Universidad Autónoma de Entre Ríos

FCyT FACULTAD DE CIENCIA Y TECNOLOGÍA

"Red Privada Virtual (VPN) sobre Protocolo de Internet versión 6 (IPv6)"

Tesis presentada como requisito para obtener el titulo Licenciado en Sistemas Informáticos (Plan 2005 –Resolución MECyT n. º 148/2005)

Por

Rodrigo Paúl Basso

Maximiliano Sebastián Toso

Director: **Mag. Ing. Julio Aldonate**

Co-Director: **Lic. Luciano Caisso**

Oro Verde, 2018

① BASSO, Rodrigo Paul DNI 34163832

Plan: 2001

Materia: Síntesis de Sistemas (11438)

Nota: 9 (nueve)

Fecha: 18/12/2018

Acta/Res: 01-0162-18

Título: Lic. en Sistemas Informáticos

② TÓSO, Maximiliano Sebastián DNI 31724899

Plan: 2001

Materia: Síntesis de Sistemas (11438)

Nota: 9 (nueve)

Fecha: 18/12/2018

Acta/Res: 01-0162-18

Título: Licenciado en Sistemas Informáticos.

Aprobación de director y co-director

En carácter de director y co-director del proyecto "Red Privada Virtual (VPN) sobre Protocolo de Internet versión 6 (IPv6)" elaborado por Rodrigo Basso y Maximiliano Toso, consideramos que el trabajo se encuentra en condiciones de ser sometido a presentación pública y evaluación.

Ciudad de Oro Verde, lunes 3 de diciembre de 2018.

Director
Mag. Ing. Julio Aldonate

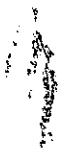
Co-director
Lic. Luciano Caisso

Agradecimientos

A nuestras familias, y a todas aquellas personas que de una u otra forma hicieron posible la realización de este trabajo. Especialmente a nuestro director Julio Aldonate y codirector Luciano Caisso por el tiempo, la motivación y ayuda brindada.

A los docentes y trabajadores de la Facultad de Ciencia y Tecnología, por su acompañamiento y sustento durante esta etapa que culmina.

A todos, muchas gracias...



INDICE

Índice de figuras

Índice de tablas

CARTILLA DE SIGLAS

3DES	*Triple Data Encryption Standard*, Estándar de Triple Cifrado de Datos
AAA	*Authentication, Authorization, and Accounting*, Autenticación, Autorización y Auditoria
ABM	Alta, Baja y Modificación
ADSL	*Asymmetric Digital Subscriber Line*, Línea de Abonado Digital Asimétrica
AES	*Advanced Encryption Standard*, Estándar de Cifrado Avanzado
AfriNIC	*Regional Registry for Internet Number Resources serving the African*, Registro Regional de Internet para África
AH	*Authentication Header*, Cabecera de Autenticación
APNIC	*Asia-Pacific Network Information Centre*, Registro Regional de Direcciones de Internet para Asia y el Pacífico
ARIN	*American Registry for Internet Numbers*, Registro Regional de Internet para América Anglosajona
ARP	*Address Resolution Protocol,* Protocolo de Resolución de Dirección
ATM	*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrona
BSD	*Berkeley Software Distribution*, Distribución de Software Berkeley
CA	*Certification Authority,* Autoridad Certificante
CDU	Concepción del Uruguay
CHAP	*Challenge Handshake Authentication Protocol,* Protocolo de Autenticación de Intercambio de Señales
CIDR	*Classless Interdomain Routing*, Enrutamiento Entre Dominios Sin Clases
DES	*Data Encryption Standard*, Estándar de Cifrado de Datos
DH	*Diffie-Hellman*
DHCP	*Dynamic Host Configuration Protocol*, Protocolo de Configuración Dinámica de Host
DMZ	*Demilitarized Zone*, Zona Desmilitarizada
DNS	*Domain Name System,* Sistema de Nombres de Dominio
EH	*Extension Header*, Encabezado de Extensión
ESP	*Encapsulating Security Payload*, Carga de Seguridad de Encapsulación
FCyT	Facultad de Ciencia y Tecnología
FTP	*File Transfer Protocol,* Protocolo de Transferencia de Archivos
GB	*Gigabyte*
GHz	*Gigahercio*
GRE	*Generic Routing Encapsulation*, Encapsulación de enrutamiento genérico
HMAC	*Hashed Message Authentication Code*, Código de Autentificación de Mensajes Basado en Hash
HTTP	*Hypertext Transfer Protocol,* Protocolo de Transferencia de Hypertexto
ICMP	*Internet Control Message Protocol,* Protocolo de Internet de Control de Mensajes
IEEE	*Institute of Electrical and Electronics Engineers,* Instituto de Ingeniería Eléctrica y Electrónica
IETF	*Internet Engineering Task Force,* Grupo de Trabajo de Ingeniería de Internet

IKE	*Internet Key Exchange*, Intercambio de Claves de Internet
IPSec	*Internet Protocol Security*, Protocolo de Internet Seguro
IPv4	Internet Protocol version 4, Protocolo de Internet versión 4
IPv6	Internet Protocol version 6, Protocolo de Internet versión 6
IPX	*Internetwork Packet Exchange*, Intercambio de Paquetes Inter Red
ISAKMP	*Internet Security Association and Key Management Protocol*, Asociación para Seguridad en Internet y Protocolo de Administración de Claves
ISO	*International Organization for Standardization*, Organización Internacional para la Estandarización
ISP	*Internet Service Provider*, Proveedor de Servicios de Internet
L2F	*Layer Two Forwarding*, Reenvío de Nivel 2
L2TP	*Layer Two Tunneling Protocol*, Protocolo de Túnel de Nivel 2
LACNIC	*Latin America & Caribbean Network Information Center*, Registro de Direcciones de Internet para América Latina y Caribe
LAN	*Local Area Network*, Red de Área Local
LCP	*Link Control Protocol*, Protocolo de Control de Enlace
MB	*Megabyte*
MBPS	*Megabits Perc Second*, Megabits por segundo
MD5	*Message-Digest Algorithm 5*, Algoritmo de Resumen del Mensaje 5
MIT	*Massachusetts Institute of Technology*, Instituto Tecnológico de Massachusetts
MPLS	*Multiprotocol Label Switching*, Conmutación Multiprotocolo Mediante Etiquetas
MTU	*Maximum Transmission Unit*, Unidad máxima de transferencia
NAT	*Network Address Translation*, Traducción de Direcciones de Red
NCP	*Network Control Protocol*, Protocolo de Control de Red
NetBEUI	*NetBios Extended User Interface*, Interfaz extendida de usuario de NetBIOS
NetBIOS	*Network Basic Input/Output System*, Sistema de Entrada Salida Básica de Red
NIST	*National Institute of Standards and Technology*, Instituto Nacional de Estándares y Tecnología
OSI	*Open System Interconnection*, Interconexión de Sistemas Abiertos
OV	Oro Verde
PAP	*Password Authentication Protocol*, Protocolo de Autenticación de Contraseña
PDA	*Personal Digital Assistant*, Ayudante personal digital
PDU	*Protocol Data Units*, Unidad de Datos de Protocolo
PFS	*Perfect Forward Secrecy*, Secreto Perfecto Hacia Adelante
PKI	*Public Key Infraestructure*, Infraestructura de Clave Pública
PPP	*Point to Point Protocol*, Protocolo Punto a Punto
PPPoE	*Point-to-Point Protocol over Ethernet*, Protocolo Punto a Punto sobre Ethernet
PPTP	Point to Point Tunneling Protocol, Protocolo de Tunelización Punto a Punto
PSK	Pre-Shared Key, Clave Secreta Compartida
PVC	*Permanent Virtual Circuit*, Circuitos Virtuales Permanente

QoS	*Quality of Service,* Calidad de Servicio
RADIUS	*Remote Dial-in User Services,* Servicio de Autenticación Remota de Llamada de Usuario
RAID	*Redundant Array of Independent Disks,* Matriz Redundante de Discos Independientes
RC	*Ron's Code,* Código de Ron
RFC	*Request For Comments,* Petición de comentarios
RIPE NCC	*Réseaux IP Européens Network Coordination Centre,* Registro Regional de Internet para Europa y Oriente Medio
RIR	*Regional Internet Registry,* Registro Regional de Internet
RPM	*Revolutions Per Minute,* Revoluciones por Minuto
RSA	*Rivest, Shamir y Adleman*
SA	*Security Association,* Asociación de Seguridad
SATA	*Serial Advanced Technology Attachment,* Adjunto de Tecnología Avanzada de Serie
SDRAM	*Double Data Rate Synchronous Dynamic Random-Access Memory,* Memoria de acceso aleatorio síncrona y dinámica
SHA	*Secure Hash Algorithm,* Algoritmo de Hash Seguro
SMTP	*Simple Mail Transfer Protocol,* Transferencia Simple de Correo
SNMP	*Simple Network Management Protocol,* Protocolo Simple de Administración de Red
SSL	*Secure Sockets Layer,* Nivel de Sockets Seguros
SSTP	*Secure Socket Tunneling Protocol,* Protocolo de Capa de Conectores Seguros
TACACS+	*Terminal Access Control Access Control Server Plus,* Servidor de Control de Acceso a Terminal y Control de Acceso
TCP	*Transmission Control Protocol, Protocolo de Control de Transmisión*
TFTP	*Trivial File Transfer Protocol,* Protocolo de Transferencia de Archivos Trivial
TTL	*Time To Live,* Tiempo de vida
UADER	Universidad Autónoma de Entre Ríos
UDP	*User Datagram Protocol,* Protocolo de Datagrama de Usuario
VCs	*Virtual Circuit,* Circuitos Virtuales
VLSM	*Variable-Length Subnet Mask,* Máscaras de Subred de Longitud Variable
VoIP	*Voice over IP,* Voz sobre IP
VPN	Virtual Private Network, Red Privada Virtual
WAN	*Wide Area Network,* Red de Área Amplia
WWW	*World Wide Web,* Web Mundial

RESUMEN

El presente estudio tiene como finalidad dar a conocer las características de las redes privadas virtuales (VPN) corriendo sobre IPv6, tecnología que permite conectar redes distantes geográficamente, de manera segura y a bajo costo, utilizando redes públicas como medio de enlace o transmisión.

Las VPN son conocidas en el ambiente de las redes de comunicación, tal es así que existen organizaciones dedicadas exclusivamente a la investigación y prestación de servicios en el campo.

La investigación realizada presenta aspectos importantes referentes a estas tecnologías, empezando por una breve introducción, donde se analizaron conceptos y diferentes elementos que se necesitan para implementarlas y se revisaron los tipos de implementaciones comunes, los requisitos, la interacción de las VPN sobre IPv6 y sus características. Y los diferentes protocolos de túnel y seguridad que se pueden contemplar.

Se propone una metodología para la implementación de redes privadas virtuales sobre IPv6 con Internet como red de enlace para las sedes de la Facultad de Ciencia y Tecnología, metodología que brindará una serie de pasos y aspectos que se deben tomar en cuenta para esta implementación.

INTRODUCCIÓN

La presente investigación tiene como finalidad estudiar la tecnología denominada Redes Privadas Virtuales corriendo sobre la infraestructura proporcionada por IPv6. En la actualidad las VPN son muy comunes dentro de las telecomunicaciones, existiendo empresas a nivel mundial que se dedican exclusivamente a la investigación y prestación de servicios de esta tecnología corriendo sobre IPv4.

Se presentan aspectos importantes referentes a los distintos tipos de redes, empezando por una breve introducción de las redes privadas, red pública y definición de red privada virtual, además estudia los diferentes tipos y beneficios que la tecnología proporciona a las organizaciones.

En los distintos tipos de redes se utiliza la pila de protocolos TCP/IP[1], por lo que es necesario hacer su estudio, en su formato de 4 capas que corresponden a la de interfaz de red, Internet, transporte y aplicación. Así como también entrar en detalle en el protocolo emblema de este modelo, como lo es IP y las diferencias dadas en sus versiones 4 y 6.

Se analizarán los diferentes tipos y protocolos de túnel que se pueden utilizar para la implementación de VPN, entre los que se pueden mencionar PPTP[2], L2F[3] y L2TP[4] que reemplazo a L2F, además se estudiarán PPP[5] e IPSec[6], protocolos muy utilizados en varios tipos de redes.

Las Redes Privadas Virtuales poseen diferentes arquitecturas que deben ajustarse a los requerimientos de las organizaciones y surgió la necesidad de estudiar cada uno de los tipos de VPN a implementar, así como también los recursos técnicos tanto de hardware como de software.

Como se verá en el transcurso de la investigación los términos de VPN y de seguridad, van de la mano, por lo que se ha decidido dedicar un capítulo al tratamiento de las seguridades en VPN, en el que se estudiarán los distintos protocolos de seguridad corriendo sobre IP en sus dos versiones, técnicas de segurización de la información, y además las características de implementar una red privada virtual sobre IPv6.

En la parte final, se presentará una metodología para la implementación de redes privadas virtuales corriendo sobre el protocolo de internet versión 6 como red de enlace, para lo cual es necesario relevar la infraestructura de comunicaciones con que cuenta la Facultad de Ciencia y Tecnología, considerando su distribución geográfica y enlaces disponibles en cada sede. Se formularán posteriormente las conclusiones pertinentes.

[1] Se definió por primera vez en Cerf y Kahn (1974), después se refinó y definió como estándar en la comunidad de Internet; es un modelo de capas utilizado para regir la comunicación entre dispositivos en una red.

[2] Point to Point Tunneling Protocol surge de la fusión de las mejores características de PPTP de Microsoft y L2F de Cisco.

[3] Layer Two Forwarding es un protocolo de encapsulamiento que funciona en la capa de Acceso a la Red proporcionando servicios de tuneling.

[4] Layer Two Tunneling Protocol es un estándar diseñado para transmitir datos y conectar de manera segura redes.

[5] Point to Point Protocol proporciona un método para enviar datagramas sobre enlaces simples entre dos partes.

[6] IP Security es un marco de trabajo estandarizado para múltiples servicios, algoritmos y niveles de granularidad

OBJETIVO GENERAL

Diseñar una metodología de implementación de una Red Privada Virtual (VPN) corriendo sobre Protocolo de Internet versión 6 (IPv6) que interconecte las sedes neurálgicas de la Facultad de Ciencia y Tecnología (FCyT) de la Universidad Autónoma de Entre Ríos (UADER).

OBJETIVOS ESPECÍFICOS

- Analizar el funcionamiento básico y funcional de las Redes Privadas Virtuales (VPN).
- Estudiar e identificar las diferencias entre Protocolo de Internet versión4 y versión6.
- Estudiar y analizar los protocolos intervinientes en una Red Privada Virtual.
- Identificar requerimientos para la implementación de una Red Privada Virtual bajo IPv6.
- Establecer diferencias en la seguridad de una Red Privada Virtual basándose en los protocolos que intervienen.
- Identificar fortalezas y debilidades de una VPN corriendo sobre IPv6 en comparación a una aplicada sobre IPv4.
- Investigar la infraestructura de comunicaciones con que cuenta actualmente la Facultad de Ciencias y Tecnología.
- Proponer una metodología para las interconexiones de las Sedes de la Facultad de Ciencias y Tecnología mediante Red Privada Virtual sobre IPv6.

ALCANCE

Se analizarán las diferentes reglas y protocolos que intervienen en la implementación de una VPN sobre el Protocolo de Internet versión 6.

LIMITACIONES

Estudio de caso: Facultad de Ciencia y Tecnología de la Universidad Autónoma de Entre Ríos.

CAPITULO 1

[REDES Y PROTOCOLO IP]

En el primer capítulo se comienza a tomar contacto con los tipos de redes, ya sean privadas o públicas, así como también las arquitecturas y tipos de VPN. Pero los principales temas tratados se centran en el estudio del protocolo IP y el Modelo TCP/IP, analizando las diferentes capas que lo componen (Capa de Red, Capa de Internet, Capa de Trasporte y la Capa de Aplicación).

RED PRIVADA

"Una red privada o subred local es un segmento de red perteneciente a una determinada LAN (Local Area Network), que por lo general va a presentar un acceso restringido a un conjunto concreto de individuos."(Alonso, 2009)[7]

Son aquellas gestionadas por particulares, empresas u organizaciones de índole privado, a las que sólo tienen acceso las terminales de los propietarios.

RED PÚBLICA

Al hablar de red pública, se hace referencia a Internet, que puede ser definida como la red de redes, ya que la misma se compone de un sin número de redes interconectadas que trabajan de manera cooperativa brindando un servicio de comunicación de datos universal. De esta manera brinda a sus usuarios la posibilidad de transferir datos a cualquier parte del mundo o acceder a recursos disponibles ubicados fuera de los límites de la red privada.

RED PRIVADA VIRTUAL

Según Alonso (2009):

> Una VPN (Virtual Private Network) es un canal de datos privados que se implementa sobre una red de comunicaciones pública, como por ejemplo puede ser Internet. Como norma habitual, una VPN se encarga de enlazar dos subredes remotas (o una subred remota y uno o varios usuarios remotos), creando para ello un túnel virtual a través del cual serán encapsulados los paquetes antes de ser inyectados. Este encapsulado consistirá en una nueva trama de datos, pero esta vez encriptado, la cual podrá albergar protocolos de red de las capas superiores.[8]

VPN es la tecnología de redes que permite la extensión de una red de área local sobre una red pública o no controlada (como Internet). Para resguardar la confidencialidad y la integridad de la información se deben definir mecanismos de protección de los datos que se trasmiten.

La comunicación entre dos host de una red privada virtual, se logra creando túneles virtuales a través de medios públicos que usan sistemas de cifrado y autenticación para resguardar la seguridad de la información transmitida.

[7] ALONSO, J. A. (2009). *Redes Privadas Virtuales*. México: Editorial Alfaomega, p. 56.
[8] Ibid., p. 42.

ACCESO REMOTO

Se denomina acceso remoto a las conexiones realizadas desde ubicaciones distantes. Realizar este tipo de conexiones a una red ha sido un logro importante en el ambiente de las comunicaciones, ya que las organizaciones promueven viajes de trabajo de sus empleados o el trabajo desde el hogar o una dependencia remota. Para lo cual los trabajadores necesitan acceso a ciertos archivos o servicios de la red organizacional, necesidades que dan énfasis a las implementaciones de VPN.

Necesidades de Acceso Remoto

El teletrabajo es una forma flexible de trabajo organizacional, que consiste en desempeñar actividades profesionales desde el domicilio del trabajador. Engloba gran cantidad de actividades, que implican el uso de computadoras y conexión permanente entre el trabajador y la organización.

Los usuarios requieren conexiones que le permitan el acceso a las corporaciones desde cualquier lugar en el mundo, dada la necesidad de contar con los recursos organizacionales en todo momento; lo cual aumenta de manera significativa el número de dependencias remotas a interconectar.

El establecimiento de un sistema de acceso remoto en una red es una situación que debe ser planeada con cautela, por lo que se debe definir claramente a quien se le dará acceso y que tecnología se utilizará.

Existen diferentes tipos de usuarios dependiendo de las necesidades de una organización, haciendo que las soluciones de acceso remoto también varíen.

A su vez, es necesario estimar los requerimientos de ancho de banda para las diferentes conexiones y determinar si es económicamente rentable para la organización.

BENEFICIOS DE LAS VPN EN LAS ORGANIZACIONES

Dentro de los beneficios que proporciona esta técnica, es importante el costo que evita desembolsar la organización, por contratar un proveedor que garantice una línea de comunicación dedicada para trasportar información critica por redes inseguras. Servicio que puede ser reemplazado perfectamente por configuraciones de VPN, que haciendo uso de técnicas de encriptación y autenticación protegerá el canal de comunicación. A su vez, puede garantizar que la información que transita por redes públicas encapsulada por la red virtual, posee seguridad similar a la utilizada en redes LAN locales.

El panorama expuesto pone a las instituciones en situación de evaluar los beneficios que puede obtener, de proporcionar accesos remotos a sus usuarios para disponer de la información organizacional de manera segura.

Se mencionan algunas de las principales ventajas de las VPN´s, propuestas por Ariganello (2014) [9]:

- SEGURIDAD: por medio de protocolos de cifrado y autenticación se protege la información de accesos no autorizados.
- COSTOS: permite el uso de redes públicas globales para interconectar dependencias emplazadas en sitios geográficamente distantes, con permisos proporcionados a usuarios remotos para acceder a los recursos corporativos, lo que elimina el costo de abonar importantes sumas de dinero para contratar líneas dedicadas.
- ESCALABILIDAD: permite que las organizaciones utilicen la infraestructura de los proveedores de servicio de Internet, lo que facilita la tarea de agregar nuevos usuarios, sin necesidad de aumentar considerablemente los costos.
- DISPONIBILIDAD: permite el acceso a los recursos organizacionales de manera segura, desde cualquier punto geográfico.

SERVICIOS VPN PROVISTOS POR UN PROVEEDOR

Una forma sencilla de utilizar los servicios VPN es contratarlos por medio de un proveedor, lo cual es una opción para reducir tiempos de implementación.

Al decidirse por una solución brindada por un proveedor, se deben tener en cuenta una serie de recomendaciones como:

Control de cambios: cualquier cambio de control de acceso a realizarse se debe prever con un tiempo de anticipación para notificarle al proveedor.

Utilización de la red: el proveedor es el encargado de manejar la VPN, pero no de supervisar la red de la compañía. Se debe conocer cómo funciona la red, si la compañía empieza a crecer, se necesitara más ancho de banda y por ende se deberá solicitar una actualización del servicio de conectividad.

Seguridad: por medio de un contrato, se fijan las técnicas que utilizará el proveedor para garantizar el cifrado de la información, así como también la manera de certificar que los datos transmitidos por medio de redes públicas no sufran alteración, proporcionando así la integridad; y también estipular quién tiene el control de la base de datos de usuarios que brinda autenticación y permitirá crear el túnel VPN hacia la organización. Si se encuentra en el dispositivo del proveedor, se debe conocer el tiempo que se requiere para que una autorización se vuelva efectiva.

[9] ARIGANELLO, E. (2014). *Redes Cisco. Guía de estudio para la certificación CCNA Routing and Switching*. Madrid, España: Editorial RA-MA, p. 370.

¿CÓMO FUNCIONA UNA VPN?

Una VPN utiliza la infraestructura de Internet para proveer conexiones remotas a redes de una organización, usualmente requiere autorización, autentificación y usa criptografía.

Para acceder a la red, los usuarios deben estar registrados y autorizados. Una vez autenticados, toda la información que transmiten es codificada por algoritmos de criptografía, y decodificada en su recepción, aumentando el nivel de seguridad.

La conexión se conforma entre dispositivos que establecen una ruta denominada "túnel", con el fin de intercambiar información haciendo uso de una red pública (como Internet) o privada. La privacidad del enlace es un punto vulnerable, por lo que los datos transmitidos son codificados (encriptados), enviados y nuevamente decodificados.

MODELO TCP/IP

TCP/IP (Transmisión Control Protocol / Internet Protocol) es un grupo de protocolos estándares diseñados para redes, utilizado en redes WAN. Es adaptable, por lo cual se puede trabajar casi en cualquier medio de red. Siendo este modelo aplicable en cualquier hardware y sistema operativo existente, ya sea en pequeñas red de área local que cuenta con dos hosts, hasta la conexión de millones de sistemas que componen Internet.

El modelo TCP/IP es muy similar al modelo OSI[10] que fue desarrollado por la Organización Internacional para la Estandarización (ISO[11]) donde se definen siete capas para organizar una red dentro de módulos funcionales y bien detallados. Cada módulo proporciona funcionalidad específica o servicios a sus capas adyacentes a través de interfaces.

La arquitectura de Internet se basa en capas, lo que facilita la implementación de nuevos protocolos.

El modelo de capas de TCP/IP

El principio de división por capas permite la resolución de problemas de manera sencilla. Ya que cada una de las capas cuenta con funciones definidas y objetivos determinados.

La suite de protocolos TCP/IP se implementa como una pila tanto en los hosts emisores como en los receptores para proporcionar una entrega de extremo a extremo de las aplicaciones a través de la red. En el host origen funciona de

[10] Publicado por ISO en 1984 con el objetivo original de crear un modelo de referencia que también se utilizaría como base para una suite de protocolos que se fuera a usar en Internet.

[11] Es el mayor desarrollador del mundo de estándares internacionales para una amplia variedad de productos y servicios.

manera descendente por las distintas capas de la pila y de manera inversa en el host destino hasta llegar a la capa correspondiente.

Ariganello (2014), dice:

> Mientras los datos de la aplicación bajan al stack del protocolo y se transmiten por los medios de la red, varios protocolos le agregan información en cada nivel. Esto comúnmente se conoce como proceso de encapsulación.
>
> La forma que adopta una porción de datos en cualquier capa se denomina "unidad de datos del protocolo (PDU)". Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar sus nuevas funciones. Aunque no existe una convención universal de nomenclatura para las PDU, se denominan de acuerdo con los protocolos de la suite OSI, como se muestra en la ilustración:
>
> - **Datos:** término general para la PDU que se utiliza en la capa de aplicación.
> - **Segmento:** PDU de la capa de transporte
> - **Paquete:** PDU de la capa de red
> - **Trama:** PDU de la capa de enlace de datos ([12]).

Las capas que componen al modelo y una breve descripción se enuncian a continuación:

- ***Capa de acceso a la red:*** determina la forma en que se utilizan los medios, ya sean inalámbricos o alámbricos.
- ***Capa de internet:*** define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino.
- ***Capa de transporte:*** controla el dialogo entre las aplicaciones por medio de los números de puerto, sus protocolos principales son TCP y UPD
- ***Capa de aplicación:*** son las aplicaciones o servicios con los que interactúa el usuario.

A diferencia del modelo OSI, TCP/IP tiene sólo 4 capas las cuales se plasman en la figura 1.1 que aparece a continuación y en ella pueden verse claramente las diferencias y similitudes entre modelos.

[12] ARIGANELLO, E., Op. cit., p. 47.

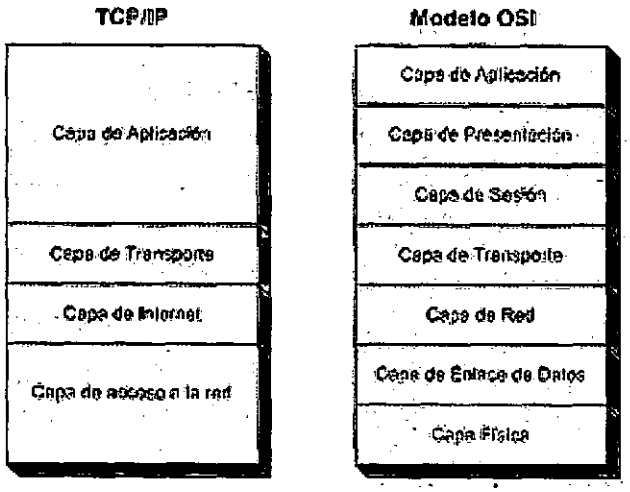


Figura 1.1 Modelo TCP/IP y Modelo OSI
Fuente: TANENBAUM, A. S.; Wetherall, D. J. (2012). *Redes de computadoras* (Quinta edición). México: Editorial. Pearson, p. 40.

Similitudes:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.

Diferencias:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina las capas de enlace de datos y física del modelo OSI en una sola capa denominada Acceso a Red.

CAPA 1: ACCESO A LA RED

Es la primer capa de la pila TCP/IP, brinda los recursos necesarios para transmitir datos a través de la red. A su vez, cuenta con protocolos que controlan la manera en que los mensajes acceden a los medios, integrando la información necesaria para ser dirigidos e interpretados al llegar a destino.

Estándares destacados utilizados en redes LAN:

- ***Ethernet.***

  Es la tecnología LAN ampliamente utilizada y soporta anchos de banda de datos de 10, 100, 1.000, o 10.000 Mbps. Se encuentra estandarizado en IEEE[13] 802.2 y 802.3[14].

- ***Protocolo inalámbrico para LAN.***

  Define la manera de comunicarse, para dispositivos no conectados a través de medios físicos. Se estandariza en IEEE 802.11[15].

[13] Es un organismo profesional para aquellos que trabajan en los campos de la electrónica y de la ingeniería eléctrica y se dedican a promover la innovación tecnológica y crear estándares
[14] *Ethernet Working Group* (Grupo de trabajo de Ethernet)
[15] *Wireless LAN Working Group* (Grupo de trabajo de LAN inalámbrica)

Protocolos estándares destacados que rigen las comunicaciones en redes WAN:

- ***Protocolo punto a punto para WAN (ppp).***

  Actualmente es el protocolo mayoritariamente elegido para su implementación en este tipo de redes. Se estandariza por medio de RFC 1661[16], se puede utilizar a través de diferentes medios físicos y se encarga de entregar tramas entre dos nodos.

- ***FrameRelay:***

  Proporciona conexiones a través de una red pública utilizando circuitos virtuales que definen el enlace extremo a extremo.

- ***MPLS (Conmutación Multiprotocolo Mediante Etiquetas)***

  Es una tecnología similar a la de conmutación de circuitos virtuales, pero en este caso el protocolo agrega una etiqueta a cada paquete; que utiliza para el reenvío, en vez de utilizar la dirección de destino.

CAPA 2: INTERNET

Es la capa encargada de realizar el enrutamiento de paquetes de datos entre origen y destino por medio de las direcciones IP. Se basa en cuatro procesos básicos:

- ***Direccionamiento:*** cada dispositivo debe tener una dirección IP única que lo identifica dentro de la red y es por medio de estas direcciones que se establece el enrutamiento o comunicación entre los mismos.
- ***Encapsulación:*** es el proceso de recibir los datos de la capa de transporte (segmento o datagrama), y agregarle un encabezado el cual contendrá las direcciones de origen y destino.
- ***Enrutamiento:*** el objetivo es dirigir los paquetes a través de diferentes redes, seleccionando el camino óptimo para llegar a un destino determinado.
- ***Desencapsulación***: se encarga de recibir los datos de la capa de acceso a la red, procesar la información contenida en el paquete verificando que sea el destinatario y extrayendo el encabezado, para luego poner a disposición de capas superiores el mensaje recepcionado.

En la capa de Internet aparecen estos tres protocolos como los más importantes:

- el protocolo IP
- el protocolo ARP
- el protocolo ICMP

Protocolo IP

Es un conjunto de reglas establecidas entre dos dispositivos que permiten la comunicación entre ambos. Los servicios y estructura de paquetes provistos, se usan para encapsular datagramas UDP o segmentos TCP para su recorrido a través de la red.

[16] *The Point-to-Point Protocol* (PPP) es un método estándar de encapsulación de protocolos de capas superiores.

Provee las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes, es el responsable del enrutamiento, del direccionamiento, de la fragmentación y ensamble.

Se lo define como un protocolo de datagramas, no confiable, sin conexión y principalmente responsable del direccionamiento y enrutamiento de los paquetes. Los datagramas son una agrupación lógica de información que se envía como una unidad de capa de red a través de un medio de transmisión, sin establecer con anterioridad un circuito de recorrido. El datagrama se compone de una cabecera y datos.

La confirmación de la entrega de los paquetes y la recuperación de paquetes perdidos es responsabilidad de un protocolo de alguna capa superior.

Cuando los datagramas viajan de un equipo a otro, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de los paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. Al tamaño máximo se le denomina MTU[17], y ninguna red puede transmitir un paquete de tamaño mayor al estipulado.

Considerado el protocolo principal de la capa, y siendo la versión 4 de IP (IPv4) ampliamente utilizada para llevar datos de usuario a través de Internet.

La versión 6 de IP (IPv6) está desarrollada y se implementa actualmente conviviendo con IPv4.

Principales características de IPv4:

- *Sin conexión:* antes de que los paquetes sean enviados, no necesita realizar un intercambio de información de control para establecer una conexión de extremo a extremo; lo cual reduce en gran medida la sobrecarga de red.
- *Mejor intento:* IP es un protocolo no confiable para la entrega datos, dado que no tiene la capacidad de administrar ni recuperar paquetes perdidos. Serán los protocolos en otras capas los encargados de administrar la confiabilidad, esto le permite a IP funcionar con mucha eficiencia en la capa de Internet.
- *Independiente de los medios:* el transporte de paquetes IP no está limitado a un medio físico en particular, tanto en su versión 4, como en la versión 6 opera transmitiendo los datos a niveles inferiores de la pila de protocolo. Pudiendo ser comunicados eléctricamente por cable, como señales ópticas por fibra, o sin cables como señales de radio, siendo la capa de Acceso a la Red la que se encarga de tomar el paquete IP y prepararlo para transmitirlo por el medio de comunicación.

[17] Tamaño en bytes de la PDU más grande que puede enviarse usando IP.

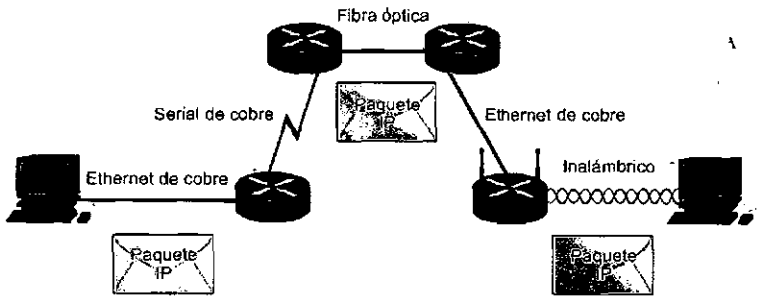


Figura 1.2 Viaje del paquete por distintos medios
Fuente: ARIGANELLO, E. (2014). *Redes Cisco. Guía de estudio para la certificación CCNA Routing y Switching.* Madrid, España: Editorial RA-MA.

ICMP: (Protocolo de internet de control de mensajes)

Es un protocolo utilizado para transferir mensajes desde los dispositivos de red y las PC a uno o varios hosts, proporcionando información de realimentación sobre problemas del entorno de la comunicación.

ARP: (Protocolo de resolución de dirección)

ARP es un protocolo de traducción de direcciones que se encarga de establecer cuál es la dirección física de destino de una trama, en base a la dirección IP lógica a la cual va destinada.

CAPA 3: TRANSPORTE

Los protocolos de la capa 3 realizan la transferencia de paquetes dividiéndolos en unidades pequeñas y pasándolos a la capa de internet.

Protocolos principales que operan en la capa de transporte de TCP/IP:

- ***TCP - Protocolo de control de transmisión:*** proporciona un servicio de comunicación confiable, orientado a conexión, punto a punto. Lo logra estableciendo un circuito virtual para las comunicaciones de red. Es responsable del establecimiento de una conexión TCP, la secuenciación y la confirmación de los paquetes enviados, y de la recuperación de los paquetes perdidos durante la transmisión.

- ***UDP - Protocolo de datagramas de usuario:*** es un protocolo simple, sin conexión que tiene la ventaja de proveer la entrega de datos utilizando escasos recursos. Es utilizado cuando la cantidad de datos a ser transferidos es pequeña y la carga de establecer la conexión para asegurar la transferencia no es necesaria (como puede ser una comunicación por VoIP o la visualización de un video).

La comunicación

Los servicios basados en TCP y UDP mantienen un seguimiento de las aplicaciones, diferenciando los segmentos y datagramas a través de identificadores únicos conocidos como número de puerto.

En el encabezado de cada segmento o datagrama hay un puerto de origen y otro de destino. El número de puerto de origen, es el número que se asocia con la aplicación que origina la comunicación en el host local. El número de puerto de destino es el número que se asocia con la aplicación de destino en el host remoto. En el servidor los números puerto son estáticos y en el cliente son dinámicos.

La capa de Transporte mantiene un seguimiento de los puertos y de la aplicación que generó la solicitud, de manera que cuando llega una respuesta, pueda ser enviada a la aplicación correcta. El número de puerto de la aplicación que realiza la solicitud se utiliza como número de puerto de destino en la respuesta que vuelve del servidor.

Existen distintos tipos y números de puerto según Ariganello (2014):

- Puertos bien conocidos (Números del 0 al 1.023): estos números están reservados para servicios estándares.
- Puertos Registrados (Números 1.024 al 49.151): estos números de puertos están asignados a procesos o aplicaciones del usuario.
- Puertos dinámicos o privados (Números del 49.152 al 65.535): también conocidos como puertos efímeros, generalmente se los asigna de forma dinámica a las aplicaciones cliente cuando el cliente inicia una conexión a un servicio.[18]

La diferencia entre TCP y UDP

TCP transporta información de un host a otro, establece una comunicación previa denominada sesión, la cual es utilizada para rastrear la comunicación de extremo a extremo.

Luego de establecida la sesión, el destino envía acuses de recibo al origen por los segmentos que recibe. Al recibir los mismos, el origen reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos. Si no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite los datos al destino. Usando el último número de acuse recibido y retransmitirá los datos a partir de él.

A diferencia de TCP, UDP no establece una conexión previa entre los extremos antes de enviar información; y a su vez, los extremos no esperan confirmación de recepción de datagramas enviados. Lo cual evita que el protocolo sobrecargue la comunicación.

[18] ARIGANELLO, E., Op. Cit., p. 50.

CAPA 4: APLICACIÓN

Engloba las aplicaciones y servicios que interactúan con los usuarios, haciendo uso de los protocolos descriptos en el modelo TCP/IP para establecer la comunicación entre los distintos host.

Incluye especificaciones para software comunes, aspectos de representación, codificación y control de diálogo entre aplicaciones. Combina todos los aspectos relacionados con las aplicaciones y asegura que los datos estén empaquetados antes de que pasen a la capa siguiente.

Protocolos destacados que operan en la capa

Soporta los protocolos de direccionamiento, transferencia, conexiones remotas, correo electrónico, así como también administración de red. Algunos protocolos destacados según Ariganello (2014).[19]

- *DNS (Domain Name System)* es el servicio que resuelve peticiones en base a un nombre de dominio determinado, devolviendo la dirección IP relacionada.
- *SMTP (Simple Mail Transfer Protocol)* maneja la transmisión de correo electrónico a través de las redes, definiendo los formatos de mensaje y cadenas de comandos necesarios. A su vez, rige la transferencia de correos salientes desde el cliente emisor al servidor de correos, así como también el transporte de emails entre servidores de correo electrónico.
- *SNMP (Simple Network Management Protocol)* es un protocolo que permite la administración remota de dispositivos de red, dando la posibilidad de monitorearlos, así como también recolectar estadísticas de desempeño y seguridad.
- *FTP (File Transfer Protocol)* es un servicio cliente-servidor, orientado a la conexión que utiliza TCP para transferir archivos entre sistemas que soportan el protocolo.
- *TFTP (Trivial File Transfer Protocol)* es un servicio utilizado para transferir archivos entre hosts, que usa UDP en la comunicación.
- *HTTP (Hypertext Transfer Protocol)* es el estándar Internet que soporta el intercambio de información en la WWW, así como también en redes internas, basándose en el modelo cliente-servidor. A través de este protocolo es que se envían las peticiones de acceder a una página web y se recibe la respuesta. Soporta muchos tipos de archivos distintos, incluyendo texto, gráfico, sonido y vídeo.

[19] Ibid., p. 48.

TOPOLOGÍAS

En el contexto de una red de comunicaciones, el término topología se refiere a la forma según la cuál se interconectan entre sí los puntos finales, o estaciones, conectados a la red. Las topologías usuales en redes LAN son bus, anillo, malla y estrella.

- **Bus:** se caracteriza por el uso de un medio multipunto, en el cual todas las estaciones se encuentran directamente conectadas, a través de interfaces físicas apropiadas conocidas como puntos de conexión, a un medio de transmisión lineal.

- **Anillo:** formado por enlaces punto a punto que unen un grupo de dispositivos llamados repetidores, creando un bucle cerrado. Cada uno de ellos es capaz de recibir datos y retransmitirlos de igual manera al siguiente, hasta llegar a su destino enviando los datos siempre en un solo sentido.

- **Malla:** cada nodo está conectado a todos los demás nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos.

- **Estrella:** cada estación está directamente conectada a un nodo central común a través de un enlaces punto a punto. Para que exista comunicación entre los clientes, el tráfico de datos deberá ir desde el cliente hasta el nodo central, que se encargará de retransmitir los datos hacia el receptor, no existiendo una conexión directa entre los extremos.

CAPITULO 2

[PROTOCOLO IP VERSIÓN 4 Y VERSIÓN 6]

En este capítulo se estudiarán las versiones operativas del protocolo IP. Además se analizarán sus características y las principales diferencias entre ambas.

PROTOCOLO IPv4

IPv4 es la primera versión comercial del protocolo de internet, estandarizado en el RFC 791[20] en septiembre de 1981. Dispone de aproximadamente 4 millones de direcciones únicas (2^32), de las cuales ninguna está disponible para ser asignadas en la actualidad.

Clases de direcciones IPv4

"*Se detallan cinco clases de direcciones nombradas alfabéticamente de A hasta E. Definiendo, las clases A, B y C para ser asignadas a países y/o empresas que las requieran, la clase D para uso multicast y la clase E para uso experimental*" (Ariganello, 2014)[21]. Se detallan los bloques de direcciones en la Tabla 2.1.

Clases de direcciones IP						
Clases	**Bits 1er. Octeto**	**Rango de Direcciones**	**Prefijo [22]**	**Máscara[23]**	**Núm. Redes**	**Núm. Host Disponible**
A	0xxxxxxx	De 0.0.0.0/8 a 127.0.0.0/8	/8	255.0.0.0	2^7= 128	2^24-2= 16.777.214
B	10xxxxxx	De 128.0.0.0/16 a 191.255.0.0/16	/16	255.255.0.0	2^14= 16.384	2^16-2= 65.534
C	110xxxxx	De 192.0.0.0/24 a 223.255.255.0/24	/24	255.255.255.0	2^21= 2.097.152	2^8-2= 254
D	1110xxxx	De 224.0.0.0 a 239.255.255.255	-	-	-	-
E	1111xxxx	De 240.0.0.0 a 255.255.255.254	-	-	-	-

Tabla 2.1 Clases de direcciones IPv4

Fuente: ARIGANELLO, E. (2014). *Redes Cisco. Guía de estudio para la certificación CCNA Routing and Switching.* Madrid, España: Editorial RA-MA.

Tipos de direcciones IPv4

Según Ariganello, E. (2014):

> Se diferencian dos tipos de direcciones según su uso: públicas y privadas. Las direcciones públicas son aquellas que pueden ser enrutadas en Internet; mientras las direcciones privadas se utilizan en las redes internas y no son reconocidas en redes como Internet.

[20] Internet Protocol - Darpa Internet Program - Protocol Specification

[21] ARIGANELLO, E., Op. cit., p. 76.

[22] Las direcciones IP de 32 bits están compuestas de una porción de red de longitud variable en los bits superiores, y de una porción de host en los bits inferiores. La porción de red tiene el mismo valor para todos los hosts en una sola red. Esto significa que una red corresponde a un bloque contiguo de espacio de direcciones IP. A este bloque se le llama prefijo.

[23] Notación binaria para determinar si dos hosts están en la misma red, tiene una longitud de 32 bits. La máscara de subred identifica qué parte de la dirección IP corresponde a la red y cuál al host. El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

Los rangos de direcciones privadas se detallan en el RFC 1918[24], mientras que las direcciones públicas son todas aquellas que no pertenecen a los rangos de direcciones privadas. ([25])

Formato de la cabecera IPv4

El protocolo IPv4 define muchos campos diferentes en el encabezado del paquete, los cuales contienen valores binarios que los servicios IPv4 toman como referencia a medida que reenvían paquetes a través de la red.

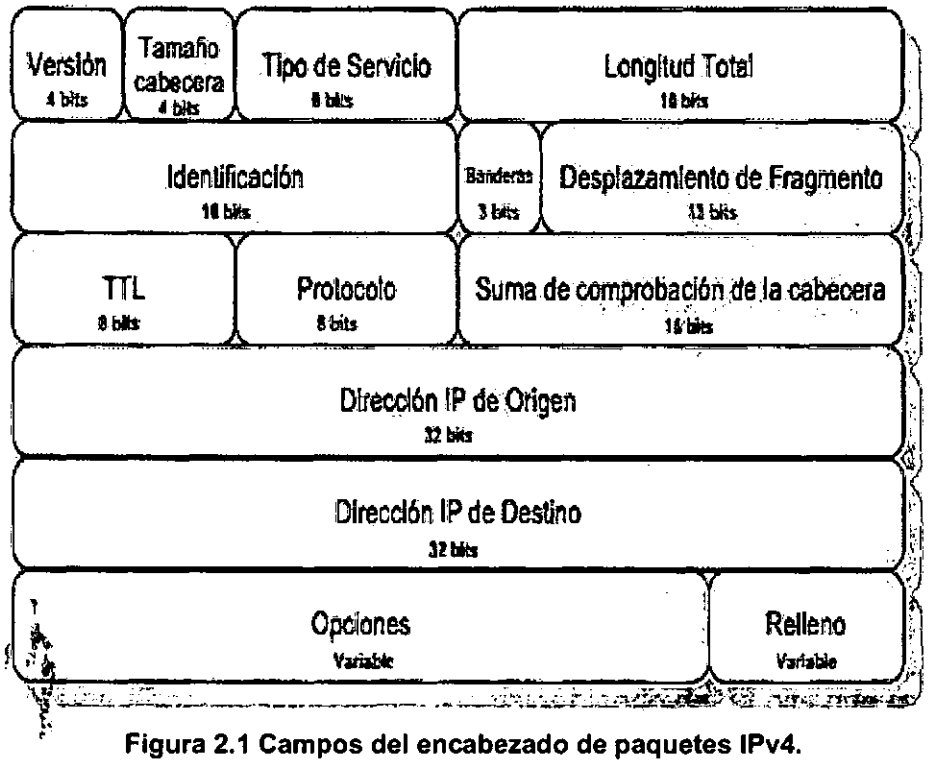


Figura 2.1 Campos del encabezado de paquetes IPv4.

Fuente: AGUIRRE SANCHEZ, Lizeth Patricia. *Rediseño de la red MPLS con soporte de IPv6 empleando las mejores prácticas de seguridad para el sistema autónomo de Telconet S.A. de la ciudad de Quito.* 2013. (Tesis de Ingeniería). Quito, Ecuador. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, p. 35.

Campos claves IPv4:

- *Versión:* campo formado por 4 bits que indica la versión del Protocolo de Internet.
- *Tamaño de la cabecera:* es un campo de 4 bits que refleja la longitud de la cabecera del paquete IP.
- *Tipo de servicio:* contiene un valor binario de 8 bits que se usa para determinar la prioridad de cada paquete. Este valor permite aplicar un mecanismo de calidad de servicio (QoS)[26] a paquetes de alta prioridad.

[24] Define la asignación de direcciones privadas para Internet.
[25] ARIGANELLO, E., Op. cit., p. 75
[26] Calidad de servicio: técnica utilizada en la red para priorizar un tráfico determinado respecto a otros.

- *Longitud del paquete:* campo que define el tamaño completo del paquete en bytes, incluidos el encabezado y los datos.
- *Identificación:* campo que se utiliza para identificar únicamente los fragmentos de un paquete IP original.
- *Banderas:* campo de 3 bits utilizado para el control de la fragmentación de un paquete.
  Bit 0: Reservado para futuras aplicaciones. Debe ser 0.
  Bit 1: El bit no se fragmenta. 1L el paquete no puede ser fragmentado, 0L está fragmentado.
  Bit 2: El bit está fragmentado. 1L fragmento intermedio, 0L último fragmento.
- *Desplazamiento de fragmentos:* identifica el orden en el cual ubicar el fragmento del paquete al momento de la reconstrucción.
- *Tiempo de vida (TTL):* es un valor binario de 8 bits que indica el resto de vida del paquete. El valor TTL disminuye al menos en uno cada vez que el paquete es procesado por un router (es decir, en cada salto). Cuando el valor se vuelve cero, el siguiente router que procesa el paquete, lo descarta y elimina el flujo de datos de la red.
- *Protocolo:* valor binario de 8 bits que indica el tipo de contenido que el paquete traslada. Permite a la capa de acceso a red pasar los datos al protocolo apropiado de capas superiores.
- *Checksum del encabezado:* este campo se utiliza para controlar errores del encabezado del paquete.
- *Dirección IP de origen:* contiene un valor binario de 32 bits que representa la dirección host de capa de Internet que da origen al paquete.
- *Dirección IP de destino:* contiene un valor binario de 32 bits que representa la dirección host de capa de Internet de destino del paquete.
- *Opciones:* campo de longitud variable (entre 0 y 40 bytes) para la implementación de pruebas y control de la red.

PROTOCOLO IPv6

IPv6 ha estado en desarrollo desde mediados de los años 90 y durante varios años. Los fundamentos de la creación de la nueva versión es la escasez de direcciones, motivo por el cual hay una gran necesidad de evolucionar para obtener un mayor direccionamiento.

Entre las principales razones por las cuales el direccionamiento de IPv4 escaseaba, es que inicialmente la distribución de direcciones se hacía de una manera poco eficiente, principalmente por la asignación a través de clases. Debido a que cualquier dispositivo en IPv4 requería una dirección IP pública

para funcionar, la IETF[27] desarrollo técnicas que optimizaron la asignación de direcciones como ser CIDR[28] (Classless Interdomain Routing) y VLSM[29] (Variable-Length Subnet Mask) que trabajan conjuntamente para mejorar el direccionamiento IPv4.

Otra de las razones de escasez de direcciones públicas es que no han sido asignadas de manera equitativa a lo largo del mundo. Una gran cantidad del direccionamiento es ocupada por Estado Unidos, en la lista le sigue Europa, mientras que Asia cuenta con una asignación que no es suficiente para la cantidad de población que posee.

La demanda de direcciones se ha disparado dada la cantidad de dispositivos que se conectan actualmente a la red, ya que en el mundo hay una fuerte tendencia a tener todos los dispositivos conectados y sincronizados.

A su vez, la necesidad de direccionamiento fue mermada con NAT[30], pero el hecho de tener sistemas intermedios manipulando los paquetes complican el diseño y la resolución de problemas.

En IPv6 se utiliza una cabecera simplificada respecto de IPv4, haciendo que el procesamiento mejore su eficiencia y admitiendo un mecanismo flexible. La seguridad es tema importante, se utiliza IPSec en cada uno de los dispositivos IPv6.

Debido a que la migración de IPv4 a IPv6 no puede ocurrir tan rápidamente como sería deseable, hay que buscar alternativas para administrar la transición.

Direccionamiento en IPv6

Las direcciones IPv6 sirven para identificar de manera única la interfaz de un dispositivo de red, de tal forma que los paquetes puedan ser enrutados de un host a otro. A diferencia de IPv4, una interfaz puede disponer de una o varias direcciones IPv6, logrando que los usuarios puedan trabajar con diferentes ISP[31] y optimizando así su servicio de Internet.

En la versión 4, las direcciones IP eran de 32 bits, mientras que en IPv6 son de 128 bits, lo que genera un espacio con mayor amplitud de direcciones.

[27] Comunidad internacional abierta de diseñadores de redes, operadores, vendedores e investigadores preocupados por la evolución de la arquitectura de Internet y el buen funcionamiento de Internet.
[28] Está definido en RFC 1517 - Applicability Statement for the Implementation of Classless Inter-Domain Routing, usa máscaras de subred de longitud variable para asignar direcciones IP a subredes de acuerdo con la necesidad individual en lugar de hacerlo según la clase.
[29] Permite usar la máscara de subred para variar los tamaños de red según la cantidad de bits que se toman prestados para una subred específica.
[30] NAT traduce direcciones internas, privadas y no enrutables a direcciones públicas enrutables.
[31] Es la empresa que brinda conexión a Internet a sus clientes.

Representación de direcciones IPv6

AGUIRRE SANCHEZ (2013) propone:

Las direcciones IPv6 se presentan en ocho grupos de cuatro nibbles[32] separados por dos puntos (:). La dirección de loopback[33] en IPv6 viene representada por ::1, a diferencia de IPv4 donde se tiene un rango de direcciones 127.0.0.0/24. Esta dirección está reservada para pruebas mediante el envío de paquetes a sí mismo y no puede ser asignada a ninguna interfaz.

Las direcciones IPv6 tienen determinadas reglas para lograr disminuir y optimizar su representación. Como ejemplo, se ha seleccionado la dirección IPv6 mostrada a continuación para aplicarle las reglas y obtener una dirección equivalente pero más corta.

2100:1234:0000:0000:065B:293A:034B:3ABC

Primera regla

Se permite omitir los ceros ubicados a la izquierda de cada grupo de cuatro nibbles. Entonces, los valores: 065B y 034B del ejemplo, se los puede reescribir como: 65B y 34B.

La dirección IPv6 de ejemplo resultaría:

2100:1234:0000:0000:65B:293A:34B:3ABC

Segunda regla

Los grupos de cuatro nibbles que estén encerrados y sean continuos pueden ser remplazados por 4 puntos (::). Esta regla puede ser ejecutada solo una vez en cada dirección IPv6, a fin de evitar confusiones de reemplazo.

Para el ejemplo quedaría:

2100:1234::65B:293A:34B:3ABC

[32] Es el conjunto de cuatro dígitos binarios (bits) o medio octeto.

[33] Se encuentre definida en el protocolo TCP/IP, como una dirección reservada que permite enrutar los paquetes de regreso al host.

Tercera regla

El número de ceros que se deben aumentar en una dirección IPv6 optimizada, es el resultado de la diferencia entre los 128 bits y el número de bits de la dirección optimizada.

Para el ejemplo quedaría:

Dirección IPv6 optimizada: 2100:1234::65B:293A:34B:3ABC

Número de bits: 16 + 16 + 16 + 16 + 16 + 16

Número de bits a aumentar: 128 – 6 (16) = 32

Dirección IPv6 representada en 128 bits:

2100:1234:0000:0000:065B:293A:034B:3ABC

Cuarta regla

Si una dirección no está especificada, se la representa con dos puntos (::) e indica que está formada por 128 ceros lógicos. Se utiliza cuando un dispositivo no conoce su propia dirección y requiere referenciarse a sí mismo. ([34])

Tipos de direcciones IPv6

Igual que IPv4 existen direcciones públicas y privadas. Las privadas se diferencian en que su primer octeto comienza con el valor hexadecimal: "0xFE". Estas direcciones se subdividen en: link-local y site-local, como se detallan en la Tabla 2.2.

PREFIJO HEXADECIMAL	TIPO DE DIRECCIÓN	DESCRIPCIÓN
FE80::/10	**link-local**	Se utilizan para la comunicación de enlaces físicos, como: las configuraciones automáticas y los descubrimientos de los vecinos. No se pueden enviar paquetes a través de estas subredes.
FEC0::/10	**site-local**	Permiten enrutar paquetes en las redes internas de una empresa. Equivalentes a las direcciones IPv4 del RFC 1918.

Tabla 2.2 Direcciones privadas IPv6.

Fuente: AGUIRRE SANCHEZ, Lizeth Patricia. *Rediseño de la red MPLS con soporte de IPv6 empleando las mejores prácticas de seguridad para el sistema autónomo de Telconet S.A. de la ciudad de Quito.* 2013. (Tesis de Ingeniería). Quito, Ecuador. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, p. 43.

[34] AGUIRRE SANCHEZ, Lizeth Patricia. *Rediseño de la red MPLS con soporte de IPv6 empleando las mejores prácticas de seguridad para el sistema autónomo de Telconet S.A. de la ciudad de Quito.* 2013. (Tesis de Ingeniería). Quito, Ecuador. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, p. 44.

Además, IPv6 maneja tres tipos de direcciones según Stallings (2004) y son:

- Unidifusión (unicast): un identificador para una interfaz individual. Un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.
- Monodifusión (anycast): un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección monodifusión se entrega a una de las interfaces identificadas por esa dirección (la más cercana, de acuerdo a la medida de distancia de los protocolos de encaminamiento).
- Multidifusión (multicast): un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección multidifusión se entrega a todas las interfaces identificadas por esa dirección. IPv6 optimiza este tipo de direcciones para enviar broadcast [35] en la red. ([36])

Formato de la cabecera IPv6

El datagrama IPv6 es una evolución de la anterior versión (IPv4). No se han introducido grandes cambios de contenido o estructura, simplemente se ha mejorado y optimizado. IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos, los cuales pueden identificarse en el grafico que se presenta a continuación.

[35] Dirección que tiene los bits de la parte de dirección de maquina con valor 1. Identifica a todos los hosts de la red.
[36] STALLINGS, W. (2004). *Comunicaciones y Redes de Computadores* (Séptima edición). México: Editorial Pearson, p. 624.

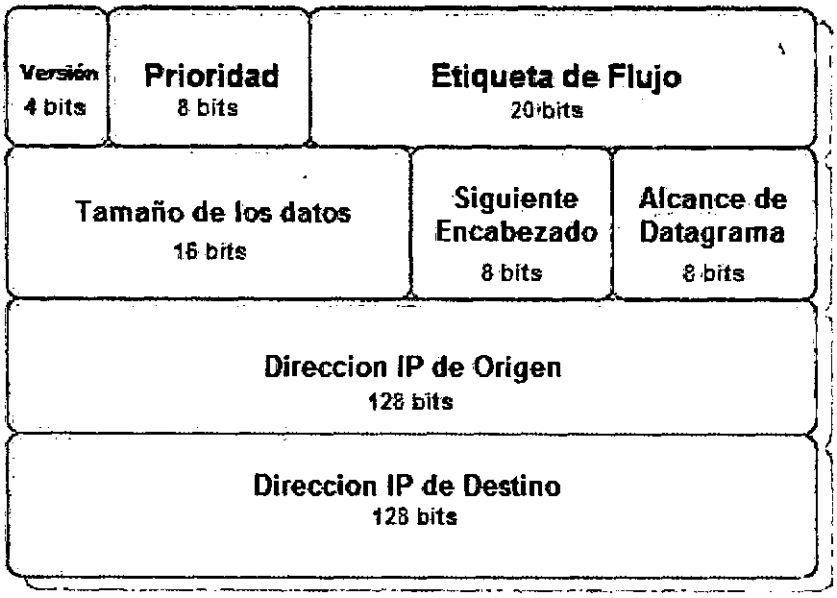


Figura 2.2 Campos del encabezado de paquetes IPv6.
Fuente: AGUIRRE SANCHEZ, Lizeth Patricia. *Rediseño de la red MPLS con soporte de IPv6 empleando las mejores prácticas de seguridad para el sistema autónomo de Telconet S.A. de la ciudad de Quito.* 2013. (Tesis de Ingeniería). Quito, Ecuador. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, p. 40.

Campos claves IPv6:

- *Versión* (4 bits): número de versión del protocolo IP, que en este caso contendrá el valor 6. Se sigue manteniendo como el primer campo del datagrama, esto es así para mantener la compatibilidad y porque permite de una forma sencilla y rápida de discriminar que versión de datagrama se recibe, facilitando a los routers el proceso de enrutamiento.
- *Prioridad o Clase* (8 bits): contiene el valor de la prioridad o importancia del datagrama que se procesa con respecto a otro datagrama proveniente de la misma fuente. Este campo es una de las nuevas contribuciones para conseguir que algunos servicios puedan utilizarse en tiempo real (videoconferencias, telefonía, etc.).
- *Etiqueta de Flujo* (16 bits): campo utilizado para indicar que el datagrama requiere un tratamiento especial por parte de los routers. Esto es aplicable por ejemplo a una serie de datagramas que van del mismo origen al mismo destino y con las mismas opciones.
- *Tamaño de los datos* (16 bits): permite un tamaño máximo de 2^16 = 65636 bytes (64k). No obstante, a diferencia de la versión 4, este número hace referencia sólo al tamaño de los datos que trasporta, sin incluir la cabecera.
- *Siguiente Cabecera* (8 bits): indica al router si tras el datagrama viene algún tipo de extensión u opción. A su vez, permite describir detalladamente las opciones del datagrama.
  En IPv6 se definen una serie de cabeceras de extensión que se colocan justo después de los datos en forma de cadena, permitiendo personalizar el datagrama.
- *Alcance del Datagrama* (8 bits): indica el número máximo de routers que puede atravesar un datagrama hasta llegar a su destino. Este campo es el

equivalente al tiempo de vida (TTL) de la versión 4. Se elimina al llegar a 0 y su valor máximo es 2^8 = 256.

- *Dirección de Origen* (128 bits): dirección del host que envía el datagrama. Su longitud es cuatro veces mayor que en versión 4.
- *Dirección de Destino* (128 bits): dirección del host de destino al cual va dirigido el datagrama.

Cabecera de extensión IPv6

Las cabeceras de extensión de IPv6 se crearon dado que en la cabecera IPv4 es obligatorio el envió de determinados campos no siempre requeridos, los cuales ocupa ancho de banda innecesario en su transmisión .

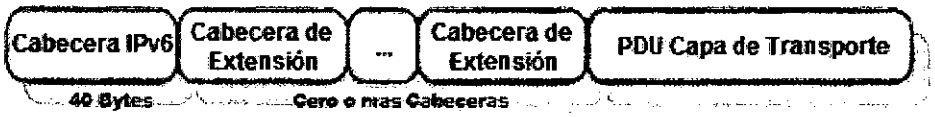


Figura 2.3 Cabecera de Extensión Paquete IPv6.
Fuente: AGUIRRE SANCHEZ, Lizeth Patricia. *Rediseño de la red MPLS con soporte de IPv6 empleando las mejores prácticas de seguridad para el sistema autónomo de Telconet S.A. de la ciudad de Quito.* 2013. (Tesis de Ingeniería). Quito, Ecuador. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, p. 41.

Según Aguirre Sanchez (2013):

> El campo "encabezado siguiente" tiene el identificador de la cabecera que viene a continuación de los 40 bytes, de lo contrario especifica el protocolo de la capa transporte que recibirá el paquete IPv6. Si se agregan más de una cabecera de extensión, se debe respetar el orden establecido a continuación:
>
> 1. Cabecera de opciones salto-a-salto
> 2. Cabecera de opciones para el destino (orientado al siguiente salto que no sea el destino final del paquete)
> 3. Cabecera de encaminamiento
> 4. Cabecera de fragmentación
> 5. Cabecera de autenticación
> 6. Cabecera de encapsulado de la carga de seguridad
> 7. Cabecera de opciones para el destino (orientado al destino final del paquete) ([37])

[37] AGUIRRE SANCHEZ, Op. cit., p. 42.

ESTADO DE ADOPCIÓN DE IPV6 EN REDES PÚBLICAS

En la actualidad, según estadísticas de Google[38], en Argentina existe una adopción de IPv6 de un 7.12%, mientras que los países con mayor desarrollo en el campo y con mas porcentaje de uso de IPv6 rondan en un 38%, como es el caso de Estados Unidos y Alemania.

Hoy por hoy en LACNIC[39] se encuentran registrados cuatro ISP que adoptaron IPV6 en sus redes, y a su vez existen otros ocho ISP que se encuentran en instancias de implementación, lo que brinda un panorama favorable a futuro del crecimiento de la tecnología en la región y por ende dar un paso para posicionar la versión del protocolo como predominante en las redes públicas.

DIFERENCIAS DE IPV6 CON RESPECTO A IPV4

Dado el agotamiento de direcciones IPv4 la IETF[40] busco una alternativa que resuelva el problema. El cual fue acrecentado por la tendencia a nivel mundial de conectar diversos dispositivos del hogar a las redes, como: laptops, teléfonos móviles, PDA[41], televisores, lavarropas y heladeras inteligentes.

Aguirre Sanchez (2013) expuso que:

> IPv6 brinda mayor flexibilidad para soportar los usuarios existentes y beneficia el incremento de estos. Mejora las debilidades de IPv4 y ofrece la oportunidad de que Internet siga creciendo.
>
> A continuación, se muestran las características sobresalientes de IPv6, que lo diferencian de IPv4:
>
> - ✓ IPv6 ofrece más de 340 sextillones de direcciones IP que posibilitan la conexión de mayor cantidad de usuarios a Internet.
> - ✓ Posee multiconexión de usuarios para que un host pueda conectarse no solo a uno sino a varios ISP.
> - ✓ Direccionamiento de extremo a extremo sin hacer uso de la traducción de direcciones públicas a privadas y viceversa. Se deja de utilizar NAT.
> - ✓ Posee un encabezado eficiente y simplificado respecto al de IPv4, para brindar mayor rapidez en el procesamiento de los paquetes a medida

[38] Fuente: Google IPv6. Estadísticas: Adopción de IPv6 por país. Recuperado el día 09 de agosto de 2018, de https://www.google.com/intl/es/ipv6/statistics.html.

[39] Fuente: LACNIC. ¿Quiénes implementan?. Qué ISP están implementando IPv6 en la región de América Latina. Recuperado el 08 de agosto de 2018, de http://www.lacnic.net/3042/1/lacnic/quienes-implementan.

[40] Comunidad internacional abierta de diseñadores de redes, operadores, vendedores e investigadores preocupados por la evolución de la arquitectura de Internet y el buen funcionamiento de Internet.

[41] Dispositivo de pequeño tamaño que combina una PC, teléfono/fax, Internet y conexiones de red. También denominado "Palmtops" o computadora de bolsillo.

que traspasan los dispositivos de la red. Establece cabeceras de extensión para no sobrecargar al encabezado con campos innecesarios.

- ✓ Mayor eficiencia en la implementación de direcciones: anycast y multicast, para brindar una red sin tormentas de broadcast.
- ✓ Mayor seguridad (IPSec), con autenticación y privacidad como características propias.
- ✓ Calidad de servicio de extremo a extremo para trabajar con aplicaciones multimedia en Internet. ([42])

Fortalezas y debilidades de una VPN corriendo sobre IPv6

Al implementar una red privada virtual sobre el protocolo de internet versión 6 se pueden mencionar:

Fortalezas:

- Desvinculan su direccionamiento y enrutamiento de los operadores de sus redes subyacentes.
- Puede mantener una dirección IP consistente en las máquinas, incluso cuando su proveedor renueve sus redes.
- Puede mantener una dirección IP consistente en las máquinas, incluso cuando se cambian de ubicación o de proveedor.
- Debido a los dos puntos anteriores, puede usar más fácilmente el control de acceso basado en IP.
- La calidad de servicio (QoS) es otro punto que tiene a favor ya que el protocolo IPv6 conserva un campo en su encabezado para este fin, lo que hace más eficiente su implementación.
- Además se tiene una mayor seguridad con IPv6 al incorporar en su estructura IPSec.

Debilidades:

- Curva de aprendizaje y adaptación de los sistemas y servicios.
- Tal vez el aspecto más importante sea el esfuerzo que significará preparar al personal de soporte, así como a los usuarios en el empleo de esta nueva tecnología.

VPN corriendo sobre IPv6, respecto de una aplicada sobre IPv4

Una de las principales ventajas de usar IPv6 en una VPN, está dada en que cada host tendrá asignada una dirección IP utilizada en toda la red pública, lo cual simplifica las tablas de enrutamiento de los dispositivos. Y a su vez, al

[42] AGUIRRE SANCHEZ, Op. cit., p. 45.

contar cada dispositivo con una IP que lo identifica públicamente será factible la utilización de VPN tipo sitio a sitio como se estudiará en capítulos posteriores.

En referencia a la priorización de tráfico en las redes, IPv4 no permite la implementación de calidad de servicio en redes administradas por terceros. En cambio, IPv6 al contener en su encabezado dos campos para la administración de prioridades, permitirá la clasificación de trafico de extremo a extremo de la comunicación. Sin embargo, en la actualidad la implementación de priorización de tráfico en los dispositivos intermedios no se encuentra disponible en las redes IPv6.

Actualmente para brindar seguridad en capa de Internet IPv4 debe adherir un protocolo complementario como IPSec, lo cual genera en el enlace una sobrecarga extra. Mientras que IPv6 implementa esta seguridad de forma nativa.

Las redes actuales disponen de equipos optimizados para funcionar con el protocolo IPv4, lo cual no implica su imposibilidad de ser actualizados a la nueva versión. Sin embargo, la performance se ve degradada en forma significativa a diferencia de los equipos modernos, que funcionan mejor con la nueva versión.

CAPITULO 3

[PROTOCOLOS DE TÚNEL QUE INTERVIENEN EN UNA VPN]

En este capítulo se estudiará en profundidad el concepto de tunneling y los diferentes protocolos utilizados para esta técnica. Además se analizarán los túneles seguros IPSec y sus componentes.

Tunneling

Utilizado en casos particulares en los cuales es necesaria una comunicación que puede ser entre hosts de una misma red, pero con la salvedad de que los paquetes deben viajar por distintas redes intermedias y luego llegar a destino. Para poder enviar las tramas el protocolo de túnel las encapsula con un encabezado adicional el cual proporciona información de enrutamiento de manera tal que la carga útil encapsulada pueda viajar a través de la red intermedia, como puede ser Internet.

Como ejemplo, se puede mencionar las sedes de la Facultad de Ciencia y Tecnología con una red el protocolo IP en su versión 6 en la sede Concepción del Uruguay (CDU) y en Oro Verde (OV), mientras que la conectividad entre las mismas a través de Internet utiliza la versión 4. Para enviar un paquete IP a un host en la oficina de CDU, un host en la red de OV construye el paquete que contiene una dirección de destino IPv6 en CDU y la envía al enrutador que conecta la red de OV con Internet. Cuando este enrutador recibe el paquete IP versión 6, le adhiere un encabezado versión 4, dirigido al lado IPv4 del enrutador que se conecta con la red de CDU. Cuando el paquete envuelto llega al router de CDU este extrae el paquete original y lo envía al host de destino.

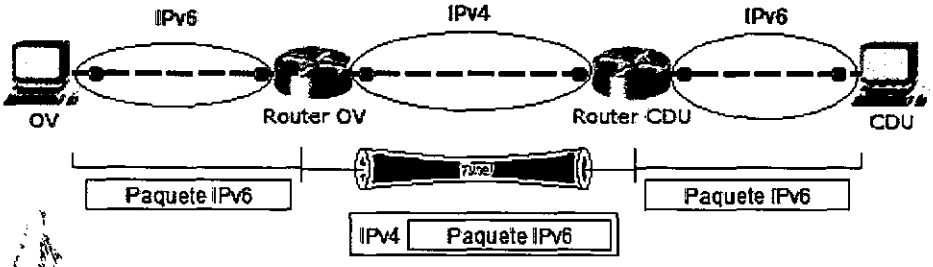


Figura 3.1 Encapsulación de paquetes IPv6 con paquetes IPv4.
Fuente: elaboración propia.

El paquete IPv6 viaja de un extremo a otro del túnel sin tener que interactuar con IPv4, como tampoco deben hacerlo los hosts de OV y CDU.
Son los router multiprotocolo de OV y CDU los que se encargan de entender y redireccionar el enrutamiento entre IPv4 e IPv6, enviando los paquetes de extremo a extremo. Según lo visto por Tanenbaum (2012):

> La tunelización se utiliza mucho para conectar hosts y redes aisladas mediante el uso de otras redes. La desventaja que tiene esta técnica es que no se puede llegar a ninguno de los hosts en la red que se tuneliza debido a que los paquetes no pueden escapar a mitad del túnel.
>
> Sin embargo, esta limitación de los túneles se convierte en una ventaja gracias a las redes VPN que simplemente es una red superpuesta que se utiliza para proporcionar una medida de seguridad.[43]

[43] TANENBAUM, A. S.; WETHERALL, D. J. (2012). *Redes de computadoras (Quinta edición).* México: Editorial Pearson. p. 369.

PROTOCOLO PUNTO A PUNTO (PPP)

El protocolo PPP proporciona un método para enviar datagramas sobre enlaces simples entre dos partes. Este tipo de enlace se da en los dos sentidos, es full dúplex y se asume que los paquetes llegarán a destino en orden.
No es un protocolo de túnel, pero es la base para PPTP, que es el protocolo de túnel punto a punto.

PPP está compuesto por:

- Un protocolo de control de enlace (LCP – Link Control Protocol) el cual se encarga de definir los parámetros de la conexión, como puede ser el tamaño del paquete, detección de errores, autenticación o finalización del enlace. Y una vez establecido realiza las pruebas sobre el enlace.
- Un protocolo de control de red (NCP – Network Control Protocol) que contiene información relacionada a protocolos de distintas capas.
- Cuadros de datos (Data Frames) adonde están contenidos los datos.

PPP define ciertos mecanismos para establecer, administrar y terminar el enlace.

- Para establecer el enlace cada dispositivo envía paquetes LCP para configurar y testear el enlace.
- Una vez establecido el enlace, se intercambian paquetes NCP para definir y configurar protocolos de capas superiores.
- Un vez seleccionado y configurados los protocolos superiores es posible enviar información a través del enlace.
- El enlace permanece activo a menos que algún terminal reciba paquetes NCP o LCP solicitando finalizar el enlace, o surja algún evento externo que interfiera en la comunicación y produzca que el enlace se cierre inesperadamente.

El PPP también tiene mecanismos de seguridad incorporados como el protocolo de autenticación de contraseña (PAP) y el protocolo de autenticación de intercambio de señales (CHAP) definidos en RFC 1334[44].

PAP es básico y realiza un enlace de dos vías para verificar la identidad de un nodo remoto. No hay encriptación: el nombre de usuario y la contraseña se envían en texto sin cifrar, si son correctas, la conexión se establece. CHAP presenta un mayor grado de seguridad, ya que provee un intercambio de tres vías de una frase compartida.

La fase de autenticación de una sesión PPP es opcional. Si se utiliza, la autenticación se lleva a cabo antes de que comience la fase de configuración del

[44] Define *PPP Authentication Protocols* - El protocolo punto a punto proporciona un método estándar para encapsular la información del protocolo de la capa de red en los enlaces punto a punto.

protocolo de capa superior. Para ello, los dispositivos pares intercambian mensajes de autenticación.

PAP no es un protocolo de autenticación sólido. Al utilizarlo, las contraseñas se envían por el enlace en texto no cifrado, y no posee protección contra intentos reiterados de prueba y error de verificación de identidad. Una vez que se establece la autenticación, PAP deja de funcionar, situación que deja la red vulnerable para los ataques.

En cambio CHAP realiza comprobaciones periódicas para asegurarse de que el nodo remoto todavía posee un valor de contraseña válido. El valor de la contraseña cambia impredeciblemente mientras el enlace existe, lo cual lo hace más difícil de atacar.

PROTOCOLO DE TÚNEL PUNTO A PUNTO (PPTP)

Proporciona medio para realizar conexiones seguras entre hosts remotos a través de un túnel seguro. Para lograrlo, un cliente establece una conexión al servidor del proveedor de servicios por medio de PPP. Una vez conectado, se establece una segunda conexión a los servicios PPTP de su organización por medio de la red pública. Este servidor oficializara de intermediario, tunelizando los datos de los clientes y reenviándolos a su correspondiente destino de la red privada. Esta estandarizado en RFC 2637[45], fue propuesto por Microsoft, es una extensión de PPP y opera en capa de acceso a la red de TCP/IP (Capa 2 OSI).

La comunicación iniciada desde los clientes hacia el servidor del proveedor debe ser aceptada, para posteriormente establecer el túnel a través de la red pública con destino al servidor de la organización.

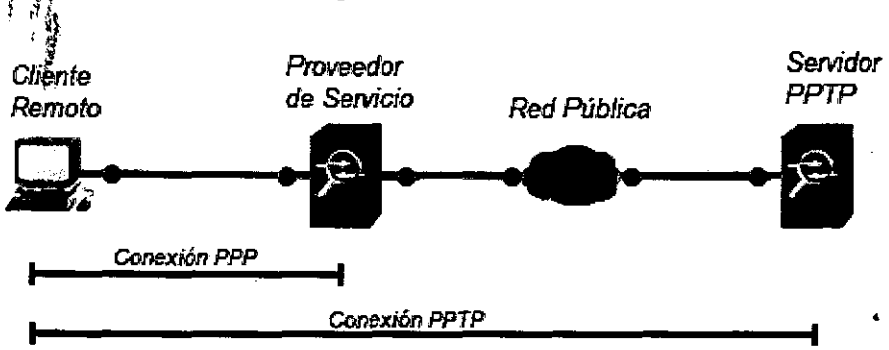


Figura 3.2 Protocolo de túnel Punto a Punto.
Fuente: elaboración propia.

El protocolo de túnel encapsula PPP en datagramas IP, cuando estos llegan al servidor son desensamblados con el fin de extraer los paquetes originales y descifrarlos de acuerdo al protocolo de red transmitido, que pueden ser IP, IPX[46]

[45] *Point-to-Point Tunneling Protocol* - Estable las especificaciones para tunelizar datos en una red IP.
[46] Protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. Es orientado a paquetes y no orientado a conexión.

o NetBEUI[47]; únicos protocolos de red aceptados por PPTP.

El protocolo se encarga de establecer, mantener y finalizar el túnel PPTP por medio de mensajes definidos. Estos mensajes de control se transmiten en paquetes dentro del segmento TCP, por lo que se componen de una cabecera IP, otra TCP y el propiamente dicho mensaje de control.

PPTP por sí solo no proporciona ningún mecanismo de seguridad, si los datos que atraviesan el túnel no están cifrados, cualquier usuario no autorizado puede apropiarse de la información; por lo que requiere de protocolos adicionales para autenticar usuarios y encriptar la información.

Autenticación de Usuarios

El servidor PPTP oficia de puerta de enlaces y se encarga de controlar todos los accesos al túnel. La autenticación de clientes remotos se realiza a través de los métodos provistos por PPP, es decir a través de PAP o CHAP. Protocolos que fijan un usuario y contraseña que se definen en el servidor, proporcionando de esta manera un método de autenticación centralizado.

Cifrado de Información

La encriptación de datos PPTP cuenta con la posibilidad de utilizar un proceso de encriptación de "secreto compartido". En el cual solo los host extremos del túnel comparten la clave, que es generada a partir de una contraseña de usuario, a la cual se le aplica un método de encriptación proporcionado por PPP.

TRANSMISIÓN DE NIVEL 2 (L2F)

El protocolo reenvío de capa 2 (L2F, Layer Two Forguarding), funciona en la capa de acceso a la red proporcionando servicios de tuneling. Es netamente un protocolo de encapsulamiento, que fue creado por Cisco Systems[48] en las primeras etapas del desarrollo de las redes privadas virtuales.

Ofrece ventajas entre las que se destacan soporte multiprotocolo, subdivisión de múltiples sesiones remotas que se comunican a través de un mismo medio, optimizando las mismas para que solo estén abiertas al momento de ser necesarias, lo que se podría denominar gestión dinámica de túneles; de esta manera se logran minimizar los recursos en los servidores.

En el interior de los túneles cada sesión remota mantiene un número de secuencia para evitar problemas de duplicidad de paquetes.

L2F difiere de PPTP en que permite múltiples sesiones dentro del túnel, los cuales se deben utilizar obligatoriamente.

[47] Introducido por IBM en 1985, es un protocolo de nivel de red sin encaminamiento y sencillo, utilizado como una de las capas en las primeras redes de Microsoft.

[48] Empresa global principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

PPTP no depende de IP, y ofrece flexibilidad para manejar distintos protocolos, además es independiente de los medios, puede correr sobre FrameRelay[49], ATM[50] o X.25[51].

Para la autenticación de usuarios L2F puede utilizar PPP u otros protocolos como ser TACACS+[52] o RADIUS[53].

PROTOCOLO DE TÚNEL DE NIVEL 2 (L2TP)

Este protocolo surge de la fusión de las mejores características de PPTP de Microsoft y L2F de Cisco. Esta aprobado y documentado por la IETF en la RFC 2661[54].

Es un estándar diseñado para transmitir datos y conectar de manera segura redes, usando internet como medio de transmisión. Puede utilizarse tanto en redes con tecnología IP como X.25, FrameRelay o ATM.

Maneja dos tipos de mensajes, uno es para mantener un túnel, llamado mensajes de control, que en las redes IP se encargan de establecer, mantener y limpiar los túneles utilizando tramas UDP y una serie de mensajes. Mientras que el otro tipo de mensajes se denomina "mensaje de datos" y es a través de los cuales la información se transmite encapsulada en tramas PPP, las cuales pueden ser cifradas o comprimidas. Si se utiliza IP como tecnología de transporte, puede combinarse con IPSec[55], lo que proporciona gran seguridad a la hora de transportar datos a través de redes públicas. Además es capaz de brindar autenticación de usuarios a través de protocolos como CHAP, autenticación por token[56] o certificados digitales[57].

El objetivo es enviar sus tramas PPP a través de túneles seguros entre un cliente remoto y un servidor que puede estar ubicado en una red LAN privada.

Las tramas PPP se transportan a través de canales de datos no confiables, encapsulado primero por con una cabecera L2TP y después por la cabecera de red TCP/IP pertinente, la cual puede ser cualquiera de las definidas en párrafos

[49] Protocolo que define cómo se direccionan las tramas en una red de paquetes en función del campo de dirección de la trama. La alta velocidad que puede obtenerse lo hacen adecuado para la conectividad de redes WAN.

[50] Modo de transferencia no síncrono que se hizo popular en 1988. Es orientado a conexión, transmite la información en paquetes pequeños, de tamaño fijo.

[51] Protocolo utilizado principalmente en una WAN sobre todo, en las redes públicas de transmisión de datos conmutadas por paquetes.

[52] Protocolo usado por los dispositivos de seguridad, routers y switches de Cisco Systems para la implementación de AAA, proporcionando el marco necesario para habilitar una seguridad.

[53] Desarrollado por Livingston Enterprises, es un protocolo usado para los registros de auditoría, abierto de estándar IETF con aplicaciones en acceso a las redes y movilidad IP. Se lo define en los RFCs 2865, 2866, 2867 y 2868.

[54] *Layer Two Tunneling Protocol* "L2TP" - Facilita la tunelización de paquetes PPP a través de una red intermedia de una manera transparente para los usuarios finales y las aplicaciones.

[55] Marco de trabajo que ofrece múltiples servicios y provee confidencialidad, integridad de datos y protección contra ataques de repetición.

[56] Utilizado para evitar la reiteración de datos de login al usuario en cada llamada. Una vez que el usuario finaliza el login, el servidor le devuelve un cadena de texto encriptada con una contraseña la cual se denomina token y será utilizado en futuros accesos para certificar su autenticación.

[57] Utiliza un archivo firmado con una clave privada de una autoridad que lo certifica, conteniendo la clave publica de la mencionada entidad y los atributos del titular del certificado.

anteriores. Mientras que los mensajes de control van a través de un canal confiable que se envía a través del mismo medio de transporte y bajo la misma cabecera que los mensajes de datos.

Creación del paquete L2TP

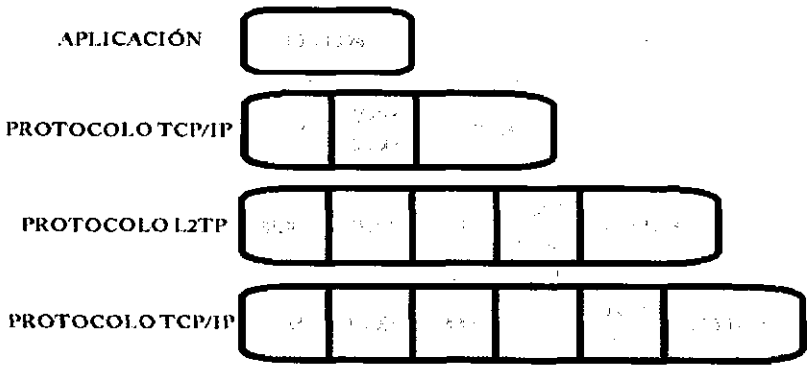


Figura 3.3 Creación del Paquete L2TP.
Fuente: elaboración propia.

Funcionamiento de L2TP

Antes de colocar las tramas en el túnel, los mensajes de control deben establecer la sesión L2TP. Pueden existir múltiples sesiones en un túnel y múltiples túneles entre un mismo cliente y servidor.

Posteriormente se debe establecer la autenticación del túnel. Generalmente utilizando el protocolo CHAP.

Una vez establecida la conexión de control, se crean las sesiones individuales necesarias. Cada sesión se corresponde con un único flujo de tramas PPP entre el cliente y el servidor.

Una vez establecido el túnel, las tramas PPP del sistema remoto son encapsuladas con el encabezado L2TP y enviadas al servidor por la sesión correspondiente identificada por los números de secuencia, los cuales también se utilizan para el transporte confiable de datos.

Tanto para mantener activa la sesión como para cerrar la misma, se utilizan mensajes previamente definidos.

Seguridad de L2TP

Opcionalmente se puede utilizar en los extremos del túnel un proceso de autenticación durante el establecimiento de la sesión. Esta autenticación tiene atributos similares a CHAP, así como también una protección razonable para pruebas de repetición.

Para el aseguramiento de los paquetes se requiere que los protocolos de transporte proporcionen servicios de seguridad, encriptación y autenticación para todo el tráfico. El transporte seguro funciona independientemente de PPP y del

protocolo que transporta empaquetado. L2TP solo se ocupa de la confidencialidad, autenticidad e integridad de los paquetes entre los extremos del túnel.

PPTP comparado con el L2TP.

Ambos protocolos utilizan PPP para proporcionar un empaquetado inicial de los datos y luego incluir sus propios encabezados adicionales, para transportarlos a través de la red. Los dos protocolos son muy similares, pero existen diferencias que se plantean a continuación mencionadas por Cosme MacArthur Ortega (2003):

- PPTP requiere que la red sea de tipo IP. Mientras L2TP requiere sólo que los medios del túnel proporcionen una conectividad punto a punto orientada a paquetes[58].
- PPTP sólo puede soportar un túnel único entre host. L2TP permite el uso de varios túneles entre puntos terminales e incluso diferentes calidades de servicio para los mismos.
- L2TP proporciona la compresión de encabezados. Cuando se activa la compresión de encabezado, opera sólo con 4 bytes adicionales, comparado con los 6 bytes para el PPTP.
- L2TP proporciona la autenticación de túnel, mientras que PPTP no. Sin embargo, cuando se utiliza cualquiera de los protocolos sobre IPSec, este se encarga de proporcionar la autenticación del túnel.([59])

PROTOCOLO DE INTERNET SEGURO (IPSEC)

El protocolo IPSec (Seguridad IP, del inglés IP Security) se describe en los RFC 2401[60], 2402[61] y 2406[62], entre otras.

"El diseño IPSec completo es un marco de trabajo para múltiples servicios, algoritmos y niveles de granularidad" (Tanenbaum y Wetherall, 2012)[63]. La razón de los servicios múltiples es que no todas las personas quieren pagar el precio por tener todos los servicios todo el tiempo, por lo que están disponibles en todo momento. Los servicios principales son confidencialidad, integridad de datos y protección contra ataques de repetición. Todos los servicios se basan en criptografía de clave simétrica[64] debido a que es imprescindible un alto desempeño.

---

[58] Se puede utilizar L2TP sobre IP (utilizando UDP), circuitos virtuales permanentes (PVCs), circuitos virtuales X.25 (VCs) o VCs ATM.

[59] COSME MACARTHUR ORTEGA, B. *Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace*. 2003. (Tesis Ingeniero en Sistemas Computacionales). Ibarra, Ecuador. Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Escuela de Ingeniería en Sistemas Computacionales, p. 64.

[60] *Security Architecture for the Internet Protocol* - Este documento especifica un protocolo de seguimiento de estándares de Internet para la comunidad de Internet y sugerencias para mejoras.

[61] *IP Authentication Header* - Encabezado de autenticación IP.

[62] *IP Encapsulating Security Payload (ESP)* - Carga de seguridad encapsulada.

[63] TANENBAUM, A. S.; WETHERALL, D., Op. cit., p. 700.

[64] Algoritmo que utiliza una única clave secreta para cifrar y descifrar los mensajes.

IPSec se encuentra en la capa IP y es orientado a la conexión, ya que para tener seguridad, se debe establecer y utilizar una clave durante cierto periodo.

En el contexto de IPSec una comunicación se conoce como "Asociación de Seguridad" (SA), que es una conexión simple entre dos puntos y tiene una identificación de seguridad asociada a ella. Los identificadores de seguridad se transportan en paquetes que viajan en conexiones seguras, y son utilizados para buscar claves e información relevante cuando llega un paquete seguro. Técnicamente, IPSec tiene dos partes principales, la primera describe dos encabezados nuevos que se pueden agregar a los paquetes para transportar el identificador de seguridad, los datos de control de integridad e información utilizada para mantener bajo control la conexión. La otra parte, asociación para seguridad en internet y protocolo de administración de claves, del inglés Internet Security Association and Key Management Protocol - (ISAKMP), se encarga de establecer las claves.

ISAKMP es un marco de trabajo en el cual se define el formato del mensaje, la mecánica del protocolo de intercambio de claves y el proceso de negociación para construir una SA para IPSec. No define cómo se administran o comparten las claves entre los pares. El protocolo principal que realiza el trabajo es Intercambio de Claves de Internet, del inglés Internet Key Exchange (IKE).

IKE entonces combina los protocolos necesarios para establecer conexiones IPSec seguras entre los dispositivos. Establece las SAs acordadas entre los pares. Cada par debe tener idénticos ISAKMP y parámetros IPSec, para establecer una VPN operacional y segura.

IPSec puede utilizarse en uno de dos modos según Ariganello y Barrientos (2010)[65].

En el **modo de transporte**, el encabezado se inserta después del de IP, modificando en el último un parámetro para indicar que sigue una cabecera IPSec, que contiene información de seguridad, principalmente el identificador SA, un nuevo número de secuencia y una verificación de integridad del campo de carga.

En **modo de túnel**, todo el paquete IP, se re encapsula en el cuerpo de otro paquete agregando nueva información. El modo de túnel es útil cuando termina en una ubicación que no sea el destino final. En algunos casos, el final del túnel es una puerta de enlace[66]; por ejemplo, el firewall de una empresa. Éste es el caso común para una VPN. En este modo, la puerta de enlace encapsula y desencapsula paquetes conforme pasan a través de ella. Al terminar el túnel en el dispositivo, los host en la LAN no interactúan con IPSec.

[65] ARIGANELLO, E.; BARRIENTOS, E. (2010). *REDES CISCO. CCNP a Fondo. Guía de estudio para Profesionales.* Madrid, España: Editorial RA-MA, p. 607.

[66] Dispositivo utilizado como medio para realizar la interconexión entre redes de igual o distinta arquitectura.

Como desventaja, se puede mencionar respecto al modo túnel que al adicionarle un encabezo IP se incrementa el tamaño del paquete, y a sù vez introduce mayor sobrecarga a los medios.

Los dos protocolos de seguridad principales de IPSec son AH y ESP, la selección entre ellos determina que bloques del marco de trabajo estarán disponibles para su selección.

Encabezado de Autentificación

Authentication Header (AH), es el protocolo IP 51[67], normalmente utilizado cuando no se requiere o no se permite la confidencialidad. Asegura que el origen de los datos es uno de los extremos del túnel IPSec y verifica que los datos no han sido modificados durante la transmisión, proporcionando de esa manera verificación de integridad y la seguridad anti-repetición, pero no la confidencialidad. En el IPv4 se interpone entre los encabezados IP y TCP. En IPv6 es sólo otro encabezado de extensión y se trata como tal.

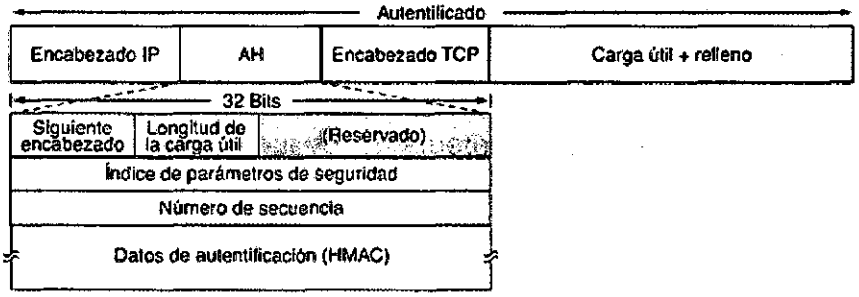


Figura 3.4 Encabezado de autenticación IPSec para IPv4.
Fuente: TANENBAUM, A. S.; WETHERALL, D. J. (2012). *"Redes de computadoras" (Quinta edición).* México: Editorial Pearson. Página 702.

Definición de los componentes del encabezado AH

Siguiente encabezado: se utiliza para almacenar el valor que tenía el campo protocolo de IP antes de reemplazarlo con 51 para indicar que sigue un encabezado AH.

Longitud de carga útil: es el número de palabras de 32 bits en el encabezado AH menos 2.

Índice de parámetros de seguridad: es el identificador de la conexión. El emisor lo inserta para indicar un registro específico en la base de datos del receptor. El registro contiene la clave compartida que se utiliza en la conexión. (Se utiliza a manera de definición de circuitos virtuales).

Número de secuencia: se utiliza para numerar todos los paquetes enviados en una SA. Cada paquete recibe un número único, incluso las retransmisiones, si bien estas obtienen aquí un número diferente al del paquete original, su número

[67] Código utilizado para identificar el protocolo AH en la parte de datos del datagrama IP.

de secuencia TCP sigue siendo el mismo. El propósito del campo es detectar ataques de repetición.

Datos de autentificación: contiene la firma digital de la carga útil. Cuando se establece la SA, los dos extremos negocian que algoritmo de firmas van a utilizar. Por lo general, puesto que IPSec se basa en la criptografía de clave simétrica y el emisor negocia con el receptor una clave compartida antes de establecer una SA, dicha clave compartida se utiliza en el cálculo de la firma.

Una forma simple es calcular el hash[68] sobre el paquete y sumarle la clave compartida. Desde luego que esa no es la clave que se transmite. Un esquema como así se conoce como HMAC. El encabezado AH no permite la encriptación de los datos, por lo que es mayormente utilizado cuando se necesita la verificación de la integridad pero no la confidencialidad.

Proceso de AH

1. Se calcula el hash del encabezado IP y los datos del paquete, utilizando la clave secreta compartida.
2. El hash genera un nuevo encabezado AH, el cual se inserta en el paquete original.
3. Se transmite el nuevo paquete hacia el otro extremo IPSec correspondiente.
4. El extremo destinatario calcula el hash del encabezado y los datos del paquete, utilizando la clave secreta compartida.
5. Extrae el hash transmitido en el encabezado AH y compara los hashes.

Observación: los hashes calculados deben coincidir perfectamente. Si se modificó al menos un bit en el paquete transmitido, el hash calculado sobre el paquete transmitido es diferente y no será igual al transmitido en el encabezado AH.

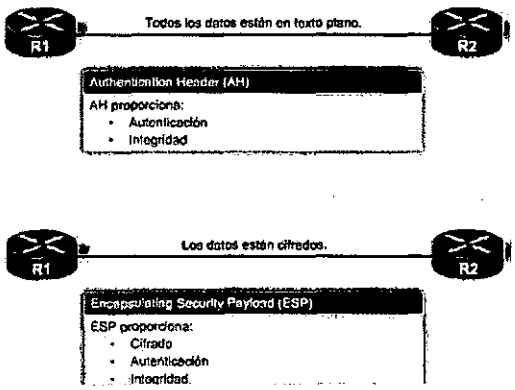


Figura 3.5 Proceso de AH.

Fuente: *Seguridad de Protocolo de Internet (IPSec)* por WALTON, Alex. Recuperado el 20 de febrero de 2018, de https://ccnadesdecero.es/ipsec-seguridad-protocolo-internet/.

[68] Función que se aplica a datos binarios, llamados mensajes y produce como resultado una cadena abreviada con un grado significativamente difícil de invertir, la cual es denominada digesto del mensaje. Es una técnica utilizada para verificar y asegurar la integridad de los datos.

Encapsulating Security Payload (ESP)

ESP es el protocolo IP 50[69], puede proveer confidencialidad y autenticación. Proporciona confidencialidad ejecutando el cifrado de los paquetes IP, resguardando los datos y la identidad tanto del origen como del destino. Provee autenticación para el paquete IP interno y el encabezado ESP proporcionando la autenticidad del origen de los datos y la integridad de los mismos. Aunque tanto el cifrado como la autenticación son opcionales, el protocolo debe seleccionar uno como mínimo.

Es el único protocolo de IPSec que proporciona encriptación de los datos pero también permite todas sus demás características. Debido a ello es utilizado unánimemente en VPN IPSec hoy en día. Los siguientes procesos de encriptación se encuentran disponibles en ESP y serán descriptos con mayor detalle en capítulos posteriores del presente estudio:

- DES (Data Encryption Standard) es un método de autenticación muy antiguo y presenta extensiones.
- 3DES (Triple Data Encryption Standard) es un bloque encriptado que utiliza tres veces DES.
- AES (Advanced Encryption Standard) es uno de los algoritmos de llaves simétricas populares en la actualidad.

Autenticación de Vecinos

A continuación se mencionan métodos para autenticar al vecino tratados por Ariganello y Barrientos (2010), lo que garantiza que el host es quien dice ser:

- *Usuario y contraseña*, ambos datos son definidos y se encuentran almacenados estáticamente en los hosts.
- *Contraseña de un sólo uso*, el método fue ideado para establecer sesiones de una en una, si se descubre una contraseña no afecta a la seguridad de la sesión.
- *Sistemas biométricos*, analizan una parte de las características del ser humano, como ser las huellas digitales, la retina u ótros rasgos identificativos. Es un método considerado seguro, ya que duplicar dichas características sería prácticamente imposible.
- *Claves pre compartidas*, se utiliza usuario y contraseña, pero los valores deben ser ingresados en los hosts extremos.
- *Certificados digitales*, es muy común y cada vez gana más terreno de utilización. Un certificado digital es emitido para cada dispositivo por parte

[69] Código utilizado para identificar el protocolo ESP en la parte de datos del datagrama IP.

de una autoridad certificante (CA) y será válido solamente en el dispositivo para el que ha sido emitido.([70])

Internet Key Exchange (IKE)

Es utilizado por IPSec para autenticar a los usuarios y dispositivos que puedan llevar a cabo comunicaciones en forma independiente estableciendo el proceso de intercambio de claves. Cuenta con variedad de tipos de autenticación, como las que ya fueron descriptas en el capítulo.

En lugar de transmitir las claves en forma directa a través de la red, IKE calcula las claves compartidas en base al intercambio de una serie de paquetes de datos. Lo que evita que un tercero pueda descifrar las claves, incluso si logra capturar todos los datos intercambiados utilizados para calcularlas.

Trabaja en el puerto UDP 500 para intercambiar la información entre los gateways de seguridad. Está definido en la RFC 2409[71]. Se trata de un protocolo que combina ISAKMP y los métodos de intercambio de claves Oakley[72] y Skeme[73]. ISAKMP define el formato del mensaje, la mecánica del protocolo de intercambio de claves y el proceso de negociación para construir un SA para IPSec. Pero no define cómo se administran o comparten las claves entre los pares IPSec, para ello Oakley y Skeme tienen cinco grupos de claves definidos, siendo el mayormente utilizado el algoritmo de Diffie-Hellman (DH)[74].

Combinando los protocolos mencionados permite establecer conexiones IPSec seguras entre los dispositivos. Establece las SAs acordadas entre los pares adonde cada par debe tener idénticos ISAKMP y parámetros IPSec, para establecer una VPN operacional y segura.

Una alternativa a la utilización de IKE es configurar en forma manual todos los parámetros requeridos para establecer una conexión. Pero este proceso es poco práctico, ya que no es escalable.

Fases de IKE

Puede dividirse en dos partes que crean una comunicación segura entre los dos extremos IPSec. Aunque son dos fases primarias y obligatorias, existe también una tercera opcional:

- Fase 1: es obligatoria. Una SA bidireccional es establecida entre los dos puntos.

[70] ARIGANELLO, E.; BARRIENTOS, E., Op. cit., p. 608.
[71] Proporciona un marco para la autenticación y el intercambio de claves, pero no los define. ISAKMP está diseñado para ser independiente del intercambio de claves.
[72] El intercambio de claves de grupo Oakley implica la generación de claves y la autenticación de claves.
[73] Fuente de intercambio de claves que permite el cifrado de clave pública y tiene la capacidad de actualizar rápidamente las teclas.
[74] Protocolo de intercambio de claves que permite la generación de claves negociada entre desconocidos.

- Fase 1.5: es opcional. Proporciona una capa adicional de autenticación llamada Autenticación Extendida, cuya finalidad es validar al usuario que va a hacer uso de la conexión segura.
- Fase 2: es obligatoria. Se establecen SA unidireccionales entre los puntos usando los parámetros acordados en la fase 1.

En la fase 1 se determinan los conjuntos de transformación y los métodos de hash. Una sesión IKE comienza con un extremo (el iniciador) que envía una propuesta al otro punto (el receptor). La propuesta enviada por el iniciador define qué protocolos de cifrado y autenticación son aceptables, por cuánto tiempo deben permanecer activas las claves y si debe aplicarse perfect forward secrecy (PFS)[75]. PFS asegura que si una clave se ve comprometida, las claves anterior y posterior permanecen seguras.

El objetivo de la fase 2 es negociar los parámetros de seguridad IPSec que serán utilizados para asegurar el túnel. La fase 2 es llamada modo rápido y sólo puede ocurrir una vez que el protocolo ha establecido el túnel seguro en la fase 1. El proceso IKE-ISAKMP negocia las SAs en nombre de IPSec, que necesita las claves de cifrado para operar. En esta fase, las SAs utilizadas por IPSec son unidireccionales. Por lo tanto, se requiere un intercambio de claves separado por cada flujo de datos.

La fase 2 ejecuta las siguientes funciones:

- Negocia los parámetros de seguridad IPSec, conocidos como conjuntos de transformación IPSec.
- Establece las SAs IPSec.
- Renegocia las SAs IPSec en forma periódica, para revalidar la seguridad.
- Opcionalmente, realiza un intercambio DH adicional.

Marco IPSec

No se encuentra limitado a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de claves, puede proteger prácticamente todo el tráfico de una aplicación, si bien funciona en capa de red, protegiendo y autenticando paquetes IP, sus servicios pueden cubrir también la capa 4 del modelo TCP/IP.

Los cuatro servicios de seguridad fundamentales de IPSec son: confidencialidad, integridad de datos, autenticación y protección anti reproducción, que es fundamental para detectar y rechazar paquetes imitados previniendo los ataques de suplantación de identidad.

[75] Propiedad de los sistemas criptográficos que asegura que las claves utilizadas para proteger los datos no sean utilizadas para derivar ninguna otra clave.

En la Figura 3.6 que aparece a continuación, se muestran que el marco IPSec está conformado de cinco bloques.

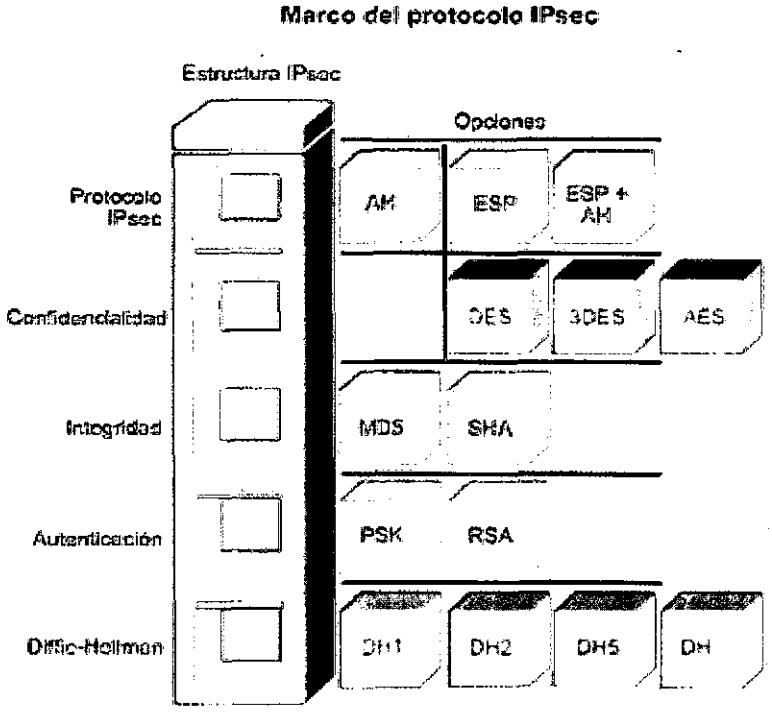


Figura 3.6 Marco IPSec.
Fuente: *Seguridad de Protocolo de Internet (IPSec)* por WALTON, Alex. Recuperado el 20 de febrero de 2018, de https://ccnadesdecero.es/ipsec-seguridad-protocolo-internet/.

El primero de ellos es el protocolo IPSec propiamente dicho, adonde las opciones son AH, ESP o una combinación de ambos. Los protocolos seleccionables ya fueron descriptos en este capítulo, pero es necesario destacar que dada la elección realizada en este punto, se condicionaran las opciones de selección del bloque siguiente, ya que se puede ver en el gráfico, que no hay opciones que proporcionen confidencialidad combinables con el protocolo AH.

La opción dos representa la confidencialidad, es válida solo si se implementa IPSec con ESP, siendo las opciones de selección DES, 3DES y AES, protocolos de cifrado que se describirán en detalle en capítulos posteriores.

El tercer punto es integridad, se puede implementar utilizando MD5[76] o SHA[77]. La principal diferencia es que SHA1 maneja una clave de 160 bits, contra los 128 de MD5, lo que proporciona mayor seguridad a costa de mayor sobrecarga. A su vez Se han desarrollado nuevas versiones de SHA-1 que producen hashes de 224, 256, 384 y 512 bits. A esas versiones se les conoce como SHA-2.

[76] Función de un solo sentido que facilita el cálculo de hash para los datos ingresados, pero vuelve inviable el cálculo de los datos originales dado un único valor de hash.
[77] Opera truncando los bits de una manera compleja como para que cada bit de salida se vea afectado por cada bit de entrada.

El bloque cuatro representa la autenticación, cuyas opciones son PSK[78] y RSA. Estos métodos de autenticación organizan la manera de establecer las claves secretas compartidas. PSK utiliza el método denominado clave pre-compartida mientras que RSA se basa en firma digital, en capítulos posteriores ambos esquemas se describen en mayor detalle.

La última opción representa la forma en que se establece la clave secreta compartida entre las partes, por medio de los distintos grupos DH. El algoritmo de intercambio de clave Diffie-Hellman se describe en detalle en capítulos posteriores del presente estudio.

Los componentes mencionados son los que forman el marco IPSec y se deben seleccionar al menos 4.

GRE VPNs

Generic routing encapsulation (GRE) es un protocolo de tunneling definido en las RFC 1702[79] y 2784[80]. Fue desarrollado originalmente por Cisco Systems para la creación de enlaces punto a punto entre routers Cisco en puntos remotos sobre una red IP.

Soporta tunneling multiprotocolo, lo que le permite encapsular paquetes de múltiples protocolos dentro de un túnel IP. Esta función se realiza agregando un encabezado GRE adicional entre el paquete de datos y el encabezado de túnel IP. El tunneling IP de esta forma permite la expansión de la red conectando subredes multiprotocolo a través de un ambiente troncal con un único protocolo. También soporta tunneling IP multicast. Los protocolos de enrutamiento utilizados a través del túnel permiten el intercambio dinámico de información de enrutamiento en la red virtual.

Los túneles son sin estados, cada extremo no mantiene información sobre el estado o disponibilidad del otro extremo del túnel. Esta característica permite a los proveedores de servicio (ISPs) proveer túneles IP a clientes que no requieren conocer la arquitectura interna del túnel en el extremo del ISP. Los clientes tienen entonces la flexibilidad de configurar o reconfigurar su arquitectura manteniendo la conectividad. Esto crea un enlace punto a punto virtual entre routers en puntos remotos de la red.

[78] Es un algoritmo asimétrico que se basa en la teoría de números para asegurar la autenticación.
[79] Encapsulación de enrutamiento genérico sobre redes IPv4. Describe el uso de GRE con IP.
[80] Encapsulación de enrutamiento genérico (GRE). Describe la encapsulación de un protocolo sobre otro protocolo de una manera general.

Protocolo de tunneling GRE

- Encapsula una amplia variedad de tipos de paquetes de protocolos dentro de los túneles IP.
- Crea un enlace virtual punto a punto entre routers Cisco en puntos remotos, a través de una red IP.
- Utiliza IP como transporte.
- Utiliza un encabezado adicional para soportar multicasting IP y cualquier otro protocolo de capa 3 del modelo OSI.

Figura 3.7 Túnel GRE.

Fuente: *Túneles GRE: Características y Configuración* por WALTON, Alex. Recuperado el 20 de febrero de 2018, de https://ccnadesdecero.es/tuneles-gre-caracteristicas-y-configuracion/.

Se encapsula el paquete original completo, con un encabezado IP estándar y un encabezado GRE. Este último contiene al menos 2 campos obligatorios de 2 bytes:

- Bandera (Flags)
- Tipo de protocolo

Se utiliza un campo de tipo de protocolo en la cabecera para soportar la encapsulación de cualquier protocolo de capa 2 del modelo TCP/IP. El encabezado, junto con el encabezado de tunneling IP, agregan al menos 24 bytes de sobrecarga adicional a los paquetes enviados a través del túnel.

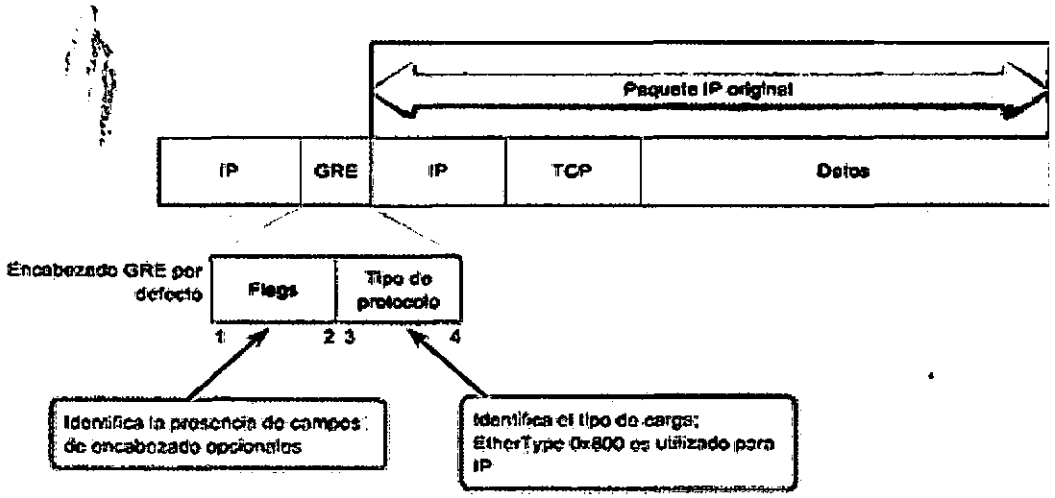


Figura 3.8 Encapsulación con GRE.

Fuente: *Túneles GRE: Características y Configuración* por WALTON, Alex. Recuperado el 20 de febrero de 2018, de https://ccnadesdecero.es/tuneles-gre-caracteristicas-y-configuracion/.

Las ventajas que presenta es que puede ser utilizado para tunelizar tráfico no IP sobre una red IP. Además, y a diferencia de IPSec que sólo soporta tráfico unicast, soporta tráfico multicast y broadcast a través del enlace del túnel.

Este protocolo no incluye ningún mecanismo de seguridad fuerte para proteger los datos transmitidos, no provee cifrado. Si fuera necesario, debe configurarse IPSec.

CUADRO DE REFERENCIA DE PROTOCOLOS DE TUNEL

PROTOCOLO	DESCRIPCION	VENTAJAS	DESVENTAJAS
PPP	Permite enviar datagramas a través de enlaces simples entre dos extremos. Cuenta con mecanismos de seguridad incorporados, conocidos como PAP y CHAP. PPP fue usado como base para la creación de PPTP.	• Es simple de configurar y rápido en la transferencia. • Posee mecanismos de seguridad con y sin encriptación, los cuales realizan verificación de identidad en los extremos del túnel.	• Es simple, adonde la seguridad no es el punto principal. • La autenticación de usuarios es opcional. • La contraseña de sesión circula por el enlace en texto plano. • No posee protección contra intentos de acceso reiterados.
PPTP	Es una extensión de PPP. Utiliza el mencionado protocolo para establecer las sesiones en la red local, mientras que las sesiones remotas son tunelizadas mediante un servidor PPTP, que agrega un encabezado a las tramas PPP.	• Es de simple configuración. • Es nativo de los Sistemas Operativos Microsoft, por lo que no requiere instalaciones adicionales. Es de rápida implementación, no requiere gran volumen de configuraciones para su utilización.	• No proporciona verificación de identidad por sí solo, requiriendo la seguridad aportada por otros protocolos. • Presentar problemas de transferencias en redes inestables. • No soporta múltiples sesiones en el túnel. • Solo funciona sobre protocolos IP.
L2F	Protocolo de encapsulamiento creado por Cisco System. Fue creado en el inicio desarrollo de las VPN.	• Ofrece soporte multiprotocolo. • Subdivisión de múltiples sesiones remotas. • Gestión dinámica de túnel. • La autenticación de usuarios es un requisito para establecer la sesión.	• Es un protocolo propietario.
L2TP	Fue creado con las mejores características de PPTP y L2F. Es un protocolo que estandariza la manera de conectar y transmitir datos seguros a través de redes públicas.	• Es un protocolo estandarizado, soportado por la mayoría de las tecnologías IP, X.25, FrameRelay y ATM y hereda las ventajas definas en L2F. • Diferencia los mensajes de control de los mensajes de datos, lo que optimiza el mantenimiento del túnel. • Los mensajes de control circulan a través del medio por un canal confiable, lo que beneficia a la seguridad.	• Al utilizarlo con un protocolo adicional como IPSec, encapsula los datos dos veces, lo cual influye en su rendimiento. • Posee mayor complejidad en su instalación, ya que es necesario definir gran cantidad de parámetros en su configuración.
IPSEC	Es un conjunto de protocolos englobados en un marco de trabajo, que proporciona seguridad a las comunicaciones de Internet en la capa IP. Posee dos modos de uso que se adaptan al tipo de comunicación a establecer. (Modo transporte o túnel)	• Utiliza criptografía de clave simétrica y es orientado a la conexión. • Tiene dos partes, la primera se encarga de transportar los identificadores de seguridad y datos de control, mientras que la segunda tiene definido un marco de protocolos que se encargan de la administración de claves, esta división en partes hace a la seguridad de la comunicación. • Es adaptable a nuevos protocolos y algoritmos de intercambio de claves.	• Proporciona seguridad a todo el tráfico, pero introduce gran sobrecarga a la comunicación. • En el modo túnel, adiciona una cabecera extra, lo que incrementa considerablemente el tamaño del paquete. • Independientemente del tipo de comunicación o aplicación que lo utilice, IPSec puede utilizarse siempre que se basen en IP.

		• En el modo de transporte, se logra identificar claramente la cabecera a diferencia de los datos que circulan encriptados. • En el modo túnel no es necesario que los hosts finales implementen IPSec.	
GRE	Protocolo de tunneling estandarizado, creado originalmente por Cisco System, para la creación de enlaces punto a punto remotos sobre una red IP.	• Soporta tunneling multiprotocolo. • Permite encapsular paquetes de distintos protocolos dentro de un túnel IP. • Soporta trafico multicast y broadcast, lo cual da soporte a protocolos de enrutamiento a través del enlace.	• No incluye ningún mecanismo de seguridad para proteger los datos transmitidos, por lo que es necesario combinarlo con otro protocolo, como puede ser IPSec. • El protocolo agrega un encabezado extra con una bandera GRE y el tipo de protocolo transportado, lo cual produce una sobrecarga adicional a los paquetes enviados por el túnel.

Tabla 3.1 Cuadro de referencia de protocolos de túnel.
Fuente: elaboración propia.

CAPITULO 4

[REQUERIMIENTOS PARA LA IMPLEMENTACIÓN DE UNA VPN]

En el capítulo se estudiarán los tipos de VPN que se pueden implementar (según arquitectura y topología). También se analizarán los requerimientos básicos necesarios para crear una VPN.

TIPOS DE VPN EXISTENTES

Arquitectura

Existen básicamente dos tipos a implementar, las VPN sitio a sitio (también llamadas punto a punto) y las de acceso remoto.

- **Acceso remoto:** permite autenticar usuarios brindándole acceso a los recursos requeridos resguardados un la red privada, pudiendo estar en una intranet[81] o extranet[82] corporativa. Para efectuar esta comunicación el usuario cuenta con un cliente remoto instalado en un dispositivo con acceso a internet, el cual se encarga de realizar y validar la conexión con el servidor VPN.

- **Sitio a sitio:** arquitectura utilizada para conectar dependencias geográficamente distantes usando redes públicas. Se encarga de validar los extremos de la comunicación, enviando la información mediante un túnel que protege su seguridad. Esta tecnología permite extender una LAN organizacional utilizando ISP locales lo cual reduce el costo de contratar una alternativa dedicada.

A su vez, de esta clasificación surge una salvedad, que puede diferenciar a las Redes Privadas Virtuales entre:

- **VPN de intranet:** se utilizan para la comunicación interna de una compañía. Enlazan una oficina central con todas sus sucursales. Se cuenta con las mismas normas que en cualquier red privada.
  Un router realiza una conexión sitio a sitio que conecta dos partes de una red privada ubicadas en distintos lugares geográficos.
- **VPN de extranet:** utilizadas para enlazar clientes, proveedores, socios o comunidades de interés con una intranet corporativa. Todos los miembros deben cumplir con las mismas normas que las de una red privada. Sin embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que debe ser cuidadosamente diseñada con muchas políticas de control de acceso y acuerdos de seguridad entre todos los integrantes.

Según su forma de implementación

Puntos trabajados por Cosme MacArthur Ortega (2003)[83]:

Proporcionada por un proveedor de servicios de red: en este tipo de servicio son los Proveedores de Servicios de Internet (ISP), los cuales se encargan de mantener el túnel entre nuestra organización y sus servicios. Se debe hacer responsable de mantener funcionando el servicio adecuadamente, y por ende debe hacerse cargo de la instalación y configuración de la misma, y si así lo requiere tiene la autorización para instalar un dispositivo en las oficinas de la organización, que se encargara de crear el túnel.

[81] Servicio que proporciona las aplicaciones claves de internet en el entorno de una organización, solo con fines internos.
[82] Es la extensión de intranet corporativa en redes públicas, pero que mantiene las propiedades de seguridad para compartir las operaciones propias de la organización.
[83] COSME MACARTHUR ORTEGA, Op. cit., p. 71.

Un tema a resolver con el proveedor es la fijación de responsabilidades sobre el servicio contratado. Se debe definir quién es responsable de la seguridad, la organización o el ISP que nos ofrece el servicio; quién se hace cargo de los equipos de comunicación; quién hace los cambios en el control de la política de acceso y el tiempo necesario para implementar los cambios. Pero además de esto, hay que definir cuáles son los requisitos obligatorios que debe cumplir el servicio de conectividad, sobre todo para los casos en que se presente algún inconveniente. Es muy importante establecer un tiempo máximo de restablecimiento de fallas, así como también tiempos de respuesta razonables de parte del call center del proveedor de servicios.

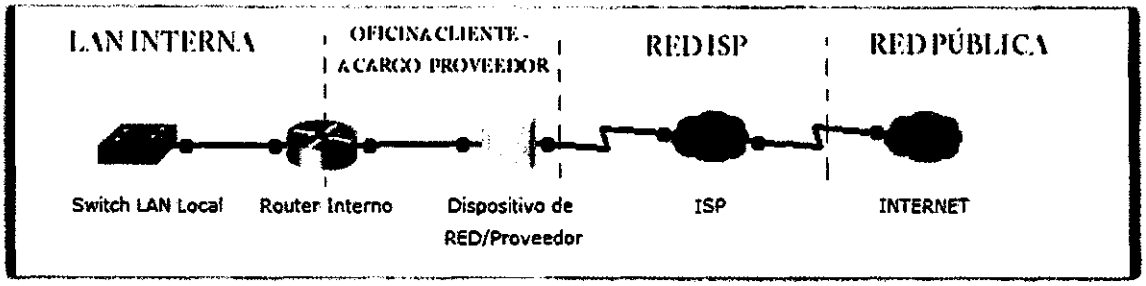


Figura 4.1 Arquitectura de una VPN proporcionada por el proveedor de servicios de Internet.
Fuente: elaboración propia.

Se debe tener en cuenta que la seguridad no debería estar en manos del proveedor de servicios de internet, aún si proporciona el equipo para establecer el túnel de la red privada. Respecto a la seguridad se debe tomar en consideración, que son las acciones de los propios usuarios las que pueden ocasionar los problemas de seguridad.

Respecto al control de cambios el proveedor de servicios de internet puede no estar disponible siempre, lo cual influiría en los tiempos de respuesta, por lo que es recomendable realizar la tarea de manera conjunta entre el ISP y los técnicos de la compañía. Al añadir nuevos servicios es posible que se requiera parar el funcionamiento de la VPN, de tal forma que eventualmente podría pasar por varios controles de cambios y necesitará seguirle la pista a cada uno de ellos y supervisarlos.

Por lo que es necesario determinar cómo monitorear el control de cambios. Si solicitó un cambio en su arquitectura existente debe saber cómo y cuándo se implementó esa solicitud.

En cualquier tipo de arquitectura de VPN, cuando las cosas van mal u ocurren problemas, ¿Quién puede ayudar? ¿Es el proveedor de servicios de Internet el llamado a solucionar los problemas, y éste estará en la predisposición de solucionarlos sin importar el tiempo que le tome?. Detallar en el contrato claramente los tiempos de respuesta y las responsabilidades del proveedor.

Es necesario detallar cómo y cuándo se añadieron usuarios a una base de datos, lo cual proporcionará los permisos para acceder a los recursos de la organización. ¿La base de datos está en el dispositivo proporcionado por el ISP o en algún servidor interno bajo su control? ¿Puede obtener acceso a él, de lo contrario, cuánto tiempo se requiere para que una autorización del usuarios se

vuelva efectiva?. Esto es importante en el caso de un empleado despedido; si un empleado deja la compañía es muy importante que su acceso se restrinja de inmediato.

Respecto a la utilización de la red es necesario ser consciente del funcionamiento general. La organización o el ISP deben monitorear y auditar el enlace para el uso del tráfico en el ancho de banda.

VPN basadas en cortafuegos: la mayoría de los proveedores ofrecen este tipo de configuración; dado que es una implementación básica, que cuenta con gran potencial de crecimiento y adaptación.

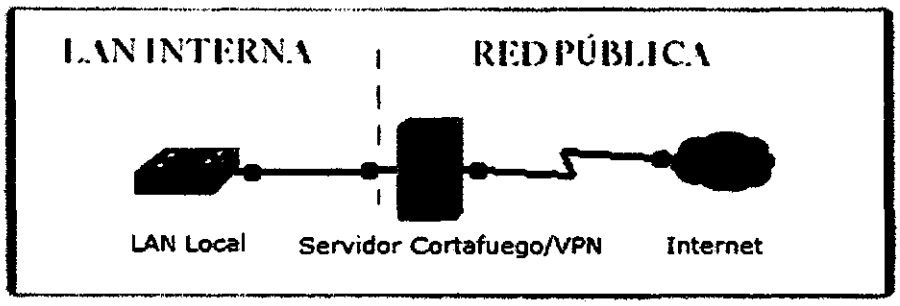


Figura 4.2 Arquitectura VPN basada en Cortafuego.
Fuente: elaboración propia.

Las organizaciones tienden a utilizar los servidores que ofician de firewall con el objetivo de crear una infraestructura VPN, reduciendo así costos de implementación y optimización de sus recursos. A su vez, la mayoría de los software cortafuegos cuentan con la capacidad para implementar las tecnologías de cifrado necesarias.

Un aspecto importante a considerar en la seguridad en el sistema operativo del cortafuegos. Es necesario estar consciente de sus vulnerabilidades y respaldar el mismo, aplicando buenas prácticas que lo resguarden en caso de contingencias.

Antes de instalar una VPN basada en cortafuego se deben conocer los protocolos de túnel existentes y decidir cual se va a utilizar. Y a su vez considerar la compatibilidad de las normas de túnel con el tipo de implementación cortafuego, como ser: inspección de estados, proxy o filtrado de paquetes. A su vez, se debe tener en cuenta que las VPN se ejecutan en los niveles más bajos de TCP/IP, por lo que el cortafuego también debe hacerlo para no dejar expuesta su seguridad.

VPN basadas en enrutador: arquitectura adecuada para organizaciones con una base de routers implementadas. A su vez, cuenta con una subdivisión; en una de ellas, el software se añade al router para permitir que el proceso de cifrado ocurra. En el segundo método se inserta una placa externa de fabricante en el chasis del equipo para que realice el proceso de cifrado y liberar cargada de procesamiento.

Este tipo de arquitectura tiene una alta carga de procesamiento para los equipos, por lo cual es necesaria la monitorización, y poner cuidado en la elección de los protocolos de cifrado a utilizar.

Se debe verificar que los enrutadores soporten todos los protocolos de seguridad de internet y aquellos que se utilizan para el establecimiento de túneles. Además, el enrutador implementará autenticación de usuarios, y para hacerlo necesitará un dispositivo independiente, como ser un servidor de autenticación, que sea compatible.

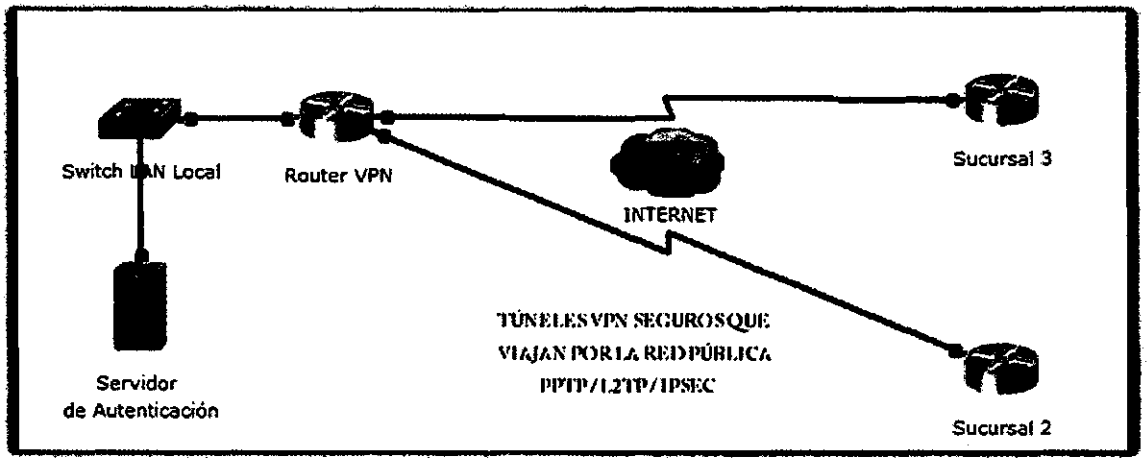


Figura 4.3 VPN basada en enrutador.
Fuente: elaboración propia.

VPN basadas en acceso remoto: la arquitectura tiene por objetivo brindar acceso a los recursos organizacionales de manera segura a clientes que se encuentran fuera de la organización. La siguiente figura muestra un escenario típico de acceso remoto.

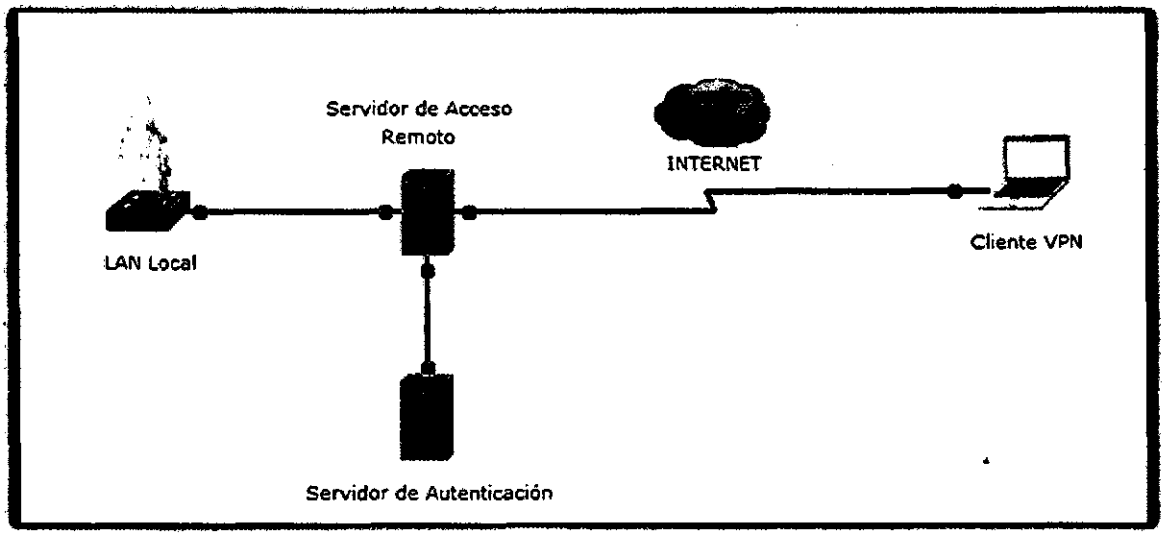


Figura 4.4 Arquitectura en VPN de Acceso Remoto.
Fuente: elaboración propia.

Esta configuración requiere de un software cliente que se ejecuta en una máquina remota la cual tiene acceso a internet y es utilizado para establecer una conexión a través de un túnel cifrado al servidor interno de la organización. El servidor otorgará permisos a los recursos en base a las credenciales de autenticación presentadas por el usuario.

VPN basadas en software: se utiliza un programa para establecer túneles o cifrado a otro host. Es un escenario cliente servidor en el cual, el software

cargado en el cliente se conecta al software cargado en el servidor y establece una sesión segura.

En la imagen a continuación se ilustran los componentes de una VPN basada en software.

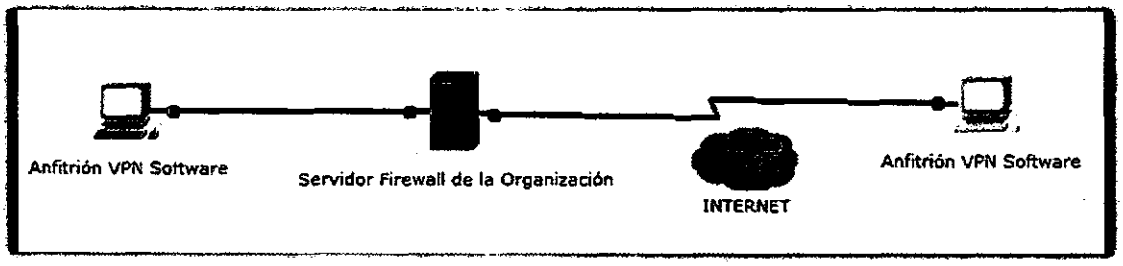


Figura 4.5 Arquitectura de VPN basada en software.
Fuente: elaboración propia.

Esta arquitectura puede utilizarse cuando un cliente necesita conectarse de manera segura a otro host en la misma red, el cliente inicia una sesión e instaura un diálogo de comunicación con el servidor VPN de la organización, el cual se encarga de controlar los parámetros de comunicación.

TOPOLOGÍAS DE RED PRIVADA VIRTUAL

Topología de cortafuego/VPN a Cliente

La mayoría de las organizaciones conectadas a Internet tienen un cortafuego instalado, y todo lo que se necesita es agregar software de VPN al cortafuego. Este tipo de topología es práctico de configurar para los que tienen un cortafuego implementado, y sólo desean aumentar la funcionalidad mediante VPN.

La topología como se muestra en la Figura 4.3 y se explica en el apartado de arquitecturas de VPN basada en enrutador.

Según Cosme MacArthur Ortega (2003) en ella existen dos componentes que deben habilitarse para establecer la comunicación:

- ✓ El dispositivo de cortafuego/VPN debe ejecutar algún tipo de código VPN, además de que deben agregar algunas reglas al cortafuego, como por ejemplo dejar pasar los datos cifrados, entre otras. El equipo portátil tiene una pila VPN instalada, debido a que una VPN transita y debe reconocer las diferentes capas del modelo TCP/IP.

- ✓ También hay que tomar en consideración que si se utiliza el cifrado propietario de un fabricante y tiene un cifrado diferente en el cortafuego/VPN, no existirá una comunicación entre ambos. Si utiliza el

encapsulamiento en el cortafuego / VPN, también deberá utilizarlo en el equipo portátil, por lo que debe haber correlación de protocolos. ([84])

Dado lo expuesto por Cosme MacArthur Ortega (2003), los siguientes pasos describen el proceso de comunicación entre el equipo cliente y el servidor posteriormente de realizar las configuraciones:

- El usuario en el equipo portátil marca a su proveedor de servicios de Internet local y establece una comunicación PPP.
- El equipo portátil solicita las claves del dispositivo del cortafuego/VPN.
- El cortafuego responde con la clave apropiada.
- El software de VPN instalado en el equipo portátil espera a que el usuario intente tener acceso al servidor interno (conocido como la dirección IP de destino). Si el usuario visita cualquier sitio distinto al de la red corporativa, no pasa nada. Pero si el usuario quiere realizar una conexión con el servidor interno, el software que se ejecuta en el equipo remoto ve la solicitud, cifra el paquete y lo envía a la dirección IP pública de la combinación cortafuego/VPN.
- El dispositivo de cortafuego/VPN le quita la dirección IP, descifra el paquete y lo envía al servidor dentro de la LAN local.
- El servidor interno responde la solicitud y envía el documento de regreso.
- El cortafuego/VPN examina el tráfico y por su tabla sabe que es una configuración de túnel de VPN. Así que toma el paquete, lo cifra y lo envía al equipo remoto.
- La pila de VPN en el equipo remoto ve el flujo de datos, sabe que viene del dispositivo de cortafuego/VPN, descifra el paquete y lo maneja en aplicaciones de niveles superiores.
- Esta configuración es la que permite que la VPN tenga una gran flexibilidad, ya que se puede utilizar Internet como medio para extender la red privada de la organización, y muchos de los ahorros en los costos vienen de esta configuración.

Hay que vigilar dos aspectos en este tipo de configuración:

[84] Ibid., p. 87.

- ✓ Las configuraciones del equipo remoto; este software tiene la tendencia a interactuar con otras aplicaciones y provoca problemas de interoperabilidad.
- ✓ Esta configuración añade una sobrecarga al proceso de cifrado / descifrado en el cortafuego. Se debe tomar en cuenta a ver si existen problemas de desempeño en el cortafuego. ([85])

Topología de VPN/LAN a LAN

El esquema permite realizar una comunicación entre host en una misma LAN pero ubicados geográficamente en distintos lugar y se conectan a través de redes públicas.

Para ellos se usa un software corriendo en servidores que soporten técnicas de cifrado estándares. Independientemente del sistema operativo, el cifrado y los software utilizados, los hosts son capaces de conectarse, siendo transparente para ellos el paso de la información privada a través de las redes no seguras.

En la Figura 4.6 se plasma una organización con una oficina remota que utiliza la arquitectura planteada, y es independiente de los software que utiliza en cada extremo del túnel.

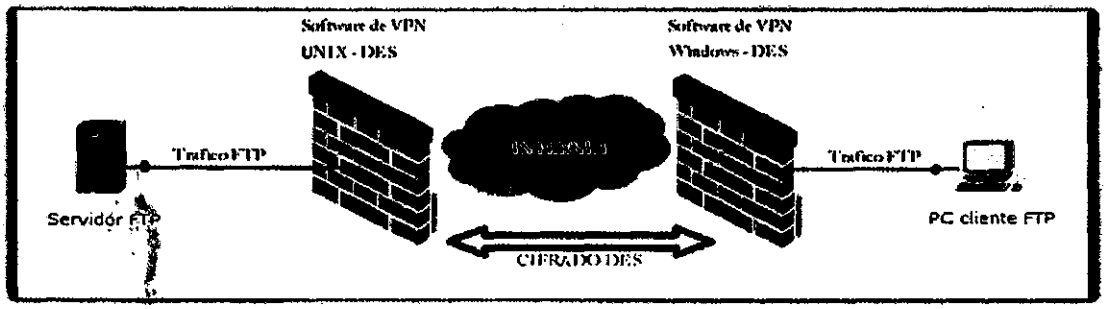


Figura 4.6 Topología de VPN de LAN a LAN.
Fuente: elaboración propia.

El ejemplo presenta a un usuario de la oficina remota que necesita conectarse al servidor de la otra oficina y hacer una transferencia FTP para transferir un archivo: antes de realizar la comunicación, los componentes que deben habilitarse son los siguientes según Cosme MacArthur Ortega (2003):

- ➢ El administrador de cada sitio está de acuerdo con el cifrado DES. El software de VPN de cada dispositivo crea una clave única.
- ➢ Si se trata de un producto de cortafuego/VPN, el administrador de cada oficina establece una regla, por ejemplo, que todo el tráfico destinado a la otra terminal debe cifrarse.

[85] Ibid., p. 88.

- El usuario final utiliza una aplicación FTP en su escritorio para intentar conectarse al servidor.
- El paquete abandona el escritorio en texto sencillo y llega al dispositivo de cortafuego/VPN.
- El paquete es cifrado y se envía a la dirección IP pública del dispositivo de cortafuego/VPN de la otra oficina.
- El cortafuego/VPN acepta y descifra el paquete y lo reenvía a su destino final.
- El servidor recibe el paquete y responde.
- Envía un paquete en texto sencillo a su dispositivo de cortafuego/VPN local.
- Después, el cortafuego/VPN lo cifra y lo envía al otro cortafuego/VPN.
- El cortafuego/VPN receptor lo descifra y finalmente lo envía de regreso al usuario original. ([86])

Es importante destacar que las operaciones de segurización de la información, son trasparentes para los hosts extremos de las comunicación.

Topología de VPN/Cortafuego a Intranet/Extranet

En la actualidad las intranet y extranet adquirieron gran popularidad en los entornos organizacionales, dando la posibilidad de brindar a sus actores intervinientes, servicios seguros tanto internamente como externamente.

Cosme MacArthur Ortega (2003) establece las siguientes condiciones:

- Primero se cuenta con flexibilidad para que un equipo se encargue de la intranet y extranet y gracias a esto se reduce la redundancia;
- Segundo se debe tener presente la seguridad, ya que existe una forma para que los usuarios externos tengan acceso a estos servidores. Es identificando a los empleados que requieren los servicios de Intranet, pero que acceden a ellos externamente, y a los clientes externos a quienes sólo se les permite el acceso a la extranet. ([87])

En la Figura 4.7 se ilustra una posible solución para ubicar los servicios de intranet y extranet. En ella el servidor web se conecta a una red expuesta, la cual

[86] Ibid., p. 91.
[87] Ibid., p. 91.

es permeable a los accesos tanto desde redes públicas como privada. El firewall se encuentra configurado para permitir solo el paso de los paquetes HTTP solicitados al servicio web a través de la DMZ1, denegando otro tipo de tráfico.

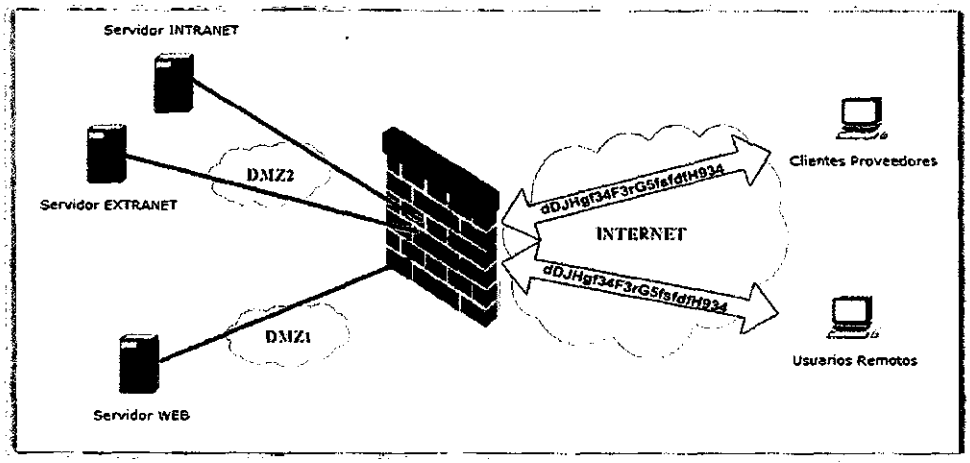


Figura 4.7 Ubicación apropiada de la Intranet, Extranet y Servidor Web.
Fuente: elaboración propia.

La extranet se coloca en una red propia con seguridad específica, que consiste en cifrar el tráfico y permitir solo las direcciones de origen necesarias.

La intranet esta resguardada por el firewall VPN y atiende peticiones de usuarios autenticados que se conectan remotamente.

Respecto a los servidores de red es importante que la seguridad aplicada a ellos se configure de acuerdo con su función. Si está permitido el acceso público, configurarlos en una DMZ[88] pública, si es para un intranet o extranet fijar que redes o que usuarios tienen acceso a ellos.

Topología de VPN/NAT

Es necesario mencionar la traducción de direcciones de red (NAT), ya que el proceso de traducción afecta el flujo de la comunicación segura cuando realiza el intercambio de las direcciones privadas por públicas y viceversa; con el fin de ocultar las estructuras de comunicaciones que no pueden enrutarse a redes públicas. Por lo que es crítica la ubicación asignada al dispositivo que regirá la VPN.

La Figura 4.8 muestra el flujo de tráfico que tiene lugar en un cortafuego que implementa NAT, mientras que el dispositivo VPN se encarga de la autenticación de usuarios.

[88] Red exclusiva para la conexión de dispositivos que brindan servicios, con configuraciones especificas que permiten consultas desde redes públicas.

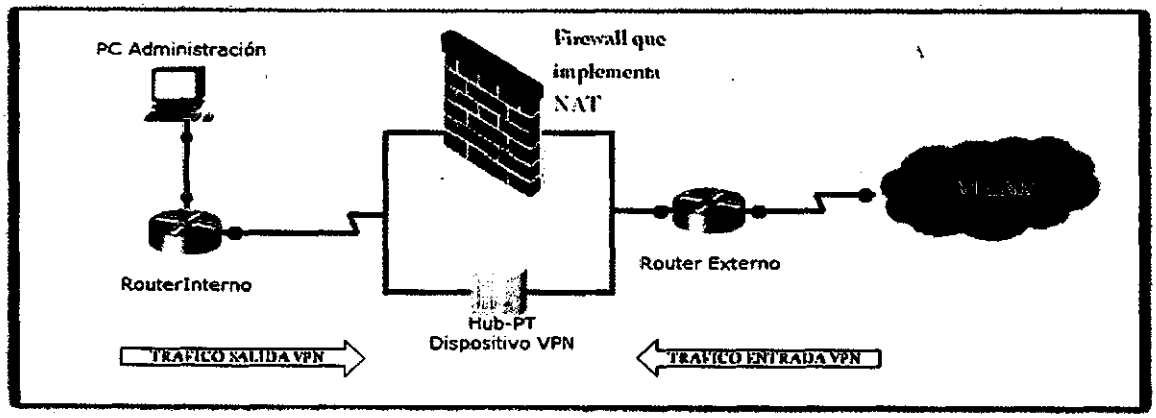


Figura 4.8 Implementación de NAT con Cortafuego y VPN.
Fuente: elaboración propia.

Cosme MacArthur Ortega (2003) destaca dos reglas que deben seguirse cuando se utilice NAT y VPN:

- Para paquetes de salida: si tienen que pasar por NAT y ser parte de una VPN, NAT debe aplicarse antes de que el dispositivo VPN cifre los paquetes.
- Para tráfico de VPN entrante: NAT debe aplicarse después de que el cifrado de VPN se haya eliminado del paquete. ([89])

REQUERIMIENTOS DE UNA VPN

Una VPN debe de contar con ciertos requerimientos que permitan el uso de la tecnología. Sin esos requerimientos, las VPN no podrán ofrecer la calidad necesaria que requieren las organizaciones para garantizar un funcionamiento óptimo.

Una solución VPN según lo analizado por Cárdenas y Quispe (2015) [90] debe ofrecer los siguientes requerimientos:

Autenticación de usuarios: es el proceso que permite a los diversos clientes de la VPN verificar su identidad. La autenticación involucra el intercambio de información secreta, como una clave o un desafío ante un servidor de acceso, encargado de validar entidades y en base a permisos, políticas y técnicas definidas, estipular que usuarios autorizados tiene acceso a qué recursos privados.

Administración de direcciones: se fijan las direcciones IP a los clientes VPN y las mismas se deben mantener ocultas. Las direcciones ocultas pertenecen a la red privada, por lo que se utiliza el protocolo IPv6 definiendo una dirección tipo unicast, lo cual brinda medidas de seguridad a los paquetes de datos que

[89] Ibid., p. 87.
[90] CÁRDENAS TORREBLANCA, M.; QUISPE RUEDAS, F. *Propuesta de una red segura para la interconexión y cooperación de las comisarias y municipalidades de Arequipa utilizando los protocolos VPN y OLSR con servidor Radius y monitoreo Nagios.* 2015. (Tesis Ingeniero de Sistemas). Arequipa, Perú. Facultad de Ciencias e Ingenierías Físicas y Formales, Universidad Católica de Santa María, Programa Profesional de Ingeniería de Sistemas, p. 29.

viajaran de extremo a extremo.

Cifrado de datos: antes de enviar los paquetes el servidor VPN cifra la información por medio de un algoritmo de encriptado, el cual trabaja con claves utilizadas para crear una única versión del mensaje cifrado.

Es de destacar que mientras más grande sea la longitud de la clave, mayor será la dificultad de desencriptar la información, pero a su vez, es directamente proporcional a la carga de procesamiento generada.

Administración de claves: "una infraestructura de claves públicas (PKI[91]) es un sistema de recursos, políticas y servicios que da soporte al uso del cifrado de claves públicas para autenticar a las partes que participan en una transacción" (IBM, 2018)[92]. Se usada con el fin de distribuir certificados ya sean propios o generados por una autoridad certificante (CA)[93].

Ancho de banda: es un punto importante a considerar, ya que el acceso a Internet con que se cuenta va a influir directamente en el rendimiento de la VPN. Si la conexión tiene pérdida de paquetes o latencia[94] indefectiblemente va a afectar la calidad del enlace, sumado a que al aplicar técnicas de encriptación produce un deterioro en el rendimiento por la sobrecarga. Por lo que es preciso que al cifrar y descifrar los paquetes de datos, estos sean transmitidos a una velocidad que se considera adecuada para la criticidad del servicio que se está implementando.
El rendimiento de la conexión, asimismo es afectado en cierta medida por la cantidad de conexiones realizadas o túneles establecidos simultáneamente desde el sitio remoto al central, los cuales se restringen en su número máximo definiendo las conexiones permitidas por la VPN, en base a la capacidad del enlace y los requerimientos a cumplir por la red privada.
Lo antes mencionado introduce al ambiente de redes el concepto de denominado calidad de servicio (QoS – Quality of Service). El cual es una solución para las VPN, que proporciona formas de control, priorización del tráfico y administración del ancho de banda.

Soporte multiprotocolo: considerado un beneficio para las VPN ya que posibilita trabajar con redes públicas mixtas, en las cuales varían los protocolos configurados, admitiendo hacer uso de servicios como IP, ATM, FrameRelay. Así como también permitir que la técnica se adapte, sea utilizada sobre distintas arquitecturas, interactúe con variados protocolos de seguridad y sea compatible con tecnologías futuras.

---

[91] Conjunto de herramientas utilizadas en el campo de la seguridad informática.

[92] IBM. *Infraestructura de clave pública (PKI).* Recuperado el 15 de noviembre de 2018, de https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q009900_.htm.

[93] Entidad de terceros fiable que emite certificados digitales que garantizan que la clave pública de una entidad pertenece realmente a dicha entidad.

[94] Suma de retardos temporales que puede tener un paquete trasmitido dentro de una red, dada la demora en la propagación y transmisión.

REQUERIMIENTO DE HARDWARE, SOFTWARE Y RECURSOS HUMANOS

Hardware

El hardware es muy variado, lo integran servidores, PC, notebooks, netbooks, smartphones, routers, gateways y switches.

Las funciones que tiene asignadas el servidor son:

- ✓ Esperar por los pedidos de conexión
- ✓ Negociar las conexiones, entre otros la encriptación y autenticación.
- ✓ Autenticar y autorizar a los clientes VPN.
- ✓ Recibir datos del cliente y enviarle los pedidos por él.
- ✓ También puede actuar como VPN gateway o VPN router.

El cliente generalmente se ejecuta en un equipo de un empleado, en su hogar en una notebook, netbook o smartphones conectados a una LAN en algún sitio con acceso a Internet o una red pública. Con el fin de realizar tareas administrativas, o son administradores remotos que realizan tareas de configuración, monitoreo y de gestión.

Requerimientos de hardware:

Servidor: no requiere recursos significativos como para generar una limitante poder implementar una solución con estas tecnologías.

Routers: en cuanto a los enrutadores, estos deben soportar el protocolo IPv6 y VPN con IPSec, PPTP y L2TP.

Como una opción se presenta el equipo router TP/Link modelo TL-ER6120; que soporta IPv6 y hasta 100 Túneles VPN IPSec. Conexiones punto a punto o cliente/servidor. Algoritmo de encriptación DES, 3DES, AES128, AES192 y AES256. Algoritmo de autenticación MD5 y SHA1. Además soporta 50 Túneles PPTP VPN y 50 Túneles L2TP sobre IPSec.

Software

Para lograr establecer una comunicación VPN segura se necesita instalar un cliente en el dispositivo remoto con acceso a internet y un servidor que escuche peticiones, verifique credenciales y proporcione acceso a la red corporativa.

A continuación se presentan software existente en el mercado, utilizado para realizar una red privada virtual.[95]

ComodoUnite: herramienta que permite crear servidores VPN. Cuenta con servicios de mensajería segura entre host, permite intercambiar archivos y cifrado la comunicación de extremo a extremo con SSL.

[95] *Las mejores herramientas para trabajar desde casa*. Recuperado el 20 de enero de 2018, de https://hipertextual.com/archivo/2013/10/trabajar-casa-con-vpn/

LogMeInHamachi: es una herramienta de software que apuesta por la facilidad de uso, además de ofrecer seguridad, así como también opciones avanzadas para crear y acceder a redes VPN. Esta herramienta concreta permite el acceso mediante cliente de escritorio o directamente desde el navegador web, tanto para acceder a la red como para gestionar accesos, permisos y usuarios.

Es gratuita para uso personal y ofrece planes de pago para uso profesional. Con esta aplicación con la licencia gratuita se pueden conectar hasta 16 ordenadores. Mientras que en la versión comercial hasta 256 equipos.

Remobo: aplicativo que permite crear redes VPN mediante un cliente y un servidor, garantizando la seguridad del acceso mediante el cifrando de la comunicación. Es útil en ambientes hogareños como profesionales, además es gratuito y cuenta con soporte para distintos sistemas operativos. Soporta múltiples conexiones.

Cisco AnyConnect: aplicación garantizada por Cisco Sistem, disponible en varios sistemas operativos. No es tan fácil de usar como las propuestas anteriores, pero a cambio ofrece funciones avanzadas para entornos profesionales. Es una herramienta de redes VPN por excelencia, pero tiene un coste elevado comparado con las opciones anteriores.

ShrewSoft VPN: es un sistema que facilita la creación de VPN, tanto en el ámbito organizacional como hogareño. Es multiplataforma y multiconexión.

Cliente VPN de Windows: Windows nos permite crear un servidor VPN o acceder como cliente, sin la necesidad de contar con otro aplicativo. Es una herramienta muy simple y de fácil configuración. En los dos casos (servidor y cliente), se configura desde el "panel de control" y luego en "centro de redes y recursos compartidos".

OpenVPN: una aplicación libre y abierta para configurar de forma práctica una VPN. Funciona de forma tradicional, instalando un servidor VPN en uno de los ordenadores y los programas clientes en el resto de las máquinas que se usaran para conectarse y formar la red.

Además es capaz de importar configuraciones de otros programas comerciales y también está incluido en algunos routers de red para una mejor adaptación.

CUADRO COMPARATIVO DE LAS APLICACIONES

Software	Tipo de licencia	Sistema Operativo	Cantidad de conexiones (Clientes)
ComodoUnite	Cuenta con una versión gratuita	Windows, Mac OS y Linux	200
LogMeInHamachi	Cuenta con una versión gratuita	Windows, Mac OS y Linux	16 (256 en la versión comercial)
Remobo	Gratuita	Windows, Mac OS y Linux	Sin especificar
Cisco AnyConnect	Privativo	Windows, Mac OS y Linux	Depende de la licencia contratada (de 25 a 250000)
ShrewSoft VPN	Cuenta con una versión gratuita	Windows, Linux y BSD	Sin especificar
Cliente VPN de Windows	Integrada en el S.O.	Windows	Sin especificar
OpenVPN	Libre y gratuita	Windows, Mac OS y Linux	Sin especificar

Tabla 4.1 Comparación de software para VPN.
Fuente: elaboración propia.

Recursos humanos

Dada la criticidad de la información en las organizaciones y la necesidad de brindarle protección, sumado a la evolución de las tecnologías. Hace necesario que todo el personal técnico se mantenga en constante capacitación y perfeccionamiento; con el fin de optimizar los recursos y garantizar la confidencialidad, integridad y disponibilidad de la información.

A la hora de implementar técnicas para resguardar información es importante determinar qué servicios son críticos, así como también los responsable y cómo se procederá ante una contingencia.

La gestión de la seguridad no es una responsabilidad exclusiva del área de tecnología de la información. Es fundamental la implicancia de la dirección, ya que es quien tiene potestad sobre las decisiones que afectan a los objetivos organizacionales.

Con referencia a lo expuesto se sugieren las buenas prácticas formalizadas en la norma ISO 27001[96], donde se destaca la importancia de la definición de las funciones y los recursos humanos implicados, desempeño de las funciones del equipo de trabajo y la finalización o cese de las responsabilidades.

A su vez, todos los usuarios que manipulen y dispongan de los recursos organizacionales tienen que conocer las posibles amenazas a la seguridad y cumplir con las políticas definidas. Por lo cual, la dirección debe coordinar instancias de capacitación, para asegurar que el personal este concientizado de la importancia de sus acciones sobre los activos y como pueden afectar la seguridad.

[96] Norma que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información.

CUADRO COMPARATIVO DE TIPOS DE VPN

TIPOS DE VPN	DESCRIPCION	DIRECCIONAMIENTO	CONFIGURACION	CONEXION
Acceso Remoto	Se utiliza para conectar un dispositivo a una red privada desde un punto remoto.	Es necesaria una IP pública fija del lado del Servidor.	Utiliza una configuración dinámica.	Los clientes pueden acceder a la red organizacional desde cualquier dispositivo conectado a la red pública.
Punto a Punto	Une dos redes privadas.	Requiere de una IP pública fija en cada extremo del túnel.	Requiere una configuración de VPN estática para conectarse a la red.	La VPN unifica las LAN de las sucursales en una misma red organizacional utilizando para ello redes públicas.

Tabla 4.2 Cuadro comparativo de tipos de VPN.
Fuente: elaboración propia.

CAPITULO 5

[SEGURIDAD DE UNA RED PRIVADA VIRTUAL]

En éste capítulo se estudiará en profundidad el concepto de seguridad en una VPN, así como también los pilares básicos de la seguridad de la información. Se analizarán los tipos de algoritmos de encriptación existentes y la seguridad en el protocolo IP, tanto en su versión 4 como la versión 6.

IMPORTANCIA DE LA SEGURIDAD

Pero las facilidades y comodidades logradas a través de la comunicación de dispositivos por medio de Internet, causa que los equipos presenten un sin número de vulnerabilidades y exposición a ataques de todo tipo, así como también contaminaciones externas, y es en ese contexto en el que adquiere importancia la seguridad. La cual abarca un gran número de aspectos de la organización, por lo cual este capítulo solo está enfocado a la seguridad de la información.

El término "seguridad" es demasiado amplio debido a la variedad de temas que engloba, por lo que para aclararlo es necesario analizar las posibles amenazas de las que puede ser víctima una red y los mecanismos para protegerla. Por lo tanto se puede definir a la seguridad de redes como un grupo de estrategias y buenas prácticas que permitan proteger a una red frente a ataques.

En base a lo mencionado es necesario definir qué información es crítica y que información no lo es, quien maneja información crítica y quien información con no tanta criticidad, a los fines de proporcionar los recursos necesarios para protegerla.

La seguridad persigue tres objetivos básicos:

- Confidencialidad:
  - ✓ Proteger la revelación de información a personas no autorizadas
  - ✓ Restringir el acceso a información confidencial
  - ✓ Proteger el sistema contra usuarios curiosos internos y externos
- Integridad:
  - ✓ Proteger los datos de cambios no autorizados
  - ✓ Restringir la manipulación de datos a programas autorizados
  - ✓ Proveer información verídica y consistente
- Disponibilidad:
  - ✓ Asegurar la continuidad operativa del sistema
  - ✓ Proteger el sistema contra acciones o accidentes que detengan los servicios o destruyan la información que brinda

La seguridad es un gran problema, y lamentablemente pocos administradores están conscientes de ello. Los sistemas informáticos se encuentran dispersos en toda la organización, los cuales se interconectan en red con las sucursales y con otras empresas. Allí es donde la seguridad es el tema central sobre Redes Privadas Virtuales, y cuando se piensa en este tema, se debe analizar puntualmente cada capa del modelo TCP/IP. En donde cada nivel es responsable de su propio conjunto de funciones individuales, por ejemplo, confiabilidad, configuración, corrección, entre otras. Es allí donde surgen problemas, ya que los ataques en la actualidad suceden a través de todos estos niveles.

Puntualmente el tema no pertenece a una capa especifica del modelo TCP/IP, sino que se encuentra presente en todas. La autenticación y el no repudio[97] se controlan en la capa de aplicación, la seguridad extremo a extremo en la capa de transporte, los firewalls usualmente trabajan en la capa de internet; mientras que la encriptación y los candados o cerraduras en la capa acceso a la red.

Cada nivel puede atacarse y verse comprometido, respecto a lo mencionado mientras más baja sea la capa OSI en la que se implemente la VPN, esta será considerada más segura, debido a las variables y vulnerabilidades que intervienen en las capas superiores. Se utilizan tecnologías de autenticación segura de usuarios, así como criptografía y cifrado en cada extremo del túnel de las VPN.

Por los motivos expuestos con anterioridad es importante para cualquier configuración de seguridad tener en cuenta los siguientes puntos trabajados por Cosme MacArthur Ortega (2003)[98]:

- **Acceso solo a personas autorizadas:** solamente a las partes autorizadas se les permite el acceso a la información, aplicaciones y servidores, ya que en este punto cualquier acción va a impactar directamente sobre los tres pilares de la seguridad de la información.
- **Imposibilidad de descifrar el mensaje:** quien quiera que intercepte el flujo de datos cifrados de la VPN no debe poder leer el mensaje, como estos viajan a través de una red pública, y cualquier host de esa red tendrá la capacidad de interceptarlos, es necesario el resguardo de la información a través de técnicas de cifrado.
- **Datos íntegros:** se refiere al hecho de asegurar que los datos no sean modificados mientras son transmitidos, pudiendo comprobar que provienen del lugar que se supone deben venir y no presenten modificaciones. Para lo cual se utilizan métodos de cifrado y hash para proteger la información.
- **Interoperabilidad:** cuando existen diversas plataformas y sistemas trabajando en conjunto, los aspectos de interoperabilidad se deben tener en cuenta, por lo que las VPN deben funcionar en todas las plataformas de uso común en la organización.
- **Facilidad de administración:** los dispositivos que intervienen en las VPN deben presentar una configuración directa, de fácil mantenimiento y actualizable. La administración, como el alta o baja de un usuario, no debe llevar mucho tiempo.

[97] Se encarga de evitar que la entidad emisora y/o receptora niegue que envió y/o recibió la información.
[98] COSME MACARTHUR ORTEGA, Op. cit., p. 121.

TÉCNICAS DE SEGURIZACIÓN DE INFORMACIÓN

El esquema de red de las VPN se basa en las redes tradicionales, por lo cual a la hora de aplicar seguridad utiliza técnicas similares, a las cuales les suma un grado mayor, propio de las redes privadas. "El mismo hecho de querer instalar una VPN indica que se quiere añadir un nivel más de seguridad a la red que se posee actualmente." (Cosme MacArthur Ortega, 2003)[99]

La seguridad de información es de gran importancia para las organizaciones que realizan negocios a través de Internet, por lo cual, en sus redes propias de comunicación implementan técnicas de seguridad que incluyen el cifrado punto a punto, dispositivos propios de la VPN, autenticación, administración centralizada, monitoreo y copias de seguridad.

A continuación se describen los requisitos y las técnicas utilizadas para garantizar el tránsito seguro de la información a través de las redes públicas:

Criptografía

Es considerada una ciencia, propone y estudia métodos para ocultar el significado real de un mensaje, de manera tal que solamente sea "entendible" por quien sea el receptor a quien va dirigida la comunicación. Para lograr la seguridad del mensaje a transmitir, hace uso de códigos, técnicas de cifrado y algoritmos matemáticos con el fin de dificultar la intrusión y perdida de confidencialidad o integridad sobre los valores transmitidos.

Los profesionales en la materia hacen una distinción entre un sistema de cifrado y un sistema de código. Un sistema de cifrado es una transformación carácter por carácter o bit por bit, sin importar la estructura lingüística del mensaje. En contraste, uno de código reemplaza una palabra con otra palabra o símbolo.

"La ciencia de encriptar datos es llamada criptografía. La ciencia de romper datos encriptados es llamada criptoanálisis. La criptología es la ciencia combinada de las dos definiciones anteriores." (Cosme MacArthur Ortega, 2003)[100]

Básicamente hay dos tipos de algoritmos de encriptación en uso hoy, de clave privada o simétrica y de clave pública o asimétrica.

Algoritmos Simétricos

Es la técnica utilizada históricamente para dar privacidad a los datos transmitidos. Las entidades de comunicación establecen y comparten una clave secreta que se utiliza para cifrar y descifrar los mensajes. Este método no prevé como se intercambiará la clave entre quien cifra el mensaje y quien lo descifra.

Según Stallings (2004) la técnica se compone de los siguientes elementos:

[99] Ibid., p. 123.
[100] Ibid., p. 124.

- **Texto Nativo:** el mensaje original que va a ser cifrado y que constituye la entrada del algoritmo;
- **Algoritmo de Cifrado:** se encarga de realizar las transformaciones de texto nativo en base a operaciones simples sobre patrones de bits;
- **Clave Secreta:** entrada del algoritmo de cifrado que influye sobre los cambios que este realiza sobre el texto nativo, dependiendo exclusivamente de estas entradas;
- **Texto Cifrado:** mensaje alterado que da como resultado el algoritmo de cifrado, posterior a procesar las variables ingresadas;
- **Algoritmo de Descifrado:** se encarga de producir el resultado inverso del algoritmo de cifrado. ([101])

La clave secreta es un código que utiliza el algoritmo de encriptación para crear una única versión de texto cifrado. Mientras mayor sea la longitud de la clave, más difícil será a resolver la incógnita del texto cifrado.

Los algoritmos de encriptación dadas las operaciones que realizan son reconocidos como cifradores de bloques. Toman un texto origen, lo procesan en bloques de tamaño fijo y generan un texto cifrado de tamaño igual a cada bloque de texto original procesado. DES y 3DES son algoritmos que trabajan de esta manera.

DES (Data Encryption Standard)

La norma de cifrado de datos (DES) utiliza un tamaño de 64 bits y una clave de 56 bits durante la ejecución (los 8 bits de paridad se quitan de la clave de 64 bits completa). El texto nativo se encripta en bloques de 64 bits, produciendo 64 bits de texto cifrado.

Según Tanenbaum y Wetherall (2012):

> El algoritmo, que se parametriza mediante una clave de 56 bits, tiene 19 etapas diferentes. La primera etapa es una transposición, independiente de la clave, del texto llano de 64 bits. La última etapa es el inverso exacto de esta transposición. La etapa previa a la última intercambia los 32 bits de la izquierda y los 32 bits de la derecha. Las 16 etapas restantes son funcionalmente idénticas, pero se parametrizan mediante diferentes funciones de la clave. El algoritmo se ha diseñado para permitir que la desencriptación se haga con la misma clave que la encriptación. Los

[101] STALLINGS, W., Op. cit., p. 727.

> pasos simplemente se ejecutan en el orden inverso. Cabe aclarar que el cifrado DES en la actualidad es considerado un algoritmo no seguro. ([102])

3DES (Triple Data Encryption Standard)

Se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto nativo en otro cifrado, utilizando dos claves y tres etapas. En la primera etapa, el texto nativo se encripta mediante DES de la forma usual con la *clave1*. En la segunda etapa, DES se ejecuta en modo de desencriptación, utilizando la *clave2* para esta tarea. Por último, se realiza otra encriptación DES con la *clave1*, por lo que resulta mucho más seguro. La razón de que se usen dos claves es que los criptógrafos coinciden en que por ahora 112 bits son suficientes para las aplicaciones comerciales. Subir a 168 bits simplemente agregaría la sobrecarga innecesaria de administrar y transportar otra clave.

AES (Advanced Encryption Standard)

El NIST (Instituto Nacional de Estándares y Tecnología, del inglés Nacional Institute of Standards and Technology) agencia encargada de aprobar estándares del gobierno, decidió que se necesitaba contar con un nuevo estándar criptográfico para uso no confidencial, y debido a la controversias surgidas con DES, adoptó una estrategia diferente, promoviendo un concurso criptográfico.

Informado por Tanenbaum y Wetherall (2012):

> En enero de 1997, los investigadores de todo el mundo fueron invitados a emitir propuestas para un nuevo estándar, que se llamaría AES fijando las siguientes reglas mencionadas a continuación:
>
> 1. El algoritmo debe ser un sistema de cifrado de bloques simétrico.
> 2. Todo el diseño debe ser público.
> 3. Se deben soportar las longitudes de claves de 128, 192 y 256 bits.
> 4. Deben ser posibles las implementaciones tanto de software como de hardware.
> 5. El algoritmo debe ser público o con licencia en términos no discriminatorios. ([103])

Se presentaron 15 propuestas y la organización instó a que los presentes buscaran errores en todas ellas, luego el NIST seleccionaría 5 finalistas en base a su seguridad, eficiencia, simplicidad, flexibilidad y requerimientos de memoria.

[102] TANENBAUM, A. S.; WETHERALL, D., Op. cit., p. 738.
[103] Ibid., p. 674.

El algoritmo ganador denominado Rijndael, creado por dos jóvenes criptógrafos belgas Joan Daemen y Vincent Rijmen, fue seleccionado en octubre de 2000 por la NIST y nombrado estándar AES en noviembre del año siguiente.

AES es uno de los algoritmos más seguros que existen hoy en día, por el momento no existen ataques llevados adelante con éxito contra AES, por lo que este algoritmo sigue siendo el estándar de cifrado preferido por gobiernos, bancos y sistemas de alta seguridad de todo el mundo.

En cuanto a su funcionamiento se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloque de datos de 16 bytes, que se repiten varias veces. Especifica que el tamaño de bloque debe ser de 128 bits y la longitud de clave debe ser de 128, 192 o 256 bits. Provee una seguridad más fuerte que DES y es computacionalmente más eficiente que 3DES.

Según Tanenbaum y Wetherall (2012):

> Al igual que el DES, Rijndael utiliza sustituciones y permutaciones, así como múltiples rondas. El número de rondas depende del tamaño de clave y del tamaño de bloque, y es de 10 para las claves de 128 bits con bloques de 128 bits y aumenta hasta 14 para la clave o el bloque más grande. Sin embargo, a diferencia del DES, todas las operaciones involucran bytes completos para permitir implementaciones eficientes tanto en hardware como en software. ([104])

DES y AES (Rijndael) son los algoritmos criptográficos de clave simétrica mayoritariamente conocidos, por lo que son considerados estándares. Sin embargo, vale la pena mencionar que históricamente han surgido otros sistemas de cifrado de clave simétrica. A continuación se listan algunos ellos, siendo posible combinarlos.

Sistema de cifrado	Autor	Longitud de clave	Comentarios
DES	IBM	56 bits	Muy débil para usarlo en la actualidad.
RC4	Ronald Rivest	1-2048 bits	Precaución: algunas claves son débiles.
RC5	Ronald Rivest	128-256 bits	Bueno, pero patentado.
AES (Rijndael)	Daemen y Rijmen	128-256 bits	La mejor opción.
Serpent	Anderson, Biham, Knudsen	128-256 bits	Muy sólido.
Triple DES	IBM	168 bits	Bueno, pero se está volviendo anticuado.
Twofish	Bruce Schneier	128-256 bits	Muy sólido; se utiliza mucho.

Tabla 5.1 Sistemas de cifrado.
Fuente: TANENBAUM, A. S.; WETHERALL, D. J. (2012). *Redes de computadoras (Quinta edición)*. México: Editorial Pearson. Página 682.

[104] Ibid., p. 675.

PSK (Pre-Shared Key)

Es un algoritmos criptográficos de clave simétrica utilizado para autenticar host, ingresando manualmente la clave pre compartida en cada extremo y validando la coincidencia de la misma. Es un método antiguo, no escalable y sin ninguna validación de integridad ni confidencialidad de clave.

Algoritmos Asimétricos

También conocidos como algoritmos de clave pública, surgen debido a que históricamente la distribución de claves fue la parte débil de la cadena en la mayoría de los criptosistemas. Si alguien podía hacerse con la clave, todo el sistema quedaba inutilizado.

Por un lado las claves se debían proteger para que la información no sea vulnerada, pero a su vez, se debían distribuir para desencriptar la información, lo que incrementaba el riesgo.

En 1976 dos investigadores de la Universidad de Stanford, Diffie y Hellman, propusieron una clase totalmente nueva de criptosistema, en donde las claves de encriptación y desencriptación eran tan diferentes que no era posible derivar una a partir de la otra, dando origen a los cifrados de clave pública.

La criptografía asimétrica requiere que cada usuario tenga dos claves: una pública, que todo el mundo utiliza para encriptar los mensajes a enviar, y una privada que el usuario necesita para desencriptar los mensajes. Denominando a estas claves como públicas y privadas, respectivamente, haciendo diferencia respecto a las claves secretas que se utilizan en la criptografía convencional de clave simétrica.

RSA (Rivest, Shamir, Adleman)

Este método fue descubierto por un grupo del M.I.T. (Instituto Tecnológico de Massachusetts) en 1978. Es conocido por las iníciales de sus tres descubridores. Ha sobrevivido a todos los intentos para romperlo y se le considera muy robusto. Su desventaja en un principio es que requiere claves de por lo menos 1024 bits para una buena seguridad, por lo que se lo considera un método lento.

El método se basa en ciertos principios de la teoría de los números. Realiza cálculos anticipadamente seleccionando al azar dos números primos generalmente de 1024 bits, los cuales después de realizar determinadas operaciones matemáticas se utilizan para encriptar y desencriptar el mensaje.

Según lo expuesto por Cosme MacArthur Ortega (2003):

> La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico influye para

> que sea más propicio un ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea inviable. ([105])

Algoritmo Diffie-Hellman

Según lo expuesto por Cosme MacArthur Ortega (2003):

> Es un protocolo de intercambio de claves que posibilita generar claves negociadas entre desconocidos. Su fortaleza radica en el campo matemático finito de exponenciación de los logaritmos.
>
> También ha establecido la función de seguridad de un acuerdo de claves secretas, por lo tanto aunque sea un algoritmo asimétrico (clave pública), tanto el emisor como el receptor pueden utilizar un cifrado simétrico. ([106])

Los sistemas de claves asimétricas resuelven este desafío dada la propiedad de usar dos claves, una privada y la otra pública.

El algoritmo matemático permite generar una clave secreta idéntica en ambos sistemas, sin haberse comunicado con anterioridad, y utilizara la misma para cifrar el tráfico entre los dos sistemas.

El intercambio propuesto por DH no autentica usuarios por lo que es necesario que se implementen otras técnicas tales como firmas digitales u otros métodos de autenticación a modo de prevenir ataques.

INTEGRIDAD CON MD5 Y SHA1

La integridad proporciona una técnica para resguardar la comunicación, dando la posibilidad al host receptor de verificar que la información enviada desde el origen no sufrió alteraciones durante la transmisión.

Lo presentado da pie al surgimiento de las funciones de hash, las cuales toman datos binarios, llamados mensaje y producen una representación abreviada del mismo, denominado digesto de mensaje o código hash. El hashing se basa en una función matemática de un solo sentido relativamente fácil de computar, pero significativamente más difícil de invertir.

Existen dos funciones de hash conocidas:

MD5 (Message Digest 5)

Es una función de un solo sentido, que se utiliza para calcular el resumen de un conjunto de datos, el cual también es enviado al destinatario. Quien al recibir los

[105] COSME MACARTHUR ORTEGA, Op. cit., p. 130.
[106] Ibid., p. 128.

datos, vuelve a calcular el hash y lo compara con el valor recibido con el fin de verificar que la información no sufrió modificaciones durante la trasmisión.

Con la utilización del método es poco probable obtener el mismo valor de hash a partir de dos conjuntos diferentes de datos. "MD5 es una secuencia compleja de operaciones binarias simples, tales como OR Exclusivo (XOR) y rotaciones, las cuales se ejecutan sobre los datos y producen un digesto del mensaje de 128 bits." (Sabolansky, 2010, p. 12)[107]

SHA-1 (Secure Hash Algorithm 1)

"El algoritmo SHA-1 toma un mensaje con menos de 2^64 bits de longitud y produce un digesto de 160 bits." (Stallings, 2004, p. 741)[108]. El algoritmo requiere mayor procesamiento que MD5, pero al generar un digesto de tamaño superior es más seguro contra ataques de colisión por fuerza bruta.

SEGURIDAD EN IPV4 e IPV6

IPSec es una opción válida que se proporciona como una base estable y duradera para la seguridad de capa de red del protocolo IP, incluye soporte para las dos familias de protocolos, IPv4 e IPv6.

Soporta todos los algoritmos criptográficos que se utilizan hoy en día y también puede ajustarse a algoritmos nuevos. Se encarga de cubrir las cuestiones de seguridad que se resaltan a continuación según IBM (2018):

- **Autenticación de origen de datos:** verifica que cada datagrama ha sido originado por el remitente indicado.
- **Integridad de datos:** verifica que el contenido de un datagrama no se ha cambiado por el camino, ni deliberadamente, ni debido a errores aleatorios.
- **Confidencialidad de datos:** oculta el contenido de un mensaje, normalmente mediante cifrado.
- **Protección de reproducción:** impide que un agresor pueda interceptar un datagrama y reproducirlo posteriormente.
- **Gestión automatizada de claves criptográficas y asociaciones de seguridad:** permite utilizar la política VPN en toda la red con poca o ninguna configuración manual.[109]

El protocolo de internet en la versión 4 no se provee intrínsecamente de ninguna capacidad de seguridad, en su versión 6 incorpora IPsec de forma nativa

[107] SABOLANSKY, A. J. *Utilizando software libre para una servicio de Sellado Digital de Tiempo*. 2010. (Tesis Licenciado en Informática). La Plata, Argentina. Facultad de Informática, Universidad Nacional de La Plata, p. 12.
[108] STALLINGS, W., Op. cit., p. 741.
[109] IBM - *Protocolos de IP Security*. Recuperado el 10 de julio de 2018, de https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_72/rzaja/rzajaipsec.htm

además de corregir sus debilidades, y hace uso de él para autenticar y cifrar los paquetes de datos, lo que no garantiza que IPv6 sea 100% fiable. Lo cual es relativo, ya que en la actualidad se pueden encontrar redes IPv4 configuradas con IPSec y redes IPv6 con IPSec sin configurar.

A su vez, en la versión 4 la fragmentación de paquete se puede dar en cualquier tramo de la red, en cambio la versión 6 solo permite la fragmentación en el host de origen y el reensamblado en el destino, por lo que los ataques de fragmentación de paquetes ya no serían tan efectivos.

IPv6 presenta como una gran ventaja de seguridad sobre IPv4, la dificultad de realización de un escaneo de fuerza bruta[110] ya que maneja un rango amplio de direcciones, aunque esta opción no se descarta completamente debido a la posibilidad de mejora de las herramientas de escaneo.

Las mejoras expuestas dotan a IPv6 de mayor seguridad, pero como no está lo suficientemente probado y utilizado, se requieren mayor cantidad de pruebas de seguridad y precaución, ya que mayoritariamente los detectores de intrusiones no son totalmente compatibles con la nueva versión del protocolo de red.

Otro problema existente es que al trabajar los dos protocolos en paralelo durante la transición a IPv6 de forma completa, es que habrá túneles de tráfico IPv6 a través de IPv4 dejando lugar a graves problemas de seguridad. Como los dispositivos para inspeccionar el tráfico a través de un túnel no son totalmente compatibles con IPv6 se podría inyectar tráfico malicioso sin ser detectado por estos mecanismos de seguridad.

Los paquetes IPv6 pueden tener información optativa como puede ser para la fragmentación, seguridad o admitir la movilidad, mediante el uso de encabezados de extensión (EH).

Respecto a la seguridad en los túneles VPN, se utilizan los protocolos IPSec, que como se describió en capítulos anteriores de esta tesina, se utiliza para proteger los datos mientras fluyen a través de la túnel seguro: AH y ESP. La otra parte de la habilitación de IPSec es el protocolo IKE (intercambio de claves de internet) o la gestión de claves. Mientras que IPSec cifra los datos, IKE soporta la negociación automatizada de las Asociaciones de Seguridad, así como también la generación y la renovación automatizadas de claves criptográficas.

Por el momento las redes IPv6 todavía no han sido el centro de atacantes, no hay muchas herramientas evolucionadas para debilitarlas, pero con seguridad a medida que el protocolo se vaya instaurando surgirán vulnerabilidades significativas, por lo que es muy importante la capacitación de los técnicos de red y definir lo antes posibles las políticas de seguridad en sus redes, con el fin de prevenir y minimizar los riesgos.

[110] Escaneo de fuerza bruta se refiere a intentos reiterados y sistemáticos de encontrar un parámetro desconocido por un atacante, como puede ser una contraseña, un nombre de usuario o una dirección IP.

Prácticas de seguridad recomendadas para IPV6

Las prácticas de seguridad en una red se centran en crear estrategias óptimas de seguridad aplicables a una determinada organización. Es responsabilidad del técnico o administrador de red no solo establecer la parte técnica, sino también alinear la estrategia con los objetivos organizacionales de manera que las políticas estén acordes con el marco interno previamente establecido.

La seguridad en una red en IPv4 ya era un tema complejo y ahora se agudiza al sumarle el protocolo IPv6. La convivencia entre los dos protocolos exige la creación de estrategias para cada uno de ellos, por lo que esta pasa a ser muy extensa, pero con trabajo y refinamiento seguramente se obtendrá una mejora sustancial en el tiempo de operación de la red ya que se disminuye el riesgo de ataque.

CUADRO COMPARATIVO DE PROTOCOLOS DE SEGURIDAD EN UNA VPN

PROTOCOLOS	DESCRIPCION	SEGURIDAD EN IPSEC
AH (Encabezado de Autentificación)	Asegura que el origen de los datos es uno de los extremos del túnel IPSec y verifica que los datos no han sido modificados durante la transmisión, proporcionando de esa manera verificación de integridad y la seguridad anti-repetición, pero no la confidencialidad.	Autenticación / Integridad
ESP (Encapsulating Security Payload)	Proporciona confidencialidad ejecutando el cifrado de los paquetes IP, resguardando los datos y la identidad tanto del origen como del destino. El encabezado ESP proporciona la autenticidad del origen de los datos. Sin embargo, tanto el cifrado de datos como la autenticación son opcionales.	Autenticación / Confidencialidad
DES (Data Encryption Standard)	Norma de cifrado de datos, que trabaja de manera simétrica y son conocidos como cifradores de bloques. Utiliza un tamaño de 64 bits y una clave de 56 bits. realiza 19 etapas de transposición de la clave y el texto nativo. Los pasos de encriptación y desencriptación son las mismas operaciones ejecutadas en orden inverso. En la actualidad el algoritmo es unánimemente considerado no seguro.	Confidencialidad
3DES (Triple Data Encryption Standard)	Se basa en DES, utiliza dos claves y tres etapas. Paso 1: encripta por medio de DES con *Clave1*; Paso 2: ejecuta DES en modo de desencriptación con *Clave2*; Paso 3: ejecuta DES en modo encriptación con *Clave1*.	Confidencialidad
AES (Advanced Encryption Standard)	Algoritmo simétrico, que se basa en sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloques de datos de 16 bytes en múltiples rondas. La longitud de clave puede ser de 128, 192 o 256 bits. Es considerado mayoritariamente como computacionalmente eficiente en comparación con las opciones anteriores.	Confidencialidad
MD5 (Message Digest 5)	Función de un solo sentido, que se utiliza para calcular el resumen de un conjunto de datos, el cual también es enviado al destinatario; al recibir los datos, se vuelve a calcular el hash y se compara con el valor recibido con el fin de verificar que la información no sufrió modificaciones durante la trasmisión.	Integridad
SHA (Secure Hash Algorithm)	El algoritmo requiere mayor procesamiento que MD5, pero al generar un valor resumen de tamaño superior es más seguro contra ataques de fuerza bruta o criptoanálisis.	Integridad

PSK (Pre-Shared KEY)	Sistema basado en una clave simétrica, en el cual se configura manualmente una contraseña pre compartida en cada extremo. Es considerado un sistema no seguro, no posee validación de integridad ni confidencialidad.	Autenticación
RSA (Rivest, Shamir, Adleman)	Algoritmo asimétrico, que se basa en ciertos principios de la teoría de números. Realiza cálculos anticipadamente seleccionando al azar dos números primos generalmente de 1024 bits, los cuales después de realizar las operaciones matemáticas se utilizan para encriptar y desencriptar el mensaje. Es considerado robusto y su principal desventaja es el tamaño de claves que utiliza.	Confidencialidad / Autenticación
Diffie-Hellman	Es un protocolo de intercambio de claves asimétrico, que permite la generación de claves negociadas entre desconocidos. Se basa en el campo matemático finito de exponenciación de logaritmos. Permite que dos usuarios intercambien una clave secreta en un medio inseguro sin secreto previo alguno.	Autenticación

Tabla 5.2 Cuadro comparativo de protocolos de seguridad en una VPN.
Fuente: elaboración propia.

CAPITULO 6

[INFRAESTRUCTURA DE COMUNICACIONES DE LA FACULTAD DE CIENCIA Y TECNOLOGÍA]

En éste capítulo se relevará y analizará la infraestructura de comunicaciones de la Facultad de Ciencias y Tecnología de la UADER en toda su extensión geográfica.

DISTRIBUCIÓN GEOGRÁFICA DE LA ORGANIZACIÓN

La Facultad de Ciencia y Tecnología (FCyT) pertenece a la Universidad Autónoma de Entre Ríos (UADER), es una institución pública de educación superior, creada en el año 2000 y abocada a la formación de docentes en disciplinas científicas, así como a la enseñanza de la ciencia y las tecnologías.

La estructura organizativa de la Facultad se encuentra distribuida en gran parte del territorio entrerriano como todas las facultades de la Universidad Autónoma de Entre Ríos, con el objetivo de brindar de manera descentralizada la posibilidad de formación superior al interior de la provincia, teniendo en cuenta sus características geográficas y demográficas.

Cuenta con 11 sedes, dos extensiones áulicas y dos escuelas pre-universitarias que se detallan a continuación:

Sedes de la FCyT-UADER

- Sede Central Oro Verde
- Sede Concepción del Uruguay
- Sede Paraná - Escuela Santa Fe
- Sede Villaguay
- Sede Diamante
- Sede Basavilbaso
- Sede Chajarí
- Sede Crespo
- Sede Federación
- Sede Gualeguaychú
- Sede Santa Elena

Extensiones Áulicas

- Extensión Áulica Gualeguay
- Extensión Áulica Nogoyá

Escuelas PRE-Universitarias

- Colegio del Uruguay "Justo José de Urquiza" en la ciudad de Concepción del Uruguay;
- Escuela Técnica N° 35 en la ciudad de Crespo;

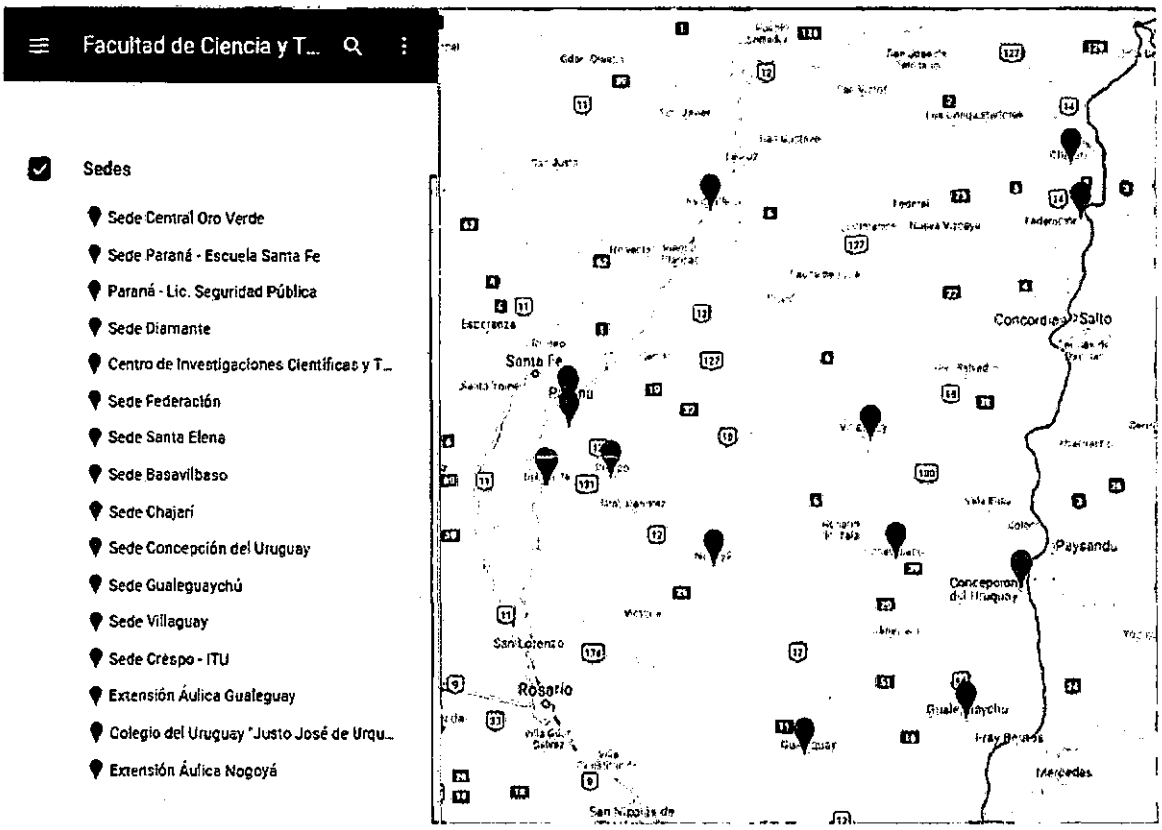


Figura 6.1 Sedes de la FCyT UADER.

Fuente: *Página Web de la Facultad de Ciencias y Tecnología de la UADER*. Recuperado el 16 de enero de 2018, de http://fcyt.uader.edu.ar/web.

INFRAESTRUCTURA ACTUAL DE COMUNICACIONES

Actualmente la infraestructura de red de la organización se encuentra distribuida por el territorio de la provincia, distintos edificios con diversas situaciones, en referencia a cantidad de alumnos, carreras que se dictan y personal, además del presupuesto y faltante de técnicos informáticos con puesto fijo en las dependencias.

En la mayoría de las sedes, la cantidad de equipos de escritorio con que cuentan se reduce a uno (1), no hay personal Informático propio que realice tareas de soporte y mantenimiento. El equipo es utilizado por todas las áreas administrativas con que cuenta la dependencia, dado que la cantidad de personal es escaso y en muchos casos es una sola persona que realiza las tareas Administrativas.

En esta situación podemos encontrar las sedes de Villaguay, Crespo, Basavilbaso, Chajarí, Santa Elena, Diamante y Federación. Además de las extensiones áulicas de Gualeguay y Nogoyá.

Se conectan a Internet a través de un módem, router o antena que proporciona el proveedor de servicios local, que en la mayoría de los casos brindan enlaces inalámbricos hogareños de baja velocidad; y ellos mismos son los que realizan la instalación de la red. Proveen además de un modem/router o antena (depende

del servicio y proveedor), un dispositivo inalámbrico que cuenta con un pequeño switch ethernet, que configuran para uso interno en el lugar y a la cual conectan las unidades de trabajo.

Resumiendo, la realidad de las pequeñas dependencias mencionadas en cuanto a infraestructura de red es de similares características a una red hogareña, prácticamente sin ninguna seguridad configurada en su ruteador, no poseen firewall o control de ancho de banda, dominio o control de usuarios.

En cuanto a sistemas utilizados en estas dependencias, en su mayoría son sistemas web alojados en los servidores del Rectorado de la Universidad Autónoma de Entre Ríos o en la sede central de la Facultad. Hay un caso particular que es el sistema de alumnado (SIU Guaraní), el cual se describe más adelante, al que los usuarios se conectan remotamente a través de un cliente que tiene una validación de la conexión en el servidor, por medio de un certificado que trabaja con claves públicas y privadas; y una vez validada la conexión se deben autenticar contra el sistema con un usuario y contraseña.

La sede Paraná cuenta con mayor cantidad de personal y por ende mayor cantidad de hosts en la red. Allí se encuentra emplazado un laboratorio de informática con 10 equipos para el dictado de cátedras que lo requieran. Mas una cantidad similar de hosts para el uso del personal administrativo. A su vez el edificio se comparte con una escuela primaria que funciona en un horario diferente al de la Facultad, y a su vez cuenta con equipos propios para llevar adelante sus tareas, los cuales se conectan para navegar a la red de datos administrada que le proporciona el personal técnico de la Facultad.

Actualmente esta red de datos se compone de un router, que se encarga de segmentar la red, hace control de ancho de banda, brinda direcciones DHCP, posee firewall y filtra navegación. La segmentación es utilizada para dividir por medio del firewall, la red utilizada por los administrativos, de la que utilizan los alumnos y una red inalámbrica libre que puede ser utilizada por quien concurra a la dependencia. Cabe destacar que la distribución de los medios de las distintas redes segmentadas es física, ya que los switches utilizados como distribución por todo el edificio son de capa 2 no administrables. En cuanto al uso de sistemas, es igual a la situación descripta para las otras dependencias mencionadas en párrafos anteriores.

En relación a las sedes Oro Verde y Concepción del Uruguay, cuentan con gran cantidad de personal y poseen servicios corriendo en la red de datos que exigen ciertos requerimientos y un mayor control. Ambas sedes cuentan con una red de datos consolidada. Dentro del equipamiento de red cuentan con router marca "Mikrotik" (modelo RB 1100 AHx2 descripto más adelante en este capítulo), el cual posee configuraciones para hacer segmentación, control de ancho de banda; a su vez cuentan con servicio de internet de distintos proveedores, red exclusiva de servidores con controles de firewall, cableado de red organizado y

medianamente estructurado, servicios disponibles en la red (los cuales serán mencionados en este capítulos en puntos posteriores).

Las dependencias mencionadas cuentan con personal técnico fijo, el cual se dedica a mantener la red de datos y constantemente aportar mejoras al rendimiento de la misma. En ambos casos la topología de red es una estrella, con medios categoría 5E[111], y dispositivos intermedios capa 2 ubicados en unidades de cableado estructuradas. A su vez, ambas Sedes poseen servicios que son consultados por las demás dependencias, estos servicios se describirán en puntos posteriores del presente capitulo.

Enlaces disponibles por Sedes y tipo de conectividad

- Sede Central Oro Verde

  Cuenta con 3 enlaces

  - ✓ ARNET 10 MB tipo ADSL
  - ✓ ARNET 10 MB tipo ADSL
  - ✓ BM Soluciones 2 MB simétricos tipo inalámbrico con IP pública fija

- Sede Concepción del Uruguay

  Cuenta con 2 enlaces

  - ✓ ARNET 7 MB tipo ADSL
  - ✓ ARNET 7 MB tipo ADSL

- Sede Paraná - Escuela Santa Fe
  - ✓ GIGARED 30 MB tipo cable módem con IP pública fija
- Sede Villaguay
  - ✓ SUPPORTINTERNET 1 MB tipo inalámbrico
- Sede Diamante
  - ✓ REDINTERCABLE SA 1 MB tipo cable módem
- Sede Basavilbaso
  - ✓ INTERNETSERVICES SA 3MB inalámbrico
- Sede Chajarí
  - ✓ REDINTERCABLE SA 1 MB tipo cable módem
- Sede Crespo
  - ✓ BM Soluciones 2 MB tipo inalámbrico
- Sede Federación
  - ✓ FEDERACIONNET 512 KB tipo inalámbrico

[111] Cable utilizado para la comunicación de redes, está formado por cuatro pares de cable de cobre trenzados recubiertos por fundas plásticas.

- Sede Gualeguaychú
  - ✓ ENTRERIOS.NET 1 MB tipo inalámbrico
- Sede Santa Elena
  - ✓ CableDOSNET 3MB tipo inalámbrico

Extensiones Áulicas

- Extensión Áulica Gualeguay
  - ✓ ENTRERIOS.NET 1 MB tipo inalámbrico
- Extensión Áulica Nogoyá
  - ✓ NETIUM 2 MB tipo inalámbrico

Escuelas PRE-Universitarias

- Colegio del Uruguay "Justo José de Urquiza" en la ciudad de Concepción del Uruguay;
  - ✓ INTERNETSERVICES SA 3 MB inalámbrico
- Escuela Técnica N° 35 en la ciudad de Crespo;
  - ✓ BM Soluciones 1 MB tipo inalámbrico

Servidores

Los servidores se encuentran ubicados en las sedes Oro Verde y Concepción del Uruguay. Desde las cuales se brindan la mayoría de los servicios para el resto de las dependencias.

- Sede Central Oro Verde

Servidor HP ProLiant ML115

- ✓ Procesador: Dual-Core AMD Opteron 1214 2.2 GHz.
- ✓ Memoria: 4GB PC2-5300 unbuffered DDR2 SDRAM (667MHz).
- ✓ Discos: 2 Discos de 160 (7,2K rpm) Non-Hot Plug 3,5 in SATA
- ✓ Integrated 4 port SATA controller with embedded RAID (0,1,5)
- ✓ DVD-RW.

Servidor HP ProLiant ML110 Gen9

- ✓ Procesador: Intel Xeon E5-2603v3 6-Core (1,60GHz 15MB).
- ✓ Memoria: 16GB (2 X 8GB) PC4-17000P-R DDR4 2133MHz RDIMM.
- ✓ Discos: 2 Discos de 1TB (7,2K rpm) Non-Hot Plug 3,5 in SATA
- ✓ Dynamic Smart Array B140i
- ✓ DVD-RW.

2 (dos) Servidores Lenovo Think Server TS150

- ✓ Procesador: Intel Xeon Processor E3-1200 v6 Series; Core i3, 8MB Cache.

- ✓ Memoria: 16GB (2 X 8GB UDIMMs) TruDDR4; 2400MHz ECC UDIMMs
- ✓ Discos: 2 Discos de 2TB (7,2K rpm) Non-Hot Plug 3,5 in SATA
- ✓ Think Server RAID 121i SW RAID 0/1/10/5 std
- ✓ DVD-RW.

2 (dos) Routerboard Mikrotik RB 1100 AHx2 (Utilizado como Firewall y respaldo)

- ✓ Procesador: Dual Core 1066 MHz
- ✓ Memoria: 2 GB
- ✓ Sistema Operativo RouterOS.
- ✓ 13 puertos Gigabit Ethernet.
- ✓ Soporta VPN.

- Sede Concepción del Uruguay

Servidor HP ProLiant ML110 Gen9

- ✓ Procesador: Intel Xeon E5-2603v3 6-Core (1,60GHz 15MB).
- ✓ Memoria: 8GB (1 X 8GB) PC4-17000P-R DDR4 2133MHz RDIMM.
- ✓ Discos: 2 Discos de 2TB (7,2K rpm) Non-Hot Plug 3,5 in SATA
- ✓ Dynamic Smart Array B140i
- ✓ DVD-RW.

Routerboard Mikrotik RB 1100 AHx2 (Utilizado como Firewall)

- ✓ Procesador: Dual Core 1066 MHz
- ✓ Memoria: 2 GB
- ✓ Sistema Operativo RouterOS.
- ✓ 13 puertos Gigabit Ethernet.
- ✓ Soporta VPN.

A continuación se resumen las principales características de los equipos router-firewall que poseen las sedes Oro Verde y Concepción del Uruguay:

Características: **Mikrotik RB 1100 AHx2**
FIREWALL
Firewall de estado
NAT de origen y destino
Filtrado por dirección IP, rango, puerto y protocolo
Personalización de coincidencias en CAPA 7
Soporte IPv6
Balanceo de carga

RUTEO
Ruteo estático, virtual, basado en políticas; protocolos de enrutamiento
Protocolos de enrutamiento dinámico en IPv6
VPN
IPSec modo transporte y túnel. Certificado PSK. Protocolos de seguridad: AH y ESP.
Soporte para IKEv2
Túneles punto a punto (OpenVPN, PPTP, PPPoE, L2TP, SSTP)
Soporte de túnel IPv6 sobre IPv4
Autenticación de clientes de red locales
Soporte RADIUS para Autenticación y Contabilidad

Tabla 6.1 Características router Mikrotik RB 1100 AHx2.
Fuente: elaboración propia.

A su vez la mayoría de los sistemas usados por el personal de la FCyT-UADER están a cargo del Área Informática dependiente del Rectorado de la Universidad. En el punto siguiente se aclara adonde se alojan físicamente los Sistemas implementados en la organización.

SERVICIOS QUE SE UTILIZAN Y SU DISTRIBUCIÓN GEOGRÁFICA

A continuación se describirán los sistemas con que cuenta la organización, se ubicaran geográficamente la dependencia que lo administra y el tipo de servicio utilizado.

Servicios que se destacan:

- *Sistema de Alumnado (SIU GUARANI)*

  Posee centralizada las bases de datos con información académica de los alumnos de las carreras de la FCyT, se encuentra ubicado físicamente en la sede central Oro Verde, exceptuando la base de datos de las carreras que se dictan en Concepción del Uruguay, que están alojadas en los servidores emplazados en dicha dependencia. Las peticiones a este sistema ya se describieron en el punto de Infraestructura de comunicaciones.

- *Sistema WEB de consulta para Alumnos y Docentes (SIU GUARANI 3W)*

  Ubicado en los servidores web de Oro Verde y es consultado por todas las sedes de la provincia. Permite hacer gestiones como, pedir historia académica, control de regularidades, inscripciones a exámenes, materias o solicitud de certificados.
  Para estas gestiones trabaja con la base de datos del sistema de alumnado, la cual a su vez tiene definidos un usuario y contraseña que valida las conexiones y peticiones.

- *Sistema de Encuestas (SIU KOLLA)*

  Sistema dirigido a los alumnos de FCyT, ya sea para informarlos de eventos y realizar encuestas sobre cátedras o determinadas actividades. Trabaja con la base de datos del sistema de alumnado e interactúa y publica las encuestas a través del sistema Guarani 3W. Funciona en los servidores web de la sede central Oro Verde.

- *Página Web de la Facultad de Ciencia y Tecnología*

  Es el sitio web Institucional, funciona en los servidores web de la sede central Oro Verde. Se publica toda la información referente a la organización y accesos a los sistemas web.

- *Sistema de Biblioteca y página WEB de Biblioteca FCyT*

  Contiene la base de datos de bibliografía, socios y disponibilidad de la biblioteca de la FCyT. Maneja préstamos, ABM[112] de socios y material bibliográfico. Es un sistema web que funciona en los servidores web de la sede Oro Verde y permite:

  - Gestionar recursos de información académica, científica y técnica promoviendo y facilitando a sus usuarios: alumnos, profesores e investigadores, el acceso a la información en distintos soportes mediante servicios de calidad.
  - Desarrollar competencias y habilidades para el acceso y uso de la información tanto en espacios físicos como virtuales, que favorezcan las condiciones de aprendizaje y apoyen los procesos de docencia e investigación.
  - Alcanzar sus fines a través de una adecuada combinación de: gestión, personal profesional, recursos materiales y tecnológicos adecuados.[113]

- *Sistema de Aula Virtual (Campus FCyT Virtual)*

  Es la plataforma o sitio de educación a distancia para todos los docentes responsables de asignaturas, seminarios y cursos presenciales de la FCyT-UADER. Servicio alojado físicamente en los servidores del Rectorado de UADER.

[112] La abreviatura ABM significa Altas, Bajas y Modificaciones, y se refiere al sistema mediante el cual las aplicaciones de bases de datos se mantienen actualizadas.

[113] SISTEMA DE BIBLIOTECAS FCYT-UADER. *Biblioteca de la Facultad de Ciencias y Tecnología*. Recuperado el 25 de enero de 2018, de http://bibliotecafcyt.uader.edu.ar/joomla/homepage/institucional-2.

El Sitio tiene como objetivos: construir un espacio de formación en crecimiento permanente, logrando y difundiendo conocimientos científico-tecnológicos a través de una oferta educativa integral y desde una relación estrecha de las funciones académica, de investigación y extensión. Proponer una consolidación y mejoramiento permanente de la calidad educativa en el área académica de grado y posgrado, para una formación profesional calificada que se proyecte en el desarrollo de la sociedad.[114]

- *Sistema de manejo de Expedientes (COMDOC)*

  ComDoc es una aplicación de seguimientos de documentación creada por el Ministerio de Economía de la Nación y cedida a las universidades a través del SIU. Actualmente se está usando la versión 3 de la misma.[115]

  Es una herramienta web, gestionada por personal de la dirección de informática de Rectorado de la Universidad. Autentica a través de usuarios y contraseña previamente solicitado y está disponible para todas las facultades de UADER. Servicio alojado físicamente en los servidores de Rectorado en la ciudad de Paraná.

- *Correo electrónico institucional*

  Los correos institucionales son aprobados por las autoridades de cada facultad y son gestionados por personal de la dirección de informática. Los servidores web y el dominio están contratados a Google y se administran a través de la plataforma de Gmail.

- *Sistema de Legajos (SIU MAPUCHE)*

  El SIU-Mapuche es un sistema que lleva adelante la gestión de Recursos Humanos de manera integrada. Mantiene el legajo del empleado actualizado y constituye una base para obtener información útil para la organización.

  Está basado en un legajo electrónico único, que es la fuente de información para la gestión de personal y para la liquidación de

[114] FCyT-UADER. *Campus FCyT UADER: Acerca del Campus*. Recuperado el 25 de enero de 2018, de http://fcytvirtual.uader.edu.ar/mod/page/view.php?id=293.

[115] UADER. *Rectorado – UADER: ComDoc*. Recuperado el 25 de enero de 2018, de http://rectorado.uader.edu.ar/?page_id=37.

haberes. El sistema se actualiza incorporando las modificaciones de la legislación vigente.

El ingreso de información en este sistema está a cargo de cada Unidad Académica, por lo que resulta vital el acceso eficaz y el conocimiento de las operaciones por parte de quienes operan la carga.[116]

Administrado por personal de la dirección de informática. Autentica a través de usuarios y contraseña previamente solicitado al personal y está disponible para todas las facultades de UADER.

- *Sistema de Asistencias de Personal (ASISTENCIA UADER)*

  Sistema de ABM de recursos humanos y control de asistencias. Administrado por personal de la dirección de informática. Es un sistema web que corre en los servidores de Rectorado y se encuentra disponible para todas las unidades académicas que lo requieran.

CUADRO DESCRIPTIVO DE LAS SEDES DE LA FCyT-UADER

SEDE	DESCRIPCION RED DE DATOS	SERVIDORES	ENLACES INTERNET	SERVICIOS EMPLAZADOS	PERSONAL TECNICO
Sede Central Oro Verde	Posee una red plana, con topología de Estrella, cableado organizado, con medios categoría 5E. Cuenta con dispositivos intermedios de Capa 2, y posee una extensión máxima de 3 dispositivos. Se encuentra segmentada físicamente en 6 LANs (Administración, Laboratorios, DMZ, Wifi limitada, Wifi Libre de limitaciones). Cuenta con 100 hosts aproximadamente.	• HP Proliant ML115 • HP Proliant ML110 Gen9 • LENOVO Think Server TS150 (Cantidad 2) • Routerboard MIKROTIK RB1100 AHx2 (Cantidad 2)	*10 MB (ADSL ARNET) *10 MB (ADSL ARNET) *2 MB Simétricos con IP Pública (INALAMBRICO BM SOLUCIONES)	• Sist. de Alumnado (SIU-GUARANI y SIU- GUARANI 3W) • Sist. de Encuestas (SIU-KOLLA) • Página WEB FCyT-UADER • Sist. de Biblioteca y Micro Sitio Biblio-FCyT	Si, 3 (tres) personas
Sede Concepción del Uruguay	Posee una red plana, con topología de Estrella, cableado organizado, con medios categoría 5e, dispositivos intermedios de Capa 2 administrables. Segmentada en 4 LANs (Administración, Laboratorios, Investigación, Inalámbrica). Cuenta con 60 hosts aproximadamente.	• HP Proliant ML110 Gen9 • MIKROTIK RB1100 AHx2	*7 MB (ADSL ARNET) *7 MB (ADSL ARNET)	• Sist. de Alumnado (SIU-GUARANI y SIU- GUARANI 3W)	Si, 1 (una) persona
Sede Paraná	Posee una red plana, con topología de Estrella, con medios categoría 5e, dispositivos intermedios de Capa 2. Segmentada en físicamente en 2 LANs (Cableada e Inalámbrica). Cuenta con 30 hosts aproximadamente.	• MIKROTIK RB750	*30 MB con IP Pública (CABLE-MODEM GIGARED)	N/C	No
Sede Villaguay	Red reducida, sin segmentación, con 6 hosts aproximadamente, sin organización. Que posee como núcleo un router hogareño proporcionada por el proveedor de servicio.	N/C	*1 MB (INALAMBRICO SUPPORTINTERNET)	N/C	No

[116] UADER. *Rectorado – UADER: Mapuche*. Recuperado el 25 de enero de 2018, de http://rectorado.uader.edu.ar/?page_id=49.

Sede Diamante	Red reducida, sin segmentación, con aproximadamente 10 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*1 MB (CABLEMODEM REDINTERCABLE SA)	N/C	No
Sede Basavilbaso	Red reducida, sin segmentación, con 3 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*3 MB (INALAMBRICO INTERNETSERVICES SA)	N/C	No
Sede Chajarí	Red reducida, sin segmentación, con 3 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*1 MB (CABLE MODEM REDINTERCABLE SA)	N/C	No
Sede Crespo	Red reducida, sin segmentación, con 5 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*2 MB (INALAMBRICO BM SOLUCIONES)	N/C	No
Sede Federación	Red reducida, sin segmentación, con 2 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*512 KB (INALAMBRICO FEDERACIONNET)	N/C	No
Sede Gualeguaychú	Red reducida, sin segmentación, con 4 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*1 MB (INALAMBRICO ENTRERIOS.NET)	N/C	No
Sede Santa Elena	Red reducida, sin segmentación, con 8 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*3 MB (INALAMBRICO CableDOSNET)	N/C	No
Extensión Áulica Gualeguay	Red reducida, sin segmentación, con 2 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*1 MB (INALAMBRICO ENTRERIOS.NET)	N/C	No
Extensión Áulica Nogoyá	Red reducida, sin segmentación, con 6 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*2 MB (INALAMBRICO NETIUM)	N/C	No
Colegio del Uruguay	Red reducida, sin segmentación, con 2 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*3 MB (INALAMBRICO INTERNETSERVICES SA)	N/C	No
Escuela Técnica Nº 35	Red reducida, sin segmentación, con 2 hosts. Que posee como núcleo un router hogareño proporcionado por el proveedor de servicio.	N/C	*1 MB (INALAMBRICO BM SOLUCIONES)	N/C	No

CASO PARTICULAR

UBICACION	DESCRIPCION	SERVICIOS EMPLAZADOS
RECTORADO UADER	La Universidad posee servicios centralizados, los cuales corren en servidores emplazados físicamente en el centro de datos de Rectorado de la Universidad, los cuales son consultados por todas las Sedes de las distintas facultades de UADER.	• Sist. de Aula Virtual (FCyT-Virtual) • Sist. de Manejo de Expedientes (COMDOC) • Servicio de Correo Electrónico • Sist. de Legajos (SIU-MAPUCHE) • Sist. de Asistencia de Personal *(ASISTENCIA UADER)

Tabla 6.2 Cuadro descriptivo de las sedes de la FCyT-UADER.
Fuente: elaboración propia.

CAPITULO 7

[METODOLOGÍA PARA LA IMPLEMENTACIÓN DE VPN EN LA FACULTAD DE CIENCIA Y TECNOLOGÍA SOBRE IPV6]

Este capítulo establece los pasos necesarios, con base en el relevamiento realizado en la unidad anterior, el estado del arte de los protocolos y conceptos teóricos abordados en los distintos capítulos, proponiendo una solución viable para brindar conexiones seguras a usuarios de las distintas sedes a los servicios organizacionales, proporcionando beneficios a FCyT-UADER en lo inmediato y dando la posibilidad de crecimiento a futuro.

METODOLOGÍA DE IMPLEMENTACIÓN DE UNA VPN

Con base en los temas expuestos, se establecen una serie de pasos para llevar adelante la ejecución de una VPN, que se considera como solución viable de implementar en una organización como FCyT-UADER.

1-Definición del equipo de trabajo

2-Fijar el alcance

3-Diseño de la VPN

4-Elección de la solución a implementar

5-Requerimientos básicos para la implementación

6-Medidas de seguridad

7-Implementación

8-Evaluación de la implementación

1 - DEFINICIÓN DEL EQUIPO DE TRABAJO

En este apartado se conforma el grupo de trabajo, teniendo en cuenta lo visto en el capítulo 4, p. 72 - apartado "Requerimiento de recursos humanos", tendrá como objetivo llevar adelante el proyecto de implementación de la tecnología acorde a las necesidades de la organización.

El grupo se integrará con personal técnico especializado en comunicaciones; jefes de departamento y futuros usuarios, los cuales pueden plantear qué información critica consideran sea transportada a través de la VPN; y a su vez deben integrar el equipo, las autoridades de la organización como ser secretarios implicados, quienes tienen poder de decisión y facultad de asignar tareas y responsabilidades al personal.

2 – FIJAR EL ALCANCE

En base a lo expuesto en el capítulo 4, p. 70 - apartado de "Requerimientos de hardware, software y recursos humanos" y en capítulo 6, p. 97 - sección "Cuadro descriptivo de las sedes de la FCyT-UADER" se fijarán los objetivos y se detectarán las necesidades de cobertura de la red privada virtual, los servicios que se podrían segurizar y que problemática se aborda relacionado al capítulo 1, p. 15 - "Beneficios de las VPN en las organizaciones".

Algunas de las cuestiones a considerar se plantean con los interrogantes expuestos a continuación:

¿Para qué tener una red privada virtual?
¿Qué servicios cree posible de transportar en la VPN?
¿Quiénes serán los usuarios?
¿Cuáles son las sedes que mas transacciones realizan con los sistemas centralizados?

Contemplando el promedio de transacciones de cada sistema. ¿Cuál sería el ranking de sistemas por sede?
¿Qué conocimientos, información o datos se van a mover en la red privada virtual?
¿Su organización posee la capacidad técnica adecuada para mantener e instalar una red privada virtual?
¿De qué manera se integrará la red privada virtual con la red de la organización en cada sede?
¿Qué respuesta o resultados cree que se podrá obtener?

Una vez llevada adelante la implementación, los temas aquí planteados serán utilizados para realizar la evaluación de la solución ejecutada.

Respecto al motivo por el cual se justifica la utilización de la tecnología VPN en la facultad; del análisis de la situación actual y de lo que se ha investigado, se propone esta tecnología, la cual le daría seguridad, unificación y mayor cobertura de su red LAN en todo el territorio, englobando las sedes que la componen. Hoy en día, se proporcionan accesos a los sistemas mediante controles de acceso deficientes y con algunas vulnerabilidades en cuestión de seguridad. Además, no existe un log[117] de las conexiones y de los usuarios que trabajan en la red, lo que puede afectar tanto a la confidencialidad como la integridad de la información.

Es importante destacar que la solución planteada se consigue a un bajo costo, ya que hay grandes diferencias entre usar una VPN a través de las redes públicas en comparación con la contratación de enlaces punto a punto rentados proporcionados por un proveedor.

Del relevamiento, se considera como sistema informático prioritario a nivel organizacional, el sistema de alumnado SIU Guaraní. El cual es consultado por todas las sedes y debe contar con protección de acceso desde redes públicas.

El personal del Departamento Alumnado, de Secretaría Académica y del Área Títulos son quienes actualmente utilizan el acceso al sistema SIU remoto; además es utilizado por los referentes técnicos del área Informática (en caso de que las sedes cuenten con uno) con el fin de realizar configuraciones, versionados o cambios significativos. Sin embargo, es necesario considerar la escalabilidad de la red y dejar abierta la posibilidad de incorporar nuevos servicios y usuarios que podrían utilizar la VPN.

3 - DISEÑO DE LA VPN

Una vez establecidos los objetivos, se procede a realizar el diseño en el cual el equipo de trabajo debe tomar en consideración la estructura general de la red de datos, los protocolos intervinientes vistos en el capítulo 3, la distribución física de

[117] En el ámbito de los profesionales en seguridad informática, es el registro secuencial de datos o información sobre quién, que, cuando, donde y por qué un evento ocurre para un dispositivo en particular o aplicación.

la organización y los sistemas o información crítica que maneja, relevados en el capítulo 6, p. 97 - "Cuadro descriptivo de las sedes de la FCyT-UADER"

En base a los puntos a considerar, sumado a los objetivos fijados como alcance, y la seguridad requerida; el equipo de trabajo planteará la solución acorde y factible a la organización. Dada la realidad actual de cada una de las sedes y el trafico de las mismas para con los sistemas institucionales se plantea el diseño de dos tipos de VPN analizados en el capítulo 4, p. 59 - apartado "Tipos de VPN".

Una arquitectura sitio a sitio basada en enrutadores entre las sedes Oro Verde y Concepción del Uruguay de la FCyT-UADER por medio de la cual, se logra la interconexión de red a un bajo costo, que si bien en la actualidad solo se utilizará para acceder un servicio (SIU Guaraní), en el futuro presenta la posibilidad de sumarle otras prestaciones o servicios logrando una red convergente.

Para la conexión sitio a sitio se recurrirá al marco IPSec, ya que ofrece conectividad flexible y escalable, proporcionando una conexión remota, rápida y confiable que permite transportar la información de una red privada de manera segura a través de una red pública. A su vez, IPSec no se limita a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de creación de claves, simplemente depende de algoritmos existentes para implementar comunicaciones seguras.

Mientras que para el resto de las dependencias (como son Paraná, Villaguay, Diamante, Basavilbaso, Chajarí, Crespo, Federación, Gualeguaychú y Santa Elena), con menor cantidad de usuarios y consultas a la base de datos del sistema implicado en el punto de fijación de alcance, un usuario remoto de red privada ya cubre la necesidad de segurizar la comunicación, validar la conexión y permitir acceso al sistema organizacional objetivo.

Para el direccionamiento como fue estudiado en el capítulo 2 - p. 26, para las LAN internas de todas las sedes se utilizará IPv6, incluyendo las interfaces VPN. Como se puede comprobar, la principal ventaja de IPv6 es que no hay problema con la sobreestimación, es decir que se pueden contemplar bloques de redes grandes, previendo el crecimiento de la organización. Pero el principal objetivo de usar IPv6 en la LAN Virtual, es que brindará mejor rendimiento junto a IPSec, dada la inclusión de este protocolo en el encabezado del paquete, como se vio en el capítulo 2, p. 37 - apartado "Fortalezas y debilidades de una VPN corriendo sobre IPv6". Para las direcciones públicas se utilizará IPv4.

La Figura 7.1 plasma el diseño de la arquitectura VPN planteada para dar conectividad a todas las sedes de la FCyT-UADER.

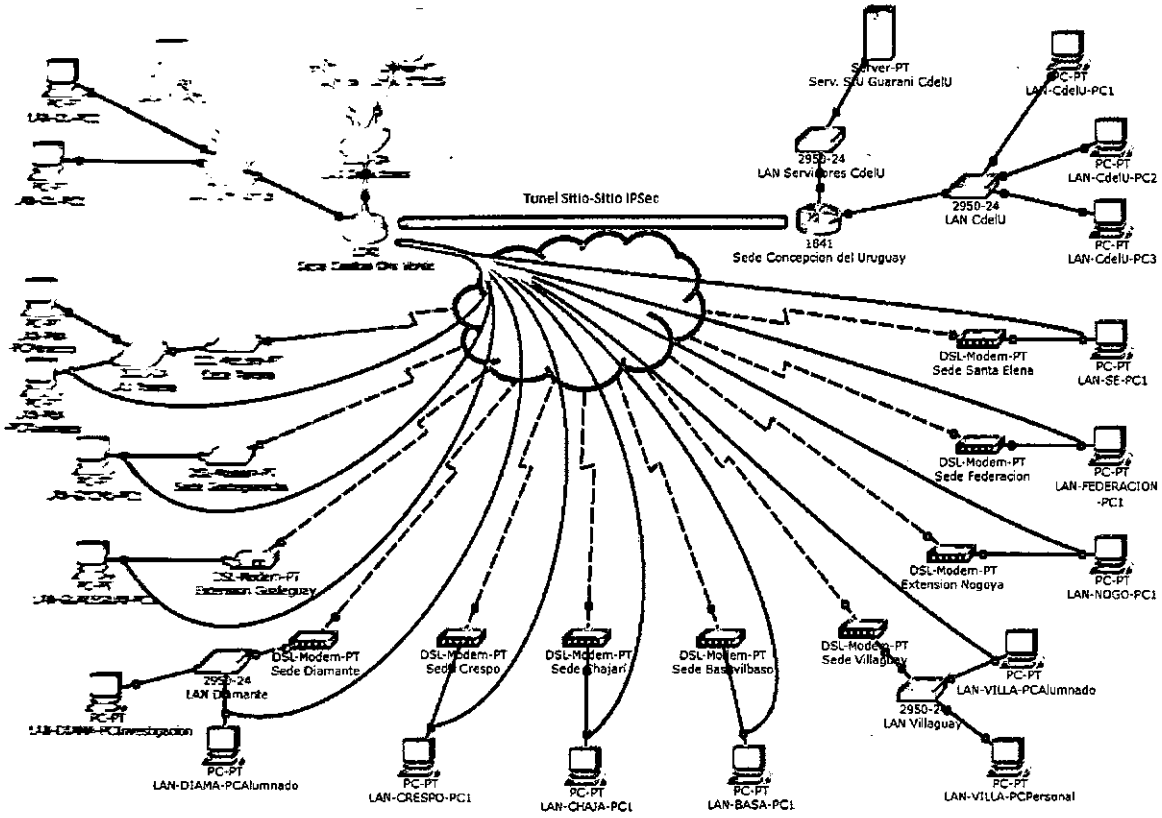


Figura 7.1 Topología de red propuesta para las sedes de la FCyT-UADER.
Fuente: elaboración Propia.

4 - ELECCIÓN DE LA SOLUCIÓN VPN A IMPLEMENTAR

De lo planteado, el análisis de la información obtenida con base en la infraestructura organizacional actual y las transacciones de red promedio de cada uno de los puntos remotos se plantean los requisitos necesarios para poner en funcionamiento la solución propuesta. A su vez se deberán acordar buenas prácticas que complementarán el diseño.

El equipo de trabajo decidirá los protocolos VPN vistos en capítulo 4 - p. 70, "Requerimientos de hardware, software y recursos humanos", así como también equipamiento necesario que ya posee la organización (capitulo 6 – p. 97 – "Cuadro descriptivo de las sedes de la FCyT-UADER") y será utilizado para la implementación de la solución.

Para el acceso y la comunicación entre las sedes Oro Verde y Concepción del Uruguay se presenta, como solución acorde, una red privada virtual del tipo punto a punto basado en enrutadores, utilizando para este caso el marco IPSec estudiado en el capítulo 3, p. 46 - apartado "Protocolo de internet seguro". Con lo cual, se logra el objetivo de ofrecer una única red LAN, para la transmisión de información de los sistemas organizacionales, permitiendo a futuro la extensión o crecimiento a otros servicios.

Para llevar adelante las conexiones VPN de acceso remoto en los equipos pertenecientes a cada sede de FCyT, se propone realizar una configuración

definida en el cliente VPN del sistema operativo Windows analizado en el capítulo 4, p. 72 - sección "Cuadro comparativo de aplicaciones". El cliente crea una interfaz virtual, la cual recibe la dirección IP del rango de la LAN organizacional (en este caso será una dirección IPv6) que permitirá comunicarse con los servidores en la sede central Oro Verde.

La conexión de acceso remoto se llevará adelante usando el protocolo L2TP/IPSec ya que L2TP utiliza IPSec para encriptar, logrando integridad y autenticación de los datos de origen. Basándonos en el estudio realizado en el capítulo 3, p. 55 - sección "Cuadro de referencia de protocolos de túnel".

Con respecto a la seguridad, se puede afirmar que actualmente en las sedes de la FCyT hay un concepto de seguridad de usuario final, donde cada usuario protege los puestos de trabajo con un antivirus. Situación que debería ser abordada a través de buenas prácticas que engloben toda la organización y unifique la manera de proteger la red. Con un firewall que proteja las conexiones y la información de ataques, como pueden ser troyanos, spam, virus, hackers y otros riesgos que convergen en una red pública como es Internet.

Si bien este último planteo va más allá de la investigación realizada, se considera que al integrar los hosts de todas las sedes en una misma LAN virtual, hay mayor cantidad de puntos débiles (hosts) que interactuarán en la red de FCyT, por lo que se presume mayores riesgos y exige tenerlo en consideración.

5 - REQUERIMIENTO BÁSICO PARA IMPLEMENTACIÓN

Según la solución a implementar y teniendo en cuenta la topología visto en capítulo 1, p. 25 - bajo el titulo "Topologías", la cantidad de host y un relevamiento organizacional completo plasmado en capítulo 6, p. 97 - ""Cuadro descriptivo de las sedes de la FCyT-UADER ".

El equipo de trabajo definirá el software, hardware y recursos humanos necesarios para cumplir con los objetivos planteados. Los cuales se pondrán en contraposición con el relevamiento organizacional realizado y se definirán los ítems faltantes que se deberán adquirir para llevar adelante el proyecto.

Tomando en cuenta las cantidades de host en cada una de las distintas sedes y los requerimientos necesarios, no hay necesidad de cambiar ningún equipo utilizado actualmente para crear la arquitectura sugerida.

Para la construcción de los túneles se utilizaran los router-firewall ya emplazados en las sedes. A su vez, dado un estudio de las especificaciones de los dispositivos actuales, se puede afirmar que estos soportan la utilización de las tecnologías definidas en el diseño, tanto para la arquitectura punto a punto como para los accesos remotos.

En cuanto a los recursos humanos se requiere personal capacitado en temas relacionados a redes de comunicación, conocimiento del modelo TCP/IP, protocolos de seguridad y experiencia en configuración de dispositivos de red.

6 - MEDIDAS DE SEGURIDAD

En el presente apartado se fijan las medidas a seguridad acorde a la solución objetivo, analizando parámetros como costo-beneficio, rendimiento y criticidad de la información visto en el capítulo 5, p. 75 - bajo el título "Importancia de seguridad".

El objetivo primario es proteger a través de políticas de seguridad la comunicación extremo a extremo de la red de datos organizacional. En cuyo aspecto se deberá tener en cuenta tanto los dispositivos que se utilizaran para los host de acceso remoto, como la seguridad de los dispositivos intermedios y aplicaciones.

La seguridad es el principal objetivo de las VPN y con IPSec la información de una red privada se logra transportar de manera segura a través de una red pública. Se establece utilizar IPSec ya que es el estándar IETF que define la forma en que se puede configurar una red privada virtual de manera segura.

Para brindar la seguridad, el marco IPSec presenta una serie de componentes de configuración, los cuales ya han sido estudiados en el capítulo 3, p. 52 - sección "Marco IPSec", y cuya combinación acorde con la solución propuesta se presenta a continuación.

Protocolo de marco IPSec: las opciones son ESP y AH o una combinación de ambos. Se utiliza ESP+AH, ya que AH por sí mismo no proporciona cifrado.

Confidencialidad: de las opciones (DES, 3DES o AES). El seleccionado es AES ya que posee mayor eficiencia computacional y proporciona opciones en cuanto a la longitud de clave a utilizar.

Integridad: los algoritmos de hash disponibles son MD5 y SHA1. SHA1 maneja una clave de 160 bits, contra los 128 de MD5, lo que proporciona mayor seguridad a costa de mayor sobrecarga. Si bien ambos son seguros, se utilizará MD5 basando la elección en su velocidad de resolución.

Autenticación: los métodos de autenticación disponibles son PSK o RSA. Se seleccionará RSA, ya que cada extremo del túnel utiliza claves públicas y privadas encriptadas para autenticar a su par opuesto.

Grupo de Algoritmos DH: visto en capítulo 5, p. 82 - "Algoritmo Diffie-Hellman" representa la forma en que se establece la clave secreta compartida entre las partes. Existen varias opciones las cuales deben ser compatibles con los algoritmos de cifrado utilizados (DH1, DH2, DH5 y DH7) siendo DH7 la que proporciona mayor seguridad.

En la Figura 7.2 se plantea el marco sugerido para la implementación de la VPN sitio a sitio con IPSec en FCyT-UADER.

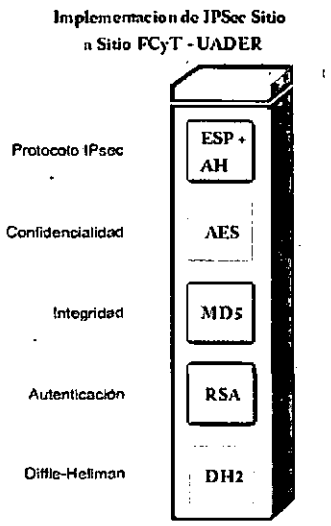


Figura 7.2 Implementación de IPSec sitio a sitio sugerida para FCyT – UADER.
Fuente: elaboración propia.

Respecto a la VPN de acceso remoto, se define utilizar la combinación de L2TP/IPSec, ya que IPSec provee seguridad a nivel de paquete utilizando ESP+AH y todos los datos L2TP se transmiten por medio de UDP/IP, lo que beneficia la conmutación de paquetes al túnel establecido. L2TP solo se encarga de enviar los datos por un túnel a través de la red pública, cuyos flujos de tráfico del origen al destino son protegidos a través de cifrado de datos con IPSec usando ESP+AH.

De esta manera L2TP se combina con IPSec para proporcionar un modo sencillo y eficiente de construir un túnel y proteger la información a través de Internet.

7 - IMPLEMENTACIÓN

Fase en la cual el equipo de trabajo utiliza los parámetros definidos en los puntos 3, 4 ,5 y 6 de la metodología. Con el fin de establecer las configuraciones necesarias, llevar adelante la implementación de la solución, y realizar capacitaciones a los usuarios; en base a los roles y funciones definidos para cada integrante, mencionado en el capítulo 4, p. 72 - "Recursos humanos".

8 - EVALUACIÓN DE LA IMPLEMENTACIÓN

El equipo de trabajo y las autoridades de la organización, como se aclaró en el capítulo 4, p. 72 - "Recursos humanos" deberán verificar que los puntos plasmados en la fijación del objetivo, en contraposición con la implementación, posea un balance acorde a las expectativas que motivaron a la organización a realizar el proyecto.

IMPLEMENTANDO VPN-IPV6 en FCYT-UADER

PASOS	DESCRIPCION	ELECCION DE LA SOLUCION
1 - Definición del equipo de trabajo	Conformación del grupo de trabajo que tendrá como objetivo llevar adelante el proyecto.	Grupo conformado por personal técnico especializado en comunicaciones, jefes de departamento, futuros usuarios y autoridades de la organización (representado a través de secretarías).
2 - Fijación del alcance	Fijar objetivos y detectar necesidades de cobertura de una Red Privada Virtual.	Proporcionar seguridad, unificación y mayor cobertura de su red LAN en todo el territorio, englobando las sedes que componen la organización a un bajo costo.
3 - Diseño de la VPN	Realizar el diseño tomando en consideración la estructura general de la red y plantear la solución factible para la organización.	Entre las sedes Oro Verde y Concepción del Uruguay se plantea una arquitectura sitio a sitio basada en enrutadores. Mientras que para el resto de las sedes con menor cantidad de usuarios y consultas, un Usuario Remoto de Red Privada cubre la necesidad de segurizar la comunicación, validar la conexión permitiendo el acceso a los sistemas organizacionales.
4 - Elección de la solución a implementar	El equipo fijará los protocolos VPN a utilizar, los requerimientos de hardware y software, así como también equipamiento necesario para la implementación de la solución.	Para la VPN punto a punto, se fija la utilización del marco IPSec corriendo a través de un enlace público y utilizando IPv6 para la red LAN y configurado en los firewall de las sedes extremos del túnel. Para la VPN de Acceso Remoto en los equipos clientes se realizara la configuración en el cliente VPN del sistema operativo Windows, que usando el protocolo L2TP/IP establecerá una conexión encriptada con el firewall de la Sede Central Oro Verde, asegurando Integridad y Autenticación de los datos de origen.
5 - Requerimientos básicos para la implementación	El equipo de trabajo definirá el software, hardware y recursos humanos faltantes para cumplir con los objetivos planteados	Para la construcción de los túneles no hay necesidad de cambiar ningún equipo, se utilizaran los router-firewall ya emplazados en las sedes Oro Verde y Concepción del Uruguay para implementar la tecnología de red privada virtual. En cuanto a los recursos humanos se requiere personal capacitado en temas relacionados a redes de datos, conocimiento del modelo TCP/IP, protocolos de seguridad y experiencia en configuración de dispositivos de red.
6 - Medidas de seguridad	El equipo de trabajo establecerá políticas de seguridad con el fin de proteger la comunicación extremo a extremo de la red de datos organizacional.	Para lograr seguridad de la VPN se establece utilizar el marco de trabajo IPSec con la configuración especificada a continuación: Confidencialidad se plantea usar ESP+AH con encriptación AES, para lograr Integridad se utilizará MD5, dada su velocidad de resolución, para Autenticación se establece utilizar RSA, basando la decisión en la utilización de Autoridades Certificantes y por ultimo como método de compartición de claves se utilizará DH2, dada la necesidad de no introducir gran sobrecarga a los enlaces y siendo esta versión compatible con el protocolo de cifrado seleccionado. A los fines de establecer una política de seguridad se fija como objetivo homogeneizar las medidas de seguridad para todas las sedes, control de cumplimiento de las medidas y capacitación constante.
7 - Implementación	El equipo de trabajo utiliza los parámetros definidos en la metodología, para establecer las configuraciones necesarias y llevar adelante la implementación de la solución acorde.	El personal técnico especializado en comunicaciones, implementara las configuración en los equipos que se definieron como básicos en los requerimientos para implementar la tecnología. Pruebas pertinentes de las comunicaciones. Realización de las capacitaciones y otorgamiento de credenciales a los usuarios.
8 - Evaluación de la implementación	El equipo de trabajo y las autoridades de la organización, verifican el cumplimiento de los objetivos fijados en el alcance de la metodología.	Chequeo de cumplimiento de objetivos fijados en el punto 2 de la metodología. Realización de análisis de seguridad, testeo de penetración, análisis de rendimiento de los enlaces, entrevistas a los usuarios evaluando conformidad y retroalimentación.

Tabla 7.1 Implementando VPN-IPv6 en FCYT-UADER.
Fuente: elaboración propia.

CONCLUSIÓN

La tecnología VPN permite a las organizaciones construir una red privada y segura sobre redes de comunicación públicas, lo que elimina el costo de contratar líneas dedicadas. A su vez provee una ventaja competitiva, al brindarle la posibilidad de acceso a la información organizacional desde cualquier punto geográfico.

Puntualmente en la Facultad de Ciencia y Tecnología, que se encuentra distribuida geográficamente en sitios distantes de la provincia de Entre Ríos, con realidades distintas en cada una de sus sedes, en cuanto al acceso a la tecnología con que cuenta, tiene la necesidad de mantener una interconectividad de cada una de las partes para el funcionamiento organizacional diario.

A su vez, para utilizar la tecnología con el riesgo que conlleva transportar información organizacional a través de redes públicas, es necesario prestar especial atención en los tres pilares básicos que garantizan la seguridad de la información (disponibilidad, confidencialidad y autenticación). Para ello la tecnología VPN cuenta con soporte de múltiples protocolos que proveen herramientas especificas para manejar autenticación de usuarios, control de acceso, administración de direcciones, cifrado de datos, administración de claves y ancho de banda.

El rendimiento de la comunicación a través de una VPN se puede ver afectado por la técnica de encriptación y encapsulación de los datos aplicada. Por lo que es primordial en el diseño evaluar correctamente los requerimientos necesarios, y así lograr un balance entre rendimiento y seguridad.

Es importante destacar que el protocolo de internet utilizado para el direccionamiento y transporte de datos en las comunicaciones, también influye en las redes privadas virtuales, por ende no es un tema menor el agotamiento de direcciones IPv4, lo cual fue un factor primordial que impulsó la búsqueda para el desarrollo de un nuevo protocolo de internet que lo reemplace. Surgiendo así IPv6, que tiene como principal ventaja la cantidad de direcciones IP soportadas, es decir, permite diseñar bloques de redes muy grandes previendo el crecimiento de la organización.

A su vez ofrece un encabezado eficiente y simplificado respecto de IPv4, para brindar eficacia al procesar los paquetes cuando atraviesan los dispositivos de la red. También provee seguridad integrada en el encabezado con IPSec, brindando autenticación y privacidad con características propias como calidad de servicio de extremo a extremo para trabajar con aplicaciones multimedia en internet.

Debido a que la migración de IPv4 a IPv6 no puede ocurrir rápidamente, hay que buscar alternativas para administrar la transición. Si bien los protocolos son conceptualmente similares, existen diferencias en la implementación, pasaran años hasta que IPv6 sea el protocolo de internet reinante, pero día a día son

cada vez más los elementos o servicios ligados a las comunicaciones que lo utilizan.

En la actualidad se ha registrado inversiones de parte de los ISP que proveen servicio en la región, para la adopción de la versión 6 de IP en sus redes, lo cual presenta un futuro prometedor para el avance de la tecnología.

La metodología propuesta puntualiza y desarrolla pasos especificos en base a los protocolos estudiados y al relevamiento de la organización objetivo. Proporcionando una herramienta para futuras implementaciones en entidades con similares características, como ser distribución geográfica y constante intercomunicación operativa entre sus dependencias.

Respecto a futuras investigaciones, esta tesis aclara el panorama y brinda apoyo a la hora de utilizar IPv6 en combinación con protocolos que protegen la confidencialidad, integridad y disponibilidad de la información. En este contexto el punto focal de investigaciones actuales apunta a la ciberseguridad de las comunicaciones con IPv6[118] y las mediciones de su rendimiento respecto a su antecesor[119].

Es de lectura obligada al momento de utilizar nuevos servicios para proteger activos de información que son trasportados a través de redes públicas. Resultando una fuente fiable a la hora de aplicar protocolos de túnel y medir el rendimiento de enlaces WAN en un ámbito definido, como ser la provincia de Entre Ríos.

[118] Repositorio institucional de la UNLP. *Servidor virtual para detección de intrusos y ataques en ipv6.* Recuperado el 16 de noviembre de 2018, de http://sedici.unlp.edu.ar/bitstream/handle/10915/67211/Documento_completo.pdf-PDFA.pdf?sequence=1.

[119] LACNIC. *Proyecto Simón*. Recupero el 16 de noviembre de 2018, de https://simon.lacnic.net/.

Bibliografía

ALONSO, J. A. (2009). *Redes Privadas Virtuales*. México: Editorial Alfaomega.

AGUIRRE SANCHEZ, Lizeth Patricia. *Rediseño de la red MPLS con soporte de IPv6 empleando las mejores prácticas de seguridad para el sistema autónomo de Telconet S.A. de la ciudad de Quito*. 2013. (Tesis de Ingeniería). Quito, Ecuador. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional.

ARIGANELLO, E. (2014). *Redes Cisco. Guía de estudio para la certificación CCNA Routing and Switching.* Madrid, España: Editorial RA-MA.

ARIGANELLO, E.; BARRIENTOS, E. (2010). *REDES CISCO. CCNP a Fondo. Guía de estudio para Profesionales.* Madrid, España: Editorial RA-MA.

CÁRDENAS TORREBLANCA, M.; QUISPE RUEDAS, F. *Propuesta de una red segura para la interconexión y cooperación de las comisarias y municipalidades de Arequipa utilizando los protocolos VPN y OLSR con servidor Radius y monitoreo Nagios.* 2015. (Tesis Ingeniero de Sistemas). Arequipa, Perú. Facultad de Ciencias e Ingenierías Físicas y Formales, Universidad Católica de Santa María, Programa Profesional de Ingeniería de Sistemas.

COSME MACARTHUR ORTEGA, B. *Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace*. 2003. (Tesis Ingeniero en Sistemas Computacionales). Ibarra, Ecuador. Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Escuela de Ingeniería en Sistemas Computacionales.

FERNANDEZ HANSEN, Y.; RAMOS VARÓN, A.; GARCÍA-MORÁN, J. P. (2008). *Sistemas basados en la autenticación en Windows y GNU/Linux.* Madrid, España: Editorial RA-MA.

RICO BAUTISTA, D. W. & MEDINA CÁRDENAS, Y. C. & SANTOS JAIMES, L. M. *IPSec de IPv6 en la Universidad de Pamplona.* Scientia Et Technica. XIV(39): 320-325. Septiembre de 2018.

SABOLANSKY, A. J. *Utilizando software libre para una servicio de Sellado Digital de Tiempo.* 2010. (Tesis Licenciado en Informática). La Plata, Argentina. Facultad de Informática, Universidad Nacional de La Plata.

SANDOVAL CARRILLO, Sandra Milena. *Análisis del Protocolo IPSec en Ambiente IPv6.* 2006. (Tesis de Ingeniería). Pamplona, Colombia. Facultad de Ingenierías y Arquitectura, Universidad de Pamplona.

STALLINGS, W. (2004). *Comunicaciones y Redes de Computadores* (Séptima edición). México: Editorial Pearson.

TANENBAUM, A. S.; WETHERALL, D. J. (2012). *Redes de computadoras* (Quinta edición). México: Editorial Pearson.

WENDELL, O (2016). *CCNA Routing and Switching 200-125 Official Cert Guide Library*. Indianapolis, EEUU: Editorial Cisco Press.

Referencias Electrónicas

IBM. *Infraestructura de clave pública (PKI)*. Recuperado el 15 de noviembre de 2018, de https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q009900_.htm.

IBM. *Redes privadas virtuales de seguridad*. Versión i7.1. Recuperado el 23 de enero de 2018, de https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_71/rzaja/rzajaprintvpn.htm.

FCyT-UADER. *Campus FCyT UADER: Acerca del Campus*. Recuperado el 25 de enero de 2018, de http://fcytvirtual.uader.edu.ar/mod/page/view.php?id=293.

LACNIC. Proyecto Simón. Recupero el 16 de noviembre de 2018, de https://simon.lacnic.net/

Las mejores herramientas para trabajar desde casa. Recuperado el 20 de enero de 2018, de https://hipertextual.com/archivo/2013/10/trabajar-casa-con-vpn/

Manual: *RouterOS Features*. Recuperado el 16 de enero de 2018, de https://wiki.mikrotik.com/wiki/Manual:RouterOS_features#VPN.

MIKROTIK. *MIKROTIK Routers and Wireless*. Recuperado el 23 de enero de 2018, de https://mikrotik.com/product/RB1100AHx2#fndtn-testresults.

Pagina Web de la Facultad de Ciencias y Tecnología de la UADER. Recuperado el 16 de enero de 2018, de http://fcyt.uader.edu.ar/web.

SISTEMA DE BIBLIOTECAS FCYT-UADER. *Biblioteca de la Facultad de Ciencias y Tecnología*. Recuperado el 25 de enero de 2018, de http://bibliotecafcyt.uader.edu.ar/joomla/homepage/institucional-2.

Repositorio institucional de la UNLP. *Servidor virtual para detección de intrusos y ataques en ipv6.* Recuperado el 16 de noviembre de 2018, de http://sedici.unlp.edu.ar/bitstream/handle/10915/67211/Documento_completo.pdf-PDFA.pdf?sequence=1.

UADER. *Rectorado – UADER: Mapuche.* Recuperado el 25 de enero de 2018, de http://rectorado.uader.edu.ar/?page_id=49.

UADER. *Rectorado – UADER: ComDoc.* Recuperado el 25 de enero de 2018, de http://rectorado.uader.edu.ar/?page_id=37.