

Urkund Analysis Result

Analysed Document: propuesta_version_urkund20194885139.docx (D50493890)
Submitted: 4/11/2019 12:06:00 AM
Submitted By: fbravod@unemi.edu.ec
Significance: 2 %

Sources included in the report:

PROY_PERALTA JOSE28-11.docx (D23864535)
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-74252013000300005

Instances where selected sources appear:

3

INTRODUCCIÓN

Una de las tendencias tecnológicas más transformadoras de la última década es la disponibilidad y la creciente expectativa de conectividad. Ya sea para revisar el correo electrónico, llevar una conversación de voz, navegar por la web o un sinnúmero de otros casos de uso, ahora esperamos poder acceder a estos servicios en línea sin importar la ubicación, la hora o la circunstancia: en la carrera, mientras estamos en la cola, en la oficina, en un metro, en vuelo, y en todas partes. Hoy en día, todavía nos vemos forzados a ser proactivos a la hora de encontrar conectividad (por ejemplo, buscar un punto de acceso WiFi cercano) pero, sin lugar a dudas, el futuro se trata de la conectividad ubicua donde el acceso a Internet es omnipresente. Las redes inalámbricas se encuentran en el epicentro de esta tendencia. En su forma más amplia, una red inalámbrica se refiere a cualquier red no conectada por cables, que es lo que permite la conveniencia y movilidad deseadas para el usuario. No es sorprendente que dada la gran cantidad de aplicaciones y casos de uso diferentes, también deberíamos esperar ver docenas de tecnologías inalámbricas diferentes para satisfacer las necesidades, cada una con sus propias características de rendimiento y cada una optimizada para una tarea y contexto específicos. Hoy en día, ya tenemos más de una docena de tecnologías inalámbricas en uso: WiFi, Bluetooth, ZigBee, NFC, WiMAX, LTE, HSPA, EV-DO, estándares 3G anteriores, servicios satelitales y más. Como tal, dada la diversidad, no es prudente hacer generalizaciones radicales sobre el rendimiento de las redes inalámbricas. Sin embargo, la buena noticia es que la mayoría de las tecnologías inalámbricas funcionan según principios comunes, tienen concesiones comunes y están sujetas a criterios y restricciones de rendimiento comunes. Una vez que descubramos y comprendamos estos principios fundamentales del rendimiento inalámbrico, la mayoría de las otras piezas comenzarán a encajar automáticamente. Además, mientras que la mecánica de la entrega de datos a través de la comunicación por radio es fundamentalmente diferente del mundo atado, el resultado experimentado por el usuario es, o debería ser, todo lo mismo: el mismo rendimiento, los mismos resultados. A la larga, todas las aplicaciones son y serán entregadas a través de redes inalámbricas; puede darse el caso de que a algunos se acceda con más frecuencia a través de la red inalámbrica que a otros. No existe tal cosa como una aplicación cableada, y no hay demanda para tal distinción. Todas las aplicaciones deben funcionar bien independientemente de la conectividad subyacente. Como usuario, no debe preocuparse por la tecnología subyacente en uso, pero como desarrolladores debemos pensar con anticipación y diseñar nuestras aplicaciones para anticipar las diferencias entre los diferentes tipos de redes. Y la buena noticia es que cada optimización que apliquemos a las redes inalámbricas se traducirá en una mejor experiencia en todos los demás contextos. La presente investigación a elaborar está compuesta por 5 Capítulos que consisten en: Capítulo 1: Este capítulo abarca el desarrollo de la temática, la descripción del problema de la investigación, sus objetivos y justificación. Capítulo 2: Es la elaboración del marco teórico de la investigación basados en repositorios científicos, libros para su elaboración. Capítulo 3: Se describe la metodología a usar en este caso es una investigación de campo-cualitativa. Capítulo 4: Es la elaboración de desarrollo del tema que es análisis de software en la implementación de VPN en LAN inalámbrica. Capítulo 5: En este se realiza las conclusiones a las que se llegaron mediante la propuesta de investigación planteada.

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema. Las redes inalámbricas están obligando a las organizaciones a replantearse por completo cómo protegen sus redes y dispositivos para evitar ataques y mal uso que exponen activos críticos y datos confidenciales. Por su propia naturaleza, las redes inalámbricas son difíciles de implementar, proteger y administrar, incluso para los administradores de redes más inteligentes. En los últimos cinco años, el mundo se ha vuelto cada vez más móvil. Como resultado, las formas tradicionales de conexión en red del mundo han demostrado ser inadecuadas para enfrentar los desafíos planteados por nuestro nuevo estilo de vida colectivo. Si los usuarios deben estar conectados a una red mediante cables físicos, su movimiento se reduce drásticamente. La conectividad inalámbrica, sin embargo, no presenta tal restricción y permite un movimiento mucho más libre por parte del usuario de la red. Como resultado, las tecnologías inalámbricas están invadiendo el ámbito tradicional de las redes "fijas" o "cableadas". Las redes de telefonía inalámbricas han tenido éxito porque permite que las personas se conecten entre sí independientemente de su ubicación. Las nuevas tecnologías dirigidas a las redes de computadoras prometen hacer lo mismo con la conectividad a Internet. La tecnología de redes de datos inalámbricas más exitosa hasta el momento ha sido 802.11 CITATION Ady04 \l 12298 (Adya, Bahl, Padhye, Wolman, & Zhou, 2004). CITATION Pér12 \l 12298 (Pérez, Herrera, Uzcátegui, & Bernardo, 2012) Detalla que para la propagación de una red inalámbrica más allá de la seguridad que debe proporcionar este se enfoca en otros aspectos para poder medir la cobertura la red puede alcanzar que también son importantes tales como: morfología, condiciones atmosféricas y topología. Ahora se puede transmitir a través de redes de transmisión de información archivos multimedia como: video, audios, imágenes. Pero esto a través de una red IP convencional nos permite visualizar una serie de retos, ya que se ajustan a las necesidades de ese tipo de tráfico, para que los elementos de red deban tener las características apropiadas para su correcto funcionamiento. De ser así de complejo en una red por medio de cables, pues se maximiza la dificultad en una red inalámbrica, ya que el medio es compartido con todo lo que en él se esté transportando CITATION Mar13 \l 12298 (Cruz, Martínez, & Crespo, 2013). Debido a todos estos problemas que conlleva el uso de una red inalámbrica es necesario conocer cuáles con las herramientas necesarias para poder tener mayor seguridad y eficiencia en el tráfico de datos.

1.2 Objetivo General Determinar la factibilidad de una red inalámbrica local mediante el uso de VPN.

1.3 Objetivos Específicos • Identificar herramientas para la implementación de VPN en LAN inalámbrica. • Analizar el funcionamiento de herramientas en la implementación de VPN en LAN inalámbrica.

• Describir los pasos que conlleva el uso de herramientas en la implementación de VPN en LAN inalámbrica.

1.4 Justificación

Los departamentos de TI deben tener un plan de acción preventivo para prevenir ataques maliciosos y el mal uso de los empleados que comprometa la privacidad de los datos de una organización y hacer cumplir las políticas de seguridad para el uso inalámbrico, tanto dentro como fuera de sus instalaciones. Ya sea que una empresa haya autorizado o no el uso de la tecnología inalámbrica o que tenga una política de "no conexión inalámbrica", sus redes, datos, dispositivos y usuarios están expuestos y en riesgo. Para garantizar una protección de amenazas inalámbricas efectiva y automatizada, las compañías y organizaciones deben implementar una solución de seguridad inalámbrica completa que cubra los activos en toda la empresa que les permita descubrir vulnerabilidades, evaluar amenazas, prevenir ataques y garantizar el cumplimiento continuo, de la manera más segura y fácil Uso y manera rentable disponible.

CAPÍTULO 2

MARCO TEÓRICO CONCEPTUAL

2.1 Redes Inalámbricas. Según CITATION Joa11 \l 12298 (Andreu, Redes inalámbricas (Servicios en red), 2011) son redes que no necesitan de un cableado y que suelen tener una comunicación

0: PROY_PERALTA JOSE28-11.docx

64%

por medios no guiados a través de ondas electromagnéticas. Tanto la transmisión de datos y la recepción de los mismos se realiza a través de antenas.

Comúnmente el emisor posee una antena, pero puede ser que tengas más de una, debido a que hay sistemas que necesitan más de una antena para su funcionamiento. Las antenas son usadas como emisores o como receptores y en algunos casos pueden realizar ambas funciones.

2.2 Red Privada Virtual (VPN) VPN ha sido una tecnología importante desde su creación a mediados de la década de 1990. PPTP (PPTP) marcó un punto de partida en la capacidad de conectar los equipos remotos a una red común. Desde entonces, existen muchos avances e innovaciones en el campo, lo que resultó en tecnologías de la competencia. A medida que las tecnologías maduran, es importante centrarse en su comparación y evaluación de sus viabilidades de nuevos casos de uso de redes y paradigmas. Uno de tales paradigma es las funciones de red de virtualización (NFV) según CITATION Jim14 \l 12298 (Esch, 2014). El NFV asume las funciones de red móvil, tal como un servidor de seguridad, punto final de VPN, equilibrador de carga, etc. Actualmente, existen dos tecnologías dominantes utilizadas en los entornos empresariales: IPSec y SSL / TLS OpenVPN base. CITATION DLa17 \l 12298 (Lacković & Tomić, 2017) Detalla que existen dos tipos de conexiones VPN de capa de red tales como: acceso remoto y de sitio a sitio. Las VPN de acceso remoto se utilizan para conectar teletrabajadores o configurar túneles temporales, y las VPN de sitio a sitio son usadas para establecer túneles de capa de red seguras permanentes entre las redes distantes. VPN es una

tecnología que proporciona a los usuarios una forma de lograr una comunicación segura por medio de un canal de comunicación inseguro, como el internet público. Ha sido aceptado ya que su flexibilidad y disponibilidad en muchas plataformas. Por lo general se utiliza como una vía alterna a las costosas líneas arrendadas. Para las configuraciones tradicionales, los puntos finales de VPN se instalan en los dispositivos de hardware, entre estos están los firewalls y los routers. En las redes actuales, que usan funciones de red de virtualización (NFV), los puntos finales VPN pueden ser virtualizados en servidores comunes. Ya que el cifrado y descifrado de datos son procesos intensivos del CPU, es necesario conocer los límites de estas configuraciones de modo que la viabilidad de la virtualización de punto final puede ser evaluada CITATION Gab14 \l 12298 (Díaz, Alzórriz, & Sancristóbal, 2014). CITATION Dee14 \l 12298 (Dhiman, 2014) Y CITATION Bor01 \l 12298 (N, I, & D, 2001) concuerdan que las redes inalámbricas son propensas a sufrir ataques tales como: acceso no autorizado, hombre en el medio (MITM), difusión de la información, degradación de servicios, entre otros. Para CITATION Ber11 \l 12298 (Hoekstra & Musulin, 2011) estos problemas son los que hacen a los usuarios utilizar redes privadas virtuales (VPN) para poder fortalecer la seguridad en la red. Una VPN proporciona confidencialidad e integridad de los datos a través del cifrado y la autenticación del tráfico de un enlace entre dos o más dispositivos de red. Este enlace entre estos dispositivos se realiza por un canal de comunicación denominado túnel, está protegido usando encriptación extremo a extremo. Para CITATION LCa17 \l 12298 (Caldas-Calle, Jara, Huerta, & Gallegos, 2017) la integridad y la autenticación se las obtienen a través de algoritmos de autenticación, mecanismos de intercambio de claves o certificados. Debido a esto, la VPN es usada para conectar dispositivos remotos a redes privadas a través de una red pública. Algunos autores estudiaron el comportamiento de los parámetros de calidad de servicio en una VPN a través de una Red Inalámbrica. Por ejemplo CITATION Sam16 \l 12298 (Kolahi, Cao, & Chen, 2016) determina el comportamiento de los parámetros de ida y vuelta y el rendimiento en los protocolos de VPN (IPSec y SSL) con Windows. Para CITATION Pra11 \l 12298 (Likhar, Yadav, & M, 2011) los resultados de las mediciones que realizó determinaron que los parámetros de variación rendimiento, la latencia, tasa de pérdida de tramas y retardo de paquetes disminuyeron la QoS de la red. CITATION CJC00 \l 12298 (Pena & Evans, 2000) Realizó un análisis de la utilización del CPU cuando se presenta la aplicación de software para la creación de VPN. CITATION Jun12 \l 12298 (Qu, Dang, & Li, 2012) Analizaron el uso de OpenVPN en una tableta con sistema operativo Android.

2.3 Red de Área Local (LAN) Una red de área local proporciona capacidad de conexión en red a un grupo de computadoras que se encuentran muy cerca unas de otras, como en un edificio de oficinas, escuela u hogar. Las LAN generalmente se crean para permitir compartir recursos y servicios como archivos, impresoras, juegos, aplicaciones, correo electrónico o acceso a Internet CITATION Joa11 \l 12298 (Andreu, Mantenimiento de LAN (Redes locales), 2011). Una LAN Wi-Fi típica opera uno o más puntos de acceso inalámbrico a los que se conectan los dispositivos dentro del rango de la señal. Estos puntos de acceso, a su vez, administran el tráfico de la red que fluye hacia y desde los dispositivos locales y también puede conectar la red local con redes externas. En una LAN doméstica, los enrutadores de banda ancha inalámbricos realizan las funciones de un punto de acceso CITATION Sha15 \l 12298 (Pongo, 2015). Una LAN Ethernet típica consiste en uno o más concentradores, conmutadores o enrutadores a los que se conectan los dispositivos individuales a través de cables Ethernet.

Tanto Wi-Fi como Ethernet también permiten que los dispositivos se conecten entre sí directamente (por ejemplo, conexiones entre pares o ad-hoc) en lugar de a través de un dispositivo central, aunque la funcionalidad de estas redes es limitada. Aunque Ethernet y Wi-Fi se usan generalmente en la mayoría de las empresas y hogares, debido a los bajos costos y los requisitos de velocidad, también puede configurar una LAN con conexiones de fibra

CITATION Rai12 \l 12298 (Onvural & Nilsson, 2012). Todos los sistemas operativos de red populares ofrecen soporte integrado para la tecnología TCP / IP requerida.

2.4 Red de Área Local Inalámbrica (WLAN) Una red de área local inalámbrica (WLAN) es una red de área local (LAN) que no se basa en conexiones Ethernet por cable. Una WLAN puede ser una extensión de una red cableada actual o una alternativa a la misma. Las WLAN tienen velocidades de transferencia de datos que van de 1 a 54 Mbps, y algunos fabricantes ofrecen soluciones propietarias de 108 Mbps. El estándar 802.11n puede alcanzar los 300 a 600Mbps

CITATION NVa05 \l 12298 (Vaidya, Dugar, Gupta, & Bahl, 2005) . Debido a que la señal inalámbrica se transmite para que todos puedan compartirla, se requieren varias precauciones de seguridad para garantizar que solo los usuarios autorizados puedan acceder a su WLAN. Se puede transmitir una señal WLAN para cubrir un área que varía en tamaño desde una oficina pequeña hasta un campus grande. Más comúnmente, un punto de acceso WLAN proporciona acceso dentro de un radio de 65 a 300 pies

CITATION Nut12 \l 12298 (García, 2012). Según

CITATION Leo11 \l 12298 (Korowajczuk, 2011) Las LAN y las WLAN se pueden combinar mediante un puente que conecta las dos redes. Muchos enrutadores inalámbricos también incluyen puertos Ethernet, que proporcionan conexiones para un número limitado de dispositivos inalámbricos. En la mayoría de los casos, los enrutadores inalámbricos actúan como un puente, combinando los dispositivos Ethernet y Wi-Fi conectados en la misma red. Esto permite que los dispositivos cableados e inalámbricos se comuniquen entre sí a través de un solo enrutador.

2.4.1 Ventajas de las WLAN La ventaja más obvia de una WLAN es que los dispositivos pueden conectarse de forma inalámbrica, eliminando la necesidad de cables. Esto permite que los hogares y las empresas creen redes locales sin cablear el edificio con Ethernet. También proporciona una forma para que los dispositivos pequeños, como teléfonos inteligentes y tabletas, se conecten a la red. Las WLAN no están limitadas por la cantidad de puertos físicos en el enrutador y, por lo tanto, pueden admitir docenas o incluso cientos de dispositivos. El rango de una WLAN se puede ampliar fácilmente agregando uno o más repetidores. Finalmente, una WLAN se puede actualizar fácilmente al reemplazar los enrutadores con nuevas versiones, una solución mucho más sencilla y económica que la actualización de cables Ethernet viejos.

2.4.2 Desventajas de las WLAN Las redes inalámbricas son naturalmente menos seguras que las redes cableadas. Cualquier dispositivo inalámbrico puede intentar conectarse a una WLAN, por lo que es importante limitar el acceso a la red si la seguridad es una preocupación. Esto se realiza normalmente mediante la autenticación inalámbrica, como WEP o WPA, que cifra la comunicación. Además, las redes inalámbricas son más susceptibles a la interferencia de otras señales o barreras físicas, como las paredes de concreto.

CAPÍTULO 3

METODOLOGÍA

Para CITATION Ber06 \ 12298 (Augusto, 2006) encontrar una estrategia de diseño de investigación es similar al proceso de investigación en su totalidad: primero, busque información general sobre el diseño y los métodos de investigación, luego obtenga conocimientos básicos sobre la metodología que abordaría de manera más apropiada el tipo de datos que recopilará y finalmente elija una metodología y prueba / medida para utilizar en su investigación.

3.1 Metodología Descriptiva Para CITATION Her04 \ 12298 (Hernández Sampieri, 2004) los estudios descriptivos son aquellos que a partir de una variable se pretende medir o recolectar información, ya sea esta de forma independiente o conjunta. Pues se busca conocer y explicar cómo es que se manifiesta el fenómeno o suceso de interés.

3.2 Investigación Documental "Es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos"

CITATION Fid12 \ 12298 (Arias, 2012).

3.3 Extracción de Información Para esta investigación es necesario extraer la información necesaria de fuentes bibliográficas confiables, en los que se detalle el funcionamiento de las redes inalámbricas.

3.4 Selección de Herramientas La selección de las herramientas a utilizar para la implementación de VPN se da en base a la obtención de la información de repositorios virtuales, donde se especifique el uso de estas en temas similares.

3.5 Pruebas Las Pruebas se realizan en base al uso de las herramientas seleccionadas, el cual se procede a verificar cuál es el comportamiento de la Tecnología a configurar y se determina cuál es la más óptima en base al comportamiento de la red inalámbrica con el uso de la VPN.

CAPÍTULO 4

DESARROLLO DEL TEMA

Una VPN se usa en la red WLAN para transmitir los datos con mayor seguridad, ya que el tráfico que se genera viaja cifrado y es más difícil para que una tercera persona tenga acceso a la información transmitida, existen servicios gratuitos y otros de pago. En el desarrollo del tema seleccionamos 3 herramientas VPN que son:

- SEED4.ME
- Windscribe

- TunnelBear

El análisis se realizó en una red inalámbrica local usando un router de 300mbps y ordenadores portátiles, para medir la velocidad de transmisión de datos se utilizó el software LAN Speed Test más adelante describiremos las características de esta herramienta.

4.1 SEED4.ME

Es una herramienta VPN que permitirá la transmisión de datos de forma segura, podemos navegar de forma anónima y privada, esta herramienta está disponible para diferentes plataformas, tiene una versión de prueba que dura 7 días.

TABLA

4.2 Windscribe Es una aplicación para ordenadores y una extensión de navegador que trabajan entre sí para bloquear anuncios, rastreadores, acceder a lugares bloqueados, protege la privacidad en línea. TABLA

4.3 TunnelBear Facilita la protección de su privacidad en línea y disfruta de un internet menos restringida. TABLA

4.4 LAN Speed Test Es una herramienta que sirve para medir archivos, velocidad de transferencia en una red de área local cableada e inalámbrica, el test consiste en la medición del tiempo que tarda esta herramienta en enviar y recibir un paquete de una carpeta compartida en la red local. Algunas de las características de LAN Speed Test 4 incluyen: • Pruebe la velocidad de su red local probando desde / hacia las carpetas compartidas de la red. • Pruebe la velocidad de sus unidades locales (unidades USB, discos duros, etc.)

• Compatible con el servidor LST (v1.5 o posterior) para resultados reales de rendimiento de red sin disco duro limitaciones: incluso pruebe la velocidad de su WAN (Internet) con el servidor LST.

• ¡Muy rápido! La mayoría de las pruebas son menos de 1 minuto.

• Completamente portátil - No necesita instalación.

• Puede ejecutarse desde un disco duro, unidades flash USB, redes compartidas, etc.

• Compatible con Windows 7 o posterior y Windows Server 2008 o posterior.

• Compatible con Mac 10.7.5 (Lion) o posterior.

• La prueba de velocidad de LAN y la prueba de velocidad de LAN (Lite) ahora son la misma descarga.

• Paquetes de hasta 9 GB de tamaño y hasta 1000 paquetes.

• Tamaño de trozo ajustable hasta 1 MB (para probadores avanzados).

• Ver resultados por promedio, máximo y rendimiento mínimo.

• Barra de progreso y botón de cancelación que permite al usuario cancelar en cualquier momento.

• Posibilidad de elegir la tarjeta de interfaz de red para computadoras con múltiples NIC.

• Posibilidad de ver los resultados de cada paquete en un gráfico o por detalles.

• Posibilidad de ver resultados como Gbps, Mbps, Kbps, GBps, MBps o KBps.

• Envíe los resultados por correo electrónico de forma manual, automática o solo cuando esté bajo una cierta velocidad.

- Registre los resultados en el archivo .csv con la ubicación del archivo configurable por el usuario. Todas las entradas son compatibles con SQL para fácil importando a SQL Server, MySql, etc.).
- Opción para registrar Avg, Max, & Min automáticamente.
- Ver / Editar registro integrado en la prueba de velocidad de LAN.
- Exploración de red (vea otros dispositivos en su red, mantenga notas sobre ellos, etc.
- Ejecute varias pruebas de forma automática: cualquier número de pruebas desde 1 segundo hasta 24 horas.
- Abrir / Guardar todas las opciones y resultados en un archivo .csv.
- Modo de línea de comandos: todas las opciones de prueba disponibles desde la línea de comandos.
- Command Line Builder (crea automáticamente las opciones de línea de comando que necesita en función de su configuración actual).

4.4.1 Instalación del software LAN Speed Test Primero vamos a la página de descarga del software y damos click en Descargar IMAGEN Figura 11 Página para descargar el software

Lo segundo que hacemos es ejecutar el instalador y esperar a que termine el proceso de instalación. IMAGEN

Figura 22 Instalación del programa LAN Speed Test

4.5 Desarrollo de pruebas Luego que tenemos instalado el programa LAN Speed Test debemos descargar las herramientas VPN que utilizaremos para las pruebas.

IMAGEN

Figura 33 Instaladores de programas que se usaran para las pruebas.

4.5.1 Pruebas sin usar VPN Primero probaremos sin usar ninguna herramienta VPN, para ello creamos una carpeta compartida en el ordenador al cual se enviara un archivo, así podremos saber la velocidad de transmisión de datos. IMAGEN

Figura 44 Prueba en red WLAN sin VPN

Se creó una carpeta llamada prueba dándole permiso de escritura, la cual se encuentra compartida en la red y pertenece al ordenador con IP 192.168.1.102 por ello en el textbox de Folder escribimos la dirección y el nombre de la carpeta \\192.168.1.102\prueba, el tamaño del paquete es de 3 Mb se puede aumentar o disminuir el tamaño. Damos click en el botón Start Test, obtuvimos lo siguiente. IMAGEN

Figura 55 Resultados sin usar VPN

IMAGEN

Figura 66 Grafico de velocidad de la red sin usar VPN

4.5.2 Pruebas usando SEED4.ME Una vez instalada la herramienta SEED4.ME la ejecutamos y procedemos hacer lo mismo que se hizo anteriormente obteniendo estos resultados. IMAGEN

Figura 77 Detalles del test realizado sin usar VPN IMAGEN

Figura 88 Resultados usando SEED4.ME

IMAGEN

Figura 99 Gráfico de velocidad usando SEED4.ME

IMAGEN

Figura 1010 Detalles del test usando SEED4.ME

4.5.3 Pruebas usando TunnelBear

IMAGEN

Figura 1112 Ejecución del programa TunnelBear

IMAGEN

Figura 1211 Resultados usando TunnelBear IMAGEN

Figura 1313 Gráfico de velocidad usando TunnelBear

IMAGEN

Figura 1414 Detalles del test usando TunnelBear

4.5.4 Pruebas usando Windscribe IMAGEN

Figura 1515 Ejecución de la herramienta Windscribe

IMAGEN

Figura 1616 Resultado con la herramienta Windscribe

IMAGEN

Figura 1717 Gráfico de velocidad de transmisión de datos usando Windscribe

IMAGEN

Figura 1818 Detalles del test realizado con la herramienta Windscribe

Una vez realizadas las pruebas pudimos observar que la velocidad de transmisión de datos varía en las diferentes herramientas usadas, cabe recalcar que para todas las herramientas el tamaño del paquete enviado fue el mismo. En el siguiente gráfico se muestra la comparación de resultados obtenidos.

TABLA

CAPÍTULO 5

CONCLUSIONES

Las redes inalámbricas locales (WLAN) como cualquier otro tipo de red son vulnerables a diferentes ataques es por eso la propuesta de usar una VPN en la red local esto nos permite tener una mayor seguridad de la información, asegura el flujo de tráfico en la red. Realizamos pruebas con diferentes herramientas VPN para constatar cual es la más viable y conveniente al momento de usar, con los resultados comprobamos que el tiempo de respuesta y carga varía, se hizo una prueba sin usar ninguna VPN, al momento de conectarnos con una VPN y realizar el test se puede notar la diferencia de velocidad de transmisión de datos uno de los motivos es porque las VPN usan el cifrado de extremo a extremo para evitar que alguien haga captura de nuestro tráfico de red, este proceso de cifrado puede ralentizar la conexión, si presentamos problemas con la velocidad podemos bajar el nivel de cifrado o cambiar el protocolo de VPN aunque esto representaría un riesgo para la integridad de los datos. Verificamos la velocidad de transmisión de los datos mediante el software LAN Speed Test es una herramienta sencilla pero muy útil, el trabajo que realiza esta aplicación es el siguiente, copia el paquete del tamaño que nosotros establecimos desde el ordenador que envía al que recibe, mide el tiempo que dura este proceso y así obtiene la velocidad que existe en la red, algo sencillo pero muy eficaz. Después de comparar los resultados obtenidos de las pruebas realizadas concluimos que la herramienta VPN mas apta para usar en la red WLAN es Windscribe, fue la que más destaco entre las otras, con una velocidad de subida de 28,90 Mbps y de descarga 49,90 Mbps. Windscribe puede conectar simultáneamente a múltiples dispositivos cuenta con tecnología OpenVPN y cifrado AES de 256 bits, ofrece un gran cifrado y anonimato total, también hay que mencionar que esta herramienta tiene varios complementos que lo hacen aún más interesante como el bloqueador de publicidad o la herramienta Split Personality que cambia el usuario del navegador para evitar dejar rastro.

REFERENCIAS BIBLIOGRÁFICAS

- Adya, A., Bahl, P., Padhye, J., Wolman, A., & Zhou, L. (29 de Octubre de 2004). [ieeexplore.ieee.org](https://ieeexplore.ieee.org/abstract/document/1363823). Obtenido de [ieeexplore.ieee.org](https://ieeexplore.ieee.org/abstract/document/1363823): <https://ieeexplore.ieee.org/abstract/document/1363823>
- Andreu, J. (2011). *Mantenimiento de LAN (Redes locales)*. Madrid: Editex.
- Andreu, J. (2011). *Redes inalámbricas (Servicios en red)*. Madrid: Editex.
- Arias, F. G. (2012). *El Proyecto de Investigación. Introducción a la Metodología Científica*. Fidas G. Arias Odón.
- Augusto, B. C. (2006). [sidalc.net](http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=zamocat.xis&method=post&formato=2&cantidad=1&expresion=mfn=027873). Recuperado el Febrero de 2019, de [sidalc](http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=zamocat.xis&method=post&formato=2&cantidad=1&expresion=mfn=027873): <http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=zamocat.xis&method=post&formato=2&cantidad=1&expresion=mfn=027873>
- Caldas-Calle, L., Jara, J., Huerta, M., & Gallegos, P. (Junio de 2017). ieeexplore.ieee.org.

Recuperado el Febrero de 2019, de ieeexplore: <https://ieeexplore.ieee.org/document/7959718>
 Cruz, M., Martínez, R., & Crespo, Y. (2013). scielo. Recuperado el 10 de 02 de 2019, de scielo.sld.cu: http://scielo.sld.cu/scielo.php?pid=S2227-18992013000100010&script=sci_arttext&tIng=en Dhiman, D. (Enero de 2014). semanticscholar. Recuperado el Febrero de 2019, de pdfs.semanticscholar.org: <https://pdfs.semanticscholar.org/cabd/a6b52dfd269e5e478ddea86220ef3abe4ef.pdf>

0: PROY_PERALTA JOSE28-11.docx

78%

Díaz, G., Alzórriz, I., & Sancristóbal, E. (2014). Procesos y herramientas para la seguridad de redes. Madrid: UNED -

Universidad Nacional de Educación a Distancia. Esch, J. (Diciembre de 2014). ieeexplore.ieee.org. Recuperado el Febrero de 2019, de ieeexplore: <https://ieeexplore.ieee.org/document/6994329?arnumber=6994329> García, N. L. (2012). Diseño e implementación de una red LAN y WLAN con sistema de control de acceso mediante servidores AAA. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. Hernández Sampieri, R. F. (2004). METODOLOGÍA DE LA INVESTIGACIÓN. Mexico: Mc Graw Hill Interamericana. Hoekstra, B., & Musulin, D. (Agosto de 2011). homepages.staff.os3.nl. Recuperado el Febrero de 2019, de homepages: <https://homepages.staff.os3.nl/~delaat/rp/2010-2011/p09/report.pdf> Kolahi, S. S., Cao, Y., & Chen, H. (Julio de 2016). ieeexplore.ieee.org. Recuperado el Febrero de 2019, de ieeexplore: <https://ieeexplore.ieee.org/document/7574043> Korowajczuk, L. (2011). LTE, WiMAX and WLAN Network Design, Optimization and Performance Analysis. West Sussex: John Wiley & Sons. Lacković, D., & Tomić, M. (Mayo de 2017). ieeexplore. Recuperado el Febrero de 2019, de ieeexplore.ieee.org: <https://ieeexplore.ieee.org/abstract/document/7973470> Likhar, P., Yadav, R. S., & M, K. R. (Noviembre de 2011). researchgate.net. Recuperado el Febrero de 2019, de researchgate: https://www.researchgate.net/publication/51969257_Securing_IEEE_80211g_WLAN_Using_Open_VPN_and_its_Impact_Analysis N, B., I, G., & D, W. (Julio de 2001). scopus. Recuperado el Enero de 2019, de www.scopus.com: <https://www.scopus.com/record/display.uri?eid=2-s2.0-0034777649&origin=inward&txGid=5d39a3f9b9b60cf8e672c179bdf7dcd> Onvural, R. O., & Nilsson, A. (2012). Local Area Network Interconnection. Springer Science & Business Media. Pena, C., & Evans, J. (Noviembre de 2000). ieeexplore.ieee.org. Recuperado el Febrero de 2019, de ieeexplore: <https://ieeexplore.ieee.org/abstract/document/891094> Pérez, N., Herrera, J., Uzcátegui, J., & Bernardo, J. (2012). scielo. Recuperado el 10 de 02 de 2019, de scielo.org.ve:

0: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-74252013000300005
 87%

http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1316-48212012000100007

Pongo, S. S. (2015). Instalación y Configuración de una Red Lan con Windows Server 2003 e Internet. Shang Shing Cutipa Pongo. Qu, J., Dang, F., & Li, T. (Agosto de 2012). researchgate.net. Recuperado el Febrero de 2019, de researchgate: <https://>

www.researchgate.net/
publication/261339243_Performance_Evaluation_and_Analysis_of_OpenVPN_on_Android
seed4.Me. (15 de Enero de 2019). seed4.Me. Recuperado el 10 de Marzo de 2019, de
seed4.Me: <https://seed4.me/> TunnelBear. (12 de Enero de 2019). TunnelBear. Obtenido de
TunnelBear: <https://www.tunnelbear.com/> Vaidya, N., Dugar, A., Gupta, S., & Bahl, P. (Octubre
de 2005). ieeexplore.ieee.org. Recuperado el Febrero de 2019, de ieeexplore: [https://
ieeexplore.ieee.org/abstract/document/1516110](https://ieeexplore.ieee.org/abstract/document/1516110) windscribe. (13 de Junio de 2018). windscribe.
Recuperado el 10 de Marzo de 2019, de windscribe: <https://esp.windscribe.com/features>

,

7

Hit and source - focused comparison, Side by Side:

Left side: As student entered the text in the submitted document.

Right side: As the text appears in the source.

Instances from: PROY_PERALTA JOSE28-11.docx

1 64%

por medios no guiados a través de ondas electromagnéticas. Tanto la transmisión de datos y la recepción de los mismos de realiza a través de antenas.

1: PROY_PERALTA JOSE28-11.docx 64%

por medios no guiados a través de ondas electromagnéticas. La transmisión y la recepción se efectúan a través de antenas.

2 78%

Díaz, G., Alzórriz, I., & Sancristóbal, E. (2014). Procesos y herramientas para la seguridad de redes. Madrid: UNED -

2: PROY_PERALTA JOSE28-11.docx 78%

Díaz, G., Alzórriz, I., & SanCristobal, E. (2014). PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES. Editorial UNED.

Instances from: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-74252013000300005

3 87%

http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1316-48212012000100007

3: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-74252013000300005 87%

http://www.scielo.org.mx/scielo.php?script=sci_arttext%26pid=S1405-74252013000300005%26