
# “Redes privadas virtuales (VPN), una respuesta a lo limitado por la ubicación”

(ELO-322)

Integrantes:

- Emilio Cornejo
- Gustavo Matamala
- Marcelo Díaz
- Martín Rojas

Fecha: X / 08 / 2019

# Resumen:

Iniciaremos el proyecto introduciendo que es una VPN, luego procederemos dando una vista técnica con enfoque a los contenidos del curso (más apegado al tercer y cuarto capítulo del libro guía); sobre seguridad y protocolos, además, veremos sus ventajas como sus desventajas al usar este tipo de tecnología, en el ámbito empresarial, por ejemplo, u otros. Más tarde comprobaremos los protocolos de la capa de transporte antes mencionados, mediante el testeo en Wireshark.

El objetivo principal del proyecto es poder materializar el contenido del curso con una tecnología que está al alcance de todos, el cual contempla el aspecto técnico de las redes privadas virtuales, sus ventajas y desventajas y su uso e influencia en el mundo de las redes de computadores.

# Introducción

**¿Qué es un VPN?**

Una VPN, o red privada virtual, es una tecnología de red de computadores, que permite una extensión segura de la red de área local (LAN), sobre una red pública o no controlada como internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

**Principales protocolos de túnel de las redes privadas virtuales**

Antes de empezar con los principales protocolos de túnel en las redes privadas virtuales debemos introducir que es un protocolo de túnel; un protocolo de túnel es aquel que incluye en su datagrama otro paquete de datos completo que utiliza un protocolo de comunicaciones diferente. Básicamente, estos protocolos crean un "túnel" entre dos puntos de una red que puede transmitir de forma segura cualquier tipo de datos entre ellos. Cabe destacar que para que se establezca una conexión, ambas partes deben conocer y utilizar el mismo protocolo de comunicación.

**Protocolo PPTP:** El principio del PPTP (Protocolo de túnel punto a punto) consiste en crear tramas con el protocolo PPP y encapsularlas mediante un datagrama de IP. Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de IP. De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan dentro de un mensaje PPP, que a su vez está encapsulado dentro de un mensaje IP.

**Protocolo L2TP:** L2TP es un protocolo de túnel estándar (estandarizado en una RFC, solicitud de comentarios) muy similar al PPTP. L2TP encapsula tramas PPP, que a su vez encapsulan otros protocolos (como IP, IPX o NetBIOS).

**Protocolo IPSec:** Es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados. IPSec se basa en tres módulos: Encabezado de autenticación IP (AH), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes; Carga útil de seguridad encapsulada (ESP), que define el cifrado del paquete y brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY; y Asociación de seguridad (SA), que define configuraciones de seguridad e intercambio clave.

**Protocolo L2F:** Desarrollado por Cisco, a diferencia del PPTP el protocolo L2F no depende de IP con lo cual es capaz de trabajar directamente bajo otros protocolos. Utiliza PPP para la autenticación de usuarios remotos. Los túneles que crea pueden soportar más de una conexión. Trabaja con un servicio de enlace llamado Virtual Dial-Up (VDU), que nos permite acceder a la utilización de toda la infraestructura de Internet, no solo para conectar a través de diferentes protocolos al IP sino también cuando las direcciones IP no son reconocidas. El protocolo L2F es capaz de encapsular payloads PPP o payloads SLIP que serán enviados a sus destinos.

**SSTP**: Es una mejora actualizada del ya existente PPTP o Point to Point Tunneling Protocol. SSTP se considera uno de los protocolos más seguros para tunelización

VPN, es muy fiable y estable, tanto es así que Windows lo lleva totalmente integrado de serie. SSTP puede ayudar a evitar la mayoría de los firewalls, mantener datos seguros y mantener la conexión estable.

| VPN Protocol | Connection Speed | Level of Encryption | Connection Stability | Media Streaming | Torrent Downloading | Compatible With | Available in CactusVPN Client |
|---|---|---|---|---|---|---|---|
| PPTP | Very Fast | Poor | Very Stable | Good | Poor | Most OSs and devices | On Windows |
| L2TP/IPSec | Medium | Medium | Stable | Good | Medium | Most OSs and devices | On Windows |
| IKEv2/IPSec | Very Fast | Good | Very Stable | Good | Good | Most OSs and devices | On Windows, macOS, and iOS |
| IPSec | Medium | Good | Stable | Good | Good | Most OSs and devices | No |
| SSTP | Fast | Good | Very Stable | Medium | Good | Windows, Ubuntu, Android, and routers | On Windows |

**Ventajas y desventajas de las redes privadas virtuales**

Ventajas:

La principal ventaja de usar una VPN es que nos permite disfrutar de una conexión a red con todas las características de la red privada a la que queremos acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directrices de seguridad y los permisos de un ordenador en esa red privada. Así se puede acceder a la información publicada para aquella red privada: bases de datos, documentos internos, etc. a través de un acceso público. En ese momento, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se llevarán a cabo con los recursos y las conexiones que tenga la red privada.

Desventajas:

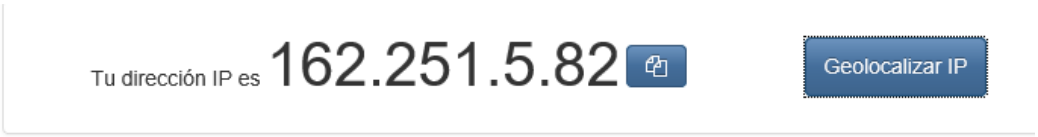
Entre las desventajas se puede mencionar una mayor carga en el cliente VPN, ya que ha de realizar la tarea adicional de encapsular los paquetes de datos una vez más. Esta situación se agrava cuando, además, se hace una encriptación de los datos que produce una mayor ralentización de la mayoría de las conexiones. También se produce una mayor complejidad en el tráfico de datos, que puede producir efectos no deseados en cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre y número IP).

# Desarrollo

Usando el servicio gratuito de VPN, flyVPN®, se comprobó que este proveedor de servicios VPN funciona, logrando tener una conexión virtual privada con servidores en Estados Unidos, esto se comprobó vía wireshark en donde todos los paquetes enviados y recibidos son en comunicación con el servidor ubicado en alguna región de Estados Unidos. Además, el servicio flyVPN ofrece conexiones UDP y TCP, elegibles al momento de conectarse al servidor, es por eso que se capturaron paquetes de ambos protocolos, en distintos servidores de Estados Unidos para revisar el correcto funcionamiento del servicio entregado.

Para la primera captura con el protocolo UDP, la IP que se nos asignó gracias a flyVPN fue la IP 162.251.5.82 cuya dirección en el mapa se encuentra cerca de la ciudad de Kansas.

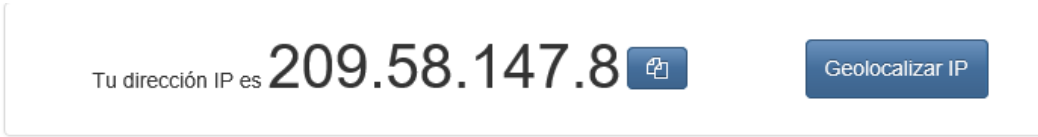
| | | | | | |
|---|---|---|---|---|---|
| 56 | 0.135322 | 10.112.1.183 | 162.251.5.82 | UDP | 156 55888 → 11013 Len=114 |
| 58 | 0.137462 | 10.112.1.183 | 162.251.5.82 | UDP | 189 55888 → 11013 Len=147 |
| 60 | 0.139891 | 10.112.1.183 | 162.251.5.82 | UDP | 210 55888 → 11013 Len=168 |
| 63 | 0.144181 | 10.112.1.183 | 162.251.5.82 | UDP | 170 55888 → 11013 Len=128 |
| 65 | 0.144402 | 10.112.1.183 | 162.251.5.82 | UDP | 179 55888 → 11013 Len=137 |
| 67 | 0.145665 | 10.112.1.183 | 162.251.5.82 | UDP | 183 55888 → 11013 Len=141 |
| 69 | 0.148445 | 10.112.1.183 | 162.251.5.82 | UDP | 171 55888 → 11013 Len=129 |
| 72 | 0.151279 | 10.112.1.183 | 162.251.5.82 | UDP | 156 55888 → 11013 Len=114 |
| 73 | 0.152076 | 10.112.1.183 | 162.251.5.82 | UDP | 196 55888 → 11013 Len=154 |




| Proveedor de Internet | Pais | Proxy |
|---|---|---|
| Virtual VM | United States | no |

Y para la segunda captura con el protocolo TCP, se nos asigno la IP 209.58.147.8 cuya dirección en el mapa se encuentra en la Dallas.

| | | | | | |
|---|---|---|---|---|---|
| 123 | 0.749820 | 10.112.1.183 | 209.58.147.8 | TCP | 66 56070 → 13926 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 154 | 0.911363 | 10.112.1.183 | 209.58.147.8 | TCP | 54 56070 → 13926 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 155 | 0.911899 | 10.112.1.183 | 209.58.147.8 | TCP | 271 56070 → 13926 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=217 |
| 183 | 1.109926 | 10.112.1.183 | 209.58.147.8 | TCP | 54 56070 → 13926 [ACK] Seq=218 Ack=31 Win=131328 Len=0 |
| 207 | 1.309566 | 10.112.1.183 | 209.58.147.8 | TCP | 54 56070 → 13926 [ACK] Seq=218 Ack=92 Win=131072 Len=0 |
| 212 | 1.344821 | 10.112.1.183 | 209.58.147.8 | TCP | 66 56072 → 13926 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 231 | 1.566533 | 10.112.1.183 | 209.58.147.8 | TCP | 54 56072 → 13926 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 232 | 1.566801 | 10.112.1.183 | 209.58.147.8 | TCP | 540 56072 → 13926 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=486 |
| 267 | 1.781552 | 10.112.1.183 | 209.58.147.8 | TCP | 54 56072 → 13926 [ACK] Seq=487 Ack=100 Win=131072 Len=0 |
| 308 | 1.968807 | 10.112.1.183 | 209.58.147.8 | TCP | 54 56072 → 13926 [ACK] Seq=487 Ack=110 Win=131072 Len=0 |
| 329 | 2.123349 | 10.112.1.183 | 209.58.147.8 | TCP | 240 56072 → 13926 [PSH, ACK] Seq=487 Ack=905 Win=130304 Len=186 |




| Proveedor de Internet | Pais | Proxy |
|---|---|---|
| Leaseweb USA | United States | no |

Con esto se comprueba el funcionamiento correcto de la VPN, en específico de flyVPN, cabe destacar también que flyVPN ocupa la tecnología de encriptación 256-AES technology la cual es un algoritmo de encriptación de los mas confiables actualmente, por lo que la seguridad, al menos con este servicio de VPN no es un problema al momento de conectarse.

# Conclusiones

Podemos concluir que VPN es un protocolo versátil, ya que como observamos mediante Wireshark, que este utiliza tanto UDP como TCP. Además de que la aplicación flyVPN te da la opción de utilizar el protocolo que tú prefieras, lo que, para ser una aplicación gratuita de VPN, es una herramienta muy importante al momento de elegir el servicio VPN a utilizar.

VPN nos entrega una herramienta muy útil, ya que con ella podemos acceder a diferentes servicios que no se encuentren disponibles en nuestra zona geográfica. Además de brindarnos seguridad, ya que protege nuestra dirección IP, similar a como funciona una NAT, contenido que vimos durante el desarrollo del curso.

Además, dependiendo de los servicios que necesites utilizar en la red, es recomendable usar alguna VPN, por ejemplo si queremos acceder a contenido no disponible en nuestra región o nuestra red local, ocupar una VPN es la mejor opción, pero si necesitamos una conexión en tiempo real, como un videojuego multijugador en línea, es recomendable no utilizar este servicio ya que el tiempo de retrasmisión es mucho mayor si la VPN esta alejada del servidor central.

# Bibliografía


https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

https://www.ecured.cu/Red_privada_virtual

https://www.kaspersky.es/resource-center/definitions/tunneling-protocol

https://www.textoscientificos.com/redes/redes-virtuales/tuneles/l2f

https://www.redeszone.net/2019/04/21/proveedores-vpn-protocolo-sstp/