Utilización y Aplicación de Túneles IPsec en ambiente de VPN empresarial

Sebastián Araya, Carlos Carvajal, Andrés Llico.

Resumen— **La utilización de un sistema VPN en nuestra universidad permite a los profesores e investigadores el acceso remoto a las bibliotecas digitales accesibles desde el interior de la red de la universidad tal cual como si estuvieran "físicamente" al interior de ella. Las redes privadas virtuales basadas en IPSec permiten hacer este trabajo de manera segura e independiente de las aplicaciones. En este informe se tratarán los aspectos generales de un VPN, un túnel y la acción de tunneling, los principios de seguridad en la red, el concepto de IPSec, sus tecnologías y términos asociados, además de cómo responde IPSec a los principios de seguridad previamente planteados, para finalizar con la implementación y funcionamiento de IPSec y el sistema VPN de la universidad. Para responder a todo esto se realizó una investigación tanto a los conceptos teóricos como a prácticas de la vida real que forman parte de un sistema como el que será acá expuesto. Los resultados obtenidos permiten tener una idea al menos básica respecto de cómo funciona y en qué consiste esta tecnología que crece cada día en el mundo (recordar gráfico de la visita a Global Crossing) con una mención especial al caso de nuestra universidad, donde también está implementada.**

Palabras Claves— **VPN, IPsec, Tunneling.**

I. Introduction

AQUIÉN ? no le agrada trabajar desde la comodidad del hogar y, además, de forma segura y confiable?. A qué multinacional no le interesa que sus centrales y sucursales estén siempre conectadas de la misma manera? Imaginemos este último escenario con distancias contientales. Si se usara una red LAN el costo de implementación es increíblemente elevado. Asimismo, si se pensara en tener un cable desde la universidad al hogar de cada profesor/investigador, el costo no es factible y se atenta contra la conectividad que otorga internet y que la diferencia de los circuitos telefónicos. La solución a esto son las VLAN o *Virtual*-LAN, que crean una red similar a una LAN pero sin que los equipos se encuentren físicamente dentro de una. Ahora, para aplicar el concepto de privacidad estn las VPN (redes privadas virtuales) que bloquean, de manera similar a una LAN privada, las intrusiones de terceros, de diversas maneras. Una de estas maneras, que es la tratada en este informe, es la que utiliza la familia de protocolos IPSec, una familia de tecnologías que permite autenticar y encriptar los paquetes IP de un stream de datos, dentro de otras cosas que serán explicitadas en la sección correspondiente. Así, creada la red virtual gracias a un *túnel* e implementando IPSec obtendremos la solución VPN que nos asegurará la compleción de los principios de seguridad en la

red también planteados en este informe.

II. Qué es VPN ?.

Se puede definir a una Red Privada Virtual VPN (sigla del inglés Virtual Private Network) como una tecnología de red que permite la extensión de una red interna de una Organización sobre una red pública o no controlada (red insegura), externa a la Organización, como por ejemplo Internet, otorgando al usuario los mismos privilegios y nivel de acceso a la información que tendría si estuviese dentro de la Organización (físicamente).

III. Qué es un túnel ?.

Se define como túnel a un conducto que traza un camino unico desde un sitio a otro para transferir datos. Es el concepto clave para entender una VPN.

A. Qué es tunneling ?.

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras.

IV. Seguridad

A. Principios de seguridad en la Red

Toda solución de seguridad debe cumplirlos. Dentro de las muchas características de seguridad que uno busca cumplir, éstas se resumen en una tríada fundamental. Los principios fundamentales son los de Disponibilidad, Confidencialidad e Integridad. Luego de estos se plantean los de no repudiación y autenticidad, los que también son muy importantes pero no estrictamente. La disponibilidad apunta a que una sesión de trabajo se lleve a cabo y termine correctamente. De la mano con la disponibilidad va la accesibilidad, pues no basta que un recurso esté disponible, si no que sea utilizable con tiempos de respuesta aceptables. "La confidencialidad es la mantención del secreto de las informaciones" ("La confidentialité est le maintien du secret des informations", cita de "Le petit Robert") es decir, puede ser vista como la proteción de los datos contra una divulgación no autorizada. La integridad se refiere a que los recursos, datos, tratamientos, transacciones o servicios no hayan sido modificados, alterados o destruidos de forma intencional o accidental. La no repudiación es "la prevención de la negación de que un mensaje ha sido enviado o recibido y asegura que el emisor del mensaje no pueda negar que lo envió o que el receptor niegue haberlo recibido. La propiedad de no repudiación de un sistema de seguridad de redes de cómputo se basa en el uso de firmas digitales". La autenticación permite verificar la identidad anunciada y de asegurarse que ésta no fue usurpada. Usa el control de acceso.

B. Qué es IPSec?

IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. Los protocolos de IPsec actúan en la

capa de red. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa de transporte, incluyendo TCP y UDP, los protocolos más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

C. Tecnologías y conceptos asociados a IPSec

C.1 Llaves.

Para asegurar la confiabilidad e integridad de los mensajes intercambiados a través de una red se distinguen 2 tipos de llaves: públicas y privadas. Por lo tanto, en una comunicación, el que transmite el mensaje lo codifica utilizando la llave pública del destinatario, el que con su llave privada podrá decodificar el mensaje. Para que el destinatario pueda responder, debe tener la llave pública del emisor y decodificará con su llave privada. A este esquema se le denomina un sistema de llaves asimétrico. Por otro lado existen sistemas de llaves simétricas, donde la misma llave se utiliza tanto para decodificar como para codificar los mensajes, por lo cual se debe compartir y mantener en absoluto secreto entre ambos participantes de la comunicación.

C.2 Certificados.

Pero la existencia de tantas llaves públicas dentro de una red hace necesaria una identificación que permita asociar cada una de ellas a sus respectivos dueños. Es de ahí que surge un documento electrónico donde se indican datos como: el propietario de la llave, algoritmo usado para su creación, su tiempo de validez, su propósito, la llave pública en sí, entre otras cosas. A este documento se le denomina certificado.

C.3 CA.

La estructura de los certificados es de conocimiento público, por ende, cualquier persona es capaz de crear el suyo propio. Pero para poder asegurar que el certificado fue emitido por una persona sin fines maliciosos, se crean entidades de confianza que son las responsables de emitir y revocar dichos certificados. A éstas se les denominan Autoridades de certificación (Certification Authority). Estas vienen incorporadas de forma nativa en la base de datos de los sistemas operativos y permiten comprobar si tras los certificados que las distintas aplicaciones requieran, existe una autoridad que acredite que dicho certificado es de confianza o no.

C.4 SA.

El establecer una comunicación entre dos máquinas para realizar un intercambio de información de forma segura se le denomina Asociación de Seguridad (Security Association) dentro de lo cual se incluyen aspectos como las llaves y los cer-

tificados a usarse, entre otras cosas.

C.5 ISAKMP.

Pero cuando se habla de comunicaciones a través de Internet, el protocolo que rige el establecimiento de asociaciones de seguridad (SA) se denomina ISAKMP (Internet Security Association and Key Management Protocol). Bajo este protocolo se definen los procedimientos para la autentificación; la creación, modificación y eliminación de SAs; técnicas para la generación de llaves, etc. ISAKMP se implementa sobre la capa de transporte y se puede implementar sobre cualquier protocolo de la misma.

C.6 IKE / IKEv2.

Pero un protocolo que diga cómo establecer las asociaciones de seguridad no es suficiente, por ende, para poder configurar una SA, en particular sobre IPsec, se requiere un protocolo que establezca cómo se realizará el intercambio secreto de llaves y para ello además se apoya en ISAKMP. A este protocolo se le denomina IKE (Internet Key Exchange). IKE consta de 2 etapas:

- Una primera etapa en donde se establece un canal de comunicación segura, generando las llaves secretas que se utilizarán para la encriptación.
- Mientras que en la segunda etapa, utilizando el canal generado, se realiza la negociación de la SA y otros servicios como por ejemplo IPsec.

Pero IKE está abierto a diferentes interpretaciones, y al contar con múltiples opciones de configuración carece de sencillez, dificultando la comunicación en que ambas partes debían contar con la misma configuración (parámetro a parámetro). De allí surge la necesidad de crear un protocolo más sencillo que permitiese implementarse de forma universal y a la vez automatizado, con lo cual surge IKEv2.

C.7 AH.

En los paquetes enviados en una comunicación utilizando IPsec, existe un elemento importante que permite garantizar la integridad y que la fuente de origen sea autentica. Por lo cual, a los paquetes de IPsec se les agrega un encabezado denominado Authentication Header donde se establecen los parámetros para llevar esto a cabo. Cabe señalar que AH además protege todos los campos no-modificables de los paquetes IP.

C.8 ESP.

Al igual que AH, ESP busca proporcionar integridad, autenticidad y confidencialidad de los paquetes. Para ello puede operar en distintas modalidades: de sólo cifrado, sólo autentificación o ambas. La última es la ms utilizada pues otorga una mayor seguridad. Por otro lado, la gran diferencia que tiene de AH es que no proporción protección contra errores en la cabecera de los paquetes IP.

C.9 KINK.

Al igual que IKE, KINK es un protocolo que permite configurar las asociaciones de seguridad (SA) pero que utiliza el protocolo Kerberos que le permite a terceros manejar la autentificación entre las máquinas que se desean comunicar y además las políticas de seguridad de forma centralizada.

D. Servicios de IPSec y cómo responden a los principios de seguridad en la red.

Dado que IP no provee por sí sólo ninguna capacidad de seguridad, IPSec fue creado para otorgárselos. Así, cifrando el tráfico nos aseguramos de la confidencialidad, con la validación nos aseguramos de la integridad, la autenticación se garantiza al autenticar los extremos (asegurar que el extremo es de confianza) y además nos aseguramos de la anti-repetición. Como fue mencionado previamente en la sección de tecnologías y conceptos asociados, los principios de seguridad se logran gracias a los protocolos AH (Authentication Header) y el ESP (Encapsulating Security Payload).

V. Conclusiones.

Los sistemas IP VPN crecen con mayor rapidez cada día. Se pudo ver en la visita a Global Crossing. A futuro este sistema será utilizado con Ipv6, pues fue pensado originalmente para él. 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 trasnferencia de datos de un lugar a otro.

Referencias

[1] *http://html.rincondelvago.com/administracion-de-redes.html*,

[2] *http://ru.wikipedia.org/wiki/RADIUS*

[3] *http://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol*

[4] *https://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html*

[5] *http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol#L2TP.2FIPsec*

[6] *http://en.wikipedia.org/wiki/VPN*

[7] *http://www.dcsc.utfsm.cl/redes/vpn/index.html*

[8] *http://www.cisco.com/en/US/products/sw/secursw/ps2308/*

[9] *http://fr.wikipedia.org/wiki/IPsec*

[10] *http://ru.wikipedia.org/wiki/IPsec*

[11] *http://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n*

[12] *http://en.wikipedia.org/wiki/Certificate_authority*

[13] *http://en.wikipedia.org/wiki/Digital_certificate*

[14] *http://en.wikipedia.org/wiki/Public_key*

[15] *http://es.wikipedia.org/wiki/IPsec*

[16] *http://en.wikipedia.org/wiki/Kerberized_Internet_ Negotiation_of_Keys*

[17] *http://en.wikipedia.org/wiki/Internet_Key_Exchange*

[18] *http://en.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol*

Contents

VI. Anexos.

A. Cómo funciona IPsec y el vpn de la universidad.

En el sistema de VPN de la universidad cada usuario que desee utilizar la VPN debe estar *inscrito*. Se le otorga un nombre de usuario y contraseña únicos (al menos el nombre de usuario). Para poder acceder al servicio, deben correr desde su ordenador el cliente sw de Cisco, donde una interfaz amigable los espera. Normalmente luego de la configuración inicial solamente deberán abrirlo e iniciar la conexión. Hecho esto, establecerán una conexión segura con la UTFSM y una IP local (de la red UTFSM). Pero esto va más allá, lo que sucede por debajo de este escenario aparente es que el cliente entabla una conexión con la $ASA5510$, que es la máquina que permite iniciar la conexión hacia la red USM, ésta confirma con el servidor RADIUS que el usuario y su contraseña son válidos (RADIUS gestiona los usuarios con el servidor LDAP) y si los parámetros son aceptados, se dará acceso al sistema y se asignan los recursos de dirección IP y el túnel (que bien podría ser L2TP: Layer 2 Tunneling Protocol). Luego de esto, el usuario navega con todas las ventajas que tendría como si estuviera físicamente en la UTFSM, pero en la comodidad de su hogar (probablemente) y a través de un canal inseguro, como es la internet, que es en sí la *gran magia* de aplicar un túnel con IPSec.