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

Pedro Luis López
Facultad Politécnica

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

Marzo - 2016

Resumen

El presente proyecto, propone plantear una alternativa para mejorar la seguridad de los datos de una empresa media-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 serían 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, permitirá 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 ayudará en la administración de los mismos, reducirá los costos y facilitará el manejo de los datos; además con la disminución de servidores el respaldo se hará en menos tiempo.
Para implementar esta infraestructura se propone el 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 se presenta en el mercado como una solución robusta, profesional y económicamente factible.

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

Abstract

The present project proposes an alternative to improve the security 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 would be immediate, be it with the reduction of the costs in infrastructure, reduction of the administrative expenses and increase in the resilience of the service among others.
A connection via VPN will allow the centralization and best management of the data without many complications for its maintenance nor the need to buy expensive or complex equipment (traditional physical servers).
Centralizing the servers will help in managing them, reduce the costs and facilitate the data management; in addition, with the reduction of servers the support will take less time.
To implement this infrastructure is intended the use of the Operative System RouterOS 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, professional and economically feasible.

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 productos 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, sistemas ERP.
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. [9]

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 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.

1.2.1. Objetivo General.

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

1.2.2. Objetivo Específicos.

- Estudiar tecnologías y metodologías para el desarrollo del proyecto.
- Realizar un radio enlaces.
- Configurar VPNs.
- Configurar conexión respaldo por medio de Internet.
- Realizar pruebas de conexión entre máquinas/clientes y servidores.

1.3. Discusión de literatura relevante.

Es apropiado discutir la literatura relevante relacionada con el problema tratado en el artículo, de manera concisa. Se debe asumir que el lector tiene un conocimiento básico del problema y no requiere una revisión exhaustiva. Una discusión de trabajos previos relevantes provee un resumen de los trabajos más recientes en el area. Debe incluirse la citación y el crédito a trabajos consultados. En la descripción de la literatura relevante se debe informar al lector si otros aspectos del trabajo en presente fueron reportados previamente y cómo el uso actual de la evidencia difiere del uso anterior.

Se debe demostrar continuidad lógica entre trabajos anteriores y el trabajo actual. El problema debe ser desarrollado con suficiente claridad para ser entendido de una manera general por la mayor cantidad posible de profesionales relacionados al área de estudio.

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.

1.5. Referencias al final del texto.

La presente plantilla se basa en el modelo IMRyD tomado de [2]. Para los artículos de las llamadas “ciencias exactas”, así como para los de divulgación tecnológica, el estándar de referenciación bibliográfica emplea el estilo IEEE Computer, i.e, una lista numerada al final del artículo y referenciada en el texto por números entre corchetes (e.g. “[1]”). Véanse los ejemplos de citas al final de este documento [1].

Deben incluirse referencias a materiales publicados y accesibles al público. Entre los reportes técnicos de Internet deben ser citados preferentemente aquellos que sean fácilmente accesibles y obtenibles por el lector [3, 5].

Las referencias deben ser claras y lo más completas que sea posible, nombrando siempre al autor o generador de la fuente del documento, como también la fecha (al menos aproximada) de su generación, refiriéndose a materiales ya publicados, ejemplos [3, 4, 5]. A libros publicados, ejemplos [6, 7]. A documento electrónico en la Web, ejemplo [8].

La lista de referencias debe titularse: “Referencias bibliográficas.” seguido de las referencias propiamente dichas como los ejemplos al final de este documento. Las fuentes bibliográficas consultadas pero no citadas en el texto se deben colocar al final de las referencias citadas como “Bibliografía complementaria” y se deben numerar de la misma forma.

2. Método.

La sección del método describe en detalle cómo fue llevada a cabo la investigación, incluyendo definiciones operacionales de las variables involucradas. Distintos tipos de investigaciones se basan en distintas metodologías, es fundamental que la metodología utilizada sea apropiada para el problema planteado y para el tipo de datos que estén siendo procesados; una completa descripción del método utilizado posibilita al lector evaluar cuán apropiado fue el método empleado y la confiabilidad y la validez de los resultados. Por otro lado, posibilita a los investigadores experimentados replicar el estudio.

Si el trabajo en cuestión es una actualización de una investigación en curso o pasada y el método fue publicado en otro lugar, se puede referir al lector a esa fuente o simplemente proveer una breve sinópsis del método. Debe tenerse en cuenta que no siempre es posible identificar una sección "Método" en un artículo. Cuando se trabaja un estudio empírico debe existir esta sección y debe ser muy rigurosa. Sin embargo, cuando se trabajan artículos teóricos, principalmente en ciencias sociales, puede aplicarse triangulación entre varios métodos.

Cuando se trate de investigaciones de ciencias físicas y matemáticas o de investigación aplicada de ingeniería suele ser necesario el empleo de entornos enunciados y numerados tales como teoremas y ecuaciones, en estos casos es de fundamental importancia el empleo del entorno LaTeX u otra herramienta de composición de documentos científicos con capacidad de gestión automática de numeración y contadores que posibiliten su adecuada referenciación cruzada como en los siguientes ejemplos (teorema 1 y Ec. 1):

Teorema 1 (Teorema de Pitágoras)**.** *El cuadrado de la hipotenusa es igual a la suma del cuadrado de los catetos:*

$$hip^2 = cat_1^2 + cat_2^2 \tag{1}$$

Es conveniente dividir la sección del método en subsecciones, que deben incluir la información esencial para comprender y replicar la investigación. Detalles insuficientes pueden dejar al lector con preguntas sin respuesta; en cambio excesivos detalles lo pueden sobrecargar con información irrelevante.

2.1. Participantes

Si el artículo se refiere a una investigación sobre sujetos, una apropiada identificación de los sujetos participantes de la investigación es crítica particularmente para la generalización de resultados y para realizar comparaciones entre diversas réplicas de un estudio. Se deben incluir detalles descriptivos de la muestra, como su tamaño, poder y precisión. Las conclusiones y las interpretaciones no deben ir más allá de lo garantizado por la muestra. Cuando se aplica estadística inferencial, se debe tomar seriamente el poder estadístico de las condiciones asociadas con la prueba de hipótesis.

2.2. Diseño de la investigación.

Debe especificarse el diseño de la investigación. Tratándose de investigación científica debe decirse si fue experimental o no, si qué nivel de profundización posee: exploratorio, descriptivo o explicativo. Tratándose de investigación tecnológica se debe describir el diseño del producto, servicio o innovación tecnológica de que se trate.

2.3. Instrumentos.

En la sección del método debe incluirse información acerca de las medidas, incluso si algunas de estas no fueren analizadas en el trabajo. Es fundamental que se mencionen los métodos empleados para recolectar la información, los instrumentos utilizados y la evidencia de su validez.

2.4. Procedimientos.

El procedimiento es al método lo que el paso es al procedimiento. Esto se refiere a la granularidad o grado de detalle de la descripción metodológica y quiere decir que el método suele constar de varios procedimientos y cada procedimiento de varios pasos.

En este apartado deben explicarse en detalle los algoritmos, las técnicas y los pasos procedimentales; las manipulaciones o intervenciones que se hubiesen realizado en el estudio. Deben incluirse los detalles de las intervenciones y manipulaciones a cada una de las variables o condiciones, incluyendo grupos control (si hubieren) y debe explicarse cómo y cuándo se realizaron las manipulaciones o intervenciones. El tiempo gramatical de la descripción típicamente es el pretérito simple.

3. Resultados.

En esta sección debe resumirse la información recolectada y el análisis realizado sobre los datos relevantes. La información debe ser reportada con el suficiente nivel de detalle para justificar las conclusiones. También en esta sección usualmente se emplea el tiempo gramatical pretérito simple. Deben mencionarse todos los resultados relevantes, inclusive aquellos que contradigan las expectativas iniciales. Deben asimismo incluirse los hallazgos no significativos aún cuando la teoría prediga hallazgos estadísticamente significativos. Solo deben incluirse puntajes individuales e información en intermedia, cuando se trate de un diseño de caso único o de ejemplos ilustrativos. El análisis de datos y el reporte de resultados de análisis son aspectos fundamentales de una investigación. Un reporte preciso, completo y sin sesgos del tratamiento analítico de datos (sean cuantitativos o cualitativos) es un componente fundamental de un artículo científico.

Para que el lector pueda apreciar la magnitud o importancia de los hallazgos de un trabajo, es casi siempre necesario incluir alguna medida del tamaño del efecto. Cuando sea posible, debe proveerse un intervalo de confianza para cada tamaño del efecto reportado con el objetivo de indicar la precisión de la estimación de dicho tamaño. Debe asumirse que el lector tiene conocimiento profesional de los métodos estadísticos tipificados en caso de que estos sean empleados. Los resultados clarifican por qué ha sido empleado el método descripto.

Utilidad de los gráficos y tablas (cuadros).

En la sección de resultados es notablemente útil la inclusión de soportes visuales para mejorar la comprensión de los datos. Si a través del estudio se ha generado diferentes presentaciones gráficas de los datos, deben seleccionarse para ser mostradas las más representativas. Se deben observar los lineamientos para la confección de cada tipo de presentación gráfica, por lo general basta incluir hasta tres objetos gráficos.

Las figuras y tablas deben insertarse en el punto apropiado dentro del texto. Cada figura debe estar seguida de un epígrafe que la identifique y numere. Cada figura debe ser citada al menos una vez a través de su número, como ilustración del código LaTeX y su apariencia, se presenta la Figura **??**, preferentemente antes de su aparición en el documento.

Se recomienda que las figuras sean en blanco y negro para facilitar su impresión en papel con tinta negra.

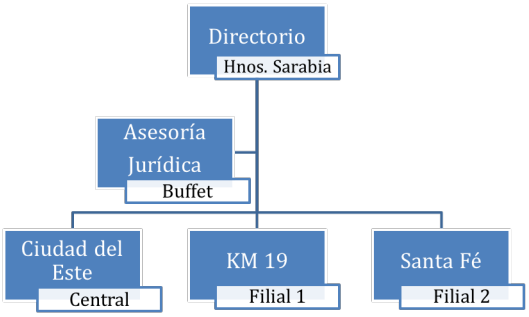

Figura 1: Organigrama de la Empresa

Igualmente, cada tabla debe estar encabezada por un epígrafe situado en su parte superior que la numere y describa. La tabla debe contener datos representativos que sinteticen información significativa del trabajo, evitando mostrar datos intermedios que pudieran dificultar la interpretación del mismo. Cada tabla debe ser referenciada al menos una vez, a través de su número, como ilustración del código LaTeX y su apariencia, se presenta la tabla 1.

Tabla 1: Ejemplo de tabla incluida.

Denominación	Sexo	Cantidad
Jeruti	hembra	20
	macho	18
Mborevi	hembra	5
	macho	5
Apere'a	hembra	50
	macho	50
Total		148

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 como Cisco. 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] J. Demasi, Formato IEEE. Estilo y Referencias Bibliográficas. Instituto de Ingeniería Eléctrica (IIE), Facultad de Ingeniería, Universidad de la República. `http://iie.fing.edu.uy/institucional/biblioteca/presentaciones/Citas-IEEE-2011.pdf`

[2] Departamento de publicaciones. Guía Introductoria de Redacción Científica. *Asociación para el avance de la ciencia psicológica (AACP).* `http://www.cienciapsicologica.org`

[3] J. F. Fuller, E. F. Fuchs, and K. J. Roesler, "Influence of harmonics on power distribution system protection", IEEE Trans. Power Delivery, vol. 3, pp. 549-557, Apr. 1988.

[4] E. H. Miller, "A note on reflector arrays", IEEE Trans. Antennas Propagat., to be published.

[5] R. J. Vidmar. (1992, Aug.). "On the use of atmospheric plasmas as electromagnetic reflectors", IEEE Trans. Plasma Sci. [Online]. 21(3), pp. 876-880. Dis-

ponible en línea: http://www.halcyon.com/pub/journals/21ps03-vidmar

[6] E. Clarke, "Circuit Analysis of AC Power Systems", vol. I. New York: Wiley, 1950, p. 81.

[7] G. O. Young, "Synthetic structure of industrial plastics", in Plastics, 2nd ed., vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15-64.

[8] S. L. Talleen. (1996, Apr.), "The Intranet Architecture: Managing information in the new paradigm", Amdahl Corp., Sunnyvale, CA. [Online]. Disponible en línea: http://www.amdahl.com/doc/products/bsg/intra/infra/ 12/08/08.

[9] Recursos-as400. (2003, Feb.), "La importancia de centralizar la información de seguridad a nivel corporativo.", [Online]. Disponible en línea: http://www.recursos-as400.com/tendenciesit004.shtml 11/03/16.