**MULTICIENCIAS**, Vol. 10, Nº 1, 2010 (79 - 84)
ISSN 1317-2255 / Dep. legal pp. 200002FA828

# Efecto de una VPN en dispositivos portátiles sometidos a ataques de DoS

**David Bracho, Alfredo Acurero, Carlos Rincón, Juan Pablo Jakymec y Wuende Villalobos**

*Unidad de Redes e Ingeniería Telemática, Departamento de Computación, Facultad Experimental de Ciencias, Universidad del Zulia. Maracaibo, Venezuela.*
*drbracho@fec.luz.edu.ve, acurero@fec.luz.edu.ve, crincon@fec.luz.edu.ve, wvillalobos64@yahoo.com*

## Resumen

El objetivo principal de esta investigación fue determinar el efecto del uso de una Red privada Virtual (*Virtual Private Network* o *VPN*) en los servicios de transferencia de información en Internet a través de dispositivos portátiles, bajo la presencia de ataques de Denegación de Servicio (Denial of Service o DoS). Dicho efecto, fue medido considerando los parámetros independientes: duración del ataque y tamaño de la trama de datos. El experimento consistió en conectar un dispositivo portátil a un enrutador de red inalámbrica, implementando el servicio de VPN bajo el Protocolo de Túneles Punto a Punto (*Point-to-Point Tunneling Protoco*l o PPTP) para someterlo a un ataque de DoS. Los resultados obtenidos determinaron que para el caso donde el dispositivo portátil estuvo conectado a la VPN y no hay presencia de ataques de *DoS,* el Tiempo de Retardo Promedio (*Round Trip Time* o *RTT*) es mayor que cuando no lo está, a diferencia del caso donde existen ataques de DoS donde la VPN ofrece un menor RTT para todos los escenarios de transferencias (variando el tamaño de la trama de datos en 64, 768 y 1518 bytes, respectivamente) en las distintas duraciones de ataques. Asimismo, se determinó que el RTT se ve afectado positivamente al no haber presencia de VPN. Sin embargo, debido a que existe un riesgo elevado de sufrir un ataque de DoS, se recomienda el uso de una VPN para los Servicios de Transferencia de Información de los dispositivos portátiles en Internet.

**Palabras clave:** VPN, transferencia de información, denegación de servicio, dispositivo portátil.

Recibido: 25-06-2009 / Aceptado: 19-02-2010

# The Effect of a VPN on Portable Devices Submitted to DoS Attacks


## Abstract

The main objective of this research was to determine the effect of using a Virtual Private Network (VPN) for information transferring services over the Internet through portable devices undergoing Denial of Service (DoS) attacks. This effect was measured considering the independent parameters of attack duration and data frame size. The experiment consisted of connecting the handheld device to a wireless router using VPN services under the Point to Point Tunneling Protocol (PPTP) to finally submit it to a DoS attack. Results determined that when the handheld device is connected to the VPN, there are no DoS attacks and the Round Trip Time (RTT) is higher than when it is not connected, unlike the case where DoS attacks exist and the VPN offers a lower RTT for all transfer scenarios (varying the data frame size in 64, 768 and 1518 bytes, respectively) and for different attack durations. Also, it was determined that the RTT is affected positively when the VPN is not present. However, because there is a high risk of undergoing a DoS attack, it is recommended that a VPN be used for Information Transfer Services on handheld Internet devices.


**Key words:** virtual Private Net, information transfer, denial of service, handheld devices.

## Introducción

En la actualidad existe una gran demanda de conexión a redes inalámbricas por medio de dispositivos portátiles, para obtener una serie de servicios, como el intercambio de información entre estos dispositivos y servidores o computadoras de escritorio, lo cual ha originado tener una movilidad real, y ha dado paso al denominado Internet Móvil.

Las redes inalámbricas han sido uno de los aspectos más importantes para ofrecer la ventaja de la movilidad, pero sus características presentan ciertos inconvenientes en términos de seguridad con respecto a las redes tradicionales. El uso de redes inalámbricas incrementa la posibilidad de intercambiar información, pero también aumenta la posibilidad de ataques a la misma, por lo que el proteger los datos se ha vuelto una necesidad prioritaria.

El rendimiento, que puede estar afectado por la seguridad de las redes de datos es una de las variables más estudiadas por los investigadores, esto debido a que uno de los retos más importantes de las Redes de Área Local Inalámbricas (*Wireless Local Area Network* o *WLAN*, por sus siglas en inglés), debido a que, utilizan el espectro electromagnético como medio de transmisión, por lo que al diseñar una red con este tipo de medio deben considerarse múltiples factores a los que es susceptible, tal como los niveles y tipos de atenuación de la señal, obstáculos entre emisor y receptor, entre otros, que podrían afectar de manera relevante el rendimiento de las transmisiones.

Por otra parte, explica Richardson [1] que para el año 2006 los virus son el primer tipo de ataque efectuado con un 65%, seguido del robo de equipos, abusos internos y acceso no autorizado a la información, con un 47%, 42% y 32% respectivamente; en el quinto lugar de este estudio se encuentran los ataques de Denegación de Servicio con un 25%; mientras que para el año 2007 son agregados nuevos tipos de ataques como la Suplantación de Identidad (*Phishing*, en inglés) y el uso indebido de Mensajes Instantáneos con un 26% y 25% respectivamente, mientras que el ataque de Denegación de Servicio no sufre cambio alguno en comparación con el año 2006. Ya para el año 2008, la tendencia en general fue a la disminución de todos los ataques presentados, en máximo de 4 puntos porcentuales, tal es el caso de la Denegación de Servicio, la cual disminuyó a un 21%. Los incidentes que mostraron un alza fueron los ataques a los Sistemas de Nombres de Dominio (DNS, por sus siglas en inglés) y los Accesos No Autorizados. Se espera que para el año 2009, la tendencia se mantenga de-

bido a las grandes inversiones que se realizan para contrarrestar dichos ataques.

Según, Verdejo [2] define los ataques de Denegación de Servicio en redes IP como la consecución total o parcial (temporal o totalmente) del cese en la prestación de servicio de un ordenador conectado a Internet. Explica Verdejo [2], que existen dos tipos de Denegación de Servicio: a) Denegación de Servicio Simple, donde el ataque es emitido por un solo origen desde el cual se realiza la denegación y b) Denegación de Servicio Distribuido (DDoS, por sus siglas en inglés), donde existen varias fuentes coordinadas donde se puede hacer un ataque progresivo, rotatorio o total.

Según INICTEL [3], una VPN es una conexión privada (segura) que se hace sobre un enlace público (no confiable) y basa principalmente en los protocolos IPSec y PPTP. Para efectos de esta investigación, se ha utilizado el protocolo PPTP el cual encapsula otros protocolos de Redes de Área Local comunes, como NetBEUI, IPX/SPX (Novell), TCP/IP, entre otros, en un paquete de IP de una forma totalmente transparente para el usuario. También explica INICTEL [3] que el protocolo PPTP funciona con dos canales de comunicación entre el cliente y el servidor. El primer canal se utiliza para control y el segundo transporta el tráfico de la red privada. El canal de control utiliza una conexión TCP estándar con el número de puerto bien conocido 1723 en el servidor de acceso, y el canal de datos, que transporta el tráfico de la red privada, utiliza el tipo de protocolo IP.

En tal sentido, la presente investigación tuvo como finalidad medir el rendimiento de una red inalámbrica ante ataques de Denegación de Servicio, a través de un dispositivo portátil y mediante el uso de una VPN como complemento del entorno de prueba creado.

## Metodología

Para el desarrollo de la investigación en cada una de sus etapas, se usó el método Análisis-Síntesis, ya que con este método el conocimiento de la realidad puede obtenerse a partir de la identificación de las partes que conforman el todo, de acuerdo con Hernández y colaboradores [4].

Inicialmente, se analizó el funcionamiento del dispositivo portátil que se utilizó en el desarrollo de la investigación. Luego, se procedió a definir el tipo y características de las pruebas tomando en cuenta dos variables básicas (duración del ataque y tamaño de la trama de datos), que describen el comportamiento de la red ante una serie de perturbaciones y configuraciones.

Para ello, se utilizó una adaptación de la metodología de Rincón y Rojas [5], para llevar a cabo los experimentos planteados, tomando como base el tamaño de la trama de datos y agregando la duración del ataque; mientras que para medir el rendimiento de la transmisión, se utilizó el tiempo de retardo promedio. Para el caso de la duración del ataque se consideró conveniente utilizar valores de 5, 7 y 10 minutos, puesto que en ensayos efectuados se pudo constatar que la conexión a la VPN, desde el dispositivo portátil, no resistía un ataque de Denegación de Servicio superior a los 15 minutos, ya que antes de que el ataque llegara a este punto, la conexión se perdía completamente.

Asimismo, para el tamaño de la trama de datos se utilizaron los valores de 64, 768 y 1518 bytes respectivamente, tomando en cuenta que los mismos cubrían las necesidades de la transmisión por ser estos considerados por Rincón y Rojas [5], los tamaños de paquetes mínimo, promedio y máximo para una transmisión. La cantidad de paquetes totales enviados varió según la duración y el tamaño de la trama de datos.

Cada uno de los tipos de pruebas fueron realizadas tres veces, ya que según Rincón y Rojas [5] y Montgomery [6] representa el número mínimo de repeticiones que deben realizarse para pruebas experimentales.

El estudio consistió en conectar un dispositivo portátil tipo Asistente Digital Personal (PDA, por sus siglas en inglés) a un enrutador de red inalámbrica bajo estándar 802.11g encargado de administrar el medio, para luego conectarse desde el dispositivo portátil a la VPN.

Asimismo, se utilizó el protocolo PPTP ya que ofrece un intercambio seguro de datos y no requiere inversión adicional para su uso en los tipos de dispositivos portátiles utilizados, ya que forma parte del sistema operativo de Microsoft (Windows Server 2003 del lado del servidor y Windows CE del lado del dispositivo) ya que el servidor utilizado, por razones de configuración, no permitía utilizar otro protocolo y al mismo tiempo garantizaba el seguro intercambio de datos.

Una vez conectado, se sometió al dispositivo a un ataque de Denegación de Servicio durante los tiempos anteriormente definidos y, variando el tamaño de la trama de datos. Para efectos de esta investigación, se utilizó un ataque de Denegación de Servicio simple, y para generar dichos ataques se utilizó la herramienta implementada utilizando el código fuente en Lenguaje C propuesto en InSecure.org [7], llamado CrazyPing, que simula un ping de la muerte, el cual consiste en enviar masivamente paquetes ICMP mayores a 65535 bytes, con el fin de colapsar el sis-

tema atacado. En la Figura 1, se muestra el ambiente de pruebas utilizado.

## Resultados y discusión

En los resultados obtenidos sobre las tramas de datos transmitidas en la ausencia de ataques de Denegación de Servicio, se puede establecer que el Tiempo de Retardo Promedio, se convierte en un factor importante que interviene de modo concluyente en la eficiencia de las redes inalámbricas, tal y como los explica Rincón y Rojas [5].

El primer experimento consistió en variar el tamaño de la trama y el uso de la VPN, sin la presencia de ataques de Denegación de Servicio. Los resultados obtenidos se presentan en la Tabla 1.

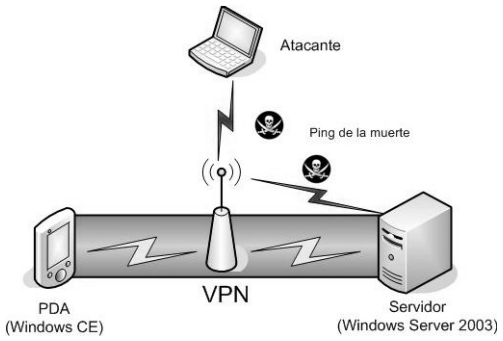
Los resultados obtenidos en el experimento permiten determinar que a medida que aumenta el tamaño de la trama, aumenta el RTT. Además se constata que el Tiempo de Retardo Promedio es mayor cuando se utiliza la VPN; esto debido a que parte de la capacidad del canal es consumida por el túnel de la VPN.

El segundo experimento consistió en variar el tamaño de la trama, el uso de la VPN y el tiempo (duración) de los ataques de Denegación de Servicio, utilizando el esquema de experimentación implementado en Rincón y Rojas [5].

Los resultados obtenidos para ambas situaciones (con y sin VPN), cuando se sometió al ataque de Denegación de Servicio y con una duración de 5, 7 y 10 minutos, se muestran en las Tablas 2, 3 y 4 respectivamente.

Puede notarse que los Tiempos de Retardo Promedio, para el caso en el que el dispositivo está conectado a la VPN, son menores (para todos los tiempos de ataques de Denegación de Servicio); esto porque al poseer la VPN un túnel de comunicación ofrece un ancho de banda exclusivo para la transferencia evitando así que el Tiempo de Retardo Promedio sea superior que para el caso en el cual no está conectado a la VPN. Esto se debe a las características propias de funcionamiento y configuración de la VPN.

Además, se observó que a medida que aumenta el tamaño de la trama de datos, el Tiempo de Retardo Promedio aumenta para las dos situaciones (con y sin el uso de VPN) y para los tres tiempos de ataques de Denegación de servicio. Lo anterior se debe a que al no existir un canal reservado que consuma ancho de banda y sin haber exposición a ningún tipo de ataque, el rendimiento del servicio de transferencia de información del dispositivo portátil, es sustancialmente mejor que cuando existe un ataque. Asimismo, otro factor que contribuye a esta situación es que a medida que el tamaño de la trama de datos aumenta el




Fuente: Villalobos [8].

Figura 1. Ambiente de prueba.

Tabla 1. Tiempo de Retardo Promedio sin Ataques (milisegundos).

| Tamaño Trama de Datos | Con VPN | Sin VPN |
|---|---|---|
| 64 bytes | 7,7 | 7,6 |
| 768 bytes | 19,7 | 12,7 |
| 1518 bytes | 31,7 | 14,0 |

Fuente: Villalobos [8].

Tabla 2. Tiempo de Retardo Promedio con Ataques de 5 minutos (milisegundos).

| Tamaño Trama de Datos | Con VPN | Sin VPN |
|---|---|---|
| 64 bytes | 374,7 | 468,8 |
| 768 bytes | 342,9 | 498,4 |
| 1518 bytes | 330,1 | 552,9 |

Fuente: Villalobos [8].

Tabla 3. Tiempo de retardo promedio con ataques de 7 minutos (milisegundos).

| Tamaño Trama de Datos | Con VPN | Sin VPN |
|---|---|---|
| 64 bytes | 378,3 | 480,6 |
| 768 bytes | 375,3 | 520,5 |
| 1518 bytes | 1628,0 | 1676,2 |

Fuente: Villalobos [8].

Tabla 4. Tiempo de retardo promedio con ataques de 10 minutos (milisegundos).

| Tamaño Trama de Datos | Con VPN | Sin VPN |
|---|---|---|
| 64 bytes | 387,9 | 511,3 |
| 768 bytes | 386,5 | 524,1 |
| 1518 bytes | 2082,0 | 2257,0 |

Fuente: Villalobos [8].

Tiempo de Retardo Promedio, obteniéndose un comportamiento similar que en ambientes de VPN y el uso de IPSec, de acuerdo con Carruyo [9].

A pesar que el rendimiento se midió a través del tiempo de retardo promedio (RTT) y no sobre el porcentaje de paquetes perdidos y recibidos, pruebas complementarias transmitiendo la misma cantidad de paquetes de distintos tamaños (64, 768 y 1518 bytes) sometidos al ataque de DoS, con variación de la duración de 5, 7 y 10 minutos los valores promedios obtenidos fueron los siguientes, para cuando la VPN no estuvo activa: a) para un data frame de 64bytes, tasa de paquetes recibidos fue del 97,8% y la tasa de paquetes perdidos fue de 2,2%. b) para un data frame de 768bytes, la tasa de paquetes recibidos fue del 95,6% y la tasa de paquetes perdidos fue del 4,4%. c) para un data frame de 1518bytes, la tasa de paquetes recibidos fue del 86,7% y la tasa de paquetes perdidos de 13,3%. Por otra parte, dada las mismas consideraciones, pero contando con la VPN activa, los valores obtenidos fueron los siguientes: a) para un data frame de 64bytes, tasa de paquetes recibidos fue del 93,3% y la tasa de paquetes perdidos fue de 6,7%. b) para un data frame de 768bytes, la tasa de paquetes recibidos fue del 88,9% y la tasa de paquete perdidos fue del 11,1%. c) para un data frame de 1518bytes, la tasa de paquetes recibidos fue del 51,1% y la tasa de paquetes perdidos de 48,9%.

En consecuencia, como el ataque genera la repetición de solicitudes, el canal se satura, por lo tanto, el túnel de la VPN no puede dar respuestas a las solicitudes del dispositivo portátil, efecto que se incrementa a medida que aumenta el tamaño del paquete, tal como se muestra en el Gráfico 1.

Finalmente y en virtud de lo discutido, se demuestra que los ataques de Denegación de Servicio, a pesar de no ser uno de los ataques más peligrosos durante el año 2008, de acuerdo con Richardson [1], siguen afectando y en buena medida el rendimiento de una red de datos, en contraparte a la seguridad que ofrece el uso de la VPN.

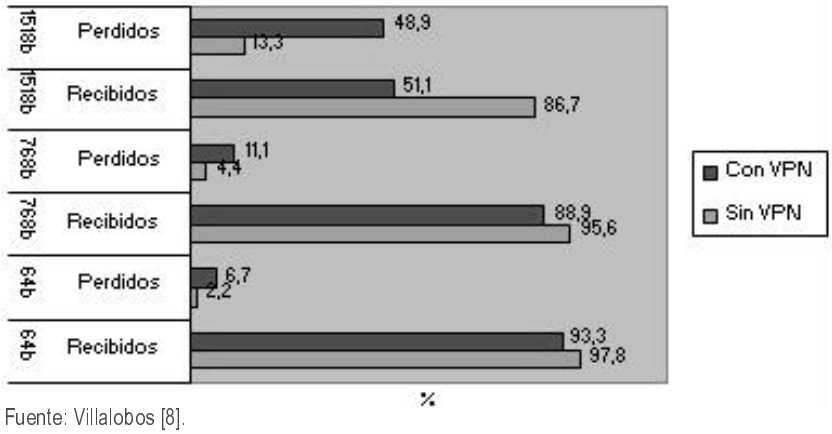
Sin embargo, los resultados obtenidos determinaron que para el caso donde el dispositivo portátil está conectado a la VPN y no hay presencia de ataques de Denegación de Servicio, el Tiempo de Retardo Promedio es mayor que cuando no está conectado a la VPN; a diferencia del caso donde existen ataques de Denegación de Servicio donde el Tiempo de Retardo Promedio es menor en todos los escenarios de transferencias y para las distintas duraciones de ataques (5, 7 y 10 minutos respectivamente).

## Conclusiones y trabajo futuro

La VPN como medio seguro para el rendimiento del servicio de transferencia de información, ofrece menor Tiempo de Retardo Promedio, cuando existen ataques de Denegación de Servicio, independientemente del tamaño de la trama o de la duración del ataque (menor o igual a 10 minutos).

Las pruebas complementarias sobre el porcentaje de paquetes recibidos y perdidos mostraron que la cantidad de paquetes perdidos fue mayor cuando la VPN estuvo activa, esto como consecuencia del tamaño de la cabecera que debe añadirse debido al túnel, no pudiendo dar respuesta a las solicitudes del Dispositivo Portátil ocasionando la pérdida reiterada de los paquetes a medida que aumenta el tamaño del data frame.

Como consecuencia de lo anterior, a partir de las variables planteadas (Tamaño de la Trama de Datos y Duración del Ataque) se demostró que, los dispositivos portátiles conectados a las Redes Privadas Virtuales bajo ataques de Denegación de Servicio (DoS) son susceptibles a la duración del ataque.




Fuente: Villalobos [8].

Gráfico 1. Porcentaje de paquetes perdidos y recibidos.

Finalmente, ante el elevado riesgo de sufrir un ataque de Denegación de Servicio, la VPN es una buena elección ya que ofrece mejor rendimiento desde el punto de vista de la seguridad para todos los casos de transferencias de información.

En futuras investigaciones con dispositivos portátiles, se pretende utilizar TCP-ER (TCP-Explicit Rate, en inglés) ya que en entornos susceptibles a pérdidas de datos, este protocolo puede distinguir entre la pérdida que se debe a la congestión y las pérdidas debido a inconsistencias del enlace, según Brassil y colaboradores [10], con lo que se busca complementar situaciones de ataques de Denegación de Servicio.

## Referencias

[1] RICHARDSON, Robert (2006), (2007), (2008). CSI/FBI Computer Crime and Security Survey (Documento en Línea), Disponible: http://gocsi.com (consulta: 2010, marzo 26).

[2] VERDEJO, Gabriel (2003). **Seguridad en redes IP.** Universidad Autónoma de Barcelona. Departamento de Informática.

[3] INICTEL (2008). **Diseño de soluciones de VPN.** Posgrado a Distancia. Redes de Comunicaciones de Datos. Módulo 4.

[4] HERNÁNDEZ SAMPIERI, R.; FERNÁNDEZ COLLADO, C.; BAPTISTA LUCIO, P. (2008). **Metodología de la Investigación**. 4° Edición. Edit. McGraw-Hill Editores, S.A. de C V México.

[5] RINCÓN, C.; ROJAS, L. (2004). Simulación del rendimiento de una red ethernet. **Ciencia** 12(3): 155-164.

[6] MONTGOMERY, D. (2004). **Diseño y Análisis de Experimentos.** Segunda Edición. Editorial Limusa Wiley.

[7] InSecure.org. (1997). Ping oF Death (Documento en Línea). Disponible http://insecure.org/sploits/ping-odeath.html (consulta: 2008. septiembre, 22).

[8] VILLALOBOS, Wuende (2009). Efecto del uso de una Red Privada Virtual en el rendimiento de las conexiones para los servicios de transferencia de información de los dispositivos móviles en Internet. Universidad del Zulia. Facultad Experimental de Ciencias. Licenciatura en Computación. Maracaibo. Venezuela.

[9] CARRUYO, Carlos (2006). Niveles de seguridad en wlan basadas en ipv6 mediante el uso de VPN. Universidad del Zulia. Facultad Experimental de Ciencias. Licenciatura en Computación. Maracaibo. Venezuela.

[10] BRASSIL, J.; McGEER, R.; RAJAGOPALAN, R.; BAVIER, A.; ROBERTS, L.; MARK, B.; SCHWAB, S. Improving VPN Performance over Multiple Access Links. Presentado en la 5th International Conference on: Broadband Communications, Networks and Systems, 2008 (BROADNETS 2008), September 2008. This document was created with Win2PDF available at http://www.daneprairie.com. The unregistered version of Win2PDF is for evaluation or non-commercial use only.