Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

Tipo de artículo: Artículo original
Temática: Tecnologías de la información y las telecomunicaciones
Recibido: 01/06/2021 | Aceptado: 17/02/2022

Solución basada en herramientas de software libre para la implementación del teletrabajo online en empresas cubanas

Solution based on free software tools for the implementation of online teleworking in Cuban companies

Rudibel Perdigón Llanes [1*] http://orcid.org/0000-0001-7288-6224
Ivis Rosa Madrigal Leiva [2] https://orcid.org/0000-0003-0999-2619

[1] Empresa Comercializadora "Frutas Selectas", Km 1 ½ Carretera a San Juan y Martínez, Pinar del Río, Cuba, CP 20100. E-mail: rperdigon90@gmail.com
[2] Estado Mayor Región Militar de Pinar del Río, Km 89 Carretera Central, Pinar del Río, Cuba. E-mail: irmadrigal92@gmail.com

*Autor para la correspondencia. (rperdigon90@gmail.com)

RESUMEN

En la actualidad la adopción del teletrabajo constituye un tema de interés para empresas y negocios. Sin embargo, su utilización en países en desarrollo como Cuba es incipiente debido fundamentalmente a restricciones económicas y tecnológicas que dificultan su implementación. El objetivo de esta investigación consiste en desarrollar una solución para implementar el teletrabajo *online* en empresas cubanas mediante el uso de herramientas de software libre. Se emplearon como métodos científicos el analítico sintético, el

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

histórico lógico, la triangulación teórica y el método experimental. Para validar la propuesta de solución se realizaron pruebas de rendimiento y de seguridad en el ambiente real de una mediana empresa agroindustrial cubana mediante las herramientas Wireshark, nmap, hping3, hydra, iPerf3 y el comando PING. Los resultados obtenidos evidenciaron que la solución garantiza el acceso remoto de los teletrabajadores a las aplicaciones digitales de la empresa de manera segura y con índices de rendimiento aceptables en correspondencia con los limitados recursos tecnológicos de la organización.

Palabras clave: acceso remoto; telemática; redes privadas virtuales; ciberseguridad.

ABSTRACT

Nowadays the adoption of teleworking is a topic of interest for companies and businesses. However, its use in developing countries such as Cuba is incipient mainly due to economic and technological restrictions that hinder its implementation. The objective of this research is to develop a solution to implement online teleworking in Cuban companies through the use of free software tools. The scientific methods used were the synthetic analytical, the historical logical, the theoretical triangulation and the experimental method. Performance and security tests were realized to validate the proposed solution in the real environment of a medium-sized Cuban agribusiness company using the tools Wireshark, nmap, hping3, hydra, iPerf3 and the PING command. The results obtained showed that the solution guarantees the remote access of teleworkers to the company's digital applications in a secure way and with acceptable performance indexes in correspondence with the limited technological resources of the organization.

Keywords: remote access; telematics; virtual private networks; cyber security.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

Introducción

Los avances científico tecnológico constituyen uno de los factores más influyentes en la sociedad actual, principalmente el desarrollo de las tecnologías de la información y las comunicaciones (TIC) que han provocado cambios significativos en las esferas social, política, laboral y económica del desarrollo humano (Perdigón y Pérez, 2020). Estas tecnologías han permitido establecer diferentes formas de gestión y organización empresarial (Villafrade y Palacios, 2013; Warner y Wäger, 2019) y son consideradas como el elemento decisivo en el surgimiento de uno de los fenómenos más novedosos dentro del mercado laboral: el teletrabajo (Peralta, Bilous, Flores y Bombón, 2020; Ulate-Araya, 2020; Vrchota, Maríková y Rehor, 2020).

Según (Fernández, Cera y Adriano 2020), el teletrabajo es la actividad laboral que se efectúa fuera del área u oficina de la empresa, ya sea a tiempo parcial o total, mediante el uso de las TIC. Las tipologías del teletrabajo se relacionan con el lugar donde el teletrabajador realiza su actividad laboral, el tiempo que le dedica, la forma de comunicación que utiliza durante esta actividad y el vínculo contractual que lo ampara (Cifuentes-Leiton y Londoño-Cardozo, 2020). Según los autores anteriores, existen dos modalidades de teletrabajo en correspondencia con la forma de comunicación que emplea el teletrabajador para realizar su actividad laboral: online y offline. En la modalidad de teletrabajo online el trabajador realiza su actividad productiva conectado a los sistemas digitales radicados en los centros de datos de su organización, mientras que en la modalidad offline el teletrabajador carece de esta conexión (Cifuentes-Leiton y Londoño-Cardozo, 2020).

La aplicabilidad del teletrabajo en actividades comunes a la mayoría de las organizaciones como el marketing, administración y contabilidad, lo convierten en un objetivo deseable para las empresas (Fernández et al., 2020). Autores como (Medina, Ávila y González 2020) destacan los beneficios que brinda el teletrabajo en períodos de crisis y para reducir la transmisión de enfermedades como la COVID-19. Esta modalidad de empleo constituye una forma tangible de sostenibilidad empresarial porque permite la reducción de costos en las organizaciones, contribuye al cuidado del medio ambiente, incrementa la productividad laboral y el bienestar del personal de las empresas (Contreras y Rozo, 2015; Benjumea-Arias, Villa-Enciso y Valencia-Arias, 2016; Fernández et al., 2020; Medina et al., 2020; Ulate-Araya, 2020); sin

embargo, la implementación del teletrabajo es limitada, principalmente en empresas de países subdesarrollados (Benjumea-Arias et al., 2016).

Los autores (Villafrade y Palacios 2013), identificaron que los factores organizacionales, legales, humanos y tecnológicos constituyen elementos significativos para la implementación del teletrabajo en las empresas. Autores como (Muñoz, Ortega y Quevedo, 2020) y (Vrchota, et al. 2020) determinaron que la implementación del teletrabajo requiere infraestructuras tecnológicas específicas y una conexión a Internet a altas velocidades. Según (Pinzón, Martínez y Ávila 2017), el teletrabajo demanda una serie de recursos tecnológicos que soporten desde una simple llamada telefónica hasta el acceso a diferentes servicios alojados en los servidores de la compañía mediante tecnologías como las redes privadas virtuales (VPN, por sus siglas en inglés) o la computación en la nube.

Las VPN de acceso remoto son ampliamente utilizadas en el ámbito del teletrabajo porque facilitan la interacción de los teletrabajadores con los sistemas digitales de sus empresas (Skendzica y Kovacic, 2017; Iqbal y Riadi, 2019; Wu, Zhang y Xiao, 2019; Bansode y Girdhar, 2021). Esta tecnología proporciona a los usuarios una vía de comunicación económica y segura a través de un canal de comunicación inseguro como Internet (Lacković y Tomić, 2017; Skendzica y Kovacic, 2017; Jianyun y Chunyan, 2018; Iqbal y Riadi, 2019).

En Cuba el teletrabajo se introdujo recientemente en la cultura de las organizaciones, suscitado fundamentalmente como medida de ahorro ante la crisis energética que afronta la nación por el recrudecimiento del bloqueo económico norteamericano y para el enfrentamiento a la COVID-19 (Medina et al., 2020). Aunque esta modalidad laboral está respaldada por la política de informatización del país, la falta de infraestructura tecnológica y la percepción de los directivos que prefieren la presencialidad frenan su desarrollo (Fernández et al., 2020).

La revisión de la literatura permitió identificar que los estudios relacionados con la implementación del teletrabajo en correspondencia con las características y limitaciones tecnológicas de las organizaciones cubanas son escasos. El objetivo de esta investigación consiste en desarrollar una propuesta para implementar el teletrabajo online en empresas cubanas mediante herramientas de software libre. Se seleccionaron soluciones de software libre porque facilitan el despliegue de servicios digitales con un aprovechamiento óptimo de los recursos de hardware y como alternativa a las restricciones económicas

internacionales que dificultan la adquisición de tecnologías de avanzada en Cuba (Perdigón y Ramírez, 2020).

Métodos o Metodología Computacional

Para el desarrollo de la presente investigación se emplearon los métodos científicos analítico sintético, histórico lógico, triangulación teórica y experimental. Los métodos analítico sintético e histórico lógico permitieron el estudio de la literatura relacionada con el objeto de estudio y analizar su evolución en el tiempo. La triangulación teórica posibilitó disminuir el sesgo en la investigación y el método experimental facilitó la validación de la propuesta de solución mediante su aplicación práctica.

Se emplearon las herramientas Wireshark, nmap, hping3 e hydra para comprobar la seguridad de la solución propuesta. Estas herramientas se utilizaron para el monitoreo de la red, realizar escaneo de puertos, ataques de denegación de servicios y de fuerza bruta, respectivamente. Para verificar el rendimiento de la solución se evaluaron elementos como el ancho de banda, latencia y el porcentaje de paquetes transferidos mediante el comando PING y la herramienta iPerf3, esta última es ampliamente utilizada en pruebas de rendimiento y escalabilidad en redes de datos (Perdigón y Ramírez, 2020).

Resultados y discusión

La solución está sustentada en el empleo de una VPN de acceso remoto para la implementación del teletrabajo *online* en las empresas cubanas. Como se muestra en la Figura 1, este tipo de VPN permite establecer un canal de comunicación seguro entre las organizaciones y sus teletrabajadores.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

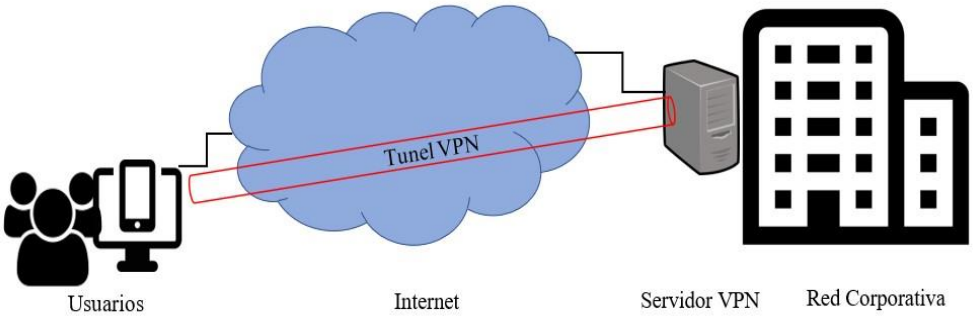

Fig. 1 – VPN de acceso remoto.

Fuente (elaboración propia)

Mediante esta alternativa el trabajador requiere únicamente de un enlace con acceso a Internet o navegación nacional para establecer comunicación con los sistemas digitales de su centro laboral, sin necesidad de infraestructura y equipos de conexión especializados.

Según (Skendzica y Kovacic 2017), algunos de los elementos considerados para seleccionar un servidor VPN son su compatibilidad con diferentes protocolos red, su capacidad para la creación de logs y su monitoreo, las aplicaciones cliente soportadas y los precios de sus licencias. En esta investigación se realizó la selección del servidor VPN en 2 pasos fundamentales y sobre la premisa de que fuera una solución libre de código abierto. En un primer momento se realizó un estudio de las principales tendencias del mercado, la Figura 2 muestra los servidores VPN líderes en el mercado mundial durante 2021 según el sitio G2 Crowd Inc.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

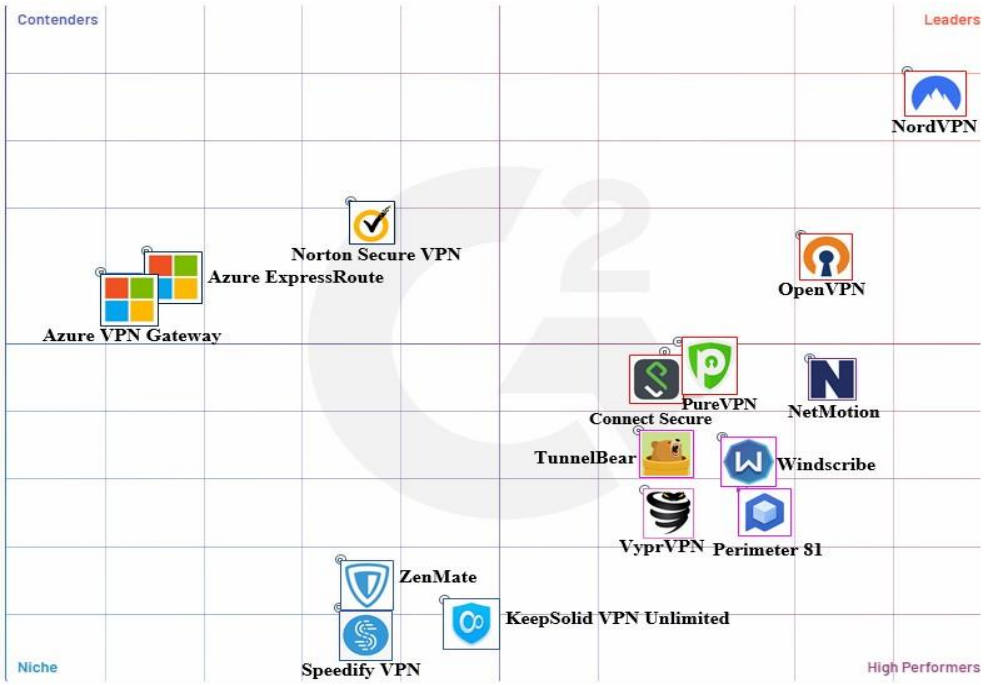

Fig. 2 – Servidores VPN líderes en el mercado en 2021.

Fuente (adaptado de G2 Crowd Inc)

Aunque las herramientas comerciales dominan ampliamente el mercado, se identificó que la solución libre OpenVPN posee un posicionamiento positivo dentro de este. En un segundo momento se realizó un análisis de la literatura y se identificaron los servidores VPN más estudiados por los autores consultados. La Tabla 1 muestra las soluciones identificadas y sus principales características.

Tabla 1 – Servidores VPN identificados en la literatura.

Autor	Servidor	Protocolo VPN	Algoritmos de cifrado
Skendzica y Kovacic, 2017; Lacković y Tomić, 2017; Zhang, Li, Zhang y Wang, 2018; León, 2018; Iqbal y Riadi, 2019; Karaymeh, Ababneh, Qasaimeh, y Al-Fayoumi, 2019; Marín, Patiño y Acevedo, 2020; Bin y Mohd, 2020	OpenVPN	OpenVPN	RC2, AES-128, AES-256, BlowFish, 3DES, BF-CBC, CAST5

Kuroda, 2017; Wu, Zhang y Xiao, 2019	SoftEther	SoftEther VPN, EtherIP, Microsoft SSTP, L2TP, IPSec, OpenVPN	RC4, AES128, AES256, DES, 3-DES
Kossingou, Dégboé, Ouya, y Mendy, 2020	WireGuard	IPSec	ChaCha20, Poly1305, Curve25519, BLAKE2s
Shaofeng, Chaoping y Weifeng, 2017	OpenSwan	IPSec	AES256, 3DES, RFC
Lacković y Tomić, 2017	strongSwan	IPSec	3DES, BlowFish, AES, AES192, AES256, camellia, camellia192, camellia256, chacha20poly1305

En la Tabla 1 se evidenció que OpenVPN fue la solución más investigada por los autores consultados. Esta herramienta ofrece una serie de beneficios en relación a las soluciones que emplean el protocolo IPSec, como son facilidades para su instalación, capacidad para configurar conexiones mediante los protocolos UDP y TCP, permite el intercambio de claves mediante conexiones SSL/TLS sobre las capas de transporte y de sesión del modelo OSI, utiliza la librería OpenSSL para el manejo de claves de autenticación y encriptación y su aplicación agente es compatible con la mayoría de los Sistemas Operativos (SO) existentes (Lacković y Tomić, 2017; Skendzica y Kovacic, 2017; León, 2018; Iqbal y Riadi, 2019). Además, OpenVPN posibilita establecer conexiones TCP mediante el protocolo UDP, elemento que disminuye la latencia de la conexión y facilita su implementación en redes con velocidades limitadas (Coonjah, Catherin y Soyjaudah, 2015).

Un aspecto significativo en las redes de datos es garantizar la confidencialidad, disponibilidad e integridad de la información que por ella se transmite (León, 2018; Iqbal y Riadi, 2019; Marín et al., 2020). Los autores (Bansode y Girdhar 2021), sugieren que para mantener altos estándares de seguridad en redes VPN es necesario actualizar regularmente las aplicaciones cliente utilizadas, aplicar diferentes modelos de autenticación de usuario, cifrar las sesiones TLS establecidas, monitorear y preservar la trazabilidad del sistema. Aunque OpenVPN mantiene la confidencialidad e integridad de los datos que son transmitidos a

través de la conexión establecida (Skendzica y Kovacic, 2017), su integración con herramientas de ciberseguridad como los firewalls incrementa sus niveles de seguridad (Segura y Ramírez, 2018; Karaymeh et al., 2019). La solución propuesta en la presente investigación consiste en la integración del servidor OpenVPN con el firewall pfSense y el sistema de detección de intrusiones (IDS, por sus siglas en inglés) Snort. Se emplearon las últimas versiones disponibles de estas herramientas hasta la fecha de realizada la presente investigación: pfSense 2.5.0, OpenVPN 2.5.0 y Snort 2.9.17.

pfSense es un potente firewall de código abierto basado en FreeBSD con diversas características y servicios avanzados que mantiene un rendimiento adecuado en disímiles entornos organizacionales, reduce los costos y la complejidad en las redes de datos y es fácil de gestionar (Patel y Sharma, 2017; León, 2018). Esta herramienta posee integrado por defecto el servidor OpenVPN, soporta diferentes modos de autenticación de usuario, posibilita la extensibilidad de sus funciones, es compatible con diferentes IDS y se encuentra disponible en los repositorios nacionales.

Snort es uno de los IDS de código abierto más utilizados en los esquemas de ciberseguridad en la actualidad (Perdigón y Orellana, 2021). Esta herramienta opera como un Sistema de Prevención de Intrusos (IPS, por sus siglas en inglés) bloqueando automáticamente los paquetes que identifica como sospechosos en las redes de datos. En la solución propuesta Snort fue configurado en modo IPS mediante el uso de una base de reglas conformada por las listas Emerging Threats Rules y AppID Open Text Rules que son de distribución gratuita y accesibles para Cuba. Estas reglas fueron actualizadas con fecha 4 de mayo de 2021.

Validación de la propuesta de solución

La validación de la propuesta de solución se efectuó en 2 escenarios diferentes, inicialmente se efectuaron pruebas de seguridad y rendimiento en un ambiente controlado (escenario A), posteriormente se verificó el rendimiento de la solución en el entorno real de una mediana empresa agroindustrial cubana (escenario B). La Figura 3 describe las características del escenario de pruebas A.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

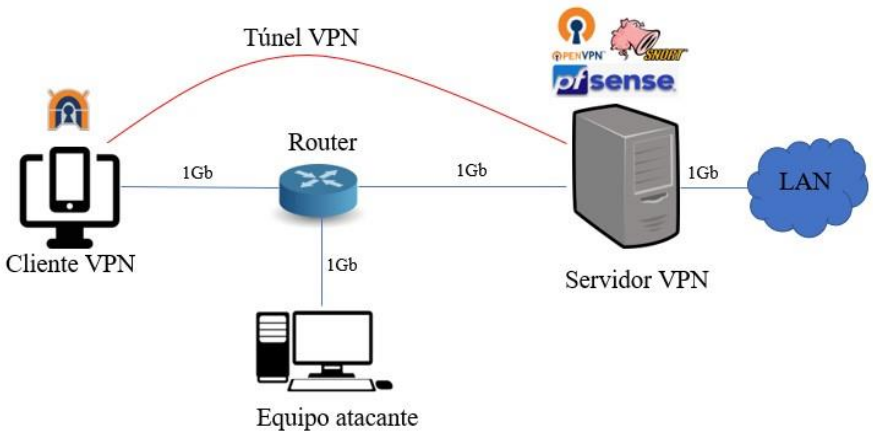

Fig. 3 – Escenario de pruebas A.

Fuente (elaboración propia)

En el escenario B, la solución fue implementada en una mediana empresa agroindustrial de la provincia de Pinar del Río, Cuba. Esta entidad posee un enlace a internet de 4 Mbps y diferentes servicios digitales locales como son: correo electrónico, sistema automatizado para la gestión contable financiera, sistema estadístico, sistema de metrología, sistema para el control de los portadores energéticos y sistema de balance de producciones agrícolas. La solución se desplegó en un ordenador de propósito general en correspondencia con los limitados recursos de hardware disponibles en la organización: CPU: Corei3-4160, RAM: DDR3 4Gb, HDD: 500Gb, 2 NIC: 1Gbps (WAN y LAN).

El monitoreo de los paquetes de red desde un cliente de la VPN evidenció que su conexión fue realizada mediante un túnel TLS cifrado, en correspondencia con la configuración realizada en el servidor OpenVPN. La Figura 4 muestra la captura de un paquete de red con la herramienta Wireshark durante el establecimiento de la conexión VPN.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

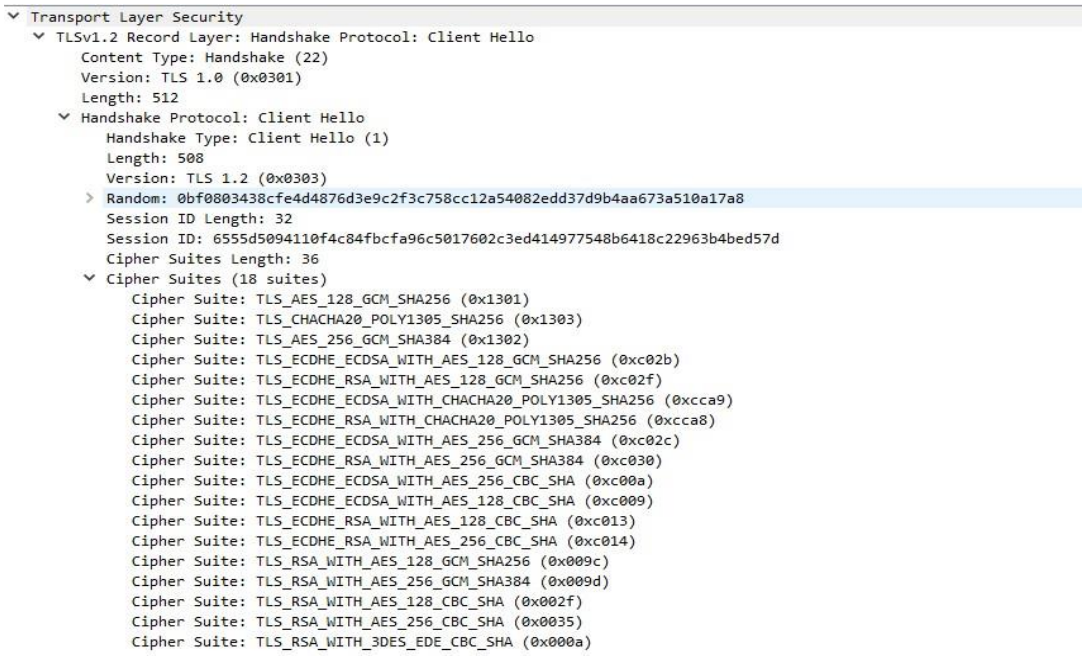

Fig. 4 – Monitoreo de paquetes en la red VPN.

Fuente (elaboración propia)

OpenVPN crea por defecto un túnel de conexión mediante el protocolo UDP por el puerto 1194, por tal motivo, se realizó un escaneo de puertos al firewall pfSense con la herramienta nmap para identificar posibles vulnerabilidades asociadas a este servicio. Durante el escaneo se solapó la dirección IP del ordenador atacante para evadir el IDS utilizado y se verificó la existencia de puertos adicionales abiertos para servicios UDP y TCP. Snort identificó esta actividad como tráfico de red malicioso y automáticamente bloqueó los IP atacantes, la Figura 5 describe las alertas arrojadas por Snort durante el empleo de nmap.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

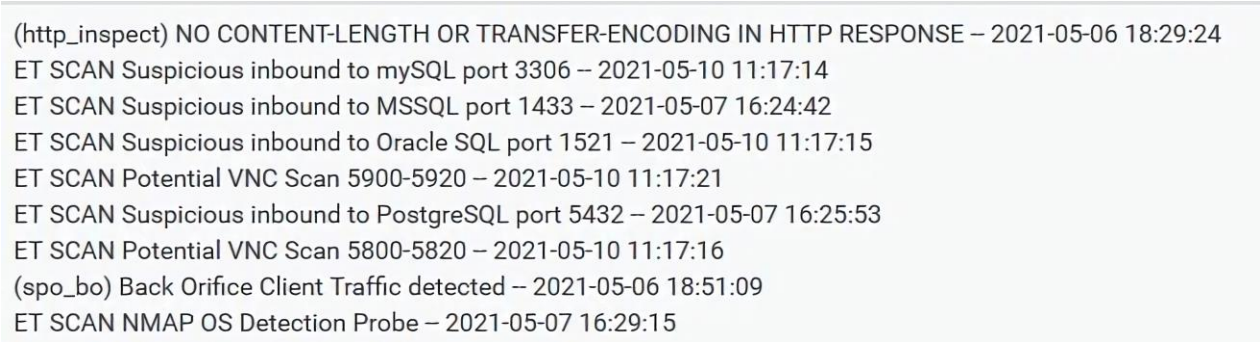

Fig. 5 – Alertas de Snort durante el escaneo de puertos.

Fuente (elaboración propia)

Se realizaron ataques de denegación de servicios (DoS, por sus siglas en inglés) mediante inundación PING Flood, SYN Flood y UDP Flood con hping3 para comprobar el comportamiento de la solución ante este tipo de transgresiones. En este proceso se enmascaró la dirección IP del ordenador atacante y se modificaron los períodos de tiempo entre cada ataque con el propósito de burlar el IDS. Aunque las conexiones VPN no fueron afectadas, se observó un aumento de los índices de utilización del CPU y memoria RAM en el ordenador de la solución y se evidenció que el IDS Snort no fue capaz de detectar y bloquear estas transgresiones. Con el objetivo de disminuir las afectaciones de este tipo de ataque fueron configuradas varias reglas en la interfaz WAN del firewall pfSense para limitar la atención a solicitudes de conexiones entrantes de hosts externos durante determinado período de tiempo. La Tabla 2 muestra los niveles de utilización de RAM y CPU de la solución durante los ataques de denegación de servicios antes y después de realizadas las configuraciones anteriores.

Tabla 2 – Consumo de recursos de hardware durante ataques DoS.

Ataque DoS	**Consumo de recursos de hardware**			
	Anterior a la configuración		**Posterior a la configuración**	
	RAM (%)	CPU (%)	RAM (%)	CPU (%)

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

PING Flood	17%	10%	13%	8%
UDP Flood	22%	33%	14%	24%
SYN Flood	25%	67%	18%	41%

Las reglas configuradas en la interfaz WAN del firewall permitieron disminuir el consumo de RAM y CPU de la solución durante los ataques DoS realizados, esto contribuye a garantizar la disponibilidad de estos recursos para atender las solicitudes de conexión de los clientes con acceso a la VPN.

El empleo de la herramienta hydra posibilitó evaluar el comportamiento de la solución ante ataques de fuerza bruta, lo cuales estuvieron dirigidos fundamentalmente a los servicios telnet, smtp y rdp que son ampliamente utilizados en actividades relacionadas con el teletrabajo. Snort detectó la ejecución de este tipo de ataque y automáticamente bloqueó el IP del atacante, la Figura 6 muestra las alertas de Snort durante el uso de hydra.

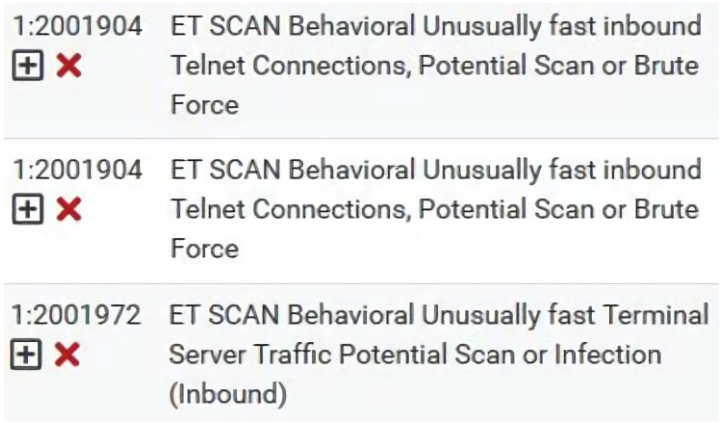

Fig. 6 – Alertas de Snort durante ataques de fuerza bruta.

Fuente (elaboración propia)

La calidad de las conexiones VPN es limitada por las condiciones del servicio de Internet sobre el que operan, esto puede ocasionar variaciones en la velocidad de transmisión, bajas de rendimiento o fallas

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 1, Enero-Marzo, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 92-112

externas resultado de condiciones climáticas o del entorno (León, 2018). Para comprobar el rendimiento de la solución se ejecutó la herramienta iPerf3 y el comando PING en los escenarios A y B respectivamente. En ambos escenarios las pruebas se ejecutaron con 10 clientes conectados simultáneamente a la solución, en el caso del escenario B, los clientes se ubicaron a 11 km de distancia de la empresa y utilizaron como punto de acceso a Internet los datos móviles de sus teléfonos celulares. La Tabla 3 muestra la latencia, ancho de banda y pérdida de paquetes de las conexiones VPN establecidas en ambos escenarios.

Tabla 3 – Rendimiento de la solución.

Clientes	**Escenario A**			**Escenario B**		
	Latencia media (ms)	**Ancho de banda (Mbps)**	**Pérdida de paquetes (%)**	**Latencia media (ms)**	**Ancho de banda (Mbps)**	**Pérdida de paquetes (%)**
Cliente 1	1	12.9	0	240	0.370	0
Cliente 2	1	12.3	0	244	0.345	0
Cliente 3	1	13.5	0	207	0.303	0
Cliente 4	0	14.0	0	196	0.498	0
Cliente 5	2	10.8	0	320	0.292	0
Cliente 6	1	13.1	0	301	0.394	0
Cliente 7	0	13.9	0	157	0.458	0
Cliente 8	1	12.4	0	252	0.422	0
Cliente 9	0	14.6	0	185	0.439	0
Cliente 10	0	15.2	0	200	0.501	0

En la Tabla 3 se evidenció que OpenVPN asigna a los clientes de la red VPN aproximadamente el 12 % del ancho de banda en redes con velocidades de 1 Gbps (escenario A). Asimismo, se comprobó que esta herramienta emplea la totalidad del ancho de banda disponible en redes con velocidades reducidas como en el escenario B. Se identificó que, aunque el incremento de la distancia geográfica entre los clientes y la solución incide desfavorablemente en la latencia de la conexión, no aumentó la pérdida de paquetes de red.

Según los criterios de (Pinzón et al. 2017), para implementar el teletrabajo de forma satisfactoria las organizaciones requieren desde el punto de vista tecnológico de una conexión a Internet que garantice al menos 0.2 Mbps de ancho de banda por cada uno de sus teletrabajadores. Los resultados descritos en la Tabla 3 evidenciaron que la solución propuesta supera este requerimiento y permite que organizaciones con una conexión a Internet de 4 Mbps implementen el teletrabajo online, garantizando que al menos 10 de sus trabajadores realicen sus actividades laborales mediante esta modalidad de empleo.

En su estudio (Solano 2016), analizó los rendimientos de las soluciones OpenVPN, OpenSSH y OpenSwan para la transmisión de videoconferencias. Este autor evaluó la latencia, el jitter, ancho de banda y porciento de datagramas recibidos en las redes VPN implementadas con cada solución respectivamente, e identificó que OpenSSH fue la herramienta con mejores resultados. En su investigación, (Solano 2016) no analizó el comportamiento de OpenSSH ante ataques informáticos.

El autor (León 2018) implementó una VPN mediante pfSense y OpenVPN en el entorno real de una empresa en la ciudad de Xalapa. Este autor evaluó indicadores de rendimiento como latencia, ancho de banda y pérdida de paquetes en la red VPN. Aunque la distancia geográfica entre los clientes y la solución influyó en sus índices de rendimientos, OpenVPN fue capaz de mantener la disponibilidad de los servicios en la red virtual con un uso óptimo de los recursos de hardware (León 2018). En su tesis (León 2018), no evaluó el comportamiento de la solución ante ciberataques.

Los autores (Iqbal y Riadi 2019), implementaron una VPN para fortalecer la seguridad del Laboratorio de Investigación en Ingeniería Informática Universitas Ahmad Dahlan mediante la herramienta OpenVPN. Estos autores identificaron la fortaleza de esta solución ante ataques sniffing y comprobaron su incidencia negativa en los rendimientos de la red. Sobre este aspecto, (Iqbal y Riadi 2019) determinaron que el proceso de cifrado y encapsulación de los paquetes de red realizado por OpenVPN incrementó la latencia de la red de 51.4 ms a 463.4 ms, la pérdida de paquetes de un 7.8% a un 20.2% y redujo el ancho de banda de 64786.6 a 55589 bps.

En su investigación, (Marín et al., 2020) desarrollaron una propuesta para elevar la ciberseguridad en pequeñas empresas de Colombia basada en la combinación de sistemas firewall, IDS y VPN, mediante las herramientas de software libre IPtables, Denyhost y OpenVPN, en un Raspberry Pi B con SO Raspbian. Los autores mencionados, evaluaron la seguridad de la solución ante ataques DoS y de fuerza bruta, pero no analizaron los índices de rendimiento de la conexión VPN de su propuesta.

En correspondencia con los criterios de (León 2018), los resultados obtenidos en este estudio permitieron identificar que la integración de las herramientas pfSense, Snort y OpenVPN, posibilitó el despliegue de una red VPN segura con rendimientos adecuados en una organización con conectividad limitada y escasos recursos tecnológicos. Contrario a los resultados obtenidos por (Iqbal y Riadi, 2019), se evidenció que la herramienta OpenVPN mantiene índices de rendimiento adecuados en redes VPN incluso con clientes ubicados a 11 km de distancia de la herramienta. Esto se debe al nivel de madurez alcanzado por esta solución.

Conclusiones

En esta investigación se desplegó una solución basada en herramientas de software libre para facilitar la implementación del teletrabajo *online* en pequeñas y medianas empresas cubanas en correspondencia con sus limitados recursos tecnológicos. La solución propuesta está integrada por el firewall pfSense, el IDS Snort y el servidor OpenVPN y permite establecer conexiones VPN remotas seguras y con rendimientos adecuados entre las organizaciones y sus teletrabajadores. El funcionamiento efectivo de Snort en modo IPS depende esencialmente de la actualización de sus reglas de detección, por esta razón, los autores de la presente investigación sugieren realizar actualizaciones periódicas de las mismas para garantizar la seguridad de la solución propuesta.

La aplicación de estas herramientas en el sector empresarial cubano posibilitará mantener las actividades laborales de sus trabajadores y el funcionamiento de estas organizaciones ante situaciones de crisis como la

impuesta por la COVID-19. Además, contribuirá a impulsar la recuperación económica de la nación luego de más de 1 año de pandemia.

Referencias

Bansode, R.; Girdhar, A. Common Vulnerabilities Exposed In Vpn - A Survey. Journal Of Physics: Conference Series, 2021, 1714: 012045. Https://Doi.Org/10.1088/1742-6596/1714/1/012045

Benjumea-Arias, M.L.; Villa-Enciso, E.M.; Valencia-Arias, J. Beneficios E Impactos Del Teletrabajo En El Talento Humano. Resultados Desde Una Revisión De Literatura. Revista Cea, 2016, 2(4): P. 59-73. Https://Ssrn.Com/Abstract=3519571

Bin, S. K. H.; Mohd, H. B. Alternative Vpn Solution Using Raspberry Pi As Router. Journal Of Computing Technologies And Creative Content, 2020, 5(2): P. 18-21.

Cifuentes-Leiton, D. M.; Londoño-Cardozo, J. Teletrabajo: El Problema De La Institucionalización. Aibi Revista De Investigación, Administración E Ingeniería, 2020, 8(1): P. 12-20. Https://Doi.Org/10.15649/2346030x.749

Contreras, O. E.; Rozo, I. Teletrabajo Y Sostenibilidad Empresarial. Una Reflexión Desde La Gerencia Del Talento Humano En Colombia. Suma De Negocios, 2015, 6(13): P. 74-83. Http://Dx.Doi.Org/10.1016/J.Sumneg.2015.08.006

Coonjah, I.; Catherine, P. C.; Soyjaudah, K. M. S. (2015). Experimental Performance Comparison Between Tcp Vs Udp Tunnel Using Openvpn. En: International Conference On Computing, Communication And Security (Icccs). Pointe Aux Piments: Ieee, 2015, P. 1-5. Https://Doi.Org/10.1109/Cccs.2015.7374133

Fernández, R.; Cera, G.; Adriano, K. Contabilidad En La Nube: Una Alternativa Para El Teletrabajo. Revista Cubana De Finanzas Y Precios, 2020, 4(4): P. 19-31.

Iqbal, M.; Riadi; I. Analysis Of Security Virtual Private Network (Vpn) Using Openvpn. International Journal Of Cyber-Security And Digital Forensics, 2019, 8(1): P. 58-65. Http://Dx.Doi.Org/10.17781/P002557

Jianyun, C.; Chunyan, L. Research On Meteorological Information Network Security System Based On Vpn Technology. En: 2nd International Conference On Electronic Information Technology And Computer Engineering (Eitce), 2018. Https://Doi.Org/10.1051/Matecconf/201823201001

Karaymeh, A.; Ababneh, M.; Qasaimeh, M.; Al-Fayoumi, M. Enhancing Data Protection Provided By Vpn Connections Over Open Wifi Networks. En: 2nd International Conference On New Trends In Computing Sciences (Ictcs). Amman: Ieee, 2019, P. 1-6. Https://Doi.Org/10.1109/Ictcs.2019.8923104

Karaymeh, R. Secure Protocols And Virtual Private Networks: An Evaluation. Issues In Information Systems, 2019, 20(3): P. 37-46. Https://Doi.Org/10.48009/3_Iis_2019_37-46

Kossingou, G. M. S; Dégboé, B. M.; Ouya, S.; Mendy, G. Mutualisation Of Ict Laboratory Resources Between West And Central African Universities In Post-Crisis Situations: The Case Of Senegal And The Central African Republic. En: Sixth International Conference On E-Learning (Econf). Sakheer: Ieee, 2020, P. 1-5. Https://Doi.Org/10.1109/Econf51404.2020.9385470

Kuroda, T. A Combination Of Raspberry Pi And Softether Vpn For Controlling Research Devices Via The Internet. Jrnl Exper Analysis Behavior, 2017, 108, P. 468-484. Https://Doi.Org/10.1002/Jeab.289

Lacković, D.; Tomić, M. Performance Analysis Of Virtualized Vpn Endpoints. En: 40th International Convention On Information And Communication Technology, Electronics And Microelectronics (Mipro). Opatija: Ieee, 2017, P. 466-471. Https://Doi.Org/10.23919/Mipro.2017.7973470

León, A. N. Monitoreo De Rendimiento Para La Seguridad De Vpn A Través De Pfsense Y Openvpn. Tesis De Maestría. Universidad Veracruzana, México, 2018.

Marín, J. J.; Patiño, A.; Acevedo, J. C. Implementación De Un Sistema De Seguridad Perimetral Informático Usando Vpn, Firewall E Ids. Revista Universidad Católica De Oriente, 2020, 31(45): P. 84-99.

Medina, A.; Ávila, A.; González, Y. F. Teletrabajo En Condiciones De Covid-19. Ventajas, Retos Y Recomendaciones. Revista Cubana De Salud Y Trabajo, 2020, 21(3): P. 59-63.

Muñoz, A.; Ortega, J.; Quevedo, S. Adopción Del Teletrabajo En Las Empresas Manufactureras De La Ciudad De Cuenca. Primeros Pasos. Revista De I+D Tecnológico, 2020, 16(1): P. 46-53. Https://Doi.Org/10.33412/Idt.V16.1.2439

Patel, K. C.; Sharma, P. A Review Paper On Pfsense – An Open Source Firewall Introducing With Different Capabilities & Customization. International Journal Of Advance Research And Innovative Ideas In Education, 2017, 3(2): P. 635-641.

Peralta, A. R.; Bilous, A.; Flores, C. R.; Bombón, C. F. El Impacto Del Teletrabajo Y La Administración De Empresas. Recimundo, 2020, 4(1): P. 326-335. Https://Doi.Org/10.26820/Recimundo/4.(1).Enero.2020.326-335

Perdigón, R; Orellana, A. Sistemas Para La Detección De Intrusiones En Redes De Datos De Instituciones De Salud. Revista Cubana De Informática Médica, 2021, 13(2): E440.

Perdigón, R.; Pérez, M. T. Análisis Holístico Del Impacto Social De Los Negocios Electrónicos En América Latina, De 2014 A 2019. Paakat: Revista De Tecnología Y Sociedad, 2020, 10(18). Http://Dx.Doi.Org/10.32870/Pk.A10n18.459

Perdigón, R.; Ramírez, R. Plataformas De Software Libre Para La Virtualización De Servidores En Pequeñas Y Medianas Empresas Cubanas. Revista Cubana De Ciencias Informáticas, 2020, 14(1): P. 40-57.

Pinzón, S. A.; Martínez, A. M.; Ávila, E. A. State Of Art On Telematic Infrastructure For Telework. Visión Electrónica, 2017, 11(2): P. 261-278. Https://Doi.Org/10.14483/22484728.12114

Shaofeng, L.; Chaoping, G.; Weifeng, S. Design And Implementation Of An Enhanced Vpn Isolation Gateway. En: 2017 International Conference On Robots & Intelligent System (Icris). Huai An City: Ieee, 2017, P. 82-85. Https://Doi.Org/10.1109/Icris.2017.27

Segura, P.; Ramírez, M. Informatics Security – Vpn. Tekhnê, 2018, 15(1): P. 45 -53.

Skendzic, S.; Kovacic, B. Open Source System Openvpn In A Function Of Virtual Private Network. Iop Conf. Ser.: Mater. Sci. Eng., 2017, 200, 012065. Https://Doi.Org/10.1088/1757-899x/200/1/012065

Solano, J. E. Análisis De Las Arquitecturas De Conexión De Redes Privadas Virtuales Vpns Para La Transmisión De Videoconferencia. Tesis De Maestría. Escuela Superior Politécnica De Chimborazo, 2016.

Ulate-Araya, R. Teletrabajo Y Su Impacto En La Productividad Empresarial Y La Satisfacción Laboral De Los Colaboradores: Tendencias Recientes. Revista Tecnología En Marcha, 2020, 33(7): P. 23–31. Https://Doi.Org/10.18845/Tm.V33i7.5477

Villafrade, A.; Palacios, J. I. Propuesta De Implementación De Un Modelo De Teletrabajo. Risti - Revista Ibérica De Sistemas E Tecnologias De Informação, 2013, 12: P. 17-31. Https://Dx.Doi.Org/10.4304/Risti.12.17-31

Vrchota, J.; Maríková, M.; Rehor, P. Teleworking In Smes Before The Onset Of Coronavirus Infection In The Czech Republic. Management, 2020, 25(2): P. 151-164. Https://Doi.Org/10.30924/Mjcmi.25.2.8

Warner, K. S.; Wäger, M. Building Dynamic Capabilities For Digital Transformation: An Ongoing Process Of Strategic Renewal. Long Range Plan, 2019, 52: P. 326–349. Https://Doi.Org/10.1016/J.Lrp.2018.12.001

Wu, Z.; Zhang, Y.; Xiao, M. Topology Design Of Vpn Based On Communication Performance And Server Load. En: International Conference On Communications, Information System And Computer Engineering (Cisce). Haikou: Ieee, 2019, P. 130-135. Https://Doi.Org/10.1109/Cisce.2019.00037

Zhang, Q.; Li, J.; Zhang, Y.; Wang, H.; Gu, D. Oh-Pwn-Vpn! Security Analysis Of Openvpn-Based Android Apps. En: Capkun S., Chow S. (Editores), Cryptology And Network Security. Springer, Cham, 2018, P. 373-389. Https://Doi.Org/10.1007/978-3-030-02641-7_17

Conflicto de interés

Los autores declaran que no existe conflicto de intereses y autorizan la distribución y uso de su artículo.

Contribuciones de los autores

1. Conceptualización: Rudibel Perdigón Llanes.
2. Curación de datos: Rudibel Perdigón Llanes e Ivis Rosa Madrigal Leiva
3. Análisis formal: Rudibel Perdigón Llanes e Ivis Rosa Madrigal Leiva
4. Adquisición de fondos:
5. Investigación: Rudibel Perdigón Llanes e Ivis Rosa Madrigal Leiva
6. Metodología: Rudibel Perdigón Llanes
7. Administración del proyecto: Rudibel Perdigón Llanes
8. Recursos: Rudibel Perdigón Llanes

9. Software: Rudibel Perdigón Llanes
10. Supervisión: Rudibel Perdigón Llanes
11. Validación: Rudibel Perdigón Llanes e Ivis Rosa Madrigal Leiva
12. Visualización: Rudibel Perdigón Llanes e Ivis Rosa Madrigal Leiva
13. Redacción – borrador original: Rudibel Perdigón Llanes
14. Redacción – revisión y edición: Rudibel Perdigón Llanes e Ivis Rosa Madrigal Leiva

Financiación

Esta investigación no recibió ninguna subvención específica de organismos de financiación de los sectores público, comercial o sin fines de lucro.