INFLUENCIA DEL VOLUMEN DE TRÁFICO SOBRE TÚNEL VPN IPSEC/UDP EN ENLACES WAN

(Traffic volume influence on a VPN IPSEC/UDP tunnel performance thru wan links)

Recibido: 11/01/2012 **Aceptado:** 16/05/2012

Vega, Oscar David
Universidad Privada Dr. Rafael Belloso Chacín, Venezuela
osdavega@gmail.com

Núñez, Steve
Universidad Rafael Urdaneta, Venezuela
nunezsd@pdvsa.com

RESUMEN

La finalidad de la investigación fue determinar la influencia del volumen de tráfico sobre rendimiento en túnel VPN IPSEC/UDP en enlaces WAN; con el objetivo de establecer una relación entre el volumen de tráfico generado por un constructor de paquetes y el rendimiento de los enlaces con la presencia de redes privadas virtuales IPSEC, en una conexión de tipo punto a punto. La investigación fue catalogada de tipo explicativa, con un diseño experimental de campo. Las muestras de los datos se obtuvieron de 2 escenarios creados por el investigador, en el primero se establece el montaje de la topología sin configurar el túnel VPN, sirviendo como punto de referencia; el segundo es idéntico al primero, con la adición de un túnel IPSEC. Luego, se procede a fijar los volúmenes de tráficos del experimento donde se crean paquetes de prueba con tamaños de 12.500 bytes, los cuales se incrementan por la misma unidad hasta completar la serie de veinte muestras en total y proceder a trasmitirlas por ambos escenarios, logrando el primer objetivo del trabajo titulado establecimiento de los escenarios de prueba. Más tarde, a las mediciones del tráfico enviado en las pruebas 1 y 2, se le aplicaron las fórmulas correspondientes para obtener el rendimiento, cumpliendo el segundo objetivo llamado determinar la influencia del volumen de tráfico sobre el rendimiento en túneles. Finalmente, por medio del método de estimación de curvas se obtuvo que la gráfica más asertiva fuera la logarítmica, de la cual se generó un modelo con una ecuación $R=16{,}335 + 1{,}669\ V_t \mathrm{Ln}(t)$ dando cumplimiento al último objetivo de modelar la influencia del tráfico, permitiendo concluir que si existe influencia del volumen de tráfico en túneles IPSEC/UDP.

Palabras claves: Rendimiento, Volumen de tráfico, Túneles, Estimación curvilínea.

ABSTRACT

The purpose of the investigation was to determine the traffic volume influence on a VPN IPSEC/UDP tunnel performance thru WAN links; with the aim to establish a relationship between the traffic volume generated by a package's builder and the link's performance with the presence of a virtual private network IPSEC in a point to point link. The investigation was catalogued as explanatory, with experimental and field design. The

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

samples of the information were obtained from 2 scenes created by the investigator, in the first,the topology assembly was established without forming the VPN tunnelas a reference point; the second is identical to the first, with the addition of anIPSEC tunnel. Then, proceeding to establish the experiment traffic volumes where test packages were created in sizes of 12.500 bytes, which were increasedby the same volumeuntil completing the total of twenty sample series and proceeding to transmit them to both scenes, achieving the first goal titled Establishment of the Test Scenes. Later, the corresponding formulaswere applied to the traffic measurements sent of tests 1 and 2, obtaining the performance, fulfilling the second aim called Determining the Volume Traffic Influence on the Tunnels Performance. Finally, using thecurve's estimation method, the most assertive graph was obtained, which was logarithmic, which generated a model with the equation $R = 16{,}335 + 1{,}669\ V_t\ Ln(t)$, giving fulfillment to the last goalwhich was to mold the traffic influence, allowing to conclude that there exists traffic volume influence in IPSEC/UDP tunnels.

Keywords: Performance, Traffic volume, Tunnels, Curvilinear estimation.

INTRODUCCIÓN

Con el inicio del siglo XXI, el uso del internet se incrementó en valores exponenciales con respecto al siglo pasado, las personas actualmente pueden realizar transacciones bancarias, enviar y recibir correos electrónicos desde sus hogares, sus dispositivos telefónicos móviles o inclusive sitios públicos. En Venezuela las empresas se han abierto a esta tendencia, utilizando internet como herramienta para comercializar sus productos, realizar negocios y principalmente como medio de comunicación, gracias a los proveedores de servicios de internet (ISP) locales, que se han esforzado por hacer esta promesa realidad.

Los ISP se encargan de llevar las conexiones de datos a cualquier usuario en el país por diversos medios, coincidiendo con el estándar de la norma E1 ofrecido por las empresas nacionales, a través de conexiones E1 o múltiplos de ella, para la mayoría de sus enlaces dedicados. Es de suma importancia señalar que la autopista binaria no es un medio seguro para ciertas transacciones como consultas bancarias, datos de ventas, consultas de bases de datos en línea, entre otras, debido a la gran tendencia actual del espionaje electrónico y robo de información digital.

Por tales razones, surge el protocolo de seguridad de internet IPSEC, el cual ofrece la bondad de establecer un túnel lógico seguro encriptado para proteger la información que viaja por la web. Dado que el estándar E1, es el más utilizado por los ISP y el protocolo de seguridad IPSEC es el protocolo predominante anti espías, surge la inquietud de realizar un estudio que permita examinar la influencia del volumen de tráfico sobre un túnel VPN IPSEC/UDP en enlaces WAN, siendo UDP el protocolo para el tipo de datos que se desea trasmitir por ese medio.

Por tales razones, surge la necesidad de predecir el comportamiento de los datos UDP transmitidos mediante redes privadas virtuales VPNs, estableciendo un modelo o guía de referencia que permita estimar la cantidad de conexiones E1 necesarias, de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

acuerdo a una determinada necesidad. Para logro de los objetivos de la presente investigación, se ha estructurado su desarrollo en las siguientes cuatro fases metodológicamente estructuradas:

Primera fase: conformada por el diseño de los escenarios donde serán realizados los experimentos, así como también la selección del hardware y del software a ser implementados en estos escenarios de pruebas, para obtener los volúmenes de tráfico en ambos escenarios.

Segunda fase: en la cual se establecen los volúmenes de tráfico para el experimento, determinando el tamaño de los archivos a ser transmitidos tanto en el escenario de referencia (sin túnel), así como por el escenario con túnel VPN.

Tercera fase: en esta fase, se realiza la captura de los volúmenes de tráfico, registrando los distintos tamaños de archivos transferidos, así como el tiempo requerido en su transmisión, tanto en el escenario sin túnel, como por el escenario con túnel VPN, para determinar el efecto del volumen de tráfico sobre el rendimiento del enlace.

Cuarta fase: en esta última fase, se realizan los análisis y cálculos necesarios para generar las curvas y modelado del rendimiento durante la transmisión de datos en el túnel VPN.

BASES TEÓRICAS

TRÁFICO

El tráfico en redes de área local, de acuerdo a lo establecido por Aguilar (2002) se mide como la cantidad de información promedio que se transfiere a través del canal de comunicación, y a la velocidad que se transfiere, por ello la importancia del conocimiento sobre la teoría de la información y sus diferentes elementos para poder evaluar de forma más eficiente y eficaz el tráfico en la red.

ANÁLISIS DE TRÁFICO

El autor Aguilar (2002) define el análisis de tráfico como el conjunto de mediciones relacionadas con la transmisión de paquetes en un segmento de la red de datos. Dichos paquetes están originados por las aplicaciones que corren sobre la red, los servicios que se prestan en ella o los protocolos que administran su funcionamiento.

ANALIZADOR DE PAQUETES

Las investigaciones del portal www.guimi.net establecen que los analizadores de paquetes captan todos los paquetes que llegan a la tarjeta de red (NIC) configurándola en modo promiscuo. Después facilitan un análisis de dichos paquetes de red según los protocolos utilizados en los paquetes. El más utilizado es Wireshark, inicialmente llamado Ethereal, que dispone de interfaz gráfica.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

RENDIMIENTO

La tasa de transferencia o rendimiento, para la Academia de redes de Cisco Systems (2004), se refiere al ancho de banda real medido en un momento concreto del día, empleando rutas concretas de internet, mientras se trasmite un conjunto específico de datos por la red. Desafortunadamente por muchas razones, la tasa de transferencia es con frecuencia menor que el máximo ancho de banda digital posible del medio que se está empleando.

Los siguientes son algunos de los factores que determinan la tasa de transferencia: Dispositivos de internetworking, tipos de datos que se van a transferir topología de la red, número de usuarios en la red, la computadora del usuario, el servidor, condiciones de energía y congestión.

REDES PRIVADAS VIRTUALES (VPNs)

Los autores Morgan y Lovering (2007) definen una red privada virtual proporciona mediante procesos de encapsulación y cifrado, una red privada de datos, sobre infraestructura de telecomunicaciones públicas, como internet. Las VPN logran esto al permitir que se realice un túnel seguro a través de una red pública de tal forma que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que están disponibles en las redes privadas.

PROTOCOLO DE SEGURIDAD DE INTERNET (IPSEC)

Morgan y Lovering (2007), definen IPSEC como el mejor medio, o de cómo un conjunto de características protegen la data IP de cómo esta viaja de una localización a otra. Las localizaciones que están involucradas en la VPN son las que típicamente definen las VPN.

Una localización debería ser un cliente final, tal como un computador, una pequeña oficina remota, una sucursal, un centro de operaciones corporativos, un data center, o un proveedor de servicios. La combinación de una o dos de estas localizaciones determina el tipo de VPN en uso. Por ejemplo una remota oficina conectándose a un centro de operaciones corporativas debería ser un site-to-site VPN.

Es importante recordar que IPSEC puede proteger solo la capa tres o capa de red y superiores. IPSEC no puede extender sus servicios a la capa física del modelo OSI. Si se requiere protección de la capa física, algunas de las formas de encriptación son necesitadas.

PROTOCOLO DE DATAGRAMA DE USUARIO (UDP)

El estúdio de Dye (2008) indica que UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de transporte envía estos datagramas como "mejor intento". Cada datagrama UDP posee 8 bytes de carga en el encabezado, que encapsulan los datos de la capa de aplicación.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

REDES DE ÁREA AMPLIA (WAN)

En www.guimi.net se define una red de área amplia a diferencia de las redes locales, cuya infraestructura es generalmente propiedad y responsabilidad del usuario, las redes de área extensa (WAN) normalmente utiliza redes de proveedores. Inicialmente estas redes eran únicamente instaladas para la transmisión de voz por las compañías telefónicas, pero hoy en día se utilizan también para redes creadas específicamente para datos por distintos proveedores (compañías de telecomunicaciones).

E1

Un E1 es una norma Europea que contiene 30 señales más 2 de control, es decir, 32x64 Kbps= 2.048 Mbps. Maneja una tasa de línea: 2,048 Mbps ± 50 bps. Su sincronización: El PLL digital sincroniza todos los transmisores a una de las siguientes fuentes: la línea E3, cualquiera de las líneas E1 o el reloj de 8 kHz del MGX 8220. El código de línea utilizado es: HDB3, AMI. El entramado de línea: multitrama de 16 tramas según ITU G.704.

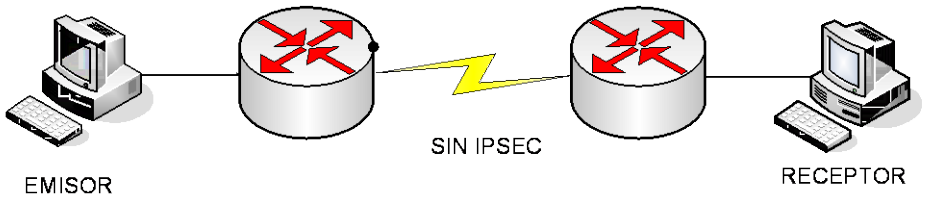
FASE I. DISEÑO Y SELECCIÓN DE LOS ELEMENTOS PARA LOS ESCENARIOS DE PRUEBA

El primer escenario, por el cual se transferirán archivos de tipo UDP entre dos elementos desprovisto de túnel. En este envío de información involucra la capa de red del modelo OSI como el segmento evaluado, sin considerar el encapsulado Ethernet, siendo encapsulada la información por las cabeceras IP y UDP, las cuales suman un total de 28 bytes respectivamente.

La transferencia de datos del segundo escenario, involucran las cabeceras del primer escenario, pero en la tercera capa del modelo OSI se aplica el protocolo IPSEC, el cual agrega un peso de 20 bytes de cabecera como mínimo, según Ranjbar (2007). Totalizando 48 bytes de cabecera, es decir, casi el doble del escenario sin VPN.

Planteadas las características generales anteriores es notorio que al generar diversos volúmenes de datos con el protocolo de seguridad IPSEC, se incrementará los tamaños de archivos, dando como consecuencia más ocupación del canal E1, afectando su rendimiento. Para conceptualizar el experimento se plantean los dos escenarios descritos anteriormente y los cuales se componen según se muestran en los gráficos 1 y 2.

Gráfico 1. Escenario sin IPSEC



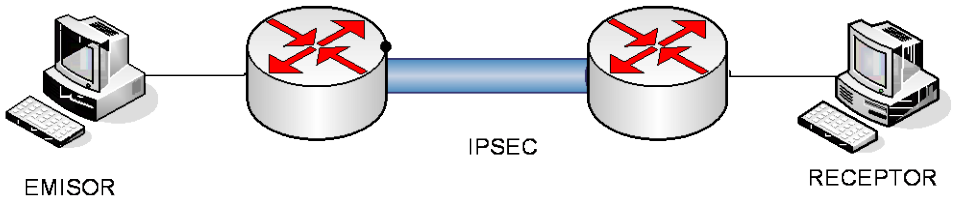
Fuente: elaboración propia.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

El experimento inicial está compuesto de dos computadores, dos enrutadores, dos cables cruzados ethernet y un cable cruzado configurado para el E1 (Gráfico 1). Los dos enrutadores están conectados por medio del cable cruzado E1, simulando la nube de internet, luego en cada extremo de cada enrutador se conecta una estación de trabajo por medio de un cable cruzado ethernet. Finalmente, el computador de uno de los extremos llevará instalado un generador de trafico UDP, el cual enviará información hasta el otro equipo, pasando por los enrutadores, lo que significa que la data sufrirá las encapsulaciones y desencapsulaciones de una condición normal; como se muestra en la gráfica 1.

El segundo experimento está estructurado del mismo modo que el primario, con la diferencia que entre los dos enrutadores se estable un túnel IPSEC, lo que agrega un nuevo empaquetado y desempaquetado de la data, referenciado en el gráfico 2.

Gráfico 2. Escenario con IPSEC



Fuente: elaboración propia.

FASE II. ESTABLECIMIENTO DE LOS VOLÚMENES DE TRÁFICO PARA EL EXPERIMENTO DE LA INVESTIGACIÓN

Una vez ensamblados los escenarios experimentales de la primera fase, se procede a establecer y especificar los diversos volúmenes de tráficos con los cuales se procederán a realizar las transferencias.

Para establecer los volúmenes de tráfico de ambos escenarios, se determinan los tamaños de los archivos en cien mil bits, incrementándose su tamaño en igual medida, hasta completar el máximo umbral de canal establecido de dos millones de bits, basados en la metodología implementada por Naveda (2009), quien a su vez se sustentó metodológicamente y técnicamente en la investigación de Chen (2002).

Mediante este procedimiento se establecen veinte puntos de observación, generados en orden creciente o ascendente, permitiendo observar un crecimiento de la tasa de transferencia en un orden exponencial, resultando en una mejor óptica de la curva de rendimiento. La tabla 1, muestra los tamaños de los archivos prefijados anteriormente y sus respectivas descomposiciones, considerando las cabeceras para un escenario sin túnel.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

Tabla 1. Cálculos de archivos de muestra sin IPSEC

Archivo en Bit	Archivo en Bytes	N° de fragmentos del Archivos (Bytes)	Redondeo hacia arriba	N° de bytes por Cabeceras de Protocolos en Bytes Ip+Udp	N° de bytes por Cabeceras de Protocolos en Bits Ip+Udp	Tamaño del archivo en bits	Tamaño del archivo en bytes	Tamaño del archivo en hexadecimal
100,000	12,500	8.491847826	9	252	2,016	97,984	12,248	00002FD8
200,000	25,000	16.98369565	17	476	3,808	196,192	24,524	00005FCC
300,000	37,500	25.47554348	26	728	5,824	294,176	36,772	00008FA4
400,000	50,000	33.9673913	34	952	7,616	392,384	49,048	0000BF98
500,000	62,500	42.45923913	43	1204	9,632	490,368	61,296	0000EF70
600,000	75,000	50.95108696	51	1428	11,424	588,576	73,572	00011F64
700,000	87,500	59.44293478	60	1680	13,440	686,560	85,820	00014F3C
800,000	100,000	67.93478261	68	1904	15,232	784,768	98,096	00017F30
900,000	112,500	76.42663043	77	2156	17,248	882,752	110,344	0001AF08
1,000,000	125,000	84.91847826	85	2380	19,040	980,960	122,620	0001DEFC
1,100,000	137,500	93.41032609	94	2632	21,056	1,078,944	134,868	00020ED4
1,200,000	150,000	101.9021739	102	2856	22,848	1,177,152	147,144	00023EC8
1,300,000	162,500	110.3940217	111	3108	24,864	1,275,136	159,392	00026EA0
1,400,000	175,000	118.8858696	119	3332	26,656	1,373,344	171,668	00029E94
1,500,000	187,500	127.3777174	128	3584	28,672	1,471,328	183,916	0002CE6C
1,600,000	200,000	135.8695652	136	3808	30,464	1,569,536	196,192	0002FE60
1,700,000	212,500	144.361413	145	4060	32,480	1,667,520	208,440	00032E38
1,800,000	225,000	152.8532609	153	4284	34,272	1,765,728	220,716	00035E2C
1,900,000	237,500	161.3451087	162	4536	36,288	1,863,712	232,964	00038E04
2,000,000	250,000	169.8369565	170	4760	38,080	1,961,920	245,240	0003BDF8

Fuente: elaboración propia.

De igual forma, la tabla 2 muestra los archivos prefijados con IPSEC donde se puede apreciar la diferencia de los tamaños de las cabeceras, con respecto a la data sin túnel.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

Tabla 2. Cálculos de archivos de muestra con IPSEC

Archivo en Bit	Archivo en Bytes	N° de fragmentos del Archivos (Bytes)	Redondeo hacia arriba	N° de bytes por Cabeceras de Protocolos en Bytes (Ip+Udp+Ipsec)	N° de bytes por Cabeceras de Protocolos en Bits (Ip+Udp+Ipsec)	Tamaño del archivo en bits	Tamaño del archivo en bytes	Tamaño del archivo en hexadecimal
100,000	12,500	8.903133903	9	432	3,456	96,544	12,068	00002F24
200,000	25,000	17.80626781	18	864	6,912	193,088	24,136	00005E48
300,000	37,500	26.70940171	26	1248	9,984	290,016	36,252	00008D9C
400,000	50,000	35.61253561	35	1680	13,440	386,560	48,320	0000BCC0
500,000	62,500	44.51566952	44	2112	16,896	483,104	60,388	0000EBE4
600,000	75,000	53.41880342	53	2544	20,352	579,648	72,456	00011B08
700,000	87,500	62.32193732	63	3024	24,192	675,808	84,476	000149FC
800,000	100,000	71.22507123	71	3408	27,264	772,736	96,592	00017950
900,000	112,500	80.12820513	80	3840	30,720	869,280	108,660	0001A874
1,000,000	125,000	89.03133903	90	4320	34,560	965,440	120,680	0001D768
1,100,000	137,500	97.93447293	98	4704	37,632	1,062,368	132,796	000206BC
1,200,000	150,000	106.8376068	107	5136	41,088	1,158,912	144,864	000235E0
1,300,000	162,500	115.7407407	116	5568	44,544	1,255,456	156,932	00026504
1,400,000	175,000	124.6438746	125	6000	48,000	1,352,000	169,000	00029428
1,500,000	187,500	133.5470085	134	6432	51,456	1,448,544	181,068	0002C34C
1,600,000	200,000	142.4501425	143	6864	54,912	1,545,088	193,136	0002F270
1,700,000	212,500	151.3532764	152	7296	58,368	1,641,632	205,204	00032194
1,800,000	225,000	160.2564103	161	7728	61,824	1,738,176	217,272	000350B8
1,900,000	237,500	169.1595442	170	8160	65,280	1,834,720	229,340	00037FDC
2,000,000	250,000	178.0626781	179	8592	68,736	1,931,264	241,408	0003AF00

Fuente: elaboración propia.

FASE III: DETERMINAR EL EFECTO DEL VOLUMEN DE TRÁFICO SOBRE EL RENDIMIENTO DEL ENLACE

La primera condición (sin túnel) del estudio arroja una ocupación del canal del 84% hasta el 94%, desde el primer punto de observación hasta el décimo noveno. Sin embargo, el vigésimo valor presentó una caída de la ocupación del canal al 1%.

La segunda condición (con túnel IPSEC), presenta un manejo de tráfico del 32% hasta el 42% en los veinte volúmenes de tráfico establecidos, es decir que no presentó pérdidas de datos en ningún punto. Estos resultados son apreciados en la tabla 3.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

Tabla 3. Resultados de rendimiento de los escenarios 1 y 2

Items	Volúmen	Rendimiento	R (%)	Items	Volúmen	Rendimiento	R (%)
Nº	Bytes	UDP Simple	UDP Simple	Nº	Bytes	UDP IPSEC	UDP IPSEC
1	12500	0.841582	84.16%	1	12500	0.335202	33.52%
2	25000	0.912703	91.27%	2	25000	0.328860	32.89%
3	37500	0.850893	85.09%	3	37500	0.338928	33.89%
4	50000	0.844683	84.47%	4	50000	0.338370	33.84%
5	62500	0.911265	91.13%	5	62500	0.338549	33.85%
6	75000	0.842419	84.24%	6	75000	0.340096	34.01%
7	87500	0.874453	87.45%	7	87500	0.343703	34.37%
8	100000	0.858734	85.87%	8	100000	0.345621	34.56%
9	112500	0.850880	85.09%	9	112500	0.352567	35.26%
10	125000	0.842103	84.21%	10	125000	0.350957	35.10%
11	137500	0.893013	89.30%	11	137500	0.355615	35.56%
12	150000	0.851058	85.11%	12	150000	0.359093	35.91%
13	162500	0.855558	85.56%	13	162500	0.363739	36.37%
14	175000	0.878238	87.82%	14	175000	0.370374	37.04%
15	187500	0.891709	89.17%	15	187500	0.378123	37.81%
16	2000000	0.873994	87.40%	16	2000000	0.389698	38.97%
17	2125000	0.905011	90.50%	17	2125000	0.407365	40.74%
18	2250000	0.908138	90.81%	18	2250000	0.409465	40.95%
19	2375000	0.947967	94.80%	19	2375000	0.408009	40.80%
20	2500000	0.010000	01,00%	20	2500000	0.420804	42.08%

Fuente: elaboración propia.

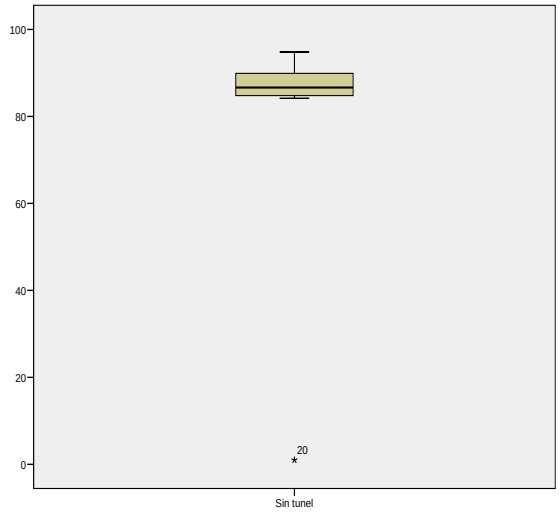
Al analizar los resultados de la tabla 3, se observa que a pesar de aumentar la cantidad de bytes en los escenarios, ambos se mantienen por debajo de la capacidad máxima del canal; en el primer experimento se observan altas y bajas en las transmisiones, pero no llega al valor establecido de 2000000 de bits/seg, mas la última muestra que aplicó el tamaño del valor nominal del enlace presento pérdidas de hasta el 99%. En el segundo experimento, tampoco se superó el valor del canal de datos, ya que presentó una ocupación creciente y decreciente exceptuando la segunda muestra con una diferencia del 1%.

FASE IV: GENERACIÓN DE CURVAS Y MODELADO DEL RENDIMIENTO DURANTE LA TRANSMISIÓN DE DATOS EN EL TÚNEL VPN

Los resultados obtenidos del volumen de tráfico o variable independiente y el rendimiento como variable dependiente, representados en la tabla 3 de la fase III, para determinar la adecuacion de los datos a las condiciones que permitan elaborar el modelo. En primer lugar, se realizó el análisis exploratorio de los datos, aplicando el gráfico de Caja y Bigote para la condición del rendimiento sin tunel y con túnel, ilustrados en los gráficos 3 y 4.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

Gráfico 3. Prueba de caja y bigote sin túnel

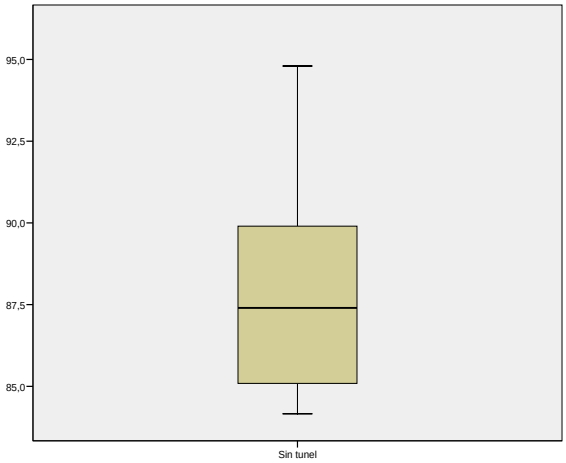


Fuente: elaboración propia.

En el gráfico 3, se observa un valor o dato extremadamente atípico de la condición sin túnel, debido a que en la última prueba de volumen de tráfico se aplica el valor máximo del canal de dos millones de bits (2.000.000), observándose una saturación del umbral que arrojó una pérdida de los datos del 99%, situación que se torna constante en los puntos siguientes de la evaluación, por lo cual no fueron considerados, eliminando inclusive el vigésimo valor.

Adicionalmente, el vigésimo valor representa el colapsamiento del canal al ser superado su capacidad, por lo cual, la eliminación del mismo se justifica en el hecho de que al eliminarlo, el error típico disminuye de 4,37 a 0,7 apoyado de igual forma que la curtosis y la asimetría se ubican en el rango de +/- 2.

Gráfico 4. Prueba de caja y bigote con túnel



Fuente: elaboración propia.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

Una vez ajustado el error típico, se aplicó la prueba T de Student para muestras independientes, detectándose diferencias altamente significativas que comprueban la influencia del volumen de tráfico sobre rendimiento en túnel VPN IPSEC/UDP en enlaces WAN. La hipótesis alternativa, popo ya que el valor de t para varianzas iguales de 53,524 está asociado a una significancia menor a 0,01, como muestra la tabla 4.

Tabla 4. Prueba de muestras independiente con varianzas iguales

Prueba de muestras independientes

		Prueba de Levene para la igualdad de varianzas		Prueba T para la igualdad de medias						
									95% Intervalo de confianza para la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Error típ. de la diferencia	Inferior	Superior
dependiente	Se han asumido varianzas iguales	,146	,704	53,524	37	,000	51,17400	,95609	49,23678	53,11122
	No se han asumido varianzas iguales			53,422	36,431	,000	51,17400	,95791	49,23206	53,11594

Fuente: elaboración propia.

En consecuencia, el rendimiento de 87,55 para la condición sin túnel difiere en gran medida, de la condición con túnel con valor de 36,37; lo que corrobora estadísticamente la influencia del volumen de tráfico en túneles VPN IPESEC/UDP en enlaces E1. Ver tabla 5.

Tabla 5. Influencia del rendimiento

Estadísticos de grupo

	Factor	N	Media	Desviación típ.	Error típ. de la media
dependiente	Sin tunel	19	87,5500	3,09362	,70973
	Con tunel	20	36,3760	2,87711	,64334

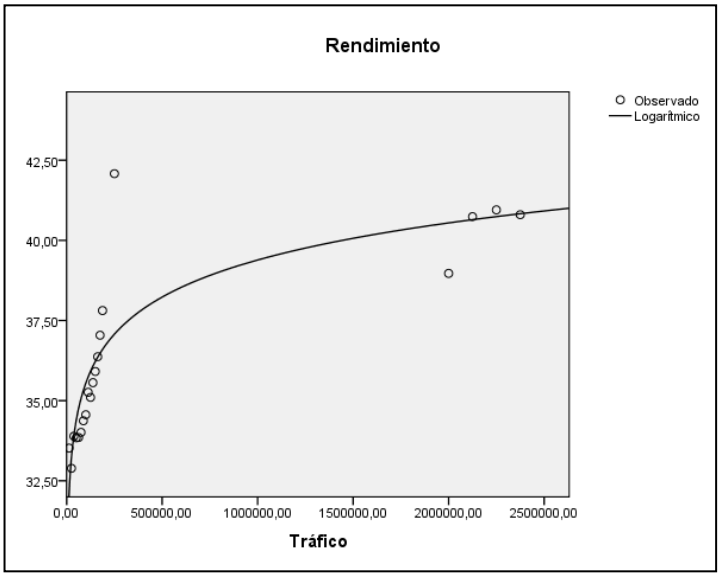
Fuente: elaboración propia.

Finalmente, se aplica el método de correlación para estimación de la curva del escenario sin túnel, denotando que la gráfica es logarítmica, a pesar que R^2 es igual a 0,88; es decir, es un valor menor al resto de las estimaciones referenciadas. Por otra parte, la mejor estimación para el experimento con túnel también es la logarítmica, dado que su R^2 es igual a 0,765; siendo mayor a los otros métodos.

Por las razones antes expuestas, se escoge la regresión de estimación logarítmica para poder graficar los valores correspondientes al escenario 2, donde se puede observar gran dispersión de los puntos de cortes de los ejes, obteniendo valores por encima y por debajo de la curvilínea de la gráfica 10, dicha curva inicia en orden ascendente manteniéndose en tal sentido, ajustándose al comportamiento real de las transmisiones de paquetes de datos, donde se aprecia que existe una relación y efecto entre las variables de estudio.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

Gráfico 5. Curva del rendimiento con túnel



Fuente: elaboración propia.

El resultado establece un modelo que se ajusta al comportamiento de la influencia del volumen de tráfico en túneles VPN IPESEC/UDP en enlaces WAN de tipo E1 y el cual es representado por la siguiente ecuación:

Logarítmico: $Y= B_0 + B_1 Ln(t)$

Rendimiento= $16,335 + 1,669\ V_t\ Ln(t)$

Fase V: Discusión de los resultados

El diseño del escenario de prueba en conjunto con los criterios de selección de hardware y software, son los adecuados para la obtención de los niveles de rendimiento, en función al volumen de tráfico en túneles VPN.

El establecimiento de tamaños específicos de los volúmenes de tráfico para la ejecución de situaciones experimentales en sus diversas muestras de cien mil bits en cien mil bits, permiten calcular el rendimiento de forma óptima, tal y como lo establece la investigación de Chen (2002).

La metodología empleada por Ramírez (2008) en el cálculo de los valores del rendimiento en función del volumen de tráfico, se aplican a plenitud para obtener los resultados del desempeño de IPSEC en la presente investigación. Se determinó que un enlace E1 puede ser sometido a volúmenes de tráficos constantes y permanentes hasta un límite de un millón novecientos mil bits, dado que al superar ese valor, sus niveles de transferencia decaen por la saturación de canal de transmisión.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

El empleo de redes privadas virtuales establece un mejor control del tráfico, dado que al utilizar archivos que lleguen al límite de su MTU de 1500 bytes, el protocolo de seguridad los fracciona por la adición de los 20 bytes del encapsulado, generando que por cada paquete de salida, entren 2 de llegada, los cuales a pesar de establecer mas procesamiento no afectan el rendimiento.

Los resultados de los diferentes cálculos del rendimiento en túneles VPN, demuestran que se pueden emplear videoconferencias de alta calidad de 2 megabits con esta tecnología de seguridad sin inconvenientes; por otra parte, se puede transmitir un estimado de 11 videoconferencias de 15 cuadros por segundo y 8 de 30 cuadros por segundo simultaneas aplicando técnicas de calidad de servicio.

El buen desempeño de los túneles IPSEC permite generar de acuerdo a la norma un total de 30 llamadas simultáneas, ya que una llamada con IPSEC consume un total de 56 kbps, lo que cumple con las demandas de los consumidores y empresas de telecomunicaciones.

En contraste con los resultados de las investigaciones de Lunar (2008) y Fuenmayor (2008), cuyos ajustes de curvas se amoldaron a la interpolación cúbica; en la presente investigación la estimación curvilínea adecuada resultó ser la logarítmica, dado que su comportamiento creciente es una representación similar al comportamiento real de los datos.

CONCLUSIONES

Es provechoso implementar generadores de tráfico para datos de tipo UDP, con respecto a la evaluación del rendimiento; dado cumplen con la cantidad de datos a emitir, con las encapsulaciones, correcciones de errores, propios de la capa 3 del modelo OSI.

Se determinó que existe influencia del volumen de tráfico al implementar túneles IPSEC comprobando la hipótesis alternativa, debido a que los resultados del rendimiento con la presencia de VPN, no exceden el 40% del canal.

Las redes privadas virtuales permiten un mejor control de los datos y aprovechamiento del canal, los cuales pueden ser significativos para aplicaciones de video, llamadas IP y transferencia de archivos.

Por otra parte, los túneles VPN permiten seguir avanzando a la tendencia de convergencia de los servicios, ya que permiten establecer llamadas IP, videoconferencias, consultas en la WEB por un mismo canal aplicando técnicas de calidad de servicio.

Se determina que el comportamiento de los túneles corresponde a la estimación curvilínea logarítmica, ya que su coeficiente de correlación r^2 es de 0,765, es decir, que se encuentra entre los valores 0,61 y 0,80; obteniendo una correlación alta.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

RECOMENDACIONES

Luego de haber finalizado la investigación en sus fases de desarrollo, análisis y conclusiones, es importante realizar una serie de recomendaciones que puedan aportar a mejorar los lineamientos por parte de la Universidad Dr. Rafael Belloso Chacín, en su programa de Telemática, a sus grupos de investigadores que deseen desarrollar trabajos de este tipo; entre los cuales mencionamos:

A los investigadores en caso de utilizar enrutadores de gama media recuerde desactivar las técnicas de encolado, debido a que son argumentos que permiten mejorar, priorizar y optimizar el envío de los datos, ya que se busca obtener resultados de la forma más simple posible.

Para los docentes, es importante al momento de utilizar los capturadores de tráfico verificar la sincronización de los tiempos de los paquetes, de no existir esa opción, se debe realizar de forma manual, identificando el primer paquete UDP y ubicando el último paquete de señalización y control del enrutador anterior al paquete inicial. Luego ese valor servirá de constante y será restado a todos los datos capturados sea del lado emisor o receptor según sea el caso.

En el caso de las empresas de telecomunicaciones, se recomienda a los administradores de red tomar en cuenta los resultados de la presente investigación, ya que puede servir de referencia para escenarios donde se necesite estimar el número de conexiones E1 requeridas y en el mejor de los casos, estimar los volúmenes de información que pueden ser trasmitidos en túneles, en ocasiones donde se requiera datos, video, telefonía o videoconferencia.

Finalmente, a la maestría en telemática es importante tener en cuenta que los túneles IPSEC, ofrecen una gran alternativa de seguridad de la información y puede ser un tema de amplio estudio para enriquecer la línea de investigación gestión de redes en su proyecto de comportamiento en redes de área local.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, L. (2002). Midiendo redes. Guía sobre el análisis de tráfico de datos. Argentina. Ediciones Galápago.

Academia de redes de Cisco Systems (2004). Guia del Primer año. España. Pearson Education, S.A.

Chen, S. (2002). Una metodología para el análisis de tráfico de una red de transmisión de datos. Revista InterSedes Año/Vol. III, número 004.

Dye, M. (2008). CCNA EXPLORATION 4.0. Aspectos básicos de networking. USA. Editorial Prentice Hall.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012

Fuenmayor, G. (2008). Efecto del volumen de tráfico sobre el retardo producido por el intercambio de datos entre los protocolos IEEE 802.3ab y 802.11g. Tesis de Maestría. Universidad Privada Dr. Rafael Belloso Chacín. Venezuela.

Lunar, R. (2008). Efecto del volumen de tráfico sobre el retardo producido por el intercambio de datos entre los protocolos IEEE 802.3U e IEEE 802.11G. Tesis de Maestría. Universidad Privada Dr. Rafael Belloso Chacín. Venezuela.

Morgan, B. y Lovering, N. (2007). CCNP ISCW. Guía oficial de examen de certificación. USA. Cisco Press.

Naveda, E. (2009). Volumen de tráfico sobre el retardo en el intercambio de datos UDP/IP/IEEE 802.3u y UDP/IP/IEEE 802.11g. Tesis de Maestría en Telemática. Universidad Privada Dr. Rafael Belloso Chacín. Venezuela.

Ramírez, J. (2008). Influencia de la distancia y número de host en el rendimiento del protocolo TCP/IP en las redes IEEE 802.11b modo ad hoc. Tesis de Maestría. Universidad Privada Dr. Rafael Belloso Chacín. Venezuela.

Ranjbar, A. (2007). CCNP ONT. Guía oficial de examen de certificación. USA. Cisco Press.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 11 Edición No 1 – Año 2012