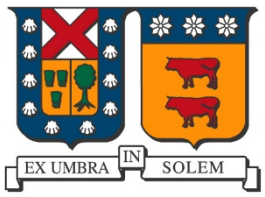

Universidad Técnica Federico Santa María

Casa Central

Redes de computadores I - ELO322

1er Semestre 2016

INFORME PROYECTO

ANÁLISIS DE SERVICIOS VPN

Profesor Agustín J. González V.

Integrantes Nicole Fernández

Sebastián Oyanadel

Fecha 1 de Julio del 2016

Resumen

El desarrollo de Internet ha permitido que los usuarios alrededor del mundo puedan acceder a una gran variedad de información mediante sólo un click, lo cuál ha traído bastantes ventajas, ya sea una disminución del tiempo de búsqueda, una mayor cantidad de fuentes de información, aumentar la conectividad a nivel global, etc. No obstante existen algunos sitios que se encuentran afectos a restricciones geográficas, por lo que para acceder a ellas es necesario cumplir con ciertos requisitos. En este trabajo se presentará una solución para este tipo de situación, mediante el análisis de dos aplicaciones que permiten establecer una conexión VPN.

Introducción

A lo largo de los años, internet se ha convertido en uno de los pilares fundamentales para la comunicación y conectividad del mundo. Permitido a los usuarios mediante sólo un click acceder a una gran variedad de información de forma rápida y sencilla, disminuyendo enormemente el tiempo de búsqueda y aumentando a su vez la conectividad a nivel global.

Sin embargo, existen ciertos sitios cuyo contenido se encuentran restringidos a ciertas regiones específicas, por lo que para acceder a dicha información es necesario cumplir con ciertos requisitos. Esto se debe principalmente a asuntos legales y/o contratos comerciales (por ejemplo, derechos de autor o transmisión exclusiva).

En este trabajo, detallaremos el funcionamiento de redes privadas virtuales VPN, empleadas por las aplicaciones web estudiadas que nos permiten acceder a los contenidos bloqueados. Además, realizaremos una comparación con redes de anonimato “Tor (The Onion Router) y expondremos el análisis práctico de las aplicaciones empleadas, estas son “Hotspot Shield” y “Hola”.

¿Qué es una red VPN?

Antes de dar alguna definición o comenzar a hablar del funcionamiento de una red VPN, es necesario partir hablando acerca de lo que es la seguridad de redes.

Seguridad de redes

Es de nuestro conocimiento que dentro de la internet podemos encontrar distintos tipos de ataques, ya sean softwares maliciosos, de denegación de servicio, de husmeadores, de enmascaramiento de orígenes y algunos de borrado y modificación de mensajes. Es por ello que surge la necesidad de dotar de seguridad a las redes frente a estos posibles ataques.

Tomando en cuenta lo que uno espera de una comunicación segura, se pueden distinguir las siguientes características:

I. **Confidencialidad**: Hace referencia a que el contenido del mensaje transmitido debe ser comprendido sólo entre emisor y receptor. Esto implica que los mensajes deberán ser cifrados, de manera que, si alguien intenta interceptar el mensaje, este no pueda comprender su contenido.
II. **Autenticación del punto terminal**: Emisor y receptor deben poder confirmar la identidad del otro en el proceso de comunicación, ya que alguien se puede estar haciendo pasar por alguno de estos.
III. **Integridad del mensaje**: Asegurar que el contenido del mensaje no ha sido modificado durante la transmisión.
IV. **Seguridad operacional**: Implementación de dispositivos operacionales (firewall, sistemas de detección de intrusos, etc.), para poder responder a ataques efectuados hacia alguna organización, ya que estas al estar conectadas a la red pública internet pueden verse invadidas por atacantes que busquen conseguir información importante de esta.

Ahora teniendo una noción más clara acerca de qué es lo que se espera de la comunicación segura, nos centraremos en el tema de seguridad de la capa de red. Cabe destacar que existen protocolos de seguridad para cada una de las cuatro capas superiores.

IPsec y VPN

Las redes privadas virtuales surgen a raíz de que instituciones con sucursales ubicadas en distintas regiones desearán tener su propia IP, para que así sus hosts y servidores puedan realizar un intercambio de datos de manera segura y confidencial.

En una primera instancia surgen las redes privadas, las cuáles constan de la implementación de una red física independiente; el problema de estas redes es que pueden llegar a ser muy costosas, es por ello que una vía más económica e igual de eficiente son las redes privadas virtuales.

Las VPN son redes creadas sobre la red internet pública, por lo que los datos enviados entre sucursales se transportan a través de internet. Ahora la pregunta es:

¿ Cómo las VPN nos otorgan seguridad y confidencialidad a la hora de enviar datos?. La respuesta a esta interrogante es que los datos enviados son cifrados antes de que estos entren a la red de internet.

A través del protocolo de seguirdad IPsec es posible la creación de redes privadas virtuales. Dentro de los protocolos IPsec podemos encontrar el protocol [1]ESP. Este protocolo proporciona todas las características deseables para una comunicación segura, por lo que de aquí en adelante las referencias de IPsec se harán con respecto a este protocolo.

El protocolo IPsec realiza un cambio del datagrama IP al que normalmente estamos acostumbrados. El formato de este nuevo datagrama tiene la siguiente forma:

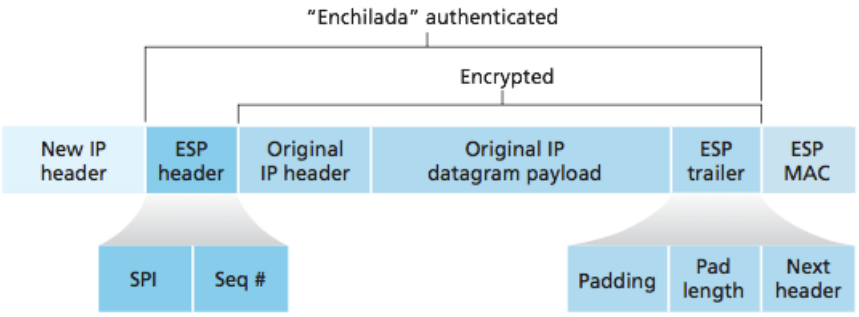

Figura 1. Formato del datagrama IPsec.

Como se puede ver en la *Figura 1*, aparecen nuevos campos los cuáles se añaden al datagrama original. Los nuevos campos añadidos son : Cola ESP, cabecera ESP, MAC ESP y una nueva cabecera IP. Estos campos nuevos permiten realizar un envío seguro de datagramas, ya que como se puede ver el datagrama original se encuentra encriptado, lo que nos asegura confidencialidad del mensaje. También destacar que el campo MAC ESP, nos proporciona la autenticación en el punto terminal. Para finalizar la nueva cabecera IP, permite que los routers por los que viajará el datagrama no detecten que el datagrama se encuentra cifrado por IPsec.

[1] ESP: Encapsulation Security Payload.

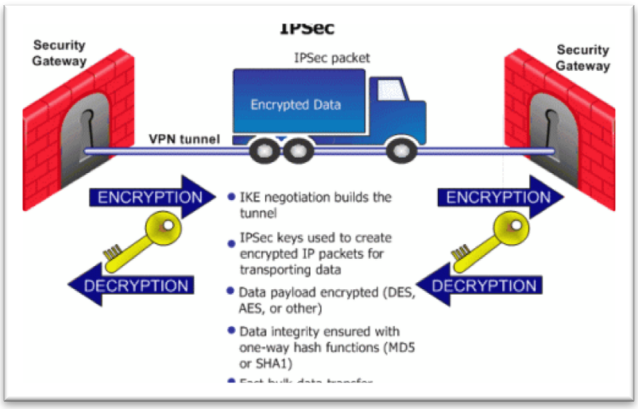

Figura 2. Ilustración del transporte vía Tunneling

Hola VPN

Es tanto una aplicación web, como móvil, tipo extensión de navegador que ofrece servicios VPN de forma gratuita y además posee una versión pagada denominada "Hola – Luminati". La principal motivación de los fundadores de este servicio fue proporcionar un servicio de internet con un acceso mucho más rápido, libre y más barato de operar. Para ello, utilizaron técnicas de enrutamiento, principalmente de carácter punto a punto.

Funcionamiento : Cuando un usuario accede a ciertos sitios que se encuentran bloqueados por área geográfica, la aplicación redirige la solicitud de ingreso a otro usuario de la aplicación que se encuentre en las zonas donde es posible acceder al contenido deseado. Dicho usuario, del país sin restricción actúa como nodo de salida y a través de su conexión a internet ingresamos a los sitios geo-bloqueados. Las conexiones son realizadas directamente de la interacción de los routers y terminales de los mismos usuarios.

Hotspot Shield

Esta es una de las soluciones al problema planteado al principio de este documento, ya que HotSpot Shield es una aplicación, desarrollada por AnchorFree, Inc., que permite el establecimiento de una VPN. A diferencia de Hola!, Hotspot Shield se conecta directamente a servidores propios, lo que otorga una mayor seguridad de los datos y además nuestro ancho de banda no se ve comprometido.

Esta aplicación posee dos versiones : Free Hotspot Shield y la versión Elite. Esta aplicación tiene servidores propios, los que están ubicados en Estados Unidos, Australia y Reino Unido. La versión Elite proporciona ciertos features importantes con respecto a la versión gratuita :

- Servicio de soporte dedicado al cliente.
- Eliminación de Ads.
- Protección completa
- Servicio de soporte dedicado al cliente.

Parte práctica

Para ver de forma práctica el funcionamiento tanto de la aplicación Hotspot Shield, como la de la extensión Hola!, se utilizó un geolocalizador, el cuál permitió conocer la IP con que se le asociaba al equipo una vez la aplicación se encontraba activa. Primero se verificó la IP asociada al tener la aplicación inactiva :

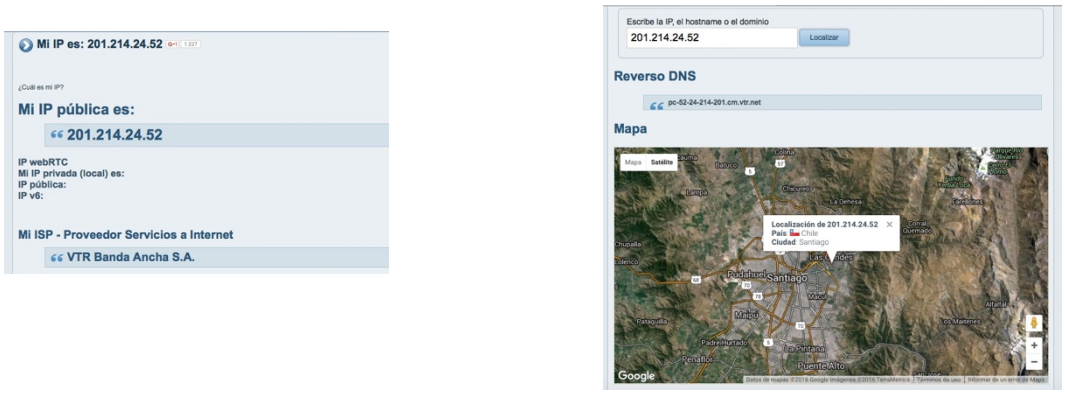

Figura 3. Comprobación de la dirección IP y geolocalización

- Activando Hotspot Shield:

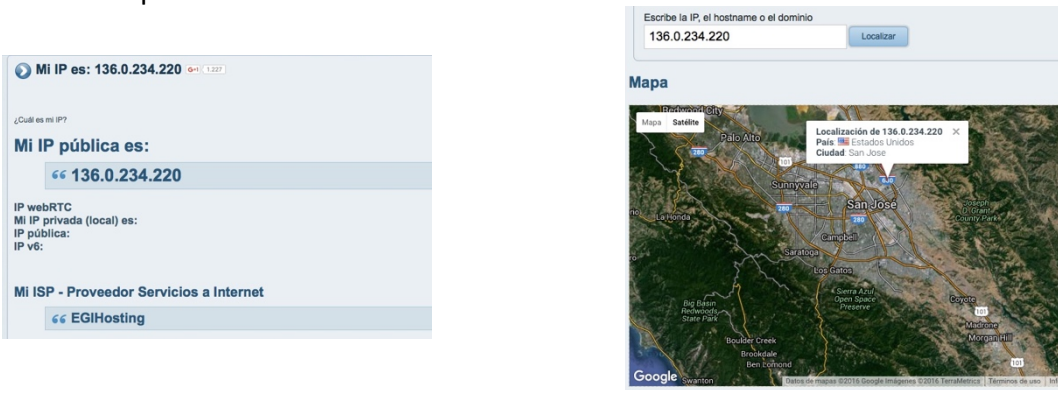

Figura 4. Comprobación IP y geolocalización.

Para el caso de la extensión Hola! ocurre la misma situación. Al activar la extensión esta inmediatamente se conecta al usuario del país que actuará como nodo de salida, de esta manera se puede acceder a aquellos sitios que se encontraban anteriormente bloqueados. Para mayor claridad el funcionamiento de Hola! se puede ver en el siguiente enlace :

https://www.youtube.com/watch?v=ZRbmkdy79OE

Conclusiones

- La redes VPN son una buena solución ante la restricción de contenido a la que se pueden encontrar los usuarios de internet a causa de su ubicación geográfica, ya que permiten una navegación anónima.
- Estas redes deben cumplir con características de navegación segura, para que de esta manera nuestros datos se encuentren protegidos ante los posibles ataques que ya han sido estudiados en el curso.
- El protocolo IPsec es el encargado de "modificar" al datagrama original, este lo realiza mediante la incorporación de campos que proporcionan la seguridad que proporcionan la seguridad que se requiere en el envío de datos.
- Algunos servicios VPN se han encontrado con muchas quejas por parte de sus usuarios, ya que estos pueden hacer un mal uso del ancho de banda.

Referencias

[1] Kurose & Ross, (2013), Computer Networking: A Top-Down Approach, 6th Edition, Amherst -Brooklyn, United States of America., Editorial Pearson

[2] Wikipedia – Red privada virtual
https://es.wikipedia.org/wiki/Red_privada_virtual

[3] Aplicación Hotspot Shield
https://www.hotspotshield.com/es/

[4] Aplicación Hola VPN
https://hola.org/

[5] Wikipedia – Ipsec
https://es.wikipedia.org/wiki/IPsec

[6] Youtube – Demostración del uso de la aplicación Hola VPN
https://www.youtube.com/watch?v=ZRbmkdy79OE