República Bolivariana de Venezuela

Ministerio del Poder Popular Para la Educación Universitaria

Universidad Politécnica Territorial de Paria "Luis Mariano Rivera"

P.N.F "Ingeniería en Informática"

Municipalización Cajigal

Yaguaraparo-Estado Sucre

Red Privada Virtual

VPN

Profesor:

Ing. Malavé Abdías

Autores:

Tsu. Cedeño Eugenio.

C.I: 24.133.226

Tsu. Gómez Zonyidey

C.I: 22.923.231

Tsu. Torres Mileidis

C.I: 23.550.991

Diciembre, 2016

Introducción

Una RED se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones). En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos. Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentas con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de
los famosos firewalls y las VPN

Índice de Contenido

¿Qué es una VPN?

Según M. N González (2002) Redes privadas virtuales **"Una VPN es una red virtual que se crea dentro de otra red, como por ejemplo Internet**". Generalmente las redes privadas se crean en redes públicas, en las que se quiere crear un entorno confidencial y privado. La VPN permiten trabajar como si estuviese en la red local, es totalmente transparente para el usuario. Una vez establecida la conexión de la red privada virtual los datos viajan encriptados de forma que sólo el emisor y el receptor son capaces de leerlos. Para poder realizar una VPN se necesita un servidor (o host) que espera conexiones entrantes, y uno o varios clientes, que se conectan al servidor para formar la red privada.

Es una Red Privada Virtual (VPN), se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un túnel definido en la red pública.

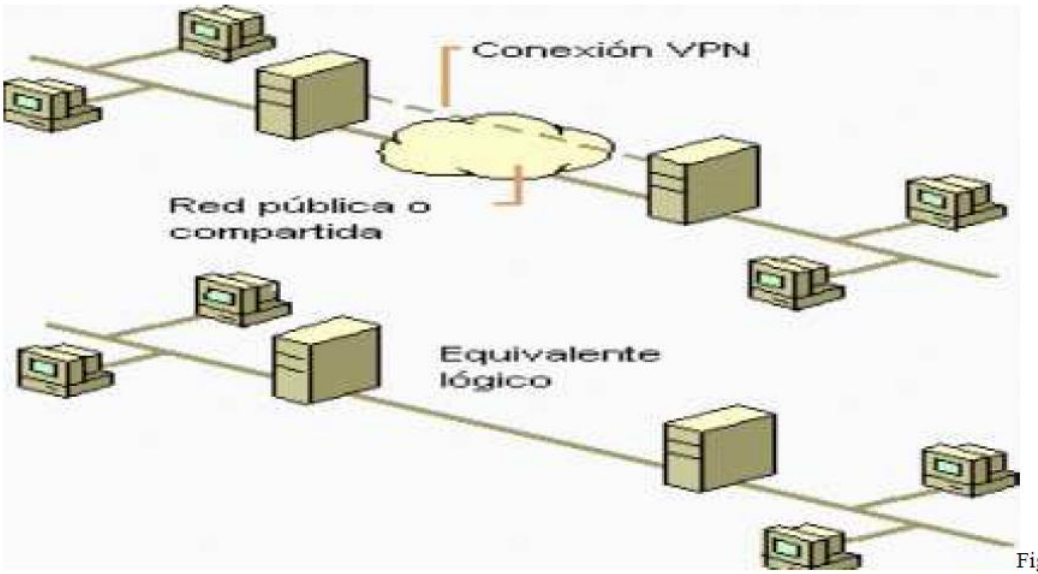

Figura 1

Tecnología de túnel:

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

Tipos de VPN:

- **VPN de acceso remoto:** Consiste en usuarios que se conectan a una empresa desde sitios remotos utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso similar a estar dentro de la red local.

- **VPN punto a punto:** Este esquema es el empleado para conectar oficinas remotas con una sede central. El servidor VPN está conectado permanentemente a Internet, acepta conexiones entrantes desde los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet y a través de ésta al túnel VPN de la oficina central. Se utiliza para eliminar las conexiones punto a punto tradicionales.

- **VPN interna (over LAN):** Funciona tal cual una red VPN normal, salvo que dentro de la misma red local LAN en lugar de a través de Internet. Sirve para aislar zonas y servicios de la misma red interna. Sirve también para mejorar las características de seguridad de una red inalámbrica WiFi.

Componentes Que Conforman Una VPN:

Según R. Nader Carreón (2007) VPN (Redes Privadas Virtuales) **"Las VPN consisten en hardware y software, y además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la red sea segura, este disponible y sea fácil de mantener".** Son necesarios ya sea que un PSI proporcione la VPN o que usted haya decidido instalar una por sí mismo.

- **Disponibilidad:** Se aplica tanto al tiempo de actualización como al de acceso.

- **Control:** Suministra capacitación, experiencia, supervisión meticulosa y funciones de alerta que ofrece algunos proveedores de servicios administrados. Una consideración significativa es que sin importar que tan grande sea la organización, es probable que solo cuente con una VPN; puede tener otros puntos de acceso pero seguirá siendo una VPN corporativa.

- **Compatibilidad:** Para utilizar tecnología VPN e internet como medio de transporte, la arquitectura Interna del protocolo de red de una compañía debe ser compatible con el IP Nativo de internet.

- **Seguridad:** Lo es todo en una VPN, desde el proceso de cifrado que implementa y los Servicios de autenticación que usted elige hasta las firmas digitales y las Autoridades emisoras de certificados que utilizan. Abarca el software que Implementa los algoritmos de cifrado en el dispositivo de la VPN.

- **Confiabilidad:** Cuando una compañía decide instalar el producto VPN de un PSI, está a merced de este.

- **Autenticación De Datos Y Usuarios:**

Datos: Reafirma que el mensaje a sido enviado completamente y que no ha sido alterado de ninguna forma.

Usuarios: clientes que se conectan a la VPN.

- **Sobrecarga De Tráfico:** En todo tipo de tecnologías existen sacrificios: velocidad contra desempeño, seguridad contra flexibilidad. Las VPN caben en la misma categoría cuando se hablan de tamaño de paquetes cifrados las sobre carga está en juego, ya que si mandamos varios paquetes se incrementa el tamaño de estos y por lo tanto se afecta la utilización del ancho de banda.

- **Sin Repudio:** Es el proceso de identificar positivamente al emisor de tal manera que no pueda negarlo.

Ventajas y Desventajas de las VPN:

Las principales ventajas son:

- Costo de acceso remoto económico
- La tecnología VPN es una de las más seguras
- Accesibilidad a información
- Simplicidad

Las principales desventajas:

- Dependencia doble de estabilidad de conexión
- Desconocimiento y descuidos usuario final
- Equipo cliente sin control de Administrador

Requerimientos básicos de una VPN:

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

Identificación de usuario:

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien accedió, que información y cuando.

Administración de direcciones:

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos:

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves:

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples:

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros.

Herramientas de una VPN:

- VPN Gateway
- Software
- Firewall
- Router

- Dispositivos con un software y hardware especial para proveer de capacidad a la VPN Software
- Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

Protocolos de VPN:

Han sido implementados varios protocolos de red para el uso de las VPN. Estos protocolos intentan cerrar todos los "hoyos" de seguridad inherentes en VPN. Estos protocolos continúan compitiendo por la aceptación, ya que ninguno de ellos ha sido más admitido que otro.

Estos protocolos son los siguientes:

Point-to-Point Tunneling Protocol (PPTP): PPTP es una especificación de protocolo desarrollada por varias compañías. Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP.

La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su fallo a elegir una única encriptación y autenticación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

Layer Two Tunneling Protocol (L2TP): El principal competidor de PPTP en soluciones VPN fue L2F, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP. L2TP existe en el nivel de enlace del modelo OSI. L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

Internet Protocol Security (IPsec):

IPsec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec existe en el nivel de red en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet.

Servidores VPN:

AceVPN: Dispone de servidores en 13 países y un servicio gratuito accesible por invitaciones. Es multiplataforma: Microsoft Windows, Apple Mac, Linux, iPhone, iPod touch, iPad, Android, etc.

AnchorFree Hotspot VPN: VPN para anonimizar tráfico en los Estados Unidos que ofrece la empresa Anchor Free. Válido para Windows y Mac. Algunos sitios como Hulu detectan los servidores de Anchor Free y los bloquean.

Free VPN by WSC: Apenas agrega una latencia de 10 a 50 ms. La reproducción de streaming contra servidores británicos y estadounidenses funciona sin problemas, sin interrupciones y la reproducción es instantánea. Tiene un diseño más simple, más servidores y es menos intrusivo que Anchor Free.

GPass: El servicio de GPass proporciona acceso gratuito a VPNs, así como un proxy muy rápido que se puede utilizar directamente desde el navegador. El servicio es muy popular en China, donde la censura en Internet es de lo más común.

Hostizzle: Servicio que te ofrece mensualmente 10 mb gratis, y funciona con Hulu, por lo tanto quiere decir que tenemos IP de USA. Lo único es que cada mes es necesario renovar el certificado para la conexión.

Hotspot Shield: Este es, posiblemente, el cliente VPN gratuito más popular del mundo. Se hizo popular cuando Hulu se puso en marcha. Ahora, tienen servicios de VPN en Estados Unidos y el Reino Unido que se pueden utilizar para protegerse de los fisgones WiFi, robos de identidad y censuras. Lo mejor de Hotspot Shield es que proporciona ancho de banda ilimitado y funciona tanto en PC como Mac.

Instalación y configuración de OpenVPN

A) Instalacion:

1) Instalando el paquete del repositorio:

• apt-get install openvpn

2) Copiamos los scripts de configuración de las entidades de certificación al directorio /etc/openvpn:

• cd /usr/share/doc/openvpn/examples/easy-rsa
• cp -a 2.0/ /etc/openvpn/easy-rsa
• cd /etc/openvpn/easy-rsa

3) Antes de crear la clave de CA se debe modificar algunas variables de entorno:

• nano vars

Nota: Se deben configurar correctamente los parámetros KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, y KEY_EMAIL.

4) Después de configurar el archivo vars es posible generar el certificado y clave para la Autoridad Certificadora (CA):

• . ./vars
• ./clean-all
• ./build-ca

5) **Luego es posible generar el certificado y clave para el servidor de VPN:**

• ./build-key-server server

Nota: Generar los certificados para los clientes (es importante que los certificados de los clientes y del servidor estén firmados por la misma CA):

• **./build-key client1**
• **./build-key client2**
• **./build-key client3**

Nota: cada vez que se reinicia la sesión, se debe ejecutar ". ./var" para configurar las variables de entorno nuevamente.

Responder 'y' dos veces para firmar y commit del certificado.
Finalmente se deben generar los parámetros Diffie-Hellman:
• **./build-dh**

Ya hemos construido nuestra PKI (Public Key Infrastructure), es decir nuestra infraestructura de autenticación y encriptación mediante clave pública.Se deben copiar los archivos de configuración de ejemplo al directorio /etc/openvpn:
• **cp -a /usr/share/doc/openvpn/examples/sample-config-files/ /etc/openvpn/**

B) Configuración del servidor

1) **Descomprimir el archivo de configuración del servidor:**

• cd /etc/openvpn/sample-config-files/
• gunzip server.conf.gz

2) **Editar el archivo de configuración del servidor:**

• nano server.conf

3) **Modificar las siguientes líneas:**

proto tcp

;proto udp

ca easy-rsa/keys/ca.crt

cert easy-rsa/keys/server.crt

key easy-rsa/keys/server.key

dh easy-rsa/keys/dh1024.pem

server 10.8.0.0 255.255.255.0

De esta forma el servidor dará acceso a la red 10.8.0.0/24 y tomará la dirección IP 10.8.0.1 (los clientes tendrán una IP en el rango 10.8.0.2 a 10.8.0.254). Si es necesario enviar reglas de ruteo a los clientes se debe agregar (por ejemplo para poder llegar a la red interna 192.168.1.0/24 que se encuentra detrás de la VPN):

• **push "route 192.168.1.0 255.255.255.0"**

4) **Por último copiar el archivo de configuración al directorio /etc/openvpn**:

• cp server.conf ../

• cd /etc/openvpn

C) **Configuración de los clientes:**

1) **Editar el archivo de configuración de los clientes:**

• cd /etc/openvpn/sample-config-files

• nano client.conf

2) **Modificar las siguientes líneas:**

proto tcp
;proto udp
remote 192.168.122.169 1194
En este ejemplo la dirección IP 192.168.122.169 es la dirección en la cual el servidor escucha pedidos de conexión a la VPN 10.8.0.0/24 en el puerto 1194 (puerto por defecto de OpenVPN).

3) **Empaquetar el archivo de configuración junto con los certificados y clave:**

- cd /etc/openvpn
- mkdir client1
- cp sample-config-files/client.conf client1/
- cp easy-rsa/keys/ca.crt client1/
- cp easy-rsa/keys/client1.crt client1/client.crt
- cp easy-rsa/keys/client1.key client1/client.key
- zip -Z deflate -r client1.zip client1/*

Repetir el procedimiento para el resto de los clientes.

INICIAR EL SERVIDOR PARA VERIFICAR LA CONECTIVIDAD

Nota: antes de iniciar el servidor debe habilitarse IP forwarding para que funcione el enrutamiento de paquetes.

Habilitar IP forwarding:

• **echo 1 > /proc/sys/net/ipv4/ip_forward**

Iniciar el servidor de VPN:

• **cd /etc/openvpn/**

• **openvpn server.conf**

Conclusión

Debido a las ventajas económicas que ofrecen las redes privada virtuales se puede concluir que se trata de una excelente tecnología para el acceso remoto , puesto que el uso de una VPN constituye un sustituto indispensable a los métodos tradicionales caros de marcación de telefonía de larga distancia. Además constituye una buena solución alterna a los métodos de implantación de redes WAN tradicionales.

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no está bien definido pueden existir consecuencias serias.

Una VPN puede ser utilizada en todo tipo de entorno, desde las grandes empresas con sucursales en diversas partes del país o del mundo, hasta las pequeñas empresas con una o dos sucursales en una sola ciudad; así como en las diversas dependencias del gobierno que necesiten intercambiar información, instituciones educativas como universidades y en general en cualquier lugar que se necesite compartir archivos desde una ubicación remota de manera segura.

Referencias Bibliográficas y Electrónicas

Para la realización de este trabajo se han consultado las siguientes páginas de Internet, con el fin de obtener la suficiente información:

http://www.entarasys.com/la
http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml