IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Mecanismos de seguridad

"Servidor de protección perimetral de bajo costo"
"Low cost perimeter protection server"

Ing. Rodrigo Fernández Triana[1]

Resumen
La presente investigación propone una solución de *hardware* y *software* para servidores de protección perimetral destinados a proporcionar conectividad segura a usuarios remotos en redes corporativas. Para ello se estudiaron diferentes alternativas de codificación, cortafuegos, redes privadas virtuales y microcomputadoras. El criterio fundamental era lograr una solución de bajo costo y basada en *software* de código abierto. Sobre la base de este estudio se propone una solución de un servidor de protección perimetral conformado por una microcomputadora Raspberry Pi B+ v1.2 como soporte de *hardware* a un sistema de VPN SoftEther empleando tecnología de túnel criptográfico basado en IPsec. En las pruebas realizadas se demostró la viabilidad de esta propuesta de solución. Se recomienda analizar la conveniencia de extender el empleo de servidores de protección perimetral en las redes de entidades nacionales y Organismos de la Administración Central del Estado (OACE).

Palabras claves:
Redes de Datos, Modelo OSI, Seguridad informática, Servidor de protección perimetral, *firewall*, Red Privada Virtual (VPN), SoftEther, microcomputadora Raspberry Pi.

Abstract
This research proposes a hardware and software solution for perimeter protection servers aimed at providing secure connectivity to remote users in corporate networks. For this, different alternatives for coding, firewalls, virtual private networks and microcomputers were studied. The fundamental criterion was to achieve a low-cost solution based on open source software. Based on this study, a perimeter protection server solution is proposed, consisting of a Raspberry Pi B v1.2 microcomputer as hardware support for a SoftEther VPN system using cryptographic tunnel technology based on IPsec. In the tests carried out, the feasibility of this proposed solution was demonstrated. It is recommended to analyze the convenience of extending the use of perimeter protection servers in the networks of national entities and Central Administration of the State Agencies (OACE).

Keywords:
Data Networks, OSI Model, Computer security, Perimeter Protection Server, Firewall, Virtual Private Network (VPN), SoftEther, Raspberry Pi microcomputer.

[1] Ministerio del Interior, rodfertri@gmail.com

Introducción

En la actualidad las redes de transmisión de datos se han convertido en una herramienta esencial para la gestión y funcionamiento de las organizaciones.

Desde el punto de vista de seguridad de la información, estas redes van desde las muy abiertas e inseguras como Internet, a redes muy seguras y cerradas como las empleadas por organizaciones militares, de seguridad o bancarias, por sólo mencionar algunas.

En Cuba existen redes corporativas pertenecientes a Organismos de la Administración Central del Estado y entidades nacionales para el almacenamiento, transporte y gestión de su información.

En algunas de estas entidades, debido a la naturaleza sensible de su información, es necesario establecer medidas técnicas y organizativas para la protección de la misma.

Estas redes están formadas por un conjunto de nodos principales, los que generalmente radican en la sede central de la entidad. En estos nodos es donde reside la información más importante de la organización, así como los servidores proveedores de los servicios.

En estos casos se debe implementar protocolos de codificación y cifra que permitan establecer comunicaciones seguras entre estos nodos principales de la red, los cuales son asegurados por servidores de protección perimetral (SPP), entre otros mecanismos.

Adicionalmente, muchas de estas entidades poseen usuarios en localidades remotas que tienen acceso a la red corporativa y no siempre cuentan con los niveles de seguridad comparable a la de los nodos principales.

Las soluciones comerciales, que incluyen *hardware* y *software*, para proveer conectividad a estos usuarios remotos con la seguridad requerida son muy costosas y al ser propietarias su utilización crea una dependencia tecnología con esos proveedores.

Además, las pocas soluciones disponibles comercialmente requieren licencias para su explotación, y no están a nuestro alcance debido al bloqueo de los EE. UU contra Cuba.

Es por ello que surge la necesidad de implementar soluciones de *hardware* y *software* de bajo costo, que garanticen los niveles de seguridad requeridos para establecer una comunicación segura y eficiente entre los nodos principales y remotos de una red corporativa.

La presente investigación consiste en comprobar la viabilidad de implementar un servidor de protección perimetral de bajo costo mediante el empleo de una microcomputadora Raspberry Pi B+ v1.2 como soporte de hardware a un sistema de VPN SoftEther empleando tecnología de túnel criptográfico basado en IPsec.

Protección Perimetral

Uno de los conceptos más importantes en la seguridad informática es el de protección perimetral. [1]

La protección perimetral es un método de defensa de red, que se basa en el establecimiento de recursos de seguridad en el perímetro de la misma y a diferentes niveles. Ello permite controlar el acceso de usuarios internos o externos a determinados servicios, y denegar cualquier tipo de acceso a otros, mediante la definición de niveles de confianza [2]. (Ver Figura 1)

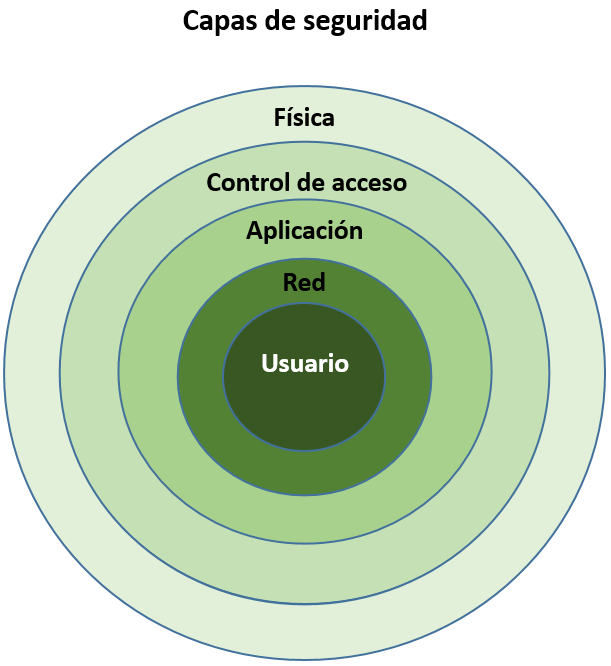

Figura 1

La protección perimetral tiene como objetivos:

- Rechazar conexiones a servicios que han sido comprometidos.
- Permitir solo ciertos tipos de tráficos (correo electrónico, servidores de ficheros, etc.).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el trafico entrante a los sistemas adecuados dentro de la intranet.
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde internet [*].
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, cuentas de usuario internos, etc.

Dentro de la protección perimetral, un concepto muy importante es el de *Perímetro de la Red*, que es la frontera entre el exterior y las computadoras y servidores internas. Este se forma por los equipos que brindan conexión a internet a las computadoras de la red, así como aquellos que la protegen de accesos externos. Equipos como pasarelas (*gateways*), *firewall*s y *proxys* forman parte de este perímetro. (Ver Figura 2) [3][4]

[*] En el presente trabajo la referencia a Internet incluye a otras redes públicas de alcance menor, tales como las redes corporativas.

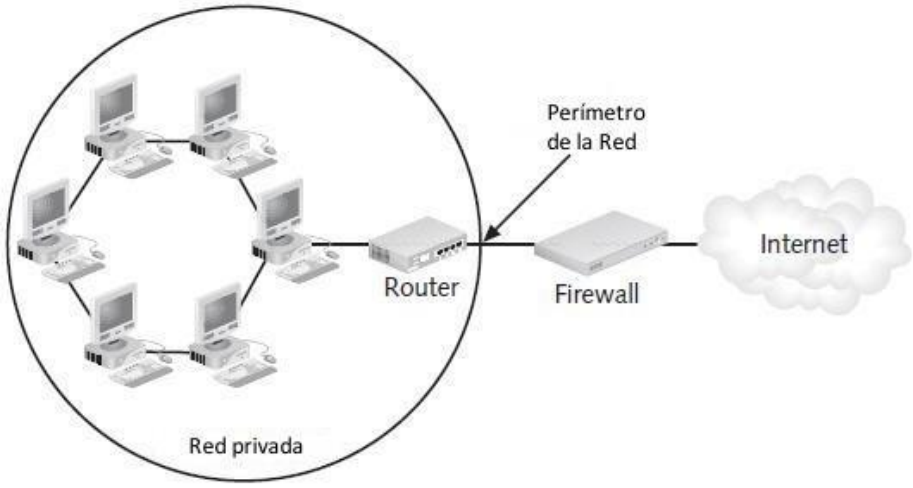

Figura 2

Análisis de Firewall, VPN y microcomputadoras de bajo costo

Firewall

En general, un cortafuego (del inglés *firewall*) es un elemento de seguridad que filtra la transmisión de información mediante paquetes digitales mientras viajan entre redes. [3] [5] [6] [7]

Los *Firewall* realizan dos funciones fundamentales de seguridad:

- **Filtrado de paquetes:** Determinan si permiten o deniegan el paso de paquetes, basados en reglas y políticas de seguridad.
- **Proxy de aplicaciones:** Proveer un servicio de red a los usuarios locales mientras protege los *hosts* individuales del tráfico del exterior de la red.

A medida que el uso de los *Firewall* se extendía, los desarrolladores de los mismos fueron añadiendo componentes de seguridad más avanzadas, [8] tales como:

- Registrar los accesos que entraban y salían de la red. Tanto los **no autorizados** como los autorizados.
- Proveer un enlace empleando VPN, (concepto que será abordado en la próxima sección), que permite conectar dos redes separadas geográficamente como si estuvieran conectadas físicamente.
- Autenticar los usuarios para que puedan ser identificados y si corresponde brindarles acceso a la red y a los servicios.
- Proteger y ocultar a los usuarios (*host*) que se encuentran dentro de la red de posibles intentos de *escaneos* (exploración) o ataques por parte de terceros.
- Filtrar el contenido que se considere inapropiado para la entidad en cuestión o ficheros peligrosos (ej. ejecutables dentro de un anexo de correo electrónico).

Una de las mejores características del *firewall* es que funcionan empleando reglas. Éstas definen cual será el objetivo del mismo, en que se va a enfocar, que tráfico y de donde se va a permitir.

Los *firewalls* supervisan los puntos de entrar y salida (llamados puertos en el modelo TCP/IP) y analizan si son empleados para el contenido al que fue destinado. Por ejemplo, el contenido web típicamente viaja mediante el puerto 80. Esto permite cumplir un criterio de seguridad donde la información puede ser analizada y se le permite que pase o no en dependencia de donde vino y hacia donde va. [9] [10]

Este análisis constante de la información trasmitida permite también detectar accesos que, a pesar de ser legales en cuanto a contenido, origen y usuario con permisos de acceso, puede que no cumplan medidas organizativas, como el no empleo de la red en ciertos horarios no institucionales. En este ejemplo el *firewall* puede ser configurado para enviar alertas en forma de mensajes o correos a los encargados de la seguridad.

Componentes de un *Firewall*

Un *firewall* es solo uno de los múltiples componentes de un sistema de seguridad informática. Los sistemas más eficientes de protección empleados por las grandes redes corporativas emplean no solo uno, sino múltiples *firewall*s. Los combinan con *routers* y otros componentes de red para delinear zonas de confianza en una subred, conocidas como una zona desmilitarizada (DMZ), que se posiciona entre la red interna y el mundo exterior. (Ver Figura 3) [11]

Esto se combina con el empleo de un *host* bastión, o sea un *host* con los servicios mínimos imprescindibles, como puede ser un servidor de correo, y un sistema de *firewall*. Al emplearse con una DMZ y conectarse a internet, se limita la interacción de la red interna con una red externa limitando incidentes y amenazas.

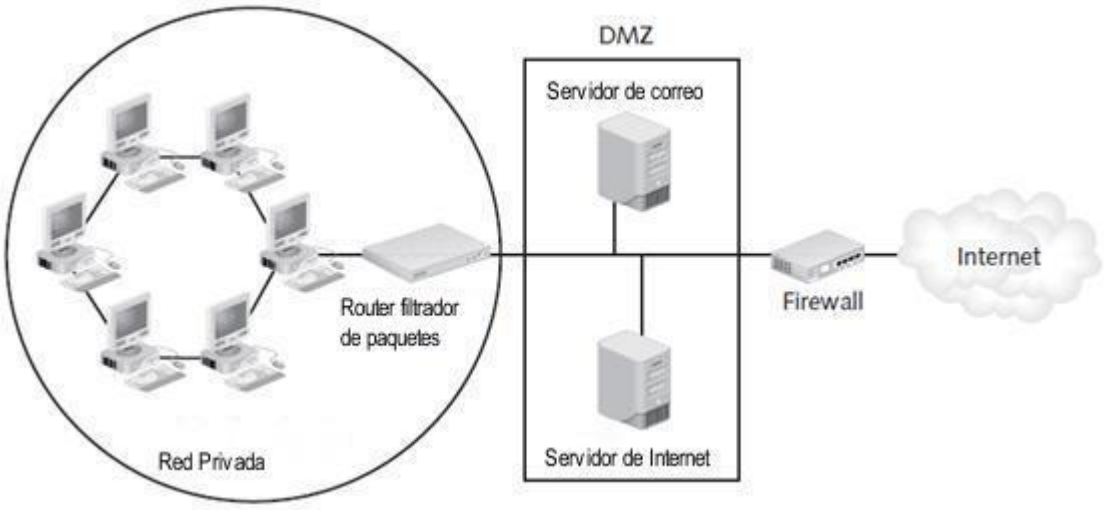

Figura 3

Red Privada Virtual (VPN)

Las VPN, *Virtual Private Networks* (Redes Privadas Virtuales) son comúnmente empleadas para interconectar redes independientes mediante internet y así permitir a los usuarios enviar y recibir datos de forma seguro entre las redes que se encuentran ubicadas en otras ubicaciones geográficamente.

Las conexiones VPN pueden ser empleadas, por ejemplo, entre dos sitios remotos de la organización (VPN de sitio-a-sitio) o entre un usuario y la organización (VPN de punto-a-punto). [3] [5] [6]

Las VPN de sitio-a-sitio les permite a las organizaciones interconectar sus oficinas mediante una red (puede ser internet o en el caso de que la organización tenga su propia red corporativa), ahorrando recursos y siendo más flexibles que construir una conectividad física dedicada a esta comunicación a larga distancia. Cuando dos sitios se conectan con VPN, las computadoras y los usuarios en ambos sitios se pueden conectar entre sí de forma segura, y pueden compartir los recursos de un sitio al otro. (Ver Figura 4)

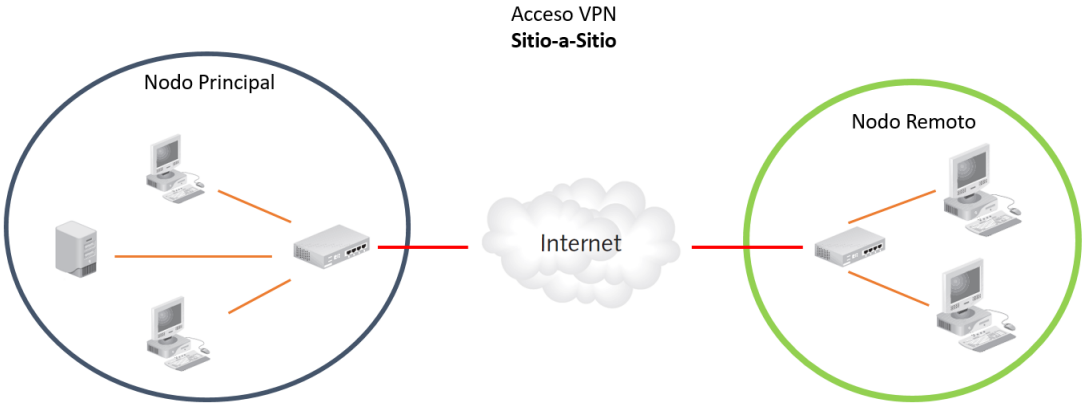

Figura 4

Las VPN de punto-a-punto son usualmente empleadas por los usuarios, que necesitan acceder de forma segura a los recursos en la red privada de la organización desde el exterior de la misma red. Este tipo de conexión permite a los usuarios trabajar desde el hogar u otras ubicaciones remotas, por lo que las VPN punto-a-punto son muy empleadas por todo tipo de entidades, empresas y organizaciones. (Ver Figura 5)

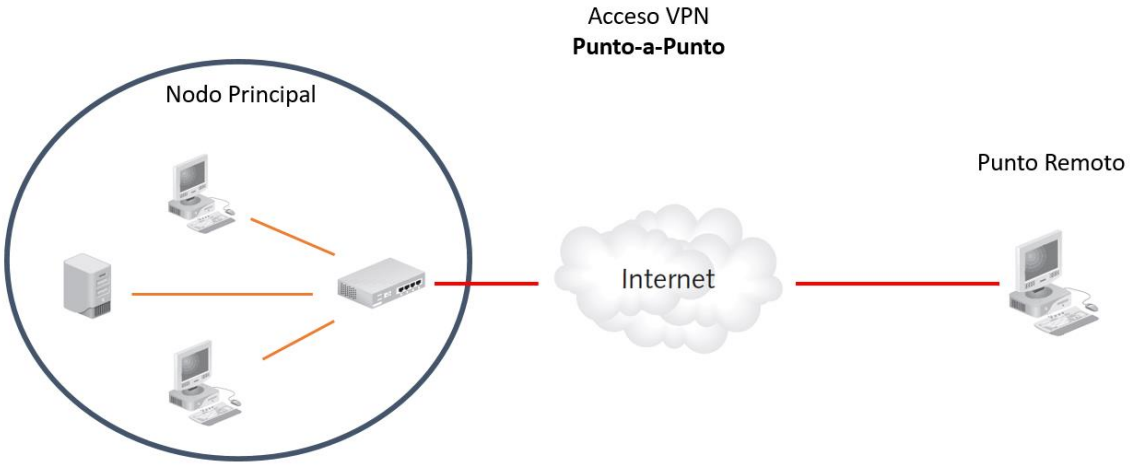

Figura 5

Usualmente, el propósito de una conexión VPN es de asegurar la autenticidad, integridad y confidencialidad del tráfico de la red. Cuando estos tres conceptos son cumplidos se puede afirmar que la conexión es privada y segura, lo que significa que los atacantes no podrán intervenir la comunicación, ni modificarla ni robar información de la misma.

Para garantizar la autenticidad, integridad y confidencialidad se emplean diferentes técnicas de túnel de VPN.

Soluciones de Código Abierto

El mercado de soluciones VPN de código abierto está dominado por dos protocolos: OpenVPN e IPsec. [12]

OpenVPN se enfoca más en sistemas con acceso VPN de Punto a Punto donde IPsec es usualmente empleada para conexiones de tipo sitio-a-sitio y su implementación es compatible con la mayoría de las soluciones comerciales.

SoftEther

SoftEther es un *software* de VPN de código abierto resultado de un proyecto académico de la Universidad de Tsukuba, Japón. Fue desarrollado por Daiyuu Nobori en el 2014. A pesar que lleva varios años desde su publicación, SoftEther no es muy conocido fuera de Asia, al existir pocos documentos de investigación o recursos escritos en español o inglés. [13]

La versión 1.0 de SoftEther era un proyecto sencillo trabajando en la capa 2 del Modelo OSI, y brindaba pocas soluciones. Pero cuando Nobori encontró que ningún servidor de VPN existente brindaba soporte a múltiples protocolos VPN, el empezó a desarrollar la versión actual de SoftEther, la cual soporta el empleo de la VPN SoftEther, IPsec, SSTP y OpenVPN, siendo lo novedoso la posibilidad de emplear todos estos protocolos simultáneamente en un único servidor de VPN.

La tecnología clave detrás de SoftEther es la virtualización de ethernet. Al virtualizar ethernet en la capa 2, SoftEther no se limita a crear un túnel para el tráfico IP y además le permite trabajar con mejor consumo de recursos de computo que otras soluciones. SoftEther crea un adaptador virtual de ethernet en el dispositivo que es cliente y un *switch* virtual de ethernet llamado *Virtual Hub* (Concentrador Virtual) en el servidor de VPN. Estos dos componentes virtualizados están conectados cada uno mediante una sesión VPN que es llamado cable ethernet virtualizado. Estas sesiones emplean conexiones TCP o UDP y están codificadas con SSL.

Los *Virtual Hub* funcionan como un *switch* de ethernet físico más que un *hub* (concentrador). Los *Virtual Hub* pueden ser conectados a interfaces físicas del servidor VPN mediante puentes locales. Esto permite al servidor VPN estar conectado a la infraestructura física y a los usuarios remotos acceder a recursos de esta infraestructura. Los *Virtual Hub* son usados por todos los protocolos que soporta SoftEther.

De ser requerido, los *Virtual Hub* pueden ser interconectados en forma de cascada, que es como un cable ethernet virtual entre dos *switch*. Las cascadas permiten, por ejemplo, interconexión entre múltiples sitios y permitiría a usuarios y computadoras conectadas acceder a los recursos de otros sitios.

Internamente el servidor de SoftEther maneja todos los protocolos VPN en la capa 2, a pesar que OpenVPN, SSTP e IPsec usan la capa 3 para realizar el tráfico por túnel. De esta forma el *Virtual Hub* es capaz de procesar el trafico entrante y saliente del túnel como cualquier tráfico nativo de SoftEther.

El conjunto de capacidades que brinda SoftEther es comparable con los demás productos VPN comerciales y de código abierto. Emplea algoritmos modernos para codificar el trafico (AES-256 y 4098 bit RSA), tiene buenas capacidades de registrar los sucesos, el *software* de servidor y cliente está disponible en todos los sistemas operativos modernos, entre otras capacidades.

Un análisis de las soluciones comerciales y de código abierto nos permite decidir que SoftEther es el Sistema VPN indicado a emplear en la propuesta de solución.

Microcomputadoras

Figura 7

Como el objetivo del proyecto es implementar un servidor de protección perimetral de bajo costo se debe emplear un dispositivo de *hardware* poco costoso pero que tenga la capacidad de soportar las tecnologías de VPN y *Firewall* seleccionadas.

Para este objetivo se analizó utilizar una microcomputadora de placa reducida, Raspberry Pi. (figura 7) [14]

La Raspberry Pi se conecta a una TV o Pantalla LCD con entrada HDMI y a un Teclado y/o mouse USB. Es una pequeña PC completamente funcional que puede ser usado para muchas de las cosas como una PC de escritorio, también reproduce videos en alta definición.

El diseño contiene un chip Broadcom BCM2835, tiene un procesador central ARM1176JZF-S a 700 MHz. Tiene un procesador gráfico (GPU) VideoCore IV, y 512 MiB de memoria RAM. El diseño no incluye un disco duro ni unidad de estado sólido, usa una tarjeta SD.

Tiene disponibles sistemas operativos basados en el núcleo de Linux. El 19 de febrero de 2012, se lanzó el primer prototipo de imagen de tarjeta SD que almacenaba un sistema operativo

Existen varias generaciones de Raspberry Pi, cada una aumentando sus capacidades tanto de procesamiento como en capacidad de puertos de entrada.

La primera generación, Raspberry Pi 1, se lanza en febrero del 2012 en un modelo básico A y luego mejorado con un modelo B.

El modelo Raspberry Pi 2 fue lanzada en febrero del 2015 y la Raspberry Pi 3 en febrero del 2016. [15]

Estos dispositivos rondan los 20$~60$ USD dependiendo del modelo.

La mayoría de los dispositivos presentan entre uno y cuatro puertos USB, Salida de video HDMI y un puerto Jack de audio 3.5mm. igualmente la mayoría trae consigo un puerto Ethernet RJ45 y en el caso del modelo Pi 3 trae consigo WiFi 802.11n y Bluetooth.

En este proyecto utilizaremos unas de las primeras versiones de esta microcomputadora: la Raspberry Pi B+ v1.2. Se escogió este modelo más antiguo ya que cumple con los requisitos necesarios, y su costo es bajo comparado con los modelos más actuales.

Componentes de la solución propuesta

La tabla 1 muestra los rangos aproximados de precios de las soluciones de *firewall*. Donde se comparan soluciones comerciales con la solución propuesta.

Costo en USD de soluciones de *Firewall*			
	Equipo de *Firewall* comercial	Computadora empresarial	Raspberry Pi
Costo *hardware*	30,000 – 300,000	400 – 1200	20 – 60
Costo *Software*		400 – 20,000 0 (*software* libre)	0 (*software* libre)
www.trustradius.com/firewalls			

Tabla 1

Después de realizar un análisis de los datos disponibles, se propone emplear como servidor de protección perimetral la **microcomputadora Raspberry Pi** (modelo B+ v1.2) con **sistema operativo Debian**, **solución de Red Privada Virtual SoftEther** y **protocolo de túnel IPsec**.

Instalación y pruebas de la solución propuesta

Descripción de la arquitectura propuesta

La propuesta de solución consiste en emplear una Raspberry Pi B+ v1.2 junto a un adaptador ethernet-USB para poder emplear este sistema como un servidor de protección perimetral.

En la microcomputadora Raspberry pi, empleando sistema operativo Debian se instalará el sistema de VPN SoftEther y mediante este es que se realizara la conexión entre los nodos principales y remoto. La figura 8. muestra una Raspberry Pi B+ v1.2 conectada a adaptador ethernet-USB.

Figura 8

Para comprobar la viabilidad del prototipo se propone establecer un polígono de prueba. La figura 9 muestra la Arquitectura del despliegue propuesto.

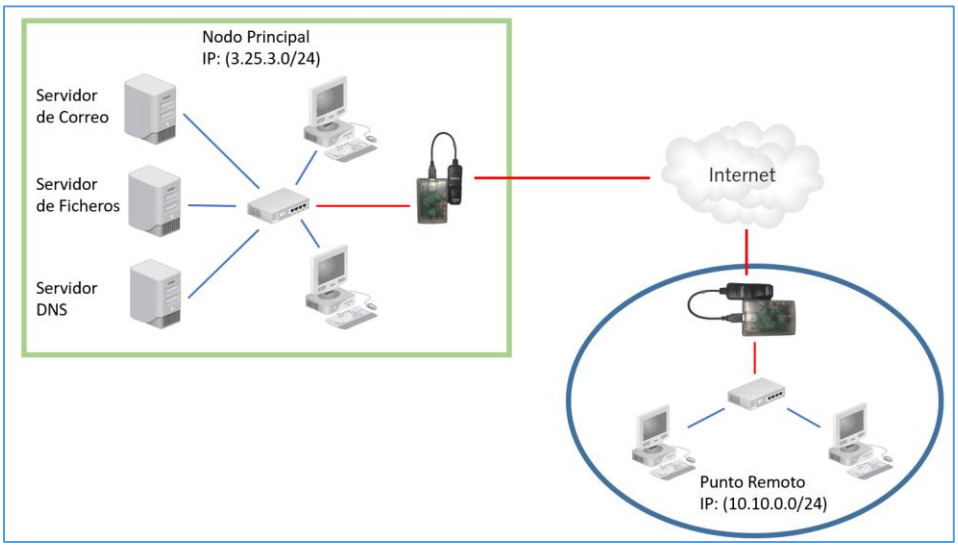

Figura 9

Como se observa en la figura 9, se establece una interconexión de tipo sitio-a-sitio donde cada ubicación se conectará mediante un *switch* a la Raspberry Pi y esta actuará como pasarela para conectarse a internet (o la red de la entidad) estableciendo un túnel con la Raspberry Pi ubicada en la oficina central donde se encuentran los servicios de correo, ficheros y DNS.

En el nodo principal de la red de la institución se ubicará un servidor de SoftEther.

Cada Raspberry Pi se conectará a la sub-red del nodo en cuestión por su puerto ethernet en la tarjeta (*on-board*) y emplearan un adaptador ethernet-USB para conectarse a internet (o en la intranet de la entidad en caso de que este despliegue se realice dentro de red corporativa, pero así y todo se desee separar este tráfico de la red pública).

De esta forma se puede establecer una conexión entre todos los puntos de oficina que tenga la entidad y los nodos principales, donde cada usuario puede consumir los recursos de la red como un todo, como si estuvieran en la misma ubicación y sub-red.

Este despliegue, es adecuado para ofrecer servicio a un usuario final o un número reducido de estos, logrando satisfacer lo propuesto de crear una conexión segura, con bajo costo y alta disponibilidad.

Implementación del sistema

Para ello es necesario instalar y configurar el sistema operativo seleccionado, en este caso Debian, y el sistema VPN SoftEther.

A la Raspberry Pi se puede acceder mediante dos métodos, o directamente conectando un teclado y un monitor al dispositivo, o mediante ethernet empleando SSH. [16]

Se instalará un servidor de SoftEther en la Raspberry Pi y el *software* de administración del servidor y cliente para acceder a la VPN en la estación de trabajo del administrador de la red.

Además, se instalarán los *softwares* cliente en las estaciones de trabajo y servidores que se conectarán a la red VPN.

Instalación y configuración de SoftEther

Para instalar SoftEther se pueden emplear dos métodos: o se descarga manualmente los componentes para instalar el *software* o se conecta inicialmente la Raspberry Pi a internet y se pasa a instalar los mismos directamente.

Una vez instalado SoftEther, se termina de preparar el servidor ejecutando desde su consola la administración de VPN Server. Las demás configuraciones se realizarán desde la estación del administrador de la red.

Una vez realizado esto, el servidor esta iniciado y funcionando.

Pruebas de conectividad

Al autenticarse en la VPN empleando el *software* cliente, el servidor de SoftEther asigna una dirección IP virtual de las disponible en el DHCP virtual en la subred **192.168.30.0/24**. (Ver figura 10)

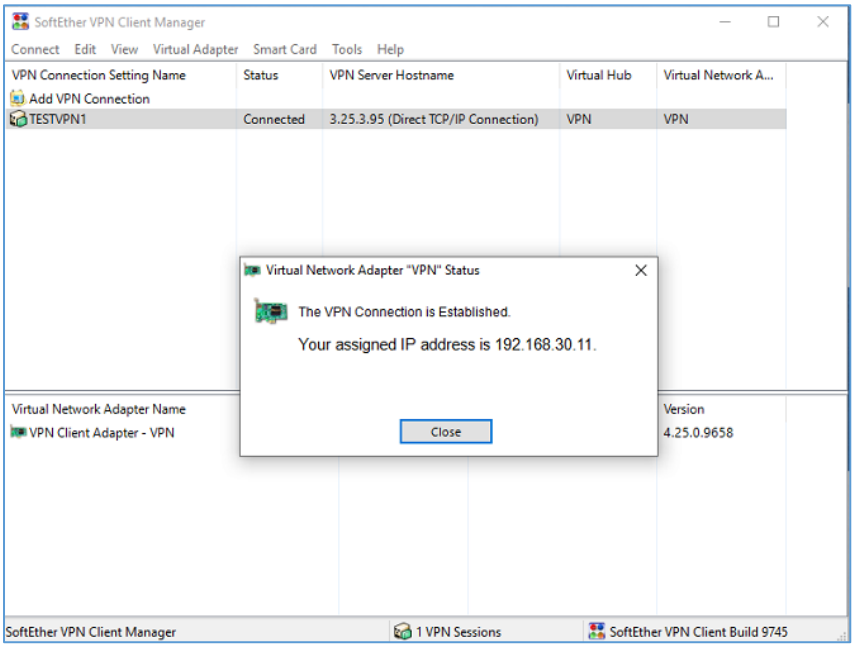

Figura 10

En este caso asignó la dirección IP **192.168.30.11** al *host* del nodo principal y **192.168.30.10** al *host* del nodo remoto. (Ver figura 11)

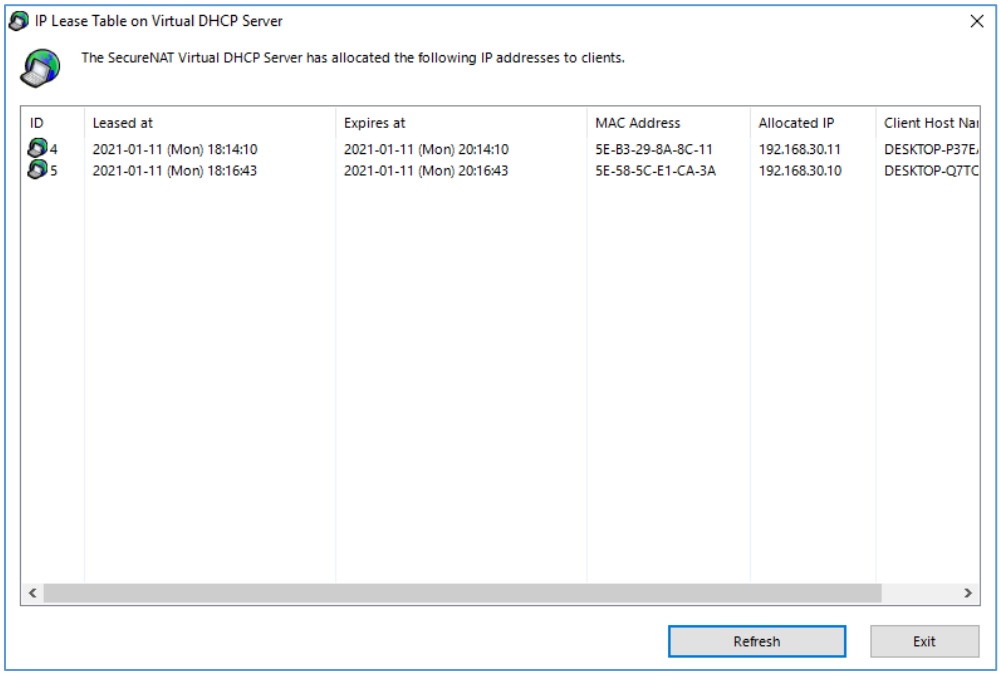

Figura 11

Al realizarse un **ping** desde el nodo principal con la nueva dirección asignada al nodo remoto, obtenemos una respuesta positiva sin pérdida de paquetes. (Ver figura 12).

```
C:\Users\GroOM>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:
Reply from 192.168.30.10: bytes=32 time=8ms TTL=128
Reply from 192.168.30.10: bytes=32 time=9ms TTL=128
Reply from 192.168.30.10: bytes=32 time=6ms TTL=128
Reply from 192.168.30.10: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 9ms, Average = 7ms
```

Figura 12

De esta manera, en este prototipo, se establece una conexión con VPN, entre un punto remoto y el nodo principal, brindándole seguridad, confidencialidad y disponibilidad a la misma. (Ver figura 13)

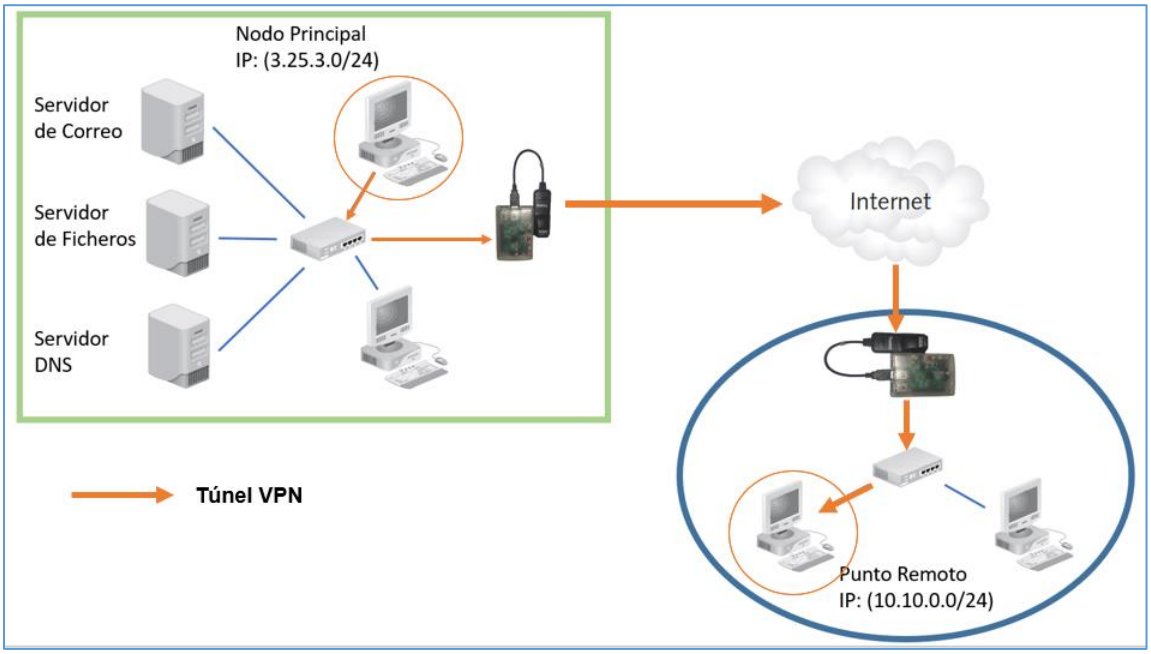

Figura 13

Al repetir los mismos pasos con los usuarios de los demás nodos, logramos agrupar en una misma subred virtual a todos los integrantes de la red corporativa.

Conclusiones

Mediante la elaboración de la fundamentación teórica de la investigación a partir del estudio del estado del arte de las técnicas de codificación, cortafuegos de red, sistemas de Redes Privadas Virtuales, y microcomputadoras de bajo costo, se determinaron los componentes de *hardware* y *software* más adecuados para la realización de un servidor de protección perimetral de bajo costo y alta seguridad.

A partir de las pruebas realizadas al prototipo se logró demostrar que el servidor de protección perimetral que emplea una Raspberry Pi junto a un sistema VPN SoftEther con codificación basada en IPsec, puede ser empleada para conectar múltiples usuarios remotos a los nodos principales de una red corporativa, cumpliendo con los estándares de seguridad requeridos.

El presente trabajo le permite a cualquier especialista que trabaje con servidores de esta categoría adquirir una base y una visión para enfrentar proyectos de este tipo, haciendo especial énfasis en las tecnologías libres, tan útiles y necesarias para un país como Cuba.

Recomendaciones

Los resultados obtenidos en este trabajo sugieren una serie de recomendaciones para profundizar en el trabajo con los servidores de protección perimetral, con la finalidad de conectar de manera segura a los usuarios remotos de redes corporativas:

- Profundizar en el estado del arte de los componentes utilizados con vista a identificar variantes más efectivas y menos costosas.
- Continuar investigando variantes de sistemas VPN, que puedan ser empleadas en soluciones de bajo costo.
- Realizar pruebas con aplicaciones que demanden alta disponibilidad.
- Analizar la conveniencia de extender el empleo de servidores de protección perimetral en las redes de entidades nacionales u Organismos de la Administración Central del Estado.

Referencias Bibliográficas

1 EC-COUNCIL (2011) Network Defense: Perimeter Defense Mechanisms, Course Technology, Cengage Learning, 2011.

2 NORTHCUTT, STEPHEN (2005) Inside Network Perimeter Security, Sams Publishing, March 04, 2005.

3 RAO, U.H., NAYAK, U. (eds.) (2014) The InfoSec Handbook: An Introduction to Information Security, Apress, Berkeley, 2014.

4 RISTIC, IVAN. (2014). Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications. London, England: Feisty. 2014

5 STEWART, J. MICHAEL & KINSEY, DENISE. (2020). Network Security, Firewalls, and VPNs, 3rd Edition. Jones & Bartlett Learning. 2020

6 WHITMAN, MICHAEL, MATTORD, HERB & GREEN, ANDREW. (2011) Guide to *Firewall*s and VPNs, 3rd Edition, Course Technology, Cengage Learning, 2011.

7 Firewalls Don't Stop Dragons A Step-by-Step Guide to Computer Security and Privacy for Non-Techies. New York, NY: APRESS. 2020

8 GUPTA, B., PEREZ, G.M., AGRAWAL, D.P., GUPTA, D. (eds.) (2020) Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Springer Nature Switzerland AG 2020

9 RAI, T. DIVYA y VERMA, RITU. (2015). Packet Filtering Technique for Network Security. International Journal of Engineering Research & Technology (IJERT), Special Issue – 2015

10 O'LEARY, MIKE. (2019) Cyber Operations: Building, Defending, and Attacking Modern Computer Networks. 2nd ed. Berlin, Germany: Apress. 2019

11 DADHEECH, KRATI, ARJUN CHOUDHARY, y GAURAV BHATIA. (2018). "De-Militarized Zone: A next Level to Network Security." En: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE. 2018

12 KORHONEN, VILLE (2019) “Future after OpenVPN and IPsec”, Master of Science Thesis, Tampere University, August 2019

13 SoftEther VPN Project (2020) SoftEther VPN Manual, 2020.

14 GALE, JAMES (ed.) (2020) The Complete Raspberry Pi Manual: Expert Tutorials To Improve Your Skills, Black Dog Media, October 2020

15 SUDHIR DAWRA y otros (2020) "Deployment Of Remote-Access Openvpn Server With Aes-256 Bit Private Keys On Raspberry-Pi", International Journal of Advanced Science and Technology, Vol. 29, No. 7s, 2020, pp. 5919-5927.

16 GOLDEN, RICK (2016) Raspberry Pi Networking Cookbook, Packt Publishing, 2nd edition, January 6, 2016