Redundancia de túnel para centralización de datos a través de VPN.

Pedro Luis López
Facultad Politécnica

Ciudad del Este - Paraguay
cde.luis@gmail.com

Junio - 2016

Resumen

El presente proyecto, implementó una alternativa para mejorar la disponibilidad de los datos de una empresa de porte media a grande centralizando servidores, mediante la implementación de una VPN por medio de radio frecuencias y respaldo de enlace vía Internet.
Los beneficios de esta implementación fueron inmediatos, ya sea con la reducción de costos de infraestructura, reducción de los gastos administrativos, y aumento de la resiliencia del servicio, entre otros.
Una conexión por medio VPN, permitió la centralización y el mejor manejo de la información, sin muchas dificultades para su mantenimiento, ni la necesidad de comprar equipamientos caros o complejos (servidores físicos tradicionales).
Centralizar los servidores ayudó en la administración de los mismos, redujo los costos y facilitó el manejo de los datos; además con la disminución de la cantidad servidores el respaldo se realiza en menor tiempo.
Para implementar esta infraestructura se hizo uso del sistema operativo RouterOS basado en GNU/Linux por su alta confiabilidad y su fácil administración por medio de un entorno gráfico, así como accesos vía Telnet, SSH y web; teniendo en cuenta lo citado, el enrutador Mikrotik utilizado en este trabajo se presenta en el mercado como una solución robusta, profesional y económicamente factible en comparación a otros enrutadores de otros fabricantes con similares prestaciones.

Descriptores: **1. VPN, 2. Mikrotik, 3. RouterOS.**

Abstract

The present project implemented an alternative to improve the availability of data on a medium-large enterprise, centralizing the servers through the implementation of a VPN by means of radio frequencies and backup link via Internet.
The advantages of this implementation were immediate, be it with the reduction of the costs in infrastructure, reduction of the administrative expenses and increase in the service resilience among others things.
A connection via VPN allowed the centralization and better management of the data without many complications for either its maintenance or the need to buy expensive or complex equipment (physical traditional servers.
Centralizing the servers helped in managing the servers themselves, reduced the costs and facilitates the data management; in addition, with the reduction of the quantity of servers the backup takes less time.
To implement this infrastructure it was made use of the RouterOS operating system based on GNU/Linux for its high reliability and its easy management through a graphical interface, as well as access via Telnet, SSH and Web, considering the aforementioned, the router Mikrotik is represented in the market as a strong solution, professionally and economically feasible in comparison to routers from other manufacturers with similar services.

Keywords: **1. VPN, 2. Mikrotik,, 3. RouterOS.**

1. Introducción

En la actualidad las redes informáticas, se han vuelto indispensables, tanto para las personas, como para las organizaciones, les da oportunidad de interactuar con el resto del mundo, ya sea por motivos comerciales, personales o emergencias.
Organizaciones con cientos de oficinas dispersas en una amplia área geográfica esperan de manera rutinaria poder examinar el estado actual incluso de la sucursal más distante con solo presionar un botón.
La aplicación de medidas de seguridad en las redes supone desplegar diversos productos: sistemas de detección de intrusos, controles de autenticación y autorización, cortafuegos y otros servicios. Habitualmente este despliegue se realiza utilizando productos y tecnologías de diferentes fabricantes. Cuando se habla de aspectos de seguridad, las empresas suelen seleccionar los produc-

tos con *pedigrí*: en cada categoría se selecciona siempre el producto con mayor renombre y mejor prensa. Esta es una tendencia que no parece cambiar a corto o medio plazo.
Esta disparidad de fabricantes origina diversas dificultades, como la problemática de gestión de los dispositivos (cada elemento de seguridad dispone de su propia aplicación de gestión), las dificultades para la interoperabilidad (los productos de seguridad tienen una mentalidad de funcionamiento aislado) y la centralización de la información generada.
Este último aspecto es posiblemente uno de los principales talones de Aquiles en virtualmente cualquier red con un mínimo nivel de complejidad. A medida que van aumentando los sistemas de seguridad, se reduce proporcionalmente la capacidad de poder disponer de una visión global del estado de la seguridad corporativa.
Ahora bien, en la red, esta visión global del estado de la seguridad no lo proporcionan únicamente los dispositivos tradicionales de seguridad, como son los cortafuegos y los sistemas de detección de intrusos. También otros muchos sistemas están generando una información vital para poder construir esta imagen: sistemas operativos, bases de datos, detectores de virus, servidores de archivos.
Ignorar estos datos sólo nos hará tener una visión distorsionada del estado de la seguridad. De hecho, son más importantes aquellas informaciones que nos puedan transmitir los otros elementos, que son clave para el funcionamiento de la empresa.
Y existe otro factor, de una importancia notable: esta visión debe ser generada en tiempo real. No importa cuántos dispositivos tengamos, ni su dispersión geográfica o los diferentes métodos que tengan para representar las alertas. La visión del estado de la seguridad estará totalmente distorsionada si esta no se genera en tiempo real.
Una vez que dispongamos de las informaciones de seguridad centralizadas, podemos aplicar reglas de correlación. De esta forma podemos identificar tendencias y similitudes en los posibles ataques que reciba la red. Con la información que se obtiene de la correlación, los equipos de seguridad pueden responder rápidamente ante un incidente, ajustando sus sistemas para ofrecer la respuesta adecuada ante el ataque (desactivar una determinada dirección, reforzando las medidas de seguridad de los sistemas más expuestos a ataques).
Otra ventaja en disponer de toda la información relativa a seguridad centralizada es la facilidad en la generación de informes, que nos presenten los diferentes ataques que sufren nuestra infraestructura, el status de las diferentes líneas de negocio, el tiempo de respuesta ante los incidentes, etc. Esta información será básica para evaluar la idoneidad de las medidas de seguridad existentes y en la justificación de las inversiones necesarias. [3].

1.1. Importancia del tema.

La elaboración de este trabajo obedece a la necesidad de satisfacer las necesidades de centralizar los servidores, con la finalidad de unificar la red y por ende los datos e informaciones de suma sustancialidad para una empresa.
En este sentido se propone dotar al sistema de una infraestructura sólida, segura y económica mediante el uso de radio enlaces entre sucursales de una empresa ya sea de medio o grande porte, teniendo como respaldo el uso de VPNs[6] a fin de garantizar la comunicación del servicio aumentando su resiliencia, y por lo tanto la robustez del enlace, y contribuyendo con la seguridad de los datos, el activo primordial de toda empresa u organización.

1.2. Objetivos.

Implementar una infraestructura de redundancia de enlaces por medio de VPNs para la centralización de servidores.

1.3. Discusión de literatura relevante.

Las empresas de medio/grande portes en Paraguay, a fin de optimizar sus infraestructuras y sus recursos económicos, se ven obligados a buscar alternativas a los medios recurrentes tales como fibras ópticas, satélites o servicios de banda ancha. Ya que en

muchas localidades servicios no se encuentran disponibles por el alto costo que implica su cobertura para las operadoras. Por tales motivos soluciones robustas como el uso de radio enlaces utilizando espectros libres, son una opción ideal.
Debido a factores imprevisibles como inclemencias del tiempo, hurtos u hechos vandálicos, se propone respaldar la conexión por medio de VPNs via internet a fin de dar mayor estabilidad a la comunicación.
Además desde el punto de vista económico, la centralización de los servidores acarrea un menor costo de implementación y mantenimiento, ya que por ejemplo para una empresa con treinta sucursales se ahorraría el costo de contar con servidores para cada local, lo que a su vez denota un ahorro tanto en simplicidad de mantenimiento como en el costo del recurso humano necesario para su correcto funcionamiento.

1.4. Hipótesis

El desarrollo de este proyecto puede generar tanto beneficiarios directos como indirectos. Por el lado de los beneficiarios directos tenemos a los funcionarios TI al facilitar la administración de la red.
Por otro lado, como beneficiarios indirectos se pueden mencionar a los funcionarios de las sucursales, por mejorar la continuidad del servicio.
Además de que dicho proyecto, puede servir de base para la generación de una empresa de servicios para brindar seguridad en redes a cualquier tipo de entidad sea cual fuere su tamaño.

2. Método.

De acuerdo a los objetivos definidos en este trabajo de investigación, se decidió trabajar en base al enfoque cuantitativo, para verificar la disponibilidad de conexión entre los equipos sea por el túnel sobre el radio enlace o por medio del túnel vía Internet.
Partiendo de los objetivos generales establecidos previamente, se ha estudiado con un enfoque más técnico para el desarrollo de la presente investigación y se han definido el universo de casos contemplados para el mismo. Por cuanto, la herramienta de prueba realizara pruebas disponibilidad es el Ping [4], así como para conocer el trayecto que esta tomando la conexión se utilizo el Tracerouter[9], y el Bandwidth Test del RouterOs [7] para verificar la tasa de transferencia [10] entre los equipos.

2.1. Variables y dimensiones

Se definió la siguiente variable, *Lista de rutas intermedios* y *Tiempo de respuesta*, con una dimensión de comparación de resultados entre ambas tecnología y contando como indicador a las diferencias encontradas entre las distintas tecnologías, ventajas y desventajas. De esta forma se realizo el análisis de los datos obtenidos y se midieron las diferencias entre los ping sobre los distintos tuneles.

2.2. Instrumentos.

Fueron utilizados para la prueba la aplicación Traceroute, que realizo pruebas del trayecto que tomaban los equipos para llegar de un punto a otro, periodo en el cual las aplicaciones Bandwidth Test y Ping realizaron capturas de métricas del rendimiento del túnel. De esta manera tanto la prueba como la recolección de datos fueron realizadas por aplicaciones especializadas, lo que permite el análisis de datos con la confianza respaldada por otros software.

2.3. Procedimientos.

Para realizar este trabajo se ha utilizado se configuró un enlace [8] entre dos enrutadores con placa wireless 5.8 Ghz , dos entutadores un servidor y un cliente discador para el túnel que se configuro sobre el enlace, estos dos enrutadores tenían placa wireless 2.4 Ghz el cual permitió conectar a un celular con la zona portátil activada [5], se configuró un segundo túnel sobre esta conexión el cual esta en modo espera y solo asume cuando el túnel primario no esta disponible. Desde maquina que estaban conectados a los enrutadores, se realizo pruebas de Ping y Traceroute para ver la disponibilidad de la conexión.

3. Resultados.

Se dividen en 4 puntos: *Pruebas de tasa de transferencia*, *Rutas por defecto*, *Ping*, *Traceroute*.

3.1. Prueba de tasa transferencia

Rendimiento obtenido con métricas de Carga general del enlace.

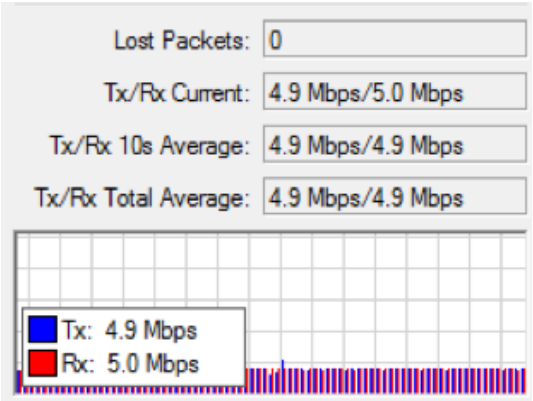

Figura 1: Prueba de tasa de transferencia de los enlaces

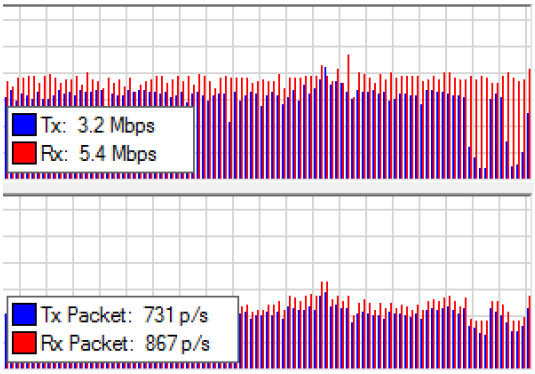

Figura 2: Prueba de tasa de transferencia de los enlaces

3.2. Rutas por defecto

Las rutas secundaria activada y la otras rutas en modo de espera.

DAS	0.0.0.0/0	192.168.43.1 reachable wlan1
DC	10.0.0.0/24	ether1 unreachable
DAC	12.0.0.1	vpn2 reachable
S	192.168.0.0/24	11.0.0.1 unreachable
AS	192.168.0.0/24	12.0.0.1 reachable vpn2
DAC	192.168.1.0/24	ether3 reachable
DAC	192.168.43.0/...	wlan1 reachable

Figura 3: Ruta por defecto inactivo

En Negro: las puertas de enlaces que están activas.
En Azul: las puertas de enlaces que están inactivas activas.

3.3. Ping

Prueba de estabilidad de ping a al enrutador que realiza el enlace.

```
C:\Users\ect2015_wp>ping 10.0.0.3

Haciendo ping a 10.0.0.3 con 32 bytes de datos:
Respuesta desde 10.0.0.3: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.0.0.3: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.0.3: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.0.0.3: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 10.0.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Figura 4: Ping desde la maquina al enrutador de la sucursal

Prueba de estabilidad de la conexión de las maquinas por medio del IP secudario configurado para tener acceso a las radios.

```
C:\Users\ect2015_wp>ping 10.0.0.101

Haciendo ping a 10.0.0.101 con 32 bytes de datos:
Respuesta desde 10.0.0.101: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.0.0.101: bytes=32 tiempo=11ms TTL=128
Respuesta desde 10.0.0.101: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.0.0.101: bytes=32 tiempo=15ms TTL=128

Estadísticas de ping para 10.0.0.101:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 15ms, Media = 7ms
```

Figura 5: Ping desde la maquina de la sucursal a la maquina de la central por medio de tunel

3.4. Traceroute

Traceroute permite obtener la ruta mas probable que siguen los paquetes IP desde un origen IP. Es decir, devuelve una lista con los enrutadores intermedios existentes entre los dos equipos.

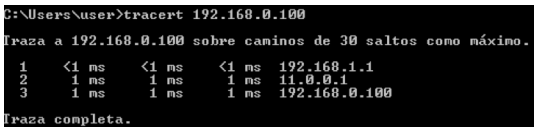

Figura 6: Camino trazado por medio del radio enlace

Con el enlace funcionando, al hacer el traceroute desde la maquina de la sucursal a la central, esta muestra que pasa por el MK4 después llegando al enrutador MK1 por medio del túnel hecho sobre el enlace pues la faja de ip es el 11.0.0.1

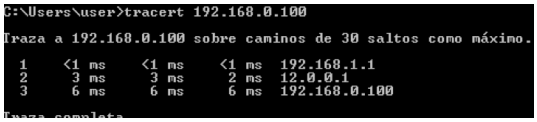

Figura 7: Camino trazado por medio del Internet

Con el enlace fuera de linea asume el túnel por medio del internet, al hacer el traceroute desde la maquina de la sucursal a la central, esta muestra que pasa por el MK4, después llegando al enrutador MK1 por medio del túnel hecho sobre el internet pues la faja de IP es el 12.0.0.1

4. Discusión.

El modelo de infraestructura que responde de manera más práctica y eficiente para la centralización de datos es utilizando VPN a través de radio enlaces y reforzando con enlaces de internet.
Los equipos hardware y software utilizados para la implementación de la centralización de datos a través de VPN responden de manera eficiente al costo beneficio, la marca Mikrotik es mucha más barata que otras tecnologías de su competencia.Presenta la robustez necesaria para los radios enlaces.
La cantidad de recursos humanos necesarios y el orden de desarrollo del trabajo para la implementación de la centralización de datos a través de VPN fueron evaluados y demostraron ventajas en costos beneficios. Antes se necesitaba si o si una persona de TI por cada local, con la implementación de la centralización ya no existe esa necesidad. Además, se economiza los costos de la locomoción.
Las recomendaciones para tener una seguridad mínima en la centralización de los datos a través de VPN es la administración eficiente de las mismas, ya que todos los equipos reúnen las condiciones necesarias para la implementación de la seguridad.
Las 21 filiales anexadas a la central y la administración de la mismas de manera remota genera una gran economía a la empresa y es un modelo replicable a otras empresas que buscan mejor infraestructura para la administración de su información. Se recomienda la instalación de enlaces con equipamientos RouterBoard por la practicidad, robustez y economía.

Referencias bibliográficas.

[1] ¿Qué es una VPN? *pctripsesp.com.* `http://www.pctripsesp.com/images/PCtripsesp/VPN/VPN.png`

[2] Escuela Policteсnica Nacional - Peru, “Diseño de un sistema de seguridad informática para la red lan de telecomunicaciones del ministerio de minas y petroleos” `http://bibdigital.epn.edu.ec/bitstream/15000/4662/1/CD-4294.pdf`

[3] La importancia de centralizar la información de seguridad a nivel corporativo. `http://www.recursos-as400.com/tendenciesit004.shtml`

[4] Internet Control Message Protocol `https://tools.ietf.org/html/rfc792`

[5] ¿Qué es la zona WIFI portátil y cómo la uso en mi Samsung Galaxy S4? `http://www.samsung.com/ar/support/skp/faq/874655`

[6] The Internet Protocol Journal `http://www.cisco.com/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html`

[7] Bandwidth Test Connection throughput evaluation tool `https://www.mikrotik.com/testdocs/ros/3.0/tools/btest.phpl`

[8] RadioLAN 5.8GHz Wireless Interface https://www.mikrotik.com/testdocs/ros/3.0/interface/radiolan.php

[9] Cómo utilizar TRACERT para solucionar problemas de TCP/IP en Windows https://support.microsoft.com/es-es/kb/314868

[10] Ermanno Pietrosemoli, "Redes Inalambricas en los paises en desarrolo", 4ta ed., Jane Butler, networktheworld.org, 2013, pp. 35.