internas; incluye clientes VPN.

- Denegar todo el tráfico IP hacia Internet desde un conjunto de direcciones IP internas; incluye todos los protocolos y solo debe permite acceso a la página web de la organización.

- Permitir el acceso http del equipo servidor ISA a las páginas publicadas en él por uso de Internet Information Server (IIS); caso común de las entidades emisoras de certificados corporativas.

- Permitir todo el tráfico saliente y entrante de los clientes de VPN, con lo cual se busca permitir la comunicación de los clientes de VPN con los *host* de la organización, habilitando de paso el uso de puertos PPTP y L2TP.

- Negar todo el tráfico saliente a sitios prohibidos, si es el caso Messenger, YouTube, hi5, Facebook, páginas web de ocio y pornografía.

- Permitir la publicación de certificados digitales para la autenticación de clientes de VPN.

- Bloqueo de audio y video: niega el audio y el video a través de protocolos http, https y FTP [13]; aplica para la red local y agencias que estén detrás del servidor *firewall*. Se habilita para optimizar el uso del canal de Internet.

Al determinar las políticas de seguridad dentro del servidor Isa Server solamente se

logra asegurar la red interna. Es claro que esta herramienta proporciona muchas facilidades para hacerlo, y quien lo administra puede cambiar con facilidad las políticas adicionando más según sea su necesidad [1].

2.6. SEGURIDAD A ATAQUES EXTERNOS

Para el eventual hecho de que se realicen ataques externos, el servicio Isa Server proporciona un mecanismo para determinar cuándo estos se están produciendo. ISA Server compara el tráfico de red con registros y patrones de ataques bien conocidos. En el momento en que un ataque es reconocido se genera una alerta y se bloquea el tráfico del punto de origen (dirección IP) del atacante, por espacios de tiempo aleatorios de cinco a sesenta minutos, según sea la concurrencia del ataque [4].

A continuación se relacionan los ataques reconocidos por ISA Server: ataques Winnuke, ataques tipo Land, ping de la muerte, ataques Half-Scan, bombas UDP, escaneo de puertos, desbordamiento de nombres de HOST sobre DNS, desbordamiento de longitud DNS, control de trasferencias de zona.

2.7. RECOMENDACIÓN

Ahora bien, el hecho de que el fabricante (Microsoft®) manifieste que la red, mediante el uso de esta herramienta, se encuentra asegurada, debe ser comprobado, para lo cual existen métodos gratuitos que pueden ayudar a este efecto y determinar que tan seguro es el *firewall*. Entre los más comunes se encuentran los siguientes [4]:

- Nmap (escaneado de puertos).
- John The Ripper (ataque de diccionario).
- Hping (ataque de denegación de servicios).
- Ataque de NetBios.
- Snort IDScenter (escaneado de paquetes).
- Nessus (escaneado de puertos).
- TSGrinder (ataque de diccionario).
- Smurf (ataque de denegación de servicios).

3. CONFIGURACIÓN DE LA RED PRIVADA VIRTUAL (VPN)

Para realizar configuraciones de VPN en la mediana empresa se deben tener en cuenta las configuraciones posibles; estas se dividen en dos grupos (conexiones VPN de acceso remoto y conexiones VPN de sitio a sitio) [2], [3].

Las conexiones VPN de acceso remoto hacen referencia a un cliente que realiza una VPN conectándose al servidor de Firewall, para este caso ISA (Internet Security and Acceleration Server), que se encarga de proporcionar acceso a toda la red a la que está

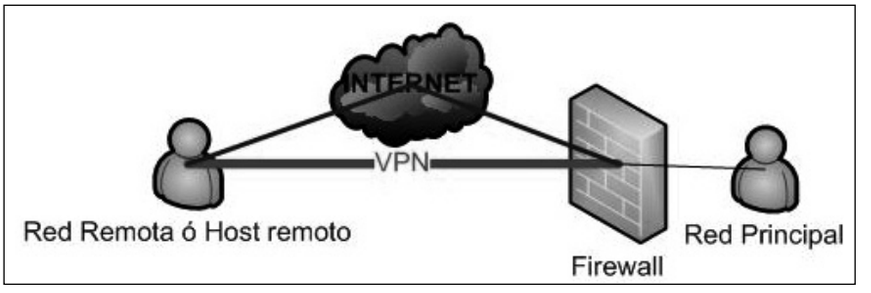

Figura 2. Conexión de host remoto VPN / Internet

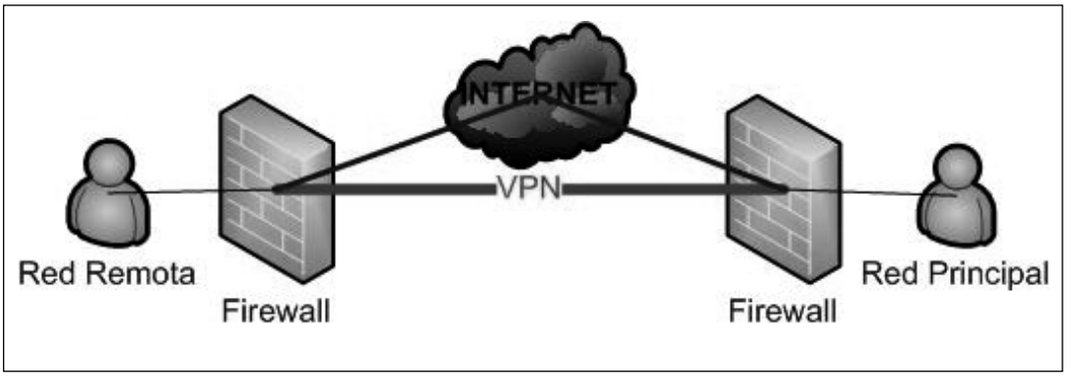

Figura 3. Conexión de sitio a sitio

conectado el servidor VPN, como se presenta en la figura 2.

La conexión VPN de sitio a sitio permite conectar dos partes de una red privada. El servidor de firewall (ISA) proporciona una conexión a la red a la que está conectado el equipo servidor, como se presenta en la figura 3.

3.1. IMPLEMENTACIÓN DE CANALES VPN

Para la mediana empresa generalmente se utilizan soluciones de entorno de VPN de acceso remoto, dado que en su mayoría, las agencias no cuentan con una infraestructura de gran tamaño para optar por otra solución. Este tipo de implementación funciona de forma correcta y concede una buena calidad de servicio. Sus requerimientos son relativamente económicos y se listan a continuación [2], [3]:

- Acceso a internet (agencias y oficina principal).
- Servidor de puerta de enlace implementado con ISA Server 2004.
- Controlador de dominio (Windows 2000 Server o superior) para autenticación de usuarios.
- Servidor DHCP [13]: que asigna dinámicamente direcciones IP a los clientes de VPN.
- Entidad emisora de certificados (CA), que se utiliza para la solución L2TP/IPsec.
- Equipos cliente con Windows XP o superior; existe soporte para clientes con Linux.
- Con base en los requerimientos y el modelo de conexión VPN de acceso remoto, en la figura 4 se presenta el diagrama topológico que tomaría la red [5].

3.2. SEGURIDAD PARA LOS CANALES VPN

Como parte de la seguridad de los canales VPN, se debe tomar en consideración cada actor que compone la solución principalmente: los usuarios, los protocolos que se pueden usar (PPTP - Point-to-Point Tunneling Protocol [6], L2TP- Layer Two Tunneling Protocol "L2TP" [7], e IPsec – Internet Protocol Security [8], [9]), junto con los certificados de autenticación X.509 emitidos por la entidad emisora de certificados o PKI (Public Key Infrastructure) [10].

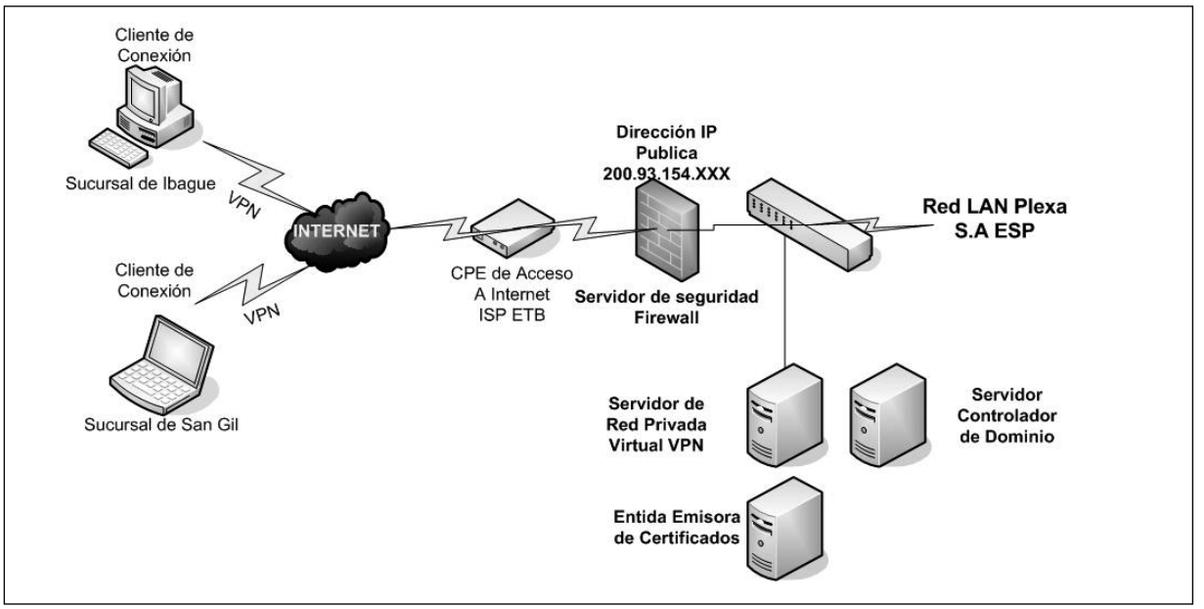

Figura 4. Topología a implementar

Los usuarios, deben ser creados dentro del dominio utilizando el directorio activo o LDAP (Lightweight Directory Access Protocol) [13], a fin de referenciar el uso de estas cuentas dentro de la red y utilizar la política de seguridad para las claves de acceso (longitud, mezcla de caracteres, uso de símbolos, restricción de secuencias lógicas, entre otros).

Para realizar las conexiones VPN existen diferentes protocolos. Los más utilizados son PPTP, L2TP e IPsec nativo y L2TP sobre IPsec; para los últimos existe la necesidad de implementar una entidad emisora de certificados (CA), con el fin de poder operar bajo sus dos modos (transporte y túnel), tal y como se muestra en la figura 5.

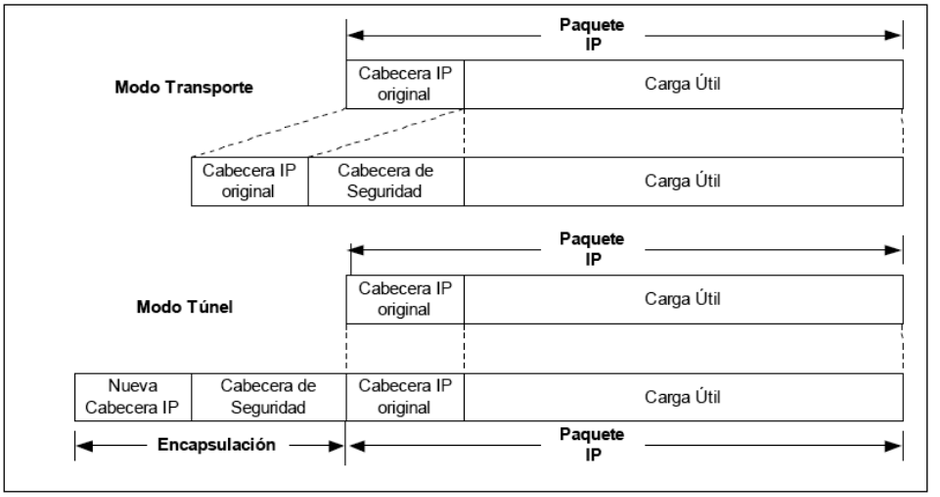

Figura 5. Modos de operación de IPsec

Los certificados se destinan únicamente para uso interno (a fin de que los utilicen sus servidores y clientes de VPN). En el proceso de instalación de la entidad raíz de servicios de certificate server, se genera un certificado de CA raíz que contiene: la clave pública y la firma digital de la CA (creada utilizando la clave privada de la raíz). Toda esta documentación se rige bajo el estándar para certificados X.509. El uso de este tipo de certificado permite los modos de operación para IPsec en túnel o transporte, y son la mayor ventaja frente al uso de los otros protocolos mencionados (PPTP y L2TP).

3.3. CONFIGURAR UNA VPN EN EL SERVIDOR FIREWALL ISA 2004

Con base en la creación de la entidad emisora de certificados, ya se pueden configurar los valores de la VPN en el equipo servidor ISA donde se habilita, así como configurar el acceso de cliente de VPN en la consola de administración de redes privadas virtuales (VPN) (ver figura 6).

Esta acción habilita automáticamente las reglas de acceso de directiva del sistema necesarias para permitir el acceso de cliente de VPN, e inicia el enrutamiento y el acceso remoto, que son necesarios para la conexión de los clientes [1].

El servidor ISA necesita dicha regla de acceso para obtener su certificado. Se debe crear un nuevo objeto de equipo que represente la entidad emisora de certificados. Este objeto de equipo se utiliza al crear la regla de acceso que permita las conexiones de VPN a la red interna de la organización. Identificar el direccionamiento es importante, porque con este se guían las peticiones de certificados en la red WAN (*Wide Area Network*). A continuación se instala el certificado en el equipo servidor ISA y en los clientes VPN,

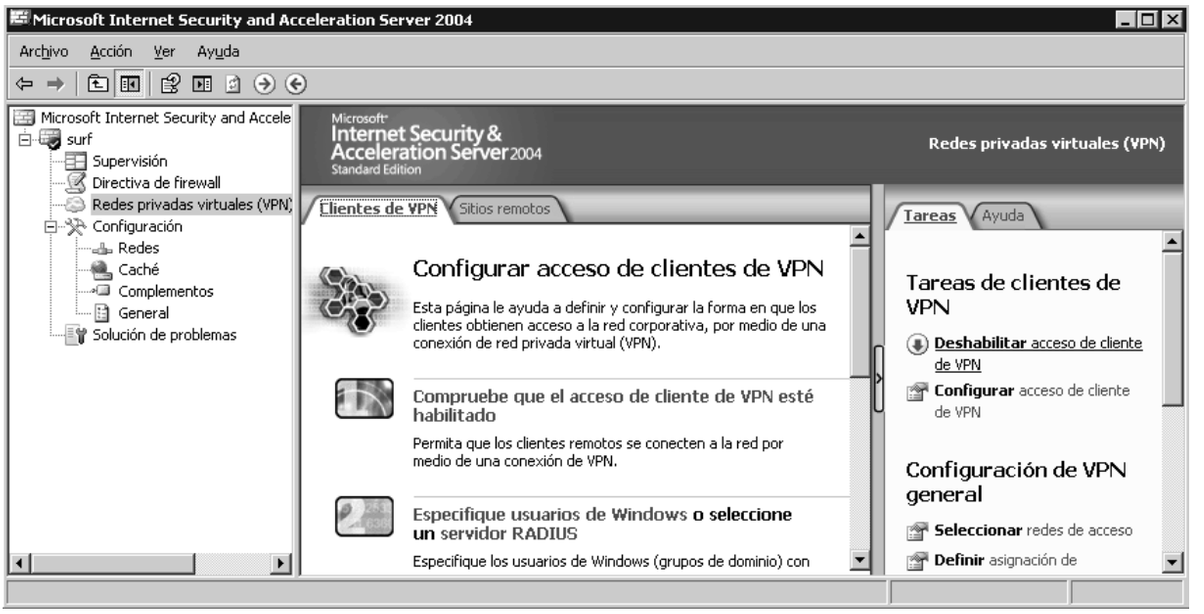

Figura 6. Configuración de acceso de clientes VPN