Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV

Safety analysis in the implementation of corporate services on the IPV6 protocol

Bareño Gutiérrez Raúl; Navarro Núñez William; Cárdenas Urrea Sonia; Sarmiento Osorio Hugo; Duarte Acosta Nixon; Germán Gonzalo Vargas Sánchez.

Resumen

Día a día los sistemas de transmisión a través de diferentes redes internas o externas son más inseguras, debido a la facilidad de analizar el tráfico por parte de diversos atacantes y a las vulnerabilidades del protocolo IPv4; Por ello servicios corporativos como FTP, DHCP y SSH deben buscar la migración e implementación sobre el protocolo IPV6, sin importar el tipo de sistema operativo libre o propietario donde opere la solución de interconectividad en la actualidad; el presente artículo evalúa mediante pruebas de configuración de estos servicios funcionando sobre IPV6, se revisan algunos criterios de seguridad y se especifica de manera detallada la mejor opción de configuración y otras sugerencias para mitigar posibles ataques o problemas en el proceso de autenticación, integridad y confidencialidad de usuarios locales o remotos a través de diversas redes con resultados de implementación confiables y seguros; Concluyendo así, que estos protocolos correctamente configurados sobre IPV6 garantizan un mayor nivel de seguridad propio y nativo sin importar el medio sobre el cual viajen los datos; sumado a esto también el protocolo es

Abstract

Day to day transmission systems through various internal and external networks are unsafe due to the ease of analyzing traffic by several attackers and IPv4 vulnerabilities; Therefore corporate services such as FTP, DHCP and SSH should seek migration and implementation on the IPv6 protocol, regardless of the type or owner free operating system which operates interconnectivity solution today; This article evaluates the configuration by testing these services running on IPv6, some safety criteria are revised and specified in detail best configuration option and other suggestions to mitigate potential attacks or problems in the process of authentication, integrity and confidentiality Local or remote users through various networks with reliable results and safe implementation; Thus concluding that these protocols properly configured for IPv6 ensure a higher level of own native security regardless of the medium on which data travel; Added to this protocol is also suitable to be implemented as a security mechanism for the infrastructure of small, medium and large enterprises as it ensures integrity and data protection. This article seeks to

Recibido / Received: Mayo 26 de 2015 **Aprobado / Aproved:** Junio 26 de 2015

Tipo de artículo / Type of paper: Investigación Científica y Tecnológica.

Afiliación Institucional de los autores / Institutional Affiliation of authors: Centro de electricidad electrónica y telecomunicaciones CEET SENA Bogotá, grupo GICS, GITIS. Universidad Manuela Beltrán, Bogotá grupo GITIS. Universidad El Bosque.

Autor para comunicaciones / Author communications: Bareño Gutiérrez Raúl., raulbare@misena.edu.co

Los autores declaran que no tienen conflicto de interés.

apto para ser implementado como mecanismo de seguridad de infraestructura en pequeñas, medianas y grandes empresas, garantizando la protección de los datos. Este artículo busca incentivar a las diferentes compañías que proveen soluciones tecnológicas y de administración de la información a la migración, instalación y configuración de estos servicios sobre el protocolo IPV6.

Palabras clave: Dhcp; Ftp; Ssh; Ipv6; Ipsec; Protocolo; Seguridad.

encourage the various companies that provide technology and information management solutions to migration, installation and configuration of these services on the IPv6 protocol.

Keywords: Dhcp; Ftp; Ssh; Ipv6; Protocol; Ipsec; Security..

Introduction

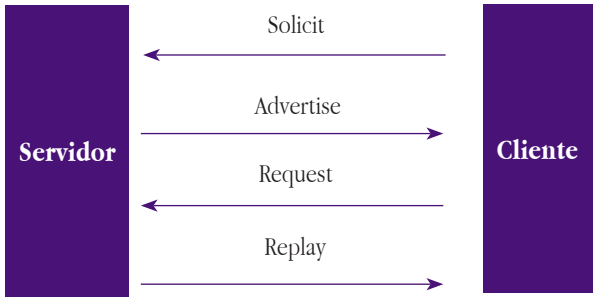
Uno de los mejores avances que ha tenido el mundo ha sido internet, como herramienta de comunicación a nivel mundial, su funcionamiento se implementa sobre un protocolo conocido como IP, protocolo de internet, con el cual se le asigna una dirección virtual a cada equipo para que este pueda acceder a la red, pero en la actualidad su escases es evidente quedando pocas por distribuir en IPv4, además de su alta tasa de vulnerabilidad y gran demanda de direcciones necesarias para cubrir todos y cada uno de los dispositivos que se quieren interconectar , por ello es necesario estandarizar y utilizar la nueva versión del protocolo IPv6 [1], que involucra un pool de direcciones mucho más amplio dadas sus mejores circunstancias de seguridad; razón a ello es necesario que las empresas empiecen a implementar sus servicios usando tecnología basada en arquitectura con direccionamiento en IPv6 [2] [3].

En el protocolo IPv4, cada dirección se compone de 32 bits, lo que permitía la existencia de 4300 millones de direcciones únicas. En comparación las direcciones IPv6 [4], las cuales se componen de 128 bits, lo que permite la existencia de aproximadamente 340 billones de direcciones IP únicas; En la actualidad muchos servicios como DHCP [5], FTP [6] y SSH [7] requieren funcionar con el nuevo estándar y que puedan ser ejecutados en este protocolo; razón válida para migrar los servicios y demás protocolos que se basaban en IPv4 a IPv6.

Uno de los primeros servicios que debe migrar es DHCP, (Dinamic Host Configuration Protocol) [8] [9] protocolo dinámico de configuración de host, el cual se encarga de brindar direcciones IP a los diferentes equipos conectados a la red de manera dinámica necesarios para que un sistema pueda comunicarse efectivamente, El objetivo principal es simplificar la administración de la red [10]. El servicio DHCP para IPv6, está definido en el RFC 3315. Trabaja sobre UDP y utiliza la arquitectura Cliente Servidor, además utiliza multicast para los mensajes [11] [12].

El funcionamiento de DHCPv6, empieza en el momento en el que el cliente escucha en el puerto 546 y los transmisores escuchan en el puerto 547, estos se comunican por medio de una dirección local y direcciones multicast (ver fig. 1) [11] [13].

Figura 1. DHCPv6



Otro de los servicios que busca la implementación hacia IPV6 es el protocolo Secure Shell (ssh), desarrollado por Tatu Ylonen [14] en la Universidad Tecnológica de Helsinki en Finlandia y OpenSSH [7] [15], nace del proyecto de un sistema operativo orientado a la seguridad que permite realizar la comunicación y transferencia de información de forma cifrada proporcionando fuerte autenticación sobre un medio inseguro. Provee la ejecución de procesos, el inicio de sesiones a servidores, la ejecución de comandos y la copia de archivos remotamente; brindando comunicaciones cifradas entre el cliente y servidor, evitando así el robo de información y manteniendo la integridad de los datos que viajan a través de la red. [16]. como se explica en el RFC de Secure Shell [17] [18]; Proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras, adicionalmente, provee seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP. Para la autentificación, puede utilizar algoritmo de cifrado como RSA o DSA [15]. Para el envío de datos a través de la red, usa 3DES, IDEA, Blowfish [19] [20].

Otro servicio fundamental es el protocolo de transferencia de archivos FTP, muy usado en Internet hoy día [21]. Su objetivo es transmitir archivos exitosamente entre máquinas en una red sin que el usuario tenga que iniciar una sesión en el host remoto o que requiera tener conocimientos sobre cómo utilizar el sistema remoto. Su funcionamiento consiste en que un equipo o host se pueda conectar a un servidor de archivos para descargar, modificar, consultar, eliminar y enviar documentos, independiente del sistema operativo del cliente. Además permite a los usuarios acceder a archivos en sistemas remotos usando un conjunto de comandos simples. Es recomendado y se describe en el RFC 959 [22] [23]. Para acceder a los archivos remotos, el usuario debe identificarse al servidor. En este punto el servidor es responsable de autentificar al cliente antes de permitir la transferencia de ficheros.

Desde el punto de vista de un usuario de FTP, el enlace está orientado a conexión. Es necesario que ambos hosts estén activos y ejecutando TCP/IP [24], para establecer una transferencia de ficheros. Hoy se usa principalmente en redes corporativas [25] [26]. Un problema básico de este servicio es la seguridad, ya que toda la transferencia de archivos con el servidor se realiza en texto plano sin ningún tipo de cifrado, dando así la opción de que un atacante acceda al servicio de archivos, los modifique o los lea sin ningún inconveniente [27].

Finalmente dentro de los alcances del trabajo se revisa la utilidad del protocolo de seguridad nativo ipsec [30] en IPV6 de host a host en lugar de punto a punto como se hace en ipv4. El encabezado AH [9] [30] se utiliza para garantizar la integridad y ataques de no repudio; y ESP [30] para la confidencialidad, integridad y anti replay uno de los problemas potenciales de ipsec en ipv6, es que no se puede garantizar su implementación como mecanismo en cualquier escenario. Es conveniente se configure de forma manual, y se adicione al servidor DHCPv6, que permite tener un control mayor sobre la asignación de direcciones y suministrar otra información como por ejemplo dirección del servidor FTP, o DNS [31]. Los algoritmos utilizados en la seguridad son MD-5 y SHA-1[30]; definido en RFC 1827[12] y 2406[13]. Este protocolo se diseñó para proveer confidencialidad, autenticación del origen de datos, integridad sin conexión y servicio contra reenvío de paquetes. En cuanto a los servicios bajo IPV6 [24], se van estandarizando y más dispositivos se actualicen para trabajar con este protocolo, nuevas implementaciones de seguridad en la infraestructura serán necesarias de implementar.

Materiales y metodología

Los protocolos DHCP, FTP y SSH son servicios de la capa de aplicación, en esta sección se describen las consideraciones y detalles de su implementación y funcionamiento bajo el protocolo IPV6 sobre diferentes sistemas operativos (Ver tabla 1) en una red local utilizando máquinas virtuales a través de la herramienta Virtual Box y WireShark para la captura de tráfico.

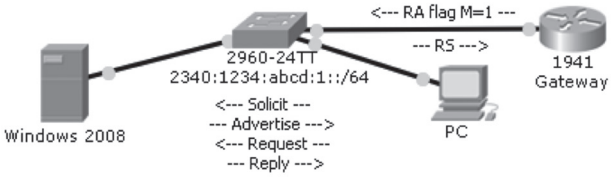
La instalación de cada uno de los servicios se efectuó bajo un escenario controlado en laboratorio, una vez configurado la máquina virtual con los servicios implementados bajo el sistema operativo Linux y Windows (Ver tabla 1).

Tabla 1. *Equipo y software utilizado*

Sistema Operativo Servidor	Windows Server 2008- 2012 R2
Linux Debían y Ubuntu	
Sistema Operativo	
cliente	Windows 7 con FileZilla 3.10.3
Herramienta de virtualización	Virtual Box
Herramienta de captura de tráfico	WireShark 1.12.5
PC1	Lenovo G40 70
PC2	Toshiba ultrabook S400u
Simulador	Cisco Packet Tracert 6.2

La figura 2 muestra el escenario sobre el cual se hicieron las respectivas pruebas de implementación y análisis de cada uno de los servicios corriendo bajo IPV6. Teniendo en cuenta el pool de direcciones asignadas bajo DHCPV6 como ámbito de pruebas.

Figura 2. *Configuración de DHCPV6*

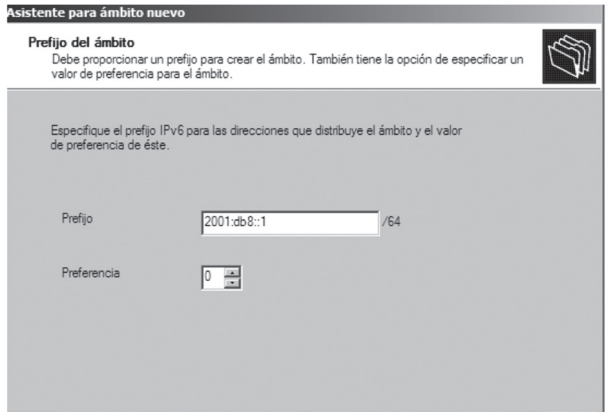


Para los demás protocolos FTP y SSH se utilizó un escenario muy similar.

Metodología

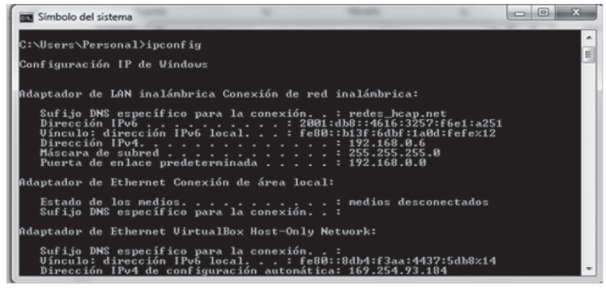
El procedimiento fue el siguiente, se utilizó Virtual Box para crear la máquina virtual y se instaló el sistema operativo Windows Server 2008 y server 2012 R2, además Linux debían y Ubuntu server, asi como dos máquinas físicas con Windows 7 como clientes. Para el servicio DHCPV6 se configuró el active Directory y el DNS. Se creó el ámbito para IPv6 el cual se definió a partir del prefijo 2001:db8:1 ver figura 3, también se solicitaron direcciones de reserva o direcciones excluidas y otras opciones como el tiempo de concesión de una dirección asignada y su tiempo de expiración.

Figura 3. *Especificación del prefijo de inicio de direcciones IPv6*



Además se hizo la conexión de red para todas las máquinas y se realizó la verificación de asignación de direcciones de ipv4 y de ipv6 dinámicas y locales en cada una. Ver figura 4.

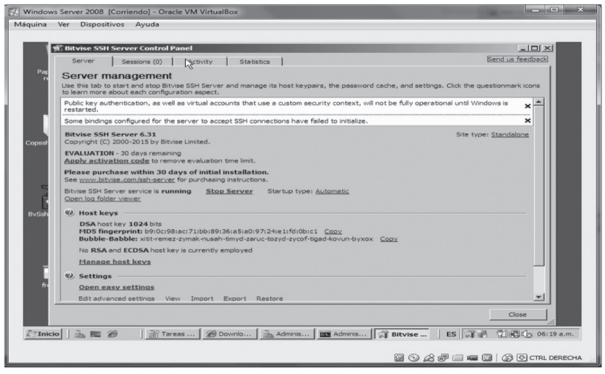
Figura 4. *Verificación IPv4 e Ipv6 en el cliente*



Para la configuración e implementación del servicio SSH bajo IPV6 en Windows Server 2008 y 2012 R2 así como en Linux Ubuntu y Debían se deben tener algunas consideraciones previas a la conexión; se deben verificar que las reglas de entrada y salida TCP del Firewall de los servidores Windows estén activas, además crear una regla de entrada y de salida del protocolo SSH a través del puerto 22, realizar una configuración estática de las respectivas direcciones IPv6 para efectuar correctamente la captura

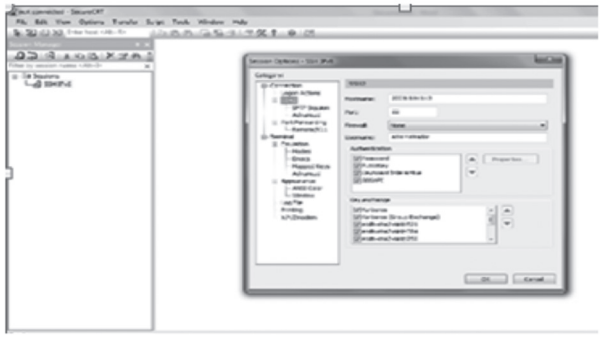
de los paquetes. Posteriormente implementar BitVise SSH Server para hacer uso de SSH sobre IPv6 ver figura 5, y sobre el cliente configurar Secure CRT para realizar la conexión respectiva, se validan ambos lados de la conexión, con la contraseña de administrador del servidor SSHv6.

Figura 5. *Configuración de ssh server para ipv6.*



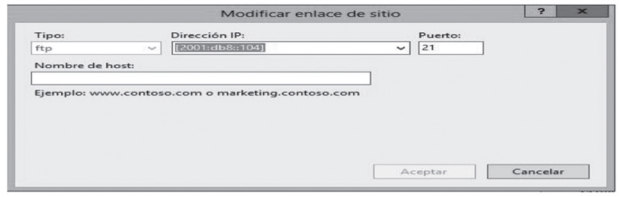
Se observa que el log del servidor SSHv6 ver figura 6 ha recibido satisfactoriamente la conexión y en el lado del cliente se ha permitido su acceso remoto.

Figura 6. *Acceso al server SSH bajo IPV6*



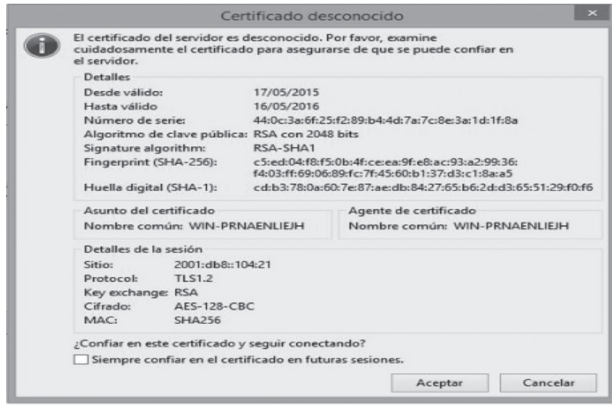
Para la configuración del servicio FTP sobre IPV6 es necesario agregar primero el rol de IIS (Internet Information Service) y activar el servicio FTP, como segunda instancia se debe crear un sitio al cual se asigna una dirección IP publica para que sea accesible por medio de internet. Además se crean carpetas personalizadas para cada usuario, en donde se almacenan todos y cada uno de sus archivos individuales. A continuación, se agrega la dirección IPv6 [2001:db8::104] incluyendo los caracteres de paréntesis cuadrados y se especifica el puerto 21 ver Figura 7.

Figura 7. *Direccionamiento IPv6 para FTP*



Para evitar problemas de seguridad se implementa un certificado SSL, para que él envío de los datos sea cifrado e ilegible por los atacantes. La seguridad de SSL, evidencia que la información viaja cifrada y es totalmente indescifrable, ver figura 8.

Figura 8. *Certificado SSL para cliente FTP*



Resultados

La implementación y configuración de los servicios FTP, DHCP y FTP bajo el protocolo IPV6 junto a los parámetros de seguridad en cuanto a autenticación, confidencialidad e integridad en cada uno de los sistemas operativos analizados se puede revisar en la tabla 2.

Tabla2. *Revisión de la seguridad en los servicios ipv6.*

	Server Windows 2018			Server Windows 2012 R2			Server Linux Debian			Server Ubuntu		
Servicios	DHCP	FTP	SSH	DHCP	FTP	SSH	DHCP	FTP	SSH	DHCP	FTP	SSH
soporta IPV6	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Parámetros de configuración (nivel de dificultda)	Baja	Baja	Baja	Baja	Baja	Baja	Alta	Alta	Alta	Media	Media	Media

	Server Windows 2018			Server Windows 2012 R2			Server Linux Debian			Server Ubuntu		
Soporta Ipsec	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
VPN	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Autenticación clave compartida y certificado digital	RSA/ DSA	RSA/ DSA	RSA/ DSA	RSA/ DSA	RSA/ DSA	RSA/ DSA	RSA/ DSA/ PSK	RSA/ DSA/ PSK	RSA/ DSA/ PSK	RSA/ DSA/ PSK	RSA/ DSA/ PSK	RSA/ DSA/ PSK
Confidencialidad entre 56 y 128 bits	DES	DES	3DES	3DES	3DES	3DES	3DES/ AES	3DES/ AES	3DES/ AES	3DES/ AES	3DES/ AES	3DES/ AES
Integridad	MD5	MD5	MD5	MD5	MD5	MD5	MD5/ SHA	MD5/ SHA	MD5/ SHA	MD5/ SHA	MD5/ SHA	MD5/ SHA

En la tabla se identifican las mejores condiciones de implementación de DHCP, FTP y SSH bajo IPV6 sobre servidores Linux con algunas ventajas claras frente a Windows en cuanto a la autenticación entre las maquinas físicas, integridad y confidencialidad.

Otro aspecto a destacar es visualizar cada uno de los protocolos implementados como DHCPv6 ver figura 9, se puede registrar la dirección 2001:db8:1 que es el servidor que está entregando la dirección IPV6 asignada dinámicamente al cliente en este caso 2001:db: 4616:3257: f6e1: a251.

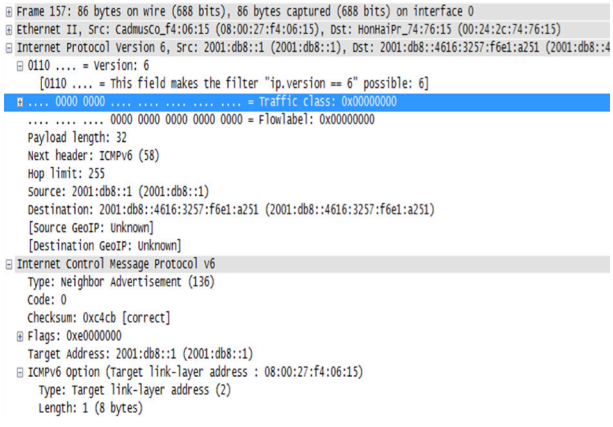
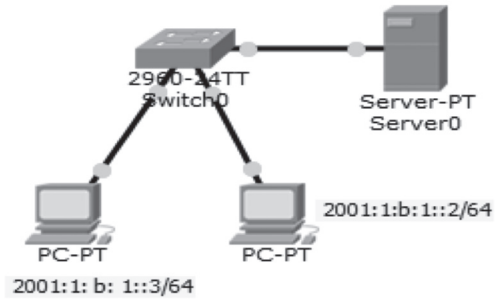


Figura 9. *Entrega de una ipv6 al cliente por DHCPv6*

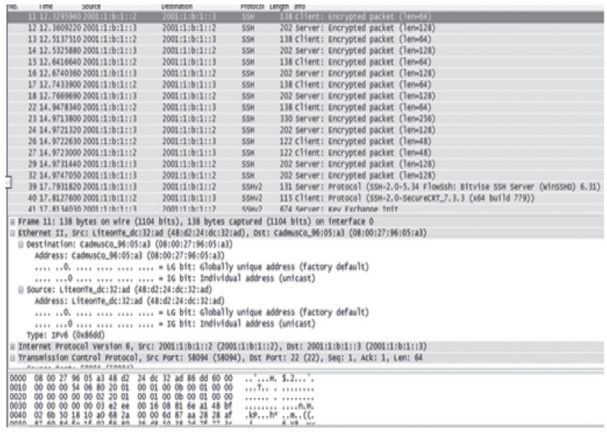
Para el acceso remoto al servidor usando el servicio SSH mediante direcciones IPV6 se configuro bajo este escenario controlado (ver figura 10).

Figura 10. *Escenario para SSH bajo IPV6*



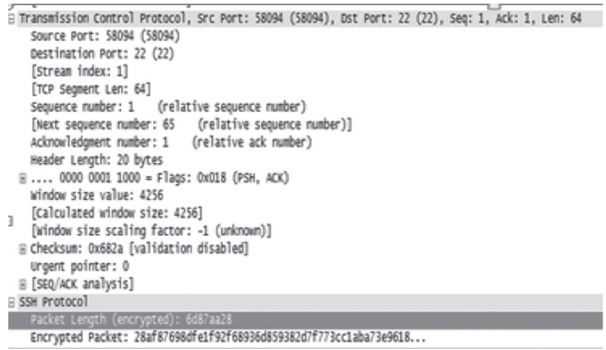
Se utilizó otro tipo de direccionamiento en el server 2001:1:b:1::3 y un cliente 2001:1:b:1::2 (ver figura 11).

Figura 11. *Acceso remoto con SSHv2 bajo IPV6*



Se observa en los dos primeros paquetes el intercambio de llaves que realiza SSH al realizar la conexión entre los extremos; en el primer paquete se revisa el cifrado que no permite ver la información. Adicionalmente TCP hace uso del puerto 22 y su mensaje está cifrado entre las partes ver figura 12.

Figura 12. *Mensaje encriptado entre extremos con IPV6*

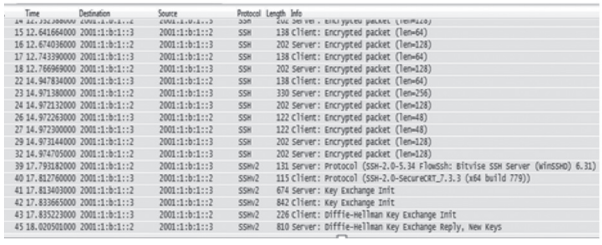


Es de destacar que se inicia el intercambio de llaves sin contacto previo de Diffie-Hellman [28] [32], para realizar el intercambio durante la sesión. Con un paquete de 84 bytes con cifrado AES-256 [29] [33], sin compresión, (ver figura 13); adicionalmente es el servidor quien proporciona la respuesta al intercambio de llaves, usando la versión de SSH v1 pero rápidamente antes del primer intercambio de llaves se realiza el cambio a SSH v2.

Figura 13. *Intercambio de claves con SSH para ipv6*

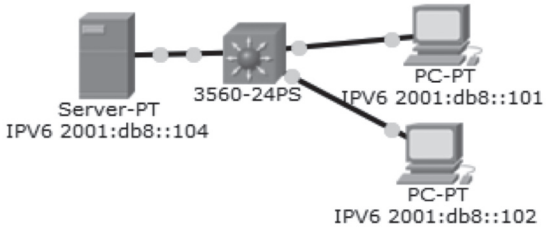
Se observa que la conexión SSH se activa y puede ser terminada por parte del cliente como del servidor. Ver figura 14.

Figura 14. *Intercambio con SSHv2 en ipv6.*



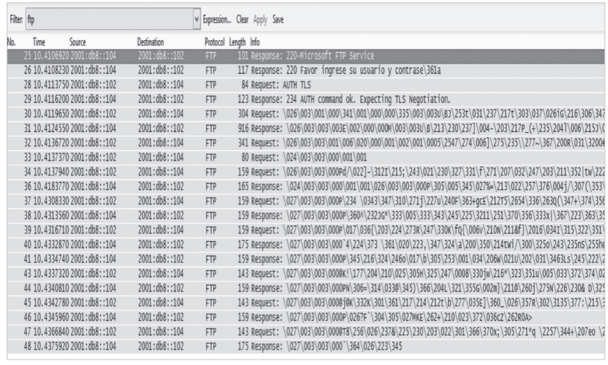
En cuanto a la implementación del servicio FTP bajo ipv6 se configuro la red LAN ver figura 15. En el servidor se crean usuarios y perfiles para el acceso con la opción de modificar e eliminar archivos de manera segura usando la validación de los puntos mediante IPSEC.

Figura 15. *Escenario para FTP bajo IPV6*



Se adiciona un certificado de seguridad SSL, para fortalecer él envió cifrado y oculto a atacantes, esto es obligatorio; también se activa la opción de usar cifrado de 128 bits [31]para estas conexiones. Una vez se activa la sesión FTP bajo ipv6 no permite la lectura del certificado de seguridad se evidencia que la información viaja cifrada y totalmente ilegible (ver figura 16).

Figura 16. *Certificado SSL entre el cliente y server IPV6.*



Discusión

La falta de despliegue del protocolo IPv6 en América Latina y el Caribe se ha demorado por la falta de capacitación del personal encargado en las organizaciones y empresas de Internet de la región, según considera el experto Hans Reyes, coordinador de la Red Nacional Académica de México.

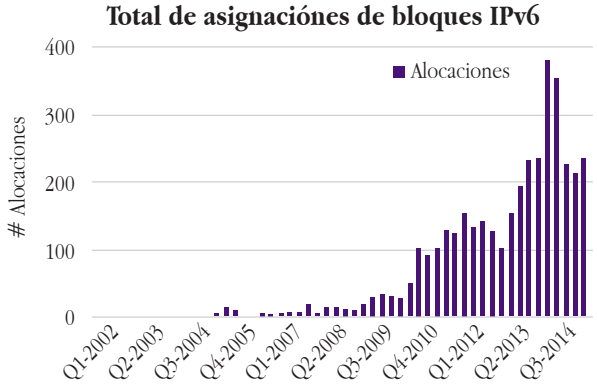
En la actualidad es una realidad que se debe apuntar hacia la implementación de IPv6 como una herramienta clave para lograr un mayor desempeño de las aplicaciones de Internet como DHCP, FTP y SSH entre otras, según google en sus estadísticas a 2014 el crecimiento y uso de este protocolo es considerable (ver figura 17).

Figura 17. *Google uso de direcciones y servicios IPV6*

El mayor problema que se vislumbra es la falta de personal idóneo para su implementación. Se debe resaltar su importancia y valor hacia redes en producción para tener un mayor desempeño en las aplicaciones que ya utilizan el estándar IPV6.

Otro problema es el poco contenido bajo IPv6, proveedores como (Google, Facebook, Microsoft, Cisco) ya lo soportan en sus redes. Se debe sensibilizar los ISP, gobiernos, empresas, universidades hacia su migración y masificación; no es solo un tema de moda es parte del todo de Internet. Según LACNIC organismo encargado de la asignación de direcciones IPV6 para américa latina se refleja el amplio rango de asignaciones IPV6 para la región (ver figura 18).

Figura 18. *Rango de ipv6 en américa latina*



Existen diferentes estudios realizados en la implementación de servicios empresariales sobre el protocolo IPv6, se destacan el análisis de la Universidad Carlos III de Madrid sobre todo en el campo de la seguridad, concluyendo que pronto existirán ataques exclusivos para IPv6 y resaltan la importancia en el uso de IPSEC que en la actualidad no es muy utilizado [31]. La Universidad de Oriente en Venezuela, intentó implementar dentro de su red el protocolo IPV6, dando como conclusión que este tipo de red presenta limitaciones de hardware y software las cuales no fueron solucionadas por la propia universidad, afectando la implementación de dicho protocolo en su red [32].

Los servicios analizados como DHCPv6 [33], son una herramienta importante en la administración de redes. SSH y FTP de igual manera y para poder utilizarlos se necesita conocimientos de sistemas operativos libres como Ubuntu o Debían y propietarios como Windows server 2008 o 2012 R2 utilizados durante esta investigación; ya que su implementación bajo IPV6 no es un tema exclusivamente de redes, también tiene impacto a nivel de servidores, aplicaciones y dispositivos de seguridad.

Conclusiones

Es evidente el gran reto durante el diseño e implementación de servicios bajo el protocolo IPv6 para las áreas de tecnología en sectores productivos y académicos, así como para los usuarios de Internet. La migración hacia este estándar permite minimizar riesgos de seguridad, de su antecesor IPV4. Este artículo revisa los mecanismos de configuración de los protocolos DHCP, FTP y SSH, además de su seguridad en los principales sistemas operativos actuales que tienen activado IPv6 por defecto, pero no las características de IPSEC que le aportan confidencialidad, autenticación e integridad tanto a los datos como a los usuarios de forma transparente, con la posibilidad de agregar las tradicionales formas de proteger la información que lo hace más robusto y confiable. Siendo fundamental formar a los administradores de red en el protocolo IPv6 para la aplicación de políticas de seguridad e implementación de nuevos servicios y formas de comunicarse conscientes de los riesgos que conlleva su utilización y conociendo los mecanismos de seguridad que deben aplicar.

El principal aporte de este trabajo de investigación es el hecho de proveer una solución real y factible para la implementación de los servicios DHCP, SSH, y FTP en IPv6; los resultados obtenidos durante las pruebas demuestran que la solución desarrollada es sencilla y funcional e incentiva el uso de estos servicios en un entorno local. Además presenta una contribución para la comunidad de administradores de redes como una alternativa sencilla y segura en la asignación de direcciones, para el acceso remoto bajo este nuevo estándar siendo altamente escalable, así como para el intercambio de archivos teniendo como premisa que el proceso será un poco más lento.

Finalmente la implementación y revisión de la seguridad de los servicios analizados en entornos integrados bajo IPV6 será un proceso continuo en el que diariamente aparecen nuevas vulnerabilidades y riesgos de seguridad. Por ello es importante mantener una buena formación

en los protocolos utilizados, porque hacia el futuro existirán nuevos riesgos que irán apareciendo a medida que se incremente la utilización del protocolo IPv6; análisis y estudios como los aquí planteados permiten medidas de protección a las nuevas y versátiles infraestructuras de telecomunicaciones.

Referencias

[1] Bareño, G, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

[2] Lee, W. J., Park, S. S., Lim, C., Kim, J., & Jeong, B. S. (2014). Server authentication for blocking unapproved WOW access. In Big Data and Smart Computing (BIGCOMP), 2014 International Conference on (pp. 155-159). IEEE

[3] Chown, T. (2005). IPv6 campus transition experiences. In Applications and the Internet Workshops, 2005. Saint Workshops 2005. The 2005 Symposium on (pp. 46-49). IEEE.

[4] Beijnum, I. (2011). An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation

[5] Becerra Cobos, J. C., Simbaqueva Buitrago, J. R., & Valenzuela Suarez, A. F. (2013). Diseño e Implementación de redes IPv6 en MIPYMES: caso laboratorio de informática.

[6] Sanguankotchakorn, T., & Somrobru, M. (2005). Performance evaluation of IPv6/IPv4 deployment over dedicated data links. In Information, Communications and Signal Processing, 2005 Fifth International Conference on (pp. 244-248). IEEE

[7] Molina Ángel, F., & Castro Domínguez, J. F. (2013). Implementación de servicios IPv6 en la Universidad Autónoma de Guerrero, México. Revista Vínculos, 10(2).

[8] Stewart, B. (2007). CCNP BSCI Official Exam Certification Guide (Exam Certification Guide). Cisco Press

[9] Kalusivalingam, V. A. (2004). Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).

[10] Carrera Buenaño, M. A. (2010). Análisis de las Técnicas de Convivencia entre IPV4 e IPV6 y su Implementación en los Servicios: Web, Mail, FTP, Proxy, DNS y DHCP de la Intranet de la ESPOCH

[11] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney. (2003). "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315

[12] Chown, T., Venaas, S., & Strauf, C. (2006). Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues.

[13] Valladares, R. A. R., Brioso, G. A. P., & Aragón, L. A. G. (2010). Metodología de Implementación de Ipv6 en La Red de La Universidad de Oriente. Ingeniería Electrónica, Automática y Comunicaciones, 29(1), 36-43

[14] Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., & Ylonen, T. (1999). SPKI certificate theory (No. RFC 2693).

[15] Aguirre, L. P., González, F., & Mejía, D. (2013). Aplicaciones de MPLS, Transición de IPv4 a IPv6 y Mejores Prácticas de Seguridad para el ISP Telconet. Revista Politécnica, 32

[16] Abasolo Aranda, S. E., & Carrera Paz y Miño, M. A. (2014). Artículo Científico-Evaluación del modelo de referencia de Internet of things (IoT), mediante la implantación de arquitecturas basadas en plataformas comerciales, open hardware y conectividad IPv6

[17] Warfield, M. H. (2003). Security implications of IPv6. Internet Security Systems, 4(1), 2-5

[18] Ylonen, T., & Lonvick, C. (2006). The secure shell (SSH) connection protocol. RFC 4254, RFC 4251.

[19] Motta Barrera, O. E., & Peláez Negro, R. (2014). De la planeación de TIC a la implementación de IPv6 un escenario deseado para desarrollar el "Internet de las cosas" en la Universidad de Ibagué Colombia

[20] Santamaría Alamar, A. P. (2014). Análisis, diseño e implementación de una red prototipo utilizando el protocolo IPv6 y QoS para la empresa Santanet (Doctoral dissertation).

[21] Flores Calahorrano, F. R. (2014). Análisis y emulación de Multihoming y de la publicación al internet

de servicios web, transferencia de archivos y correo a través de una red IPV6 (Doctoral dissertation).

[22] Warfield, M. H. (2003). Security implications of IPv6. Internet Security Systems, 4(1), 2-5.

[23] Baker, F., Li, X., Bao, C., & Yin, K. (2011). Framework for IPv4/IPv6 Translation. RFC 6144.

[24] Martínez, J. P. (2009). IPv6 para Todos: Guía de uso y aplicación para diversos entornos. Jordi Palet Martínez

[25] Jian, G. U. O. (2008). Model of FTP server based on Spring framework in IPv6 and it's implementation [J]. Computer Engineering and Design, 19, 019.

[26] Allman, M., Ostermann, S., & Metz, C. (1998). RFC 2428, FTP Extensions for IPv6 and NATs. Network Working Group.

[27] Zheng, W., Liu, S., Liu, Z., & Fu, Q. (2009). Security transmission of FTP data based on IPsec. In 2009 1st IEEE Symposium on Web Society (pp. 205-208).

[28] Kent, Stephen, and R. Atkinson. (1998) "RFC 2406,"." Encapsulating Security Protocol.

[29] Atkinson, R. (1995). RFC 1827: IP encapsulating security payload (ESP), Obsoleted by RFC2406 [KA98c].

[30] Kent, Stephen, and Randall Atkinson. (1998). RFC 2402: IP authentication header".

[31] García Martín, C. (2012). Análisis de seguridad en redes IPv6.

[32] Valladares, R. A. R., Brioso, G. A. P., & Aragón, L. A. G. (2010). Metodología de Implementación de Ipv6 en La Red de La Universidad de Oriente. Ingeniería Electrónica, Automática y Comunicaciones, 29(1), 36-43.

[33] Mrugalski, T., & Wu, P. (2012). Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for DHCPv4 over IPv6 Endpoint.

Los Autores

Raúl Bareño Gutiérrez

Ingeniero de sistemas, Magister en telecomunicaciones, Dr. (c) en ciencias computacionales enfocado a la educación con TIC, UNINI México. Docente investigador en UIS, UTS, docente en instituciones SENA, Universidad minuto de Dios, (Uniminuto), universidad militar (UMNG). Con certificaciones internacionales en CCNA, CCNP, y FWL de cisco.

Sonia Cárdenas Urrea

Ingeniera en Redes de Computadores, Especialista en Seguridad de Redes de Datos, Especialista en Gerencia de Proyectos Informáticos, Especialista en Gestión de Proyectos de Ingeniería, Estudiante de Magister. (c) en Dirección de Proyectos, Universidad Viña del Mar Chile. Docente investigadora del Servicio Nacional de Aprendizaje SENA, Docente Universidad Distrital.

William Navarro Núñez

Ingeniero en Redes de Computadores, Tecnólogo en sistematización de datos, Especialista en Seguridad de Redes de Computadores, Especialista en Gerencia de Proyectos de Ingeniería de Telecomunicaciones, Estudiante de Magister. (c) en Dirección de Proyectos, Universidad Viña del Mar Chile. Docente investigador del Servicio Nacional de Aprendizaje SENA, Docente Universidad Distrital.

Hugo Sarmiento Osorio

Ingeniero Electrónico, MSc en educación, con experiencia en diseño, implementación, y gerencia de proyectos de telecomunicaciones. Experto Américas en Cableado Estructurado en World Skills Internacional, Certificación CISCO en CCNA routing and switching 4.0. ITIL fundamental versión 3. PMI, Máster en Educación por la Universidad de Gran España.

Nixon Duarte Acosta

Ingeniero de Sistemas de datos, Magister en Ingeniería Area Sistemas y Computación Docente investigador Universidad Manuela Beltrán.

German Gonzalo Vargas Sánchez

Ingeniero de Sistemas Universidad Distrital Francisco José de Caldas. Especialista en Ingeniería de software Especialista en Informática y Ciencias de la Computación Candidato a Magister en software Libre, Universidad Autónoma de Bucaramanga Colombia. Estudiante del Doctorado en Pensamiento Complejo en la Multiversidad Mundo Real Edgar Morin México.