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

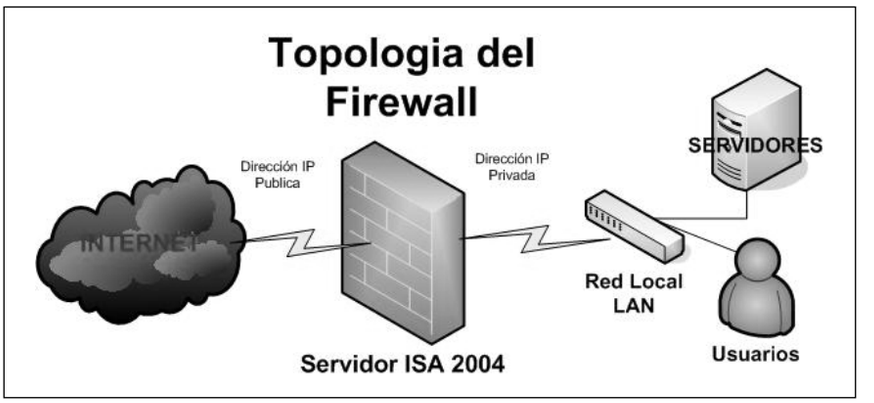


Figura 1. Topología de un firewall

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

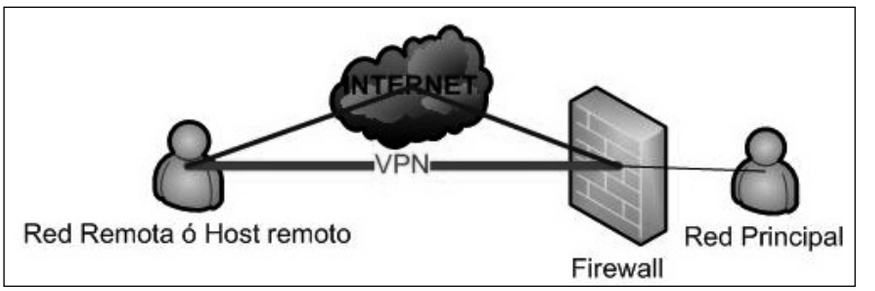


Figura 2. Conexión de host remoto VPN / Internet

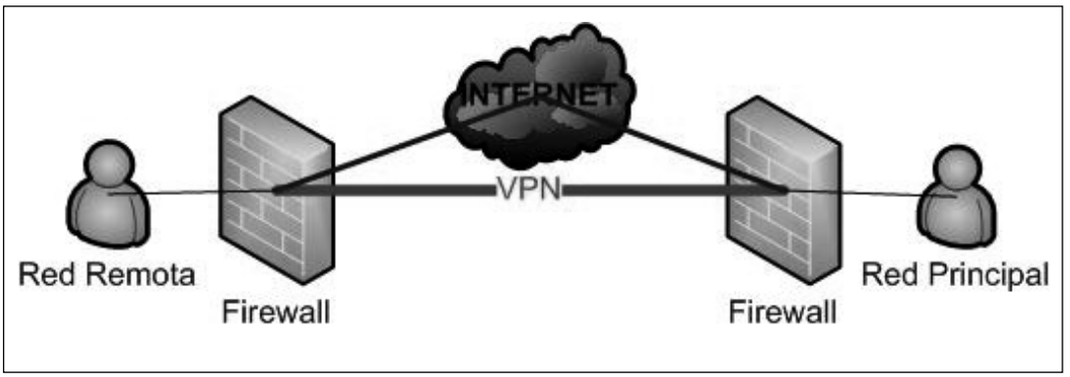


Figura 3. Conexión de sitio a sitio

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].

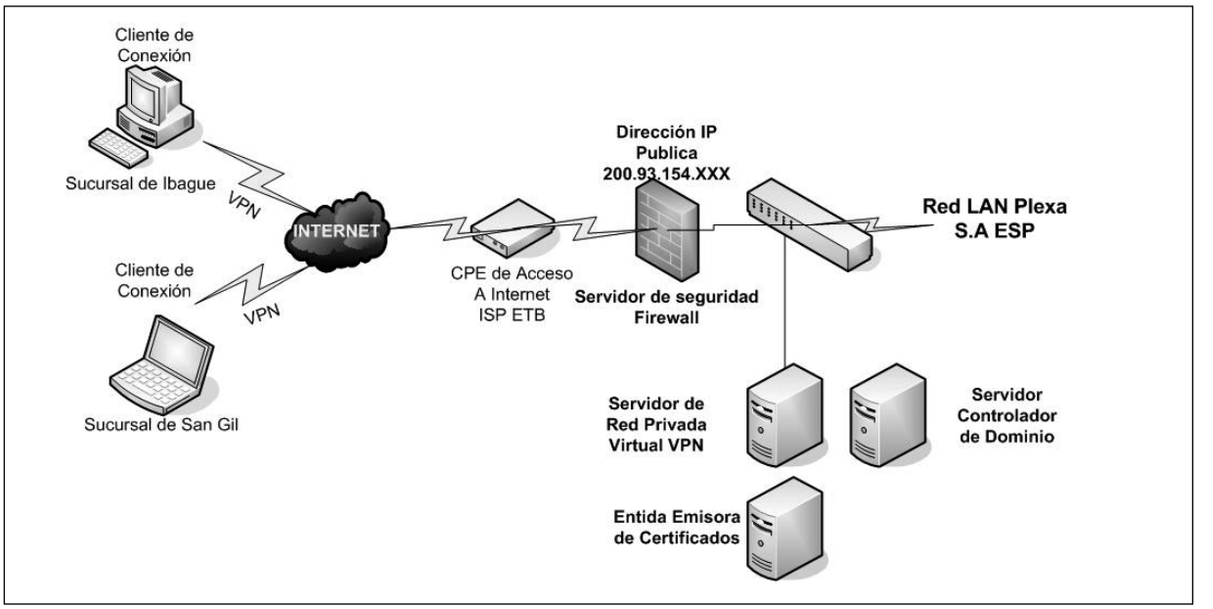


Figura 4. Topología a implementar

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.

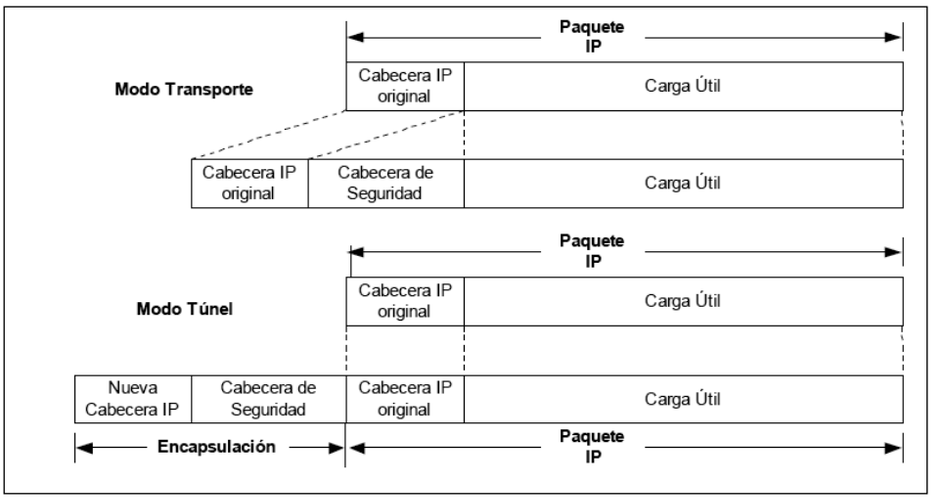


Figura 5. Modos de operación de IPsec

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,

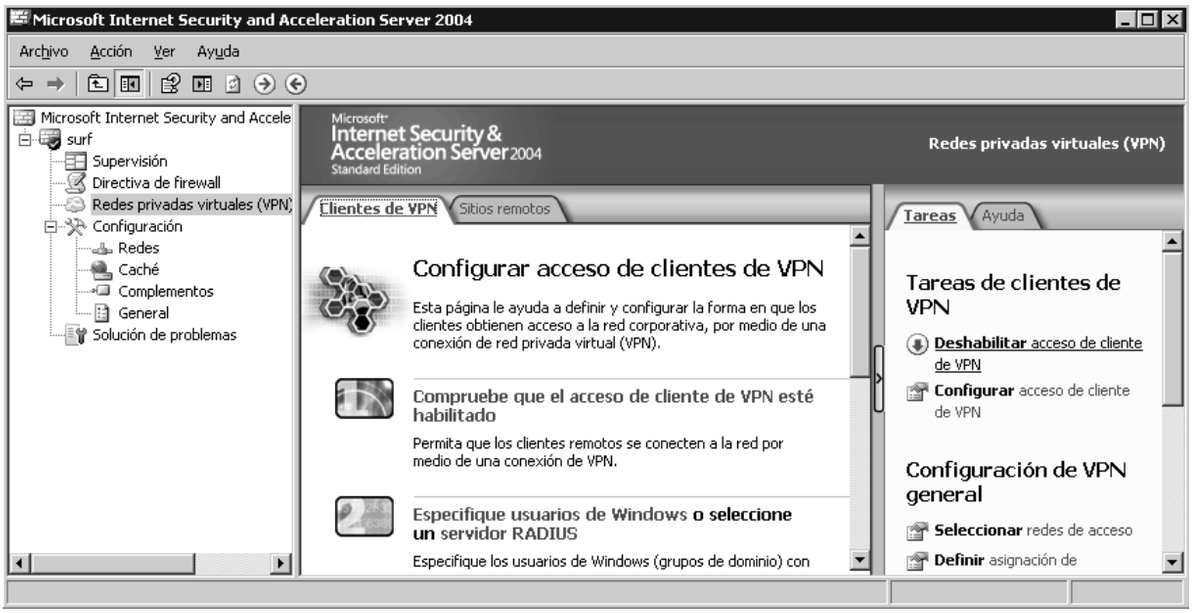


Figura 6. Configuración de acceso de clientes VPN

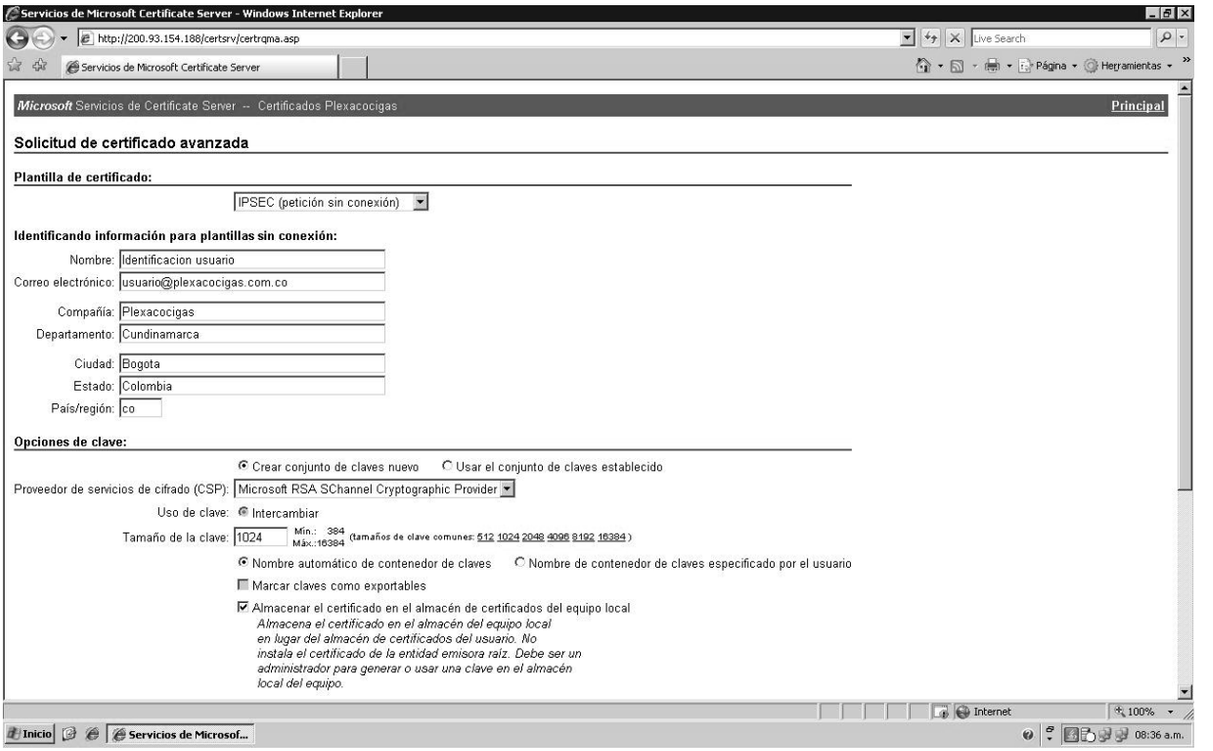


Figura 7. Entidad emisora de certificados

ingresando a la entidad emisora de certificados por medio de la página web que se crea (http://ip del servidor ISA/certsrv), como se presenta en la figura 7.

En la entidad emisora de certificados se crean e instalan los certificados necesarios, tanto para los clientes VPN como para el servidor *firewall* o VPN, de modo que se establezca una comunicación segura entre los dos.

3.4. VERIFICACIÓN DEL USO DE IPSEC

Luego de la implementación y configuración del servidor y los clientes de la VPN, se procede a realizar pruebas de funcionamiento, verificando la eficiencia y el uso a satisfacción por parte de los funcionarios de la organización. Para tal fin, se realiza la revisión de las conexiones VPN, utilizando el esquema de la figura 8, donde se encuentra el tipo de conexión realizado y la seguridad que aportan los canales VPN y el servidor ISA. Para verificar las conexiones se utilizó la herramienta Wireshark [11] y el filtro por dirección IP Ip.addr == xx.xx.xx.xx, a fin de obtener la captura de paquetes.

En la figura 9 se describen los detalles de los paquetes capturados: la dirección IP de origen y destino, el uso de un puerto seguro definido como IPsec-Nat-t (4500) tanto para la fuente como para el receptor del paquete, y la longitud del paquete, todo enmarcado bajo el protocolo UDP, descrito como UDP Encaptulation Of IPsec Packets.

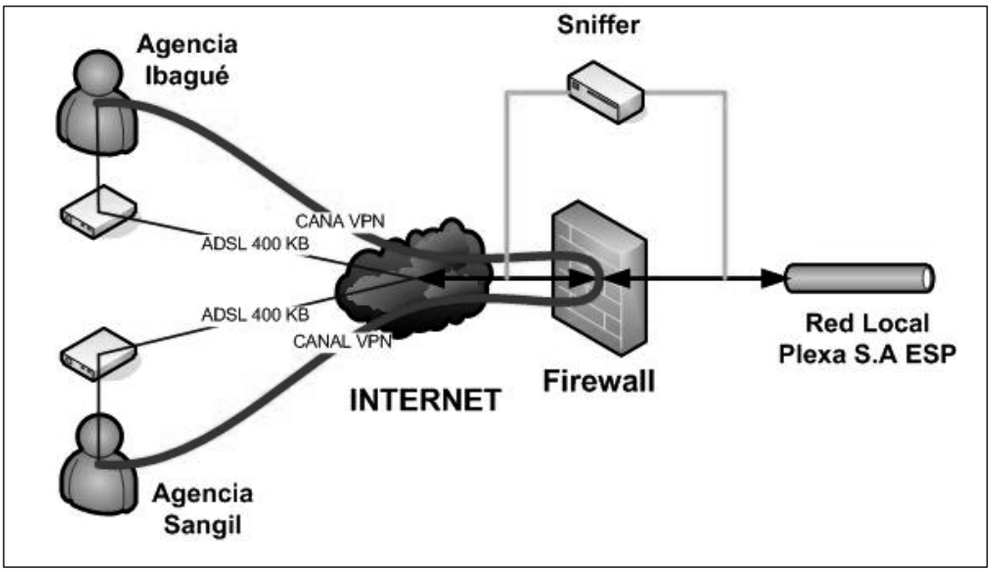
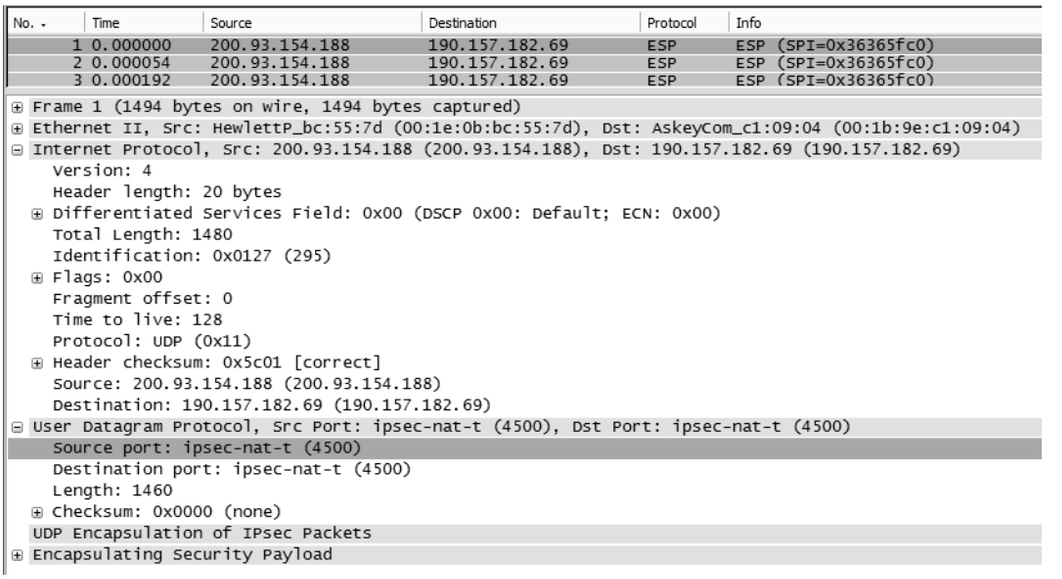


Figura 8. Entorno de evaluación de canales VPN L2TP/ IPsec

4. VERIFICACIÓN DE LATENCIA DE LOS CANALES DEDICADOS Y VPN

La latencia de los canales define el tiempo que tarda un paquete en trasladarse de un punto a otro dentro del entorno de red; hace parte de los parámetros de monitorización de QoS para redes WAN, y sirve para ver los índices de disponibilidad de los enlaces.

Dentro de la implementación se realiza la medición con base en el uso del protocolo



No.	Time	Source	Destination	Protocol	Info
1	0.000000	200.93.154.188	190.157.182.69	ESP	ESP (SPI=0x36365fc0)
2	0.000054	200.93.154.188	190.157.182.69	ESP	ESP (SPI=0x36365fc0)
3	0.000192	200.93.154.188	190.157.182.69	ESP	ESP (SPI=0x36365fc0)

```
⊞ Frame 1 (1494 bytes on wire, 1494 bytes captured)
⊞ Ethernet II, Src: HewlettP_bc:55:7d (00:1e:0b:bc:55:7d), Dst: AskeyCom_c1:09:04 (00:1b:9e:c1:09:04)
⊟ Internet Protocol, Src: 200.93.154.188 (200.93.154.188), Dst: 190.157.182.69 (190.157.182.69)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1480
    Identification: 0x0127 (295)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x5c01 [correct]
    Source: 200.93.154.188 (200.93.154.188)
    Destination: 190.157.182.69 (190.157.182.69)
⊟ User Datagram Protocol, Src Port: ipsec-nat-t (4500), Dst Port: ipsec-nat-t (4500)
    Source port: ipsec-nat-t (4500)
    Destination port: ipsec-nat-t (4500)
    Length: 1460
  ⊞ Checksum: 0x0000 (none)
  UDP Encapsulation of IPsec Packets
⊞ Encapsulating Security Payload
```

Figura 9. Captura de paquetes sobre dirección publica

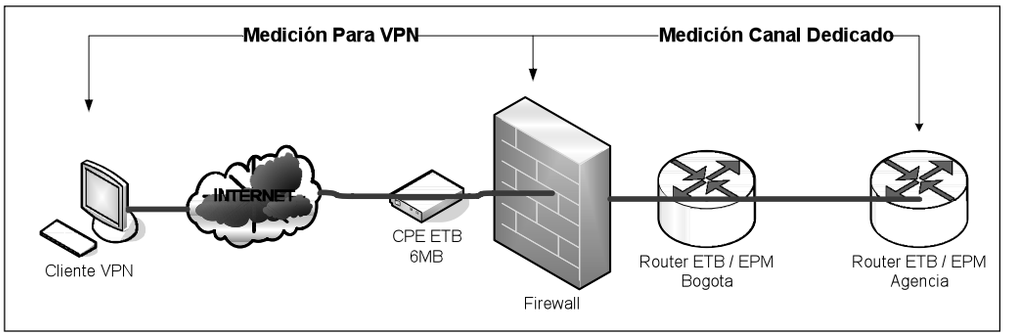


Figura 10. Medición de latencia

ICMP (*Internet Control Message Protocol*) [12], [13], *que define la utilidad ping, utilizada esta* para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos; en este caso se presentan valores reales tomados de la implementación realizada en la organización Plexa S.A ESP [5].

4.1. ENTORNO DE MEDICIÓN

Esta medición se realizó desde el servidor de firewall hacia los enrutadores terminales en las agencias sin carga y con carga, a fin de verificar este parámetro en los canales dedicados existentes. De forma similar se hizo para los canales VPN conectados desde internet, como se presenta en la figura 10.

Se utilizó la sintaxis Ping [12] (dirección IP xx.xx.xx.xx) –t, con la cual se obtienen 299 muestras por cada dirección IP evaluada. Los resultados fueron promediados utilizando la ecuación (1):

$$\text{Latencia} = (\sum m) / Nm \quad ms \quad (1)$$

donde:

m = muestras y Nm = número de muestras

Dentro de las muestras se define un valor de 4000 ms para cada valor nulo expresado durante la medición por el mensaje (tiempo de respuesta agotado para esta solicitud), el cual es habitual en las conexiones VPN, mas no en los canales dedicados.

Los resultados para los canales dedicados se aprecian en la tabla 1, en la cual se discrimina el segmento evaluado, la tecnología de última milla provista por la empresa de comunicaciones (ETB y EPM), la dirección IP de enlace del enrutador, la cantidad de host

Segmento	Tecnologia	Direccion IP	Host	Velocidad Canal	Latencia sin Carga	Latencia con Carga
Manizales	Canal dedicado ETB Cobre	192.168.10.33	13	512	37.183	43.107
Pereira	Canal dedicado ETB Radio	192.168.10.49	4	512	32	32.568
Armenia	Canal dedicado ETB Radio	192.168.10.65	5	512	18.946	19.578
Medellin	Canal dedicado EPM Cobre	192.168.10.81	9	512	51.167	51.14
Bucaramanga	Canal dedicado ETB Cobre	192.168.10.129	3	512	17.404	24.143
Puerto Salgar	Canal dedicado ETB Satelital	192.168.10.145	3	512	675.424	760.003
Cartagena	Canal dedicado ETB Cobre	192.168.10.161	9	512	52.217	55.602

Tabla 1. Resultados de latencia canales dedicados [5]

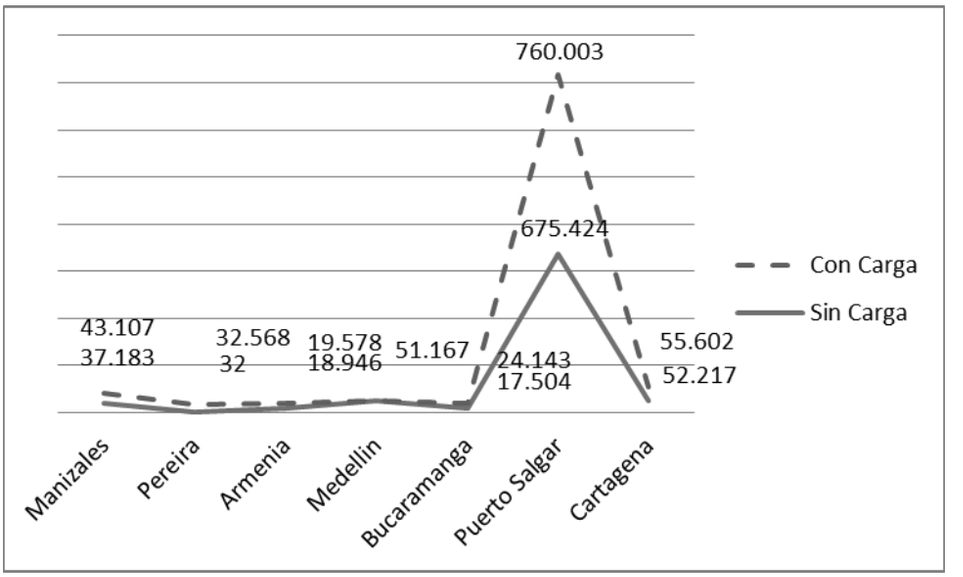


Figura 11. Comparación de los canales dedicados [5]

(carga del canal), la velocidad de los canales dedicados, y finalmente, la latencia sin carga y con carga.

En la figura 11, se presenta la comparación de los valores obtenidos sobre los canales dedicados. Se observa que la latencia es baja en la mayoría de las muestras, salvo en el canal satelital, en el cual esta aumenta debido al medio de propagación que utiliza. Por otra parte, la latencia se mantiene sin cambios considerables al colocar la carga operativa (host) en los canales. Con base en la experiencia, se definen unos parámetros de funcionamiento determinados por la latencia, que son utilizados como indicados de QoS para cualquier canal de comunicación WAN. Dichos parámetros son presentados en la tabla 2.

Como ejemplo se observa el cambio sufrido en la agencia de Manizales, que con una carga de 13 host pasa de tener una latencia de 37.183 mS a una de 43.107 mS, con un aumento porcentual del 0.011 %. Esto indica que cuentan con un canal eficiente para las labores que sobre él desarrollan.

Canal Eficiente	**X < 400 ms**
Canal Funcional tolerable	**400ms < X < 800 ms**
Canal deficiente	**X > 800 ms**

Tabla 2. Parámetros de calidad QoS [5]

Segmento	Host	Latencia sin Carga	Latencia con Carga	Aumento %
Manizales	13	37.183	43.107	0.011593201
Pereira	4	32	32.568	0.0101775
Armenia	5	18.946	19.578	0.01033358
Medellin	9	51.167	51.32	0.010029902
Bucaramanga	3	17.404	24.143	0.013872098
Puerto Salgar	3	675.424	760.003	0.011252236
Cartagena	9	52.217	55.602	0.010648256

Tabla 3. Aumento porcentual de la latencia en los canales dedicados [5]

En la tabla 3 se observa la eficiencia de los canales de comunicación provistos por los operadores de comunicación ETB y EPM.

En consecuencia, a partir del apartado anterior, se realiza el mismo procedimiento para los canales de comunicación efectuados con VPN, utilizando conexión a internet por medio del servicio provisto por ETB ADSL y Comcel 3GSM.

Como se presenta en la tabla 4, en la cual se relaciona el segmeto o ubicación de la agencia, la tecnoogia utilizada, el número de host conectados, la velocidad, y el comportamiento tanto sin carga como con carga sobre los canales VPN.

En la figura 12 se presenta la comparación de los resultados obtenidos. Se encuentra una diferencia mayor en la latencia produc-

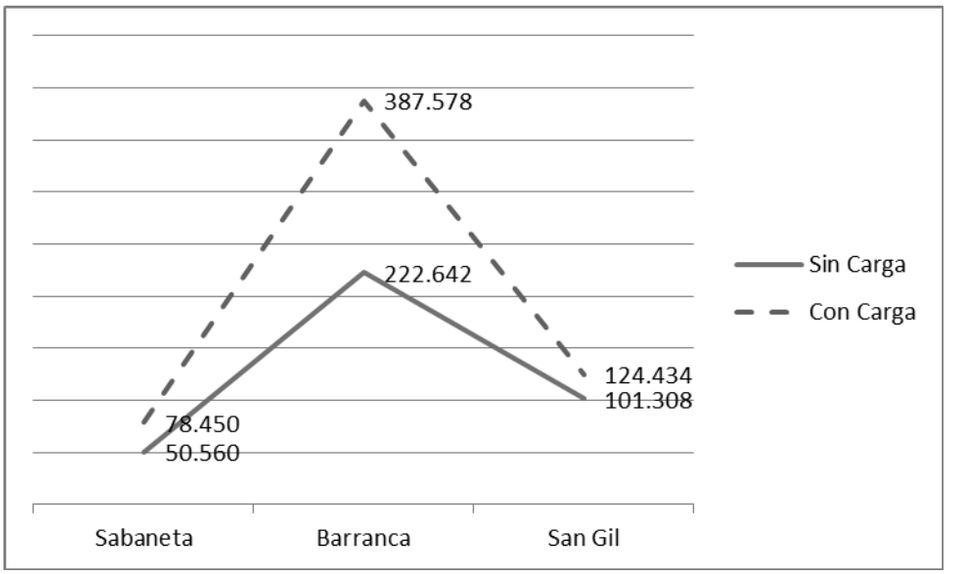


Figura 12. Comparación de los canales VPN [5]

Segmento	Tecnologia	Direccion IP	Host	Velocidad Canal	Latencia sin Carga	Latencia con Carga
Sabaneta	VPN / ADSL (1024 K)	192.168.10.242	3	1000	50.56	78.45
Barranca	VPN / 3GSM (1024 K)	192.168.10.246	1	1000	222.642	387.578
San Gil	VPN / ADSL (1024 K)	192.168.10.247	3	1000	101.308	124.434

Tabla 4. Latencia en los canales VPN [5]

to de las mediciones efectuadas con carga y sin ella.

Cabe anotar que si bien las diferencias son mayores, frente a los canales dedicados el aumento no es significativo. Al relacionarlos con los parametros de calidad definidos anteriormente, las VPN se encuentran dentro de los valores de eficiencia en un buen nivel.

Por otra parte, es de anotar que un canal dedicado mantiene la latencia sin ser afectado de forma notoria por la carga que se coloca en uno de los extremos, lo cual se debe a los parametros de calidad provistos en la red por el proveedor del servicio. Las VPN se comportan de forma diferente, dado que el tunel es realizado con base en la disponibilidad de Internet, sea este un ADSL, o sea un GSM.

5. CLASIFICACIÓN DE SEGURIDAD Y VULNERABILIDADES

En este apartado se busca realizar una comparación de las características que rigen tanto a canales dedicados como a las VPN, considerando sus fortalezas (seguridad) y vulnerabilidades. A este efecto se comparan canales dedicados provistos por una empresa de comunicaciones (ETB o EPM) y las VPN levantadas sobre accesos a Internet contratados con los mismos operadores.

Cabe anotar que se parte del hecho de que los canales dedicados son en su totalidad administrados por el proveedor del servicio, quien manifiesta que estos usan las características de MPLS (Multiprotocol Label Switching) [13].

Se define para cada característica un indicador (5=bueno, 3=aceptable, 1 =deficiente).

Las características se presentan en la tabla 5.

5.1. RESULTADOS

La calificación para los canales dedicados y VPN queda dada por el promedio de las calificaciones parciales de cada característica mencionada. Por lo tanto, para los canales dedicados es de 3.89 y para las VPN de 3.23.

Es claro que al realizar la comparativa global de las características, los canales dedicados son superiores a las VPN en varios aspectos, como la calidad del servicio (QoS), su disponibilidad, la escalabilidad y la administración.

6. CONCLUSIONES

- Las conexiones remotas que utilizan redes privadas virtuales (VPN) resultan ser una excelente solución gracias a su seguridad, flexibilidad y adaptación, lo que permite a la organización centralizar actividades concretas entre sus agencias.

- El uso de un *firewall* de puerta de enlace que controle el tráfico de acceso a internet,

permite optimizar y controlar de forma importante los recursos de la organización, en este caso limitando el uso de recursos como Internet.

- Al cifrar las conexiones remotas (VPN), los datos que atraviesan una red pública (Internet) aumentan su seguridad, de manera que la red es protegida de muchos de los riesgos existentes.

- Los análisis desarrollados sobre los canales dedicados y las conexiones de VPN muestran que la calidad del servicio QoS está dada por el medio físico que se utilice para su implementación (cobre, FO, radio, microondas, etc.), mas no de la tecnología que sobre aquellos se implemente.

- Al comparar la latencia entre los canales dedicados y los canales realizados por me-

Característica	Canal Dedicado		VPN	
	Descripción	Calificación	Descripción	Calificación
Seguridad	Definida por el Proveedor del servicio	5	Se utiliza IPsec sobre L2tp	5
Tiempo de respuesta	Proveedor garantiza la latencia	5	Depende del método de acceso a internet (ADSL, GSM ...)	3
Costo	El valor de un canal dedicado oscila entre $ 800.000 y $ 1.400.000 pesos + costo de aprovisionamiento	1	El costo para una VPN se define por el costo de acceso a internet desde $ 65.000 hasta $ 110.000,	5
Equipos	Provistos por el operador de comunicaciones, hay cobro por aprovisionamiento	1	Provistos por el operador del servicio, no hay cobro por aprovisionamiento	3
QoS	Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada	5	La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte	3
Escalabilidad	La provisión de servicio es sencilla: una nueva conexión afecta a un solo router tiene mayores opciones de crecimiento modular usa concepto (Point-to-cloud)	5	Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales	1
Accesibilidad	Permite Acceso únicamente de los router afiliados por el proveedor	3	Soporta cualquier tecnología, ADSL, GSM, se restringe por políticas de acceso	5
Administración	Efectuada por el proveedor del servicio	5	Efectuada directamente por la organización	3
Disponibilidad	Proveedor garantiza el 99.9 % de disponibilidad y dan solución a problemas en máximo 3 horas	5	Proveedor no garantiza disponibilidad, tiempo de soporte altos (horas, Días).	1

Tabla 5. Caracteristicas de canales dedicados vs. canales VPN [5]

dio de VPN, se encuentra que los primeros tienen un mejor desempeño, pero el factor obtenido sobre las VPN es aceptable para mantener la calidad de servicio QoS, por lo que estas resultan apropiados para las aplicaciones y necesidades de las empresas.

- Luego de realizar una comparación de las características de los canales dedicados frente a los canales hechos por medio de VPN, se encuentra que la diferencia no es un factor que descalifique el uso de las VPN.

- En las empresas el costo es un factor muy importante. Estas lo evalúan frente a la disponibilidad de un servicio, y es por esto que una solución de VPN con una QoS aceptable y un valor inferior en un 70% frente a un canal dedicado, hacen que este tipo de soluciones tengan gran acogida en el ámbito empresarial.

REFERENCIAS

[1] J. Little, D. Shinder y T.W. Shinder, How to Cheat at Configuring ISA Server 2004. The Barnes & Noble Review, February, 2006.

[2] Microsoft, Microsoft Internet Security & Acceleration Server 2004, consultado en marzo de 2010 en http://www.microsoft.com/isaserver.

[3] Virtual Private Network Deployment Scenarios in ISA Server 2004 Enterprise Edition, consultado en abril de 2010 en http://technet.microsoft.com/es-co/library/cc713341(en-us).aspx.

[4] A.A. Ramos Varón, F. Picouto Ramos, J. Pérez Agudín, C. Míguez Pérez y A.M. Matas García, Hacker, 1a ed. Madrid: Anaya Multimedia 2005.

[5] W. Barbosa C., "Implementación de un canal de comunicaciones por medio de VPN (red privada virtual) para las sucursales remotas de la empresa PLEXA S.A ESP" monografía de grado, Universidad Distrital, 2008.

[6] RFC2637- Point-to-Point Tunneling Protocol (PPTP), consultado en julio de 1999 en http://www.faqs.org/ftp/rfc/pdf/rfc2637.txt.pdf.

[7] RFC2661 - Layer Two Tunneling Protocol "L2TP", consultado en http://www.ietf.org/rfc/rfc2661.txt, agosto de 1999.

[8] Layer 2 Tunneling Protocol Version 3 (L2TPv3) Extended Circuit Status Values RFC 5641, consultado en http://datatracker.ietf.org/doc/rfc5641/, agosto de 2009.

[9] RFC3585 - IPsec Configuration Policy Information Model, consultado en: http://www.ietf.org/rfc/rfc3585.txt, agosto de 2003.

[10] Microsoft Corporation, "What Is IPSec?", consultado en abril de 2010 en http://technet.microsoft.com/es-co/library/cc776369(WS.10).aspx.

[11] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, consultado en http://tools.ietf.org/html/rfc3280, abril de 2002.

[12] Wireshark User's Guide (26892 for Wireshark 1.0.0), consultado en http://www.wireshark.org, junio de 2008.

[13] RFC 4884 - Internet Control Message Protocol, consultado en http://datatracker.ietf.org/doc/rfc4884/, abril de 2007.

[14] D.E. Comer, Internet Working With TCP/IP, Vol. 1: "Principles, Protocols, and Architecture, 5th Ed., Prentice Hall, 2005.