ELABORACIÓN DE UNA GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPv6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO

ING. ARTH GROSSY SABOGAL ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD EN INFORMÁTICA

MELGAR

2017

ELABORACIÓN DE UNA GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPv6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO

ING. ARTH GROSSY SABOGAL ORTIZ

Monografía de Proyecto de Grado

Asesor de Proyecto

ALEXANDER LARRAHONDO N.

Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA

PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

MELGAR

2017

*Nota de Aceptación**:***

_____

_____

_____

_____

_____

Firma del Jurado 1

_____

Firma del Jurado 2

*Fecha**:*** _____**/**_____**/**_____

CONTENIDO

Pág.

LISTA DE ANEXOS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

1. TÍTULO DEL PROYECTO

ELABORACIÓN DE UNA GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPv6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO.

INTRODUCCIÓN

Al inicio de los años 80 la Internet y sus primeros diseños, experimentó un crecimiento agigantado en la rama de las comunicaciones, dando un nuevo espacio más amplio y moderno en la vida de los usuarios y las aplicaciones. En 1981 se hace el lanzamiento del IPv4, siendo la primera versión del protocolo de Internet que se implementada de manera extensa, facilitando un gran avance en las comunicaciones de redes, dando por hecho que la necesidad de direcciones IP había terminado. Sin embargo, con la migración hacia el IPv5 se pretendía satisfacer las necesidades del internet como protocolo experimental, únicamente encausado a la orientación del procesamiento de flujo de voz, audio y video.

Con el ánimo de reparar las deficiencias de red en el año de 1992, se empezó a buscar mecanismos para mejorar y suplir los defectos de red descubiertos, por medio de la siguiente generación de Protocolos de Internet o IPng (Internet Protocol Next Generation) y sugerido por IETF (Internet Engineering Task Force), nace el IPv6, quien culminó con las especificaciones características de un protocolo IP a satisfacción, sucesor actual del IPv4 y conocido como la versión 6 del Protocolo Internet. Fue lanzado en 1999, catalogado como la nueva versión o el futuro de las comunicaciones, dando una solución acorde a todos los dispositivos que necesitan estar conectados.

Las infraestructuras de transmisión de alta velocidad son requeridas en la actualidad, a lo que las grandes empresas le han estado apuntando, encontrándose con una gran cantidad de aspectos administrativos y de seguridad. Las compañías pretenden no caer por debajo de los estándares necesarios de la globalización, ni convivir con falencias en la prestación de servicios avanzados, que puedan impedir el éxito empresarial.

Una guía abierta para la administración de riesgos de seguridad en el protocolo de internet ipv6 sobre estándares de enrutamiento dinámico en equipos con plataforma cisco seria la respuesta a múltiples interrogantes en cuanto a los diferentes estándares de seguridad y consulta rápida para aplicativos CISCO y un buen articulo pedagógico de consulta ante el personal amante de la información de vanguardia, como lo es el nuevo protocolo IPv6 a implementar en América latina.

2. DESCRIPCIÓN RESUMEN PROBLEMA

Los centros de cómputo, bases de datos, redes, ambientes virtuales, sistemas autónomos entre otros, están sujetos a la transmisión de información necesaria por el usuario de hoy, por ende la información representa un activo muy valioso a resguardar para cualquier empresa y para quien la usa, comparte y distribuye bajo el papel de usuario, es por ello que se hace necesario implementar mecanismos o guías que permitan documentarnos y proteger la información de las posibles amenazas generadas o no reconocidas por la actualización de los múltiples sistemas, a los cuales no se pueden detener tan solo aceptar y gestionar. Estas actualizaciones en sistemas están dadas en todos los niveles y capas de los sistemas, incluso los protocolos IP, siendo necesarios para su abastecimiento y provisión de transmisión de datos. Estas actualizaciones necesitan mecanismos de apoyo para adecuación a entornos, construcción de adaptabilidad, pruebas de seguridad e implementación de aplicativos, de tal forma que la construcción de herramientas de consulta para gestión y manejo de riesgos se hace necesaria tanto para establecer diferentes diagnósticos de seguridad, como para el tratamiento de riesgos y prevención de accidentes informáticos.

Adicionalmente, el desconocimiento de la normatividad y la poca experiencia en la migración hacia nuevos protocolos permite una brecha importante entre la seguridad, descubriendo deficiencias en adaptabilidad y dejando entre dicho múltiples factores de seguridad, permitiendo que personas o sistemas malintencionados aprovechen este vacío para abusar o hacer de las suyas. Todo esto nos lleva a analizar los sistemas de actualización y protocolos nuevos, para su análisis de seguridad, administración de posibles riesgos e implementación segura. El IPv6 como protocolo nuevo y con la carencia de documentación integrada ante el manejo del mismo dentro de redes CISCO, ha permitido generar la necesidad de diseñar y publicar un documento como análisis de riesgo en el uso de este protocolo con el único objeto del aumento del margen de seguridad en los múltiples sistemas.

Con este proyecto se pretende salvaguardar la información, protegerla y tener una ampliación de la información sobre IPV6, para disminuir las posibilidades de ser vulnerado o de ser sometido a amenazas de altas proporciones; por lo que se necesitan conocer los posibles riesgos, se necesita reconocer cual es el enemigo, para posterior generar la implementación de elementos de seguridad y protegerse.

Existen múltiples problemas dentro de la conectividad Ipv6, como los son los problemas de conectividad donde solo permite la web, no permiten la

sincronización de contactos, zonas horarias y demás. Otros problemas también conocidos son los impedimentos para desactivación por MSDos “Nest”, impedimentos de creación de claves de registros de parámetros IPv6 para desactivación, selección de prioridad en protocolos, problemas de actualización de servicio de IPv4 a IPv6 entre otros. Adicionalmente en algunas aplicaciones, aunque se conviertan a IPv6, no activan IPv6 de manera predeterminada, generando traumatismos.

Continuando con las diferentes dificultades en redes cisco sobre el IPV6, no se descarta que en ocasiones el ISP actual no admita IPv6 o existan problemas de túnel entre un enrutador 6to4 y un enrutador de reenvío 6to4, donde el túnel de esta característica siempre tendrá problemas de seguridad, ya que los enrutadores de reenvío de 6to4 encapsulan y desencapsulan los paquetes, pero no comprueba que los datos que contienen los paquetes sean los verdaderos y es posible que se deba configurar estas aplicaciones para activar IPv6.

Este proyecto pretende mostrar un análisis bibliográfico, investigaciones prácticas e información disponible sobre ¿Cómo podemos mejorar y estructurar los niveles de seguridad y administración en IPv6 sobre estándares de enrutamiento dinámico ejecutado en equipos con plataforma CISCO entre otros?; siendo pieza fundamental para entender el protocolo IPv6, capacitando a los administradores de este tipo de redes, generando conciencia sobre las vulnerabilidades del mismo, y planteando que posibilidades existen sobre este protocolo IP.

Finalmente, cabe resaltar que la seguridad y la protección cumplen las funciones de obtener una confiabilidad, disponibilidad, autenticidad e integridad de los datos a través de la información que se envía o recibe mediante medios electrónicos de una forma más segura y en el mundo múltiples organizaciones se encuentran implementando equipos con Cisco, debido a su gran flexibilidad, fiabilidad y alcance de gran escala, sin embargo, actualmente existe un nuevo desafío de alto compromiso y responsabilidad, consistente en la introducción del protocolo IPv6 para el crecimiento, maximización y desarrollo del internet.

La creación de nuevas amenazas en materia de seguridad obliga a mejorar el nivel de competitividad en materia de integridad y protección de información, permitiendo a las empresas estar a niveles competentes, por ende el análisis apropiado de cada uno de los aspectos y características que componen este protocolo contribuye a la tranquilidad empresarial y bienestar informático de cualquier usuario que actualice o migra a un protocolo de vanguardia como el IPv6, bajo estándares de enrutamiento dinámico ejecutados en equipos con plataforma cisco.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Estructurar las técnicas y mejoras para la administración de seguridad sobre estándares de enrutamiento dinámico ejecutado en equipos con plataforma CISCO, mediante la elaboración de una guía abierta de seguridad basada en el análisis de riesgo en el protocolo de internet IPV6.

3.2. OBJETIVOS ESPECÍFICOS

• Recopilar información de los múltiples resultados de las investigaciones actuales sobre el IPv6, amenazas, vulnerabilidades, identificando sus antecedentes de creación, contexto tecnológico y organizacional.

• Identificar y promover las habilidades necesarias para el funcionamiento de los componentes que usa IPv6, junto con los instrumentos que existen para su configuración y mantenimiento seguro en una red establecida bajo dichos parámetros.

• Realizar un diseño práctico de guía para la presentación de las investigaciones que serán objeto de publicación.

• Generar una guía abierta de seguridad con las recomendaciones que se alleguen por los usuarios de plataforma CISCO, con el fin, de actualizar la información suministrada por este a medida que se presenten modificaciones o novedades.

4. JUSTIFICACIÓN

Cada día el creciente avance de las tecnologías y la comunicación conllevan a los usos de los servicios de Internet, por ello nace la necesidad indispensable de implementar estrategias y nuevos componentes de seguridad para proteger los activos más importantes de una organización: la información. Ahora, con el crecimiento tecnológico se ha tomado el concepto de “la red de redes” y su amplia masificación en todo tipo de contexto dentro de las áreas del desenvolvimiento humano, siendo un factor apetitoso para que aquellas empresas y usuarios exploten de mejor manera sus servicios, pero a su vez sufren de un sin número de peligros y amenazas que acechan con sigilo la información que se almacena. Por ello es de vital importancia saber cómo evitarlas o asegurar una transferencia segura de paquetes de datos, dado que su vertiginoso crecimiento y demanda ha provocado que un protocolo de Internet como el versión 4 (IPv4) no pudiera dar abasto ante el desarrollo mutante de las comunicaciones globales. La Fuerza de Tarea de Ingeniería de Internet (Internet Engineering Task Force, IETF) planteó un nuevo patrón, bajo el nombre de Protocolo Internet Versión 6 (IPv6) y que según muchos expertos e investigadores del tema, se establecerá como “heredero” de la versión anterior, dado el hecho de que soluciona y solventa funciones innovadoras conformes al actual avance de la red.

El IPv6 es el nivel más reciente del protocolo de Internet (IP), desenvolviéndose como parte soporte, parte interconexión de sistemas operativos donde no cuenta con guías rápidas de consulta para manejo, revisión y gestión de riesgos informáticos en su parte de implantación y funcionamiento, lo cual limita la información útil para la prevención de ataques y minimización del riesgo informático. El tema de seguridad debe ser profundamente analizado dada la alta posibilidad de que se presenten incuestionables debilidades que no son consideradas por los administradores de redes como tal.

Por lo tanto, el desarrollo del presente documento beneficiará a los administradores de redes en plataformas CISCO, mostrando los problemas más comunes en cuanto a materia de seguridad y las múltiples características, definiciones e información apropiada para tener en cuenta en el desarrollo apropiado del protocolo IPv6. Las empresas se beneficiaran con el resultado de este análisis previniendo y tomando un plan de acción preventivo para la adecuación de su plataforma dentro del protocolo mencionado, ayudando a tomar medidas proactivas y estando al tanto de los múltiples problemas de seguridad que puedan encontrarse. Adicional a esto, la academia y los alumnos podrán tener

el bagaje suficiente en el manejo de un tema tan contemporáneo, como el IPv6, el cual se hace necesario generar un grado significativo de experiencia, para estar a la vanguardia en materia de seguridad en el IPv6, siendo lo suficientemente competente por medio de la identificación de brechas, que son aprovechadas para generar peligros a través de ataques que involucran de forma comprometedora una información confidencial y privada, asimismo como la concientización y fomento de utilización de herramientas que permitan configurar y mantener segura una red bajo este esquema.

Lo que se pretende además, es brindar la posibilidad de estar al tanto de aspectos importantes relacionados con la aplicación de normas y políticas de seguridad, instrumentos tecnológicos de auditoría, complejidad, información utilizable y aprovechable, predisposiciones, facilidades, configuraciones, restricciones, prohibiciones entre otros, variables que resultan indispensables al momento de diseñar un proyecto de red bajo un esquema IPv6 y en caso de efectuarlo, lograr alcances en el ámbito de seguridad, aplicada a los estándares de enrutamiento dinámico que se ejecuten en la red bajo una plataforma CISCO.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Esta monografía de diseño y elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO, utiliza como recurso fuentes confiables de internet, consultas a especialistas de redes CISCO y personal internacional de Perú y España, junto con LACNIC, como organización no gubernamental de registro de direcciones de internet para América Latina y Caribe.

Tiene como alcance analizar las vulnerabilidades presentadas en la implementación y desarrollo del protocolo IPv6 como protocolo guía, nuevo en nuestro país, ya que a pesar de que se encuentra circulando desde hace buen tiempo en la red y diseño de equipos, aún no se puede constatar de una implementación total por parte de entidades Colombianas dentro de sus redes. La importancia de la gestión de vulnerabilidades detectadas en IPv6, la cual comparte ciertas características con el anterior protocolo, pretende no cometer los mismos errores y prever sus causas. Sin embargo, este protocolo contiene aspectos de mejora en la seguridad y maneja diferentes técnicas de administración, las cuales el técnico o administrador de redes debe conocer, tanto como para su implementación, manejo, identificación, como para aumentar el margen de seguridad en un protocolo poco aplicado, en el cual hace falta algo de experiencia para el manejo de riesgos.

La delimitación de esta monografía comprende un desarrollo teórico dado por fuentes externas y confiables en el tema, como empresas internacionales que ya han trabajado con este protocolo, que conocen su implementación y desarrollo, junto con el aporte de profesionales, quienes han experimentado ciertas vulnerabilidades o han identificado riesgos latentes en el IPv6 y que se centran en una sola guía abierta para consulta, estructuración y administración de riesgos. Por otro lado, se realizan pruebas para explicar las soluciones a la vulnerabilidad identificada y se emiten recomendaciones para el manejo de las mismas.

Se espera alcanzar el máximo nivel de comprensión en los temas propuestos por la guía, junto con la detección de posibles amenazas a la seguridad y apoyo pedagógico que respondan a las necesidades de los diferentes estudiantes o administradores de red que deseen iniciar con el proceso de migración hacia IPv6, fortaleciendo los estándares de seguridad dentro de la implementación de este protocolo que crece cada año.

6. MARCO REFERENCIAL

6.1. MARCO TEÓRICO

El TCP (Transmission-Control-Protocol) iniciador para lo que hoy en día se conoce como IP, es uno de los ejes fundamentales en internet; fue creado entre 1973-1974 por Vint Cerf y Robert Kahn dentro del departamento de defensa estadounidense, por la necesidad de establecer conexiones, desciframiento y flujo de datos entre los diferentes sistemas de computadoras, haciéndolo de manera apropiada y soportando los requisitos de operación de red. La eficiencia de este protocolo garantizaba inicialmente que los paquetes de datos fueran enviados al destino seleccionado sin errores y el mismo orden en el que fueron transmitidos. También proporcionó un mecanismo para empezar a distinguir aplicaciones dentro de la misma maquina usada, usando un concepto de “puerto” el cual es relativamente nuevo.

Dentro del mundo del internet existen miles de interconexiones entre ordenadores de diferentes clases, ramas, hardware, software, tipos de interconexión y demás, los cuales son totalmente incompatibles entre sí, he aquí donde se encuentra una de las grandes ventajas del TCP/IP, ya que este protocolo se encargó desde hace mucho tiempo de la comunicación entre múltiples dispositivos diferentes. El TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, además no es un único protocolo, sino que en realidad es un conjunto de varios protocolos que cubren los distintos niveles del modelo OSI; el TCP es el pionero en el soporte de muchas aplicaciones más populares dentro del internet, incluidos HTTP, SMTP, SSH Y FTP.

Para que los diferentes dispositivos se conecten a través de la red, cada uno debe tener una dirección IP única, este estándar IP es comparable con el sistema de direcciones de una ciudad, cada ciudad tiene su sistema de direcciones (por nombres o por números) y dos casas no pueden tener la misma dirección, dejando claro su único valor de asignación. Así mismo, el Internet requiere de un sistema para que los dispositivos “se encuentren” en la red y que estos dispositivos no tengan el mismo número IP, siendo esta una de las principales funciones que cumple el TCP/IP. Sumergidos en el marco de conceptos, las direcciones IP son un recurso escaso y como tal requieren ser administradas, con el objeto de garantizar la comunicación y la distribución correcta de las direcciones, dicha administración consiste en distribuir las direcciones alrededor del mundo de manera equitativa y descentralizada.

Los nuevos protocolos de red para la comunicación son de carácter evolutivo, lo que quiere decir que junto con ellos nacen nuevos factores para analizar, mejorar y proteger la información. Dentro de las redes de datos donde se transporta de manera directa la información a diferentes terminales, existen servicios de redes de datos que junto con sus respectivos protocolos son vulnerables a ataques informáticos, siendo la seguridad en redes la dirigente y rectora en el manejo de información y cuya mirada global entre los diferentes protocolos, tipologías de red y plataformas para la solución de problemas de incompatibilidad es la piedra angular de la seguridad informática.

Continuando ahora hacia los años 80 en donde la internet fue diseñada bajo parámetros poco experimentados y dimensionados, nunca se imaginó que pudiese llegar a las dimensiones actuales ni mucho menos poseer las dimensiones que hoy tiene; el crecimiento agigantado tanto de usuarios, como de aplicaciones junto con un despliegue de redes de telecomunicaciones son realmente sorprendentes. Esta necesidad llevo al nacimiento de la IPv4 lanzada en el año 1981, la primera versión del protocolo de Internet, siendo el primero implementado extensamente, generando un gran avance para las comunicaciones dentro de la red, dando sensación de alivio ya que en ese momento se pensó que sería suficiente y posteriormente se migro a la IPv5 pero este solo era un protocolo experimental y fue orientado a mejorar el procesamiento de flujo de voz, audio y video.

Para arreglar las deficiencias desde 1992 se empezó a buscar mecanismos para mejorar e intentar suplir las necesidades de aceptar en la red más usuarios y aplicaciones, generando la siguiente generación de Protocolos de Internet o IPng (Internet Protocol Next Generation) surgidos del IETF (Internet Engineering Task Force), culminando con la especificación de un nuevo protocolo IP, sucesor del actual IPv4, conocido oficialmente como la versión 6 del Protocolo Internet o IPv6 siendo lanzado en el año 1999. El IPv6 es la abreviatura de "Versión 6 del Protocolo de Internet", el protocolo de Internet de última generación que se ha diseñado para sustituir al protocolo de Internet actual, la Versión 4 del Protocolo de Internet (IPv4). Esta nueva versión es el futuro de las comunicaciones, ayudando a nuevos dispositivos a estar conectados a las redes de datos con mayor seguridad.

Presentando el concepto de seguridad en redes, se puede inferir que su finalidad es preservar la información, en su integridad y disponibilidad, evitando cualquier tipo de vulnerabilidades, riesgo o amenazas que se vea representada en perdida de información. Los riesgos en las redes nacen en el momento de la creación o dejación de una norma sin tener el pleno dominio, aplicado a este caso, se agrega

que un protocolo tan nuevo como el IPv6 maneja poca información, dejando una brecha para el nacimiento de riesgos.

Ahora bien, la migración del protocolo IPv4 a IPv6 comienza debido al agotamiento de las direcciones IP, siendo esta la preocupación inicial, limitando la red a millones de usuarios, donde hoy en día son miles de millones, aclarando que no solo es la internet también son los diferentes objetos tecnológicos como la PDA, los celulares, consolas, y demás.

La necesidad de una estructura robusta y mejorada para el internet se hace inevitable y un protocolo de enrutador IP se hace inminente, dando paso del IPv4 al Ipv6, siendo este primero rezagado en crecimiento de aplicaciones de las redes de computadoras sin dar abasto a las necesidades del hoy.

La IETF decidió ceder el paso al IPv6 con el objeto de amortiguar la demanda elevada y exponencial de direcciones IP, para cada una de las aplicaciones que se sostienen en la red y las que se desea llegar a tener y donde el IPv6 tiene la capacidad de direccionar 2128 nodos, lo que es equivalente a 340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456 nodos, gracias a que su direccionar consta de 128 bits, provocando la eliminación de varias de las herramientas existentes en IPv4, optimizando el espacio de direccionamiento con el que se estaba contando con 232.

Este protocolo también trae consigo una modificación en el formato de la cabecera, así como en la forma de direccionar los nodos, en él los campos ya no serán campos de 8 bits representados en forma decimal, sino que serán campos de 16 bits representados en forma hexadecimal y que están separados con “:”, lo cual cambia la forma de direccionar, así como elimina o cambia algunas herramientas de enrutamiento y gestión que se venían utilizando con IPv4.

En cuanto a materia de seguridad, la IETF infirió que fuera obligatorio en el IPv6 el permitir que todas las aplicaciones que se creen sean mucho más seguras de las que se tenían con el anterior protocolo, junto con el IPsec, el cual agregado únicamente en la capa de Internet puede predecir en que base o capa existen debilidades y evitar las mismas vulnerabilidades dadas en el IPv4.[1]

El protocolo IPv6 lleva un tiempo considerable entre nosotros, por ende lo que está en funcionamiento desde hace cierto plazo son conexiones SMB, DNS o incluso web de la Intranet, siendo necesario conocer su funcionamiento para la protección de la red, ya que muchos de los sistemas de protección IDS están

[1] MARCELO (Admin). Migración de IPv4 a IPv6. Redes I. Blogger. Bolivia. Cochabamba, 2013.

configurados para detectar la mayoría de los ataques hacia redes con IPv4, pero no para IPv6.

IPv6 necesita múltiples pruebas para garantizar una seguridad plena, para ello se requieren más test de seguridad y pruebas abiertas, sobre todo en su despliegue inicial, instalación e implementación, entre ellos cortafuegos y detectores de intrusos, donde no todos son enteramente compatibles con este nuevo protocolo siendo aquí donde radica su mayor debilidad.

La transición a IPv6 de forma completa es la parte más peligrosa, ya que habrá túneles de tráfico IPv6 a través de IPv4 y podría presentarse algunos problemas de seguridad. Si se créase un dispositivo para inspeccionar este tráfico a través del túnel, sería de gran ayuda para evitar que se inyecten tráficos maliciosos y con el IPv6 se sabría de una forma fácil el origen del tráfico.

Análisis entre IPv4 y el IPv6

Las características de construcción del IPv4 pretendían llenar múltiples debilidades de la anterior versión, pero con el crecimiento exponencial de las redes de telecomunicaciones y el nacimiento de una nueva era, provocó la creación del IPv6, el cual minimiza ciertas carencias planteadas por el IPv4 dando paso a una versión más compleja. A continuación se mencionan algunos problemas característicos en la red IPv4 y su análisis con su siguiente versión:

• Enrutado: Este problema dado por el crecimiento del internet, es la capacidad de almacenar de manera suficiente en los routers y el tráfico de gestión preciso para mantener sus tablas de encaminamiento. El número de rutas que un nodo puede manejar es finito y como el internet crece de manera rápida a comparación de los soportes tecnológicos que la avivan, se predijo que pronto las pasarelas que la sostienen llegaran a su límite, lo cual sería la fragmentación de las subredes y posiblemente sin acceso entre ellas.

• Escalas: Cada dirección IP disponible en cada máquina y presente en la red de 32 bits, supone que hay más de 4.300 millones de máquinas diferentes, sin embargo, estas cifras no son precisas y el número asignado a cada una de ellas no es arbitrario, sino que se genera por una estructura jerárquica perteneciente a una red, la cual la genera y evita que se desperdicien, por ende en el año de 1993 se pudo visualizar este crecimiento de las redes y el internet, previendo el agotamiento del espacio de direcciones.

• Aspecto de Seguridad: Los servicios comerciales y conexiones numerosas, hacen imperativo un mecanismo de seguridad de red. Es necesario esquemas de

autenticación y privacidad, para proteger a los usuarios y la integridad de la red, de ataques o errores.

• Multiprotocolo: La diversidad de diferentes plataformas hace necesaria las convivencias en diversos protocolos (IPX, OSI, IP), donde para comodidad de los usuarios se hace una metodología orientada al aspecto de sus trabajos o aplicaciones, que a una red orientada a protocolos, como se ha venido haciendo hasta el momento.

• Tiempo real: IPv4 es una red orientada a datagramas, por ende no existe el concepto de reserva de recursos y cada datagrama compite con otros, siendo que el tiempo de tránsito en la red es variable y sujeto a congestiones. Es esencial una extensión que haga posible el envío de tráfico de tiempo real, facilitando la disponibilidad de demanda necesaria en el campo.

• Comunicación Móvil: Las comunicaciones móviles deben estar a la vanguardia, por ende experimentan nuevas estructuras con mayor flexibilidad topológica; deben ser capaces de soportar las necesidades y exigencias de los usuarios y consolidar un programa de seguridad en las aplicaciones móviles, ya que sin ellos este tipo de sistemas se ve comprometido.

• Tarificación: Redes orientadas en un mundo comercial, genera la necesidad de dotar a los sistemas con mecanismos de análisis de tráfico, tanto por motivos de facturación como para poder dimensionar los recursos de forma apropiada.

Despliegue de IPv6 en Colombia

De acuerdo a datos reportados por LACNIC6 mediante el Portal de Transición a IPv6 de América Latina y el Caribe, Colombia es el quinto país con más direcciones IPv6 asignadas, antecedido de Argentina, Venezuela, México y Brasil.

6.2. MARCO LEGAL

RFC: La mayoría de los países latinoamericanos tienen como objetivo el contribuir a la ingeniería del Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad, entre otros, para ello existe la RFC (Request for Comments o en castellano "Petición De Comentarios"), desde sus inicios en 1969, consisten en una serie de publicaciones de grupos de trabajo en ingeniería de internet, que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos y demás. Cada RFC hace llegar sus memorandos o monografías a la IETF, siendo este el consorcio de colaboración técnica más importante en Internet, donde se evalúa por la

comunidad para su estudio y publicación para que éste sea valorado por el resto de la comunidad.

Ley 527 de 1999 Comercio Electrónico: En Colombia existe esta ley que busca un marco jurídico robusto donde se define y reglamenta el uso de firmas digitales y el acceso a los mensajes de datos dentro del comercio electrónico. Con ello, se definen las entidades de certificación, tales como las cuentas de correo, entre otras.

Estrategia de Gobierno en Línea, manuales versiones 3.1: en respuesta a lo anterior y siguiendo las recomendaciones de organizaciones internacionales, el Gobierno Colombiano a través del Ministerio de Tecnologías de la Información y las Comunicaciones contando con la participación de distintos actores y sectores, ha venido trabajando en establecer un escenario normativo que impulse adopción de este protocolo. Tales lineamientos sobre IPv6 están condensados en la Estrategia de Gobierno en Línea, manuales versiones 3.1, en donde habla sobre lo relacionado con la gestión de la tecnología al interior de las organización, hecho que transforma al estado y permite al gobierno en línea potenciar cambios de forma cómo operan los estados aprovechando los avances de la tecnología para mejorar la comunicación, interacción de la ciudadanía y prestación de mejores servicios por parte del estado.

Circular No.0002 del 6 de Julio de 2011: realiza la promoción de la adopción de IPv6 en Colombia del Ministerio de Tecnologías de la Información y las Comunicaciones; con el fin de lograr servicios eficientes teniendo en cuenta la libre adopción de tecnologías, conceptos y normas, para garantizar la libre competencia y adopción del protocolo de internet IPv6, como obligación de gestión por parte de las entidades públicas, el adecuado manejo de recursos y la generación de espacio de concentración académico masificando el uso del internet y logrando en poco tiempo la puesta en marcha del IPv6 en Colombia.

Metodología para la implementación del Modelo Integrado de Planeación y Gestión 2012: El Departamento Administrativo de la Función Pública habla de la elaboración del Protocolo de Internet IPv6, refiriéndose a que cada entidad define su plan de transición del IPv4 a IPv6 en coordinación con lo que defina MINTIC, junto con sistemas de gestión de seguridad de la información.

Ley 1341 del 30 julio 2009: La cual define los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC. Se crea la agencia nacional de espectro junto con varias disposiciones, con el objetivo de garantizar el máximo aprovechamiento de

las comunicaciones y las tecnologías de la información, donde el gobierno nacional fijara mecanismos necesarios para el desarrollo de tal principio.

Ley 1450 de 16 de Junio de 2011 (Por la cual se expide el plan nacional de desarrollo): comprende el plan nacional de desarrollo y de inversiones de la nación, junto con los mecanismos para la ejecución de ese plan, en donde se contemplan los recursos para el desarrollo tecnológico y científico de la nación, como lo son las TIC´s entre otras.

Decretos 2693 de 21 de diciembre del 2012: Por el cual se establecen los lineamientos generales de las estrategia del gobierno en línea de la República de Colombia, reglamentan parcialmente las leyes 1341 del 2009 y 1450 de 2011 y se dictan otras disposiciones.

Decreto 2482 del 3 de diciembre de 2012: Donde se plantean los lineamientos generales de la planeación y la gestión con la idea de la mejora continua en la administración pública, fortalecimiento de las herramientas de gestión y la coordinación interinstitucional para la facilitación de planes programas y proyectos.

6.3. MARCO CONCEPTUAL

Amenaza Informática: Es todo tipo de amenaza informática como cualquier acción o elemento capaz de atentar con la integridad, confiabilidad y disponibilidad de la información. Las amenazas nacen de las vulnerabilidades informáticas.

Análisis de riesgos: Es un proceso que comprende la identificación de activos de información junto con las vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia e impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del mismo.

Bit: Se refiere a la numeración en binarios, la cual se destaca dentro de los múltiples sistemas de numeración y conteo en sistemas. En el sistema de numeración decimal se usa los números hasta diez, en el binario son solo dos dígitos, los unos y ceros, el cual tiene un valor representativo como lo es falso verdadero, incluso apagado o encendido, aceptado o denegado, masculinos femenino, negro o blanco. Con cualquiera de estos valores los sistemas toman sentido y ejecutan las diferentes tareas que les imponga un ordenador.

Byte: Unidad básica de almacenamiento de información, generalmente equivalente a ocho bits, pero el tamaño del byte depende del código de caracteres o código de información en el que se defina. Los prefijos kilo, mega, giga, etc. se consideran

potencias de 1024 en lugar de potencias de 1000. Esto es así porque 1024 es la potencia de 2 (210) más cercana a 1000. Se utiliza una potencia de dos porque debido a que se trabaja es en sistema binario. Sin embargo, para el SI, los prefijos mantienen su significado usual de potencias de mil[2].

CISCO: Empresa líder a nivel mundial de soluciones de red y fabricante de dispositivos de interconexión de redes de área local (LAN) y redes de área extensa (WAN), incluidos puentes, enrutadores, conmutadores token ring, conmutadores ATM, sistemas de conmutación ATM fast packet, servidores de comunicaciones, enrutadores de software y software de gestión de enrutadores.[3]

Confidencialidad de la Información: Es la garantía de que la información será protegida de tal manera que sea imposible divulgarla sin consentimiento previo del usuario asignado. Dicha garantía se deben llevar a cabo por medio de ciertos niveles de seguridad y facultades de usuario.

Datagrama: Fragmento de paquete de datos que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento.[4]

Direcciones IP: Número que identifica a una interfaz de un dispositivo en red que utilice el protocolo IP. Es habitual que un usuario que se conecta desde su hogar tenga una dirección IP asignada por un proveedor de servicios y es cambiado cada vez que se conecta (IP dinámica).[5]

Direccionamiento IPv6: Representa una etiqueta numérica de paquete, para identificar una interfaz de red, la cual sostiene una conexión IPv6 de nodos de red, facilitando el enrutamiento de los paquetes de distintos host.

Disponibilidad de la Información: Es la característica, condición o cualidad de la información segura, la cual debe encontrase a disposición de quienes tienen derecho a ella, proceso y aplicaciones. Es el acceso a la información y a los sistemas por parte de las personas autorizadas o con privilegios en el momento que así lo requieran.

DNS (Domain Name System): Conocido como Sistema de Nombres de Dominio, contiene una nomenclatura en orden jerárquico para equipos de cómputo y bases

---

[2] Gómez Marisol (2006). Unidades de almacenamiento. [En Línea]. Tomado de http://sol-cowgirl.blogspot.com.co /2006/03/tarea-3-unidades-de-almacenamiento-un.html

[3] CISCO SYSTEMS, Inc. Definición. [En Línea]. Tomado de http://www.bnamericas.com/company-profile/es/cisco-systems-inc-cisco

[4] Datagrama. Definición. Datasoft. [En línea]. Sacado de https://datagramas.wikispaces.com/1+Definicion 2016

[5] Wikipedia. Dirección Ip. Definición [En línea]. Tomado de una red que utilice el protocolo IP. Es habitual que un usuario que se conecta desde. 2015

de datos, quienes son las encargadas de indicar la asociación entre una IP un nombre de un sitio web.

Estándar: Especificación que regula la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad[6].

Encapsulamiento: Es un mecanismo usado en los túneles de comunicación hacia Internet que permiten contener paquetes IPv6 dentro de un paquete IPv4 y enviarlo por una red IPv4 o viceversa, como ejemplo está el encapsulamiento 6-en-4 o 4-en-6 .

ICMP (Internet Control Messsage Protocol for IPv6): El protocolo de mensajes de control ICMPv6, es utilizado por los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de internet como el diagnóstico, combina funciones que anteriormente estaban contempladas por varios protocolos tales como ICMP, IGMP y ARP, adicionalmente introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso en el ICMPv4.[7]

Integridad de la Información: Se refiere a la corrección y complementación de los datos en una base de datos cuando deban ser modificados o no deban ser alterados. Es la seguridad propuesta la que garantiza la inserción de caracteres, la modificación de los mismos, e incluso la supresión de toda la información. Cuando hablamos de integridad es encontrar la información tal cual la dejamos.

Internet: Corresponde a un conjunto de redes comunicadas entre sí por protocolos TCP/IP, que enlazados gráficamente y amigable permite la búsqueda de hipertextos, garantizando que las redes físicas heterogéneas por las cuales está compuesta, puedan funcionar como una red única y mundial. Uno de sus componentes es la Word Wide Web.

IP (Protocolo de Internet): Cada computador que se conecta a Internet se identifica por medio de una dirección IP. Ésta se compone de 4 campos comprendidos entre el 0 y el 255 y separados por puntos. No es posible que existan varias computadoras con la misa dirección IP, ya que la información solicitada por algún terminal no sabría hacia dónde dirigirse.[8]

---

[6] MARTOS N. FERNANDO &NAVARRO E. JOSE L. Gestión de la función administrativa dl sergas. Estándar. definición. volumen 4. pág. 411.2006

[7] MINTIC. Valverde R. Santiago J. (2015). Seguridad y Privacidad de la Información. Guía para el Aseguramiento del Protocolo IPV6. 10. 4. TERMINOS Y DEFINICIONES Análisis de riesgos. Bogotá 2015.

[8] Servicio y protocolo. Definición. [En Línea]. Tomado de http://kassandra.udea.edu.co/lms/moodle19/mod/resource/view.php?inpopup=true&id=11095

IPsec (IP Security): Protocolo de seguridad definido por el estándar IETF desde 1999 y basado inicialmente en los RFC 2401 y 2412, pero en la tercera generación de documentos nacieron los RFC 4301 y 4309, que le dieron la abreviatura IPsec como hoy en día se conoce; ofrece integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores, actúa como un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad en un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.[9]

IPv4: Es una versión complementaria del Protocolo de Internet (IP o Internet Protocol), la cual constituye la primera versión de IP que es implementada de manera completa, nombrada IPv4, cuyo principio es ser usada como protocolo a Nivel de Red del Modelo TCP/IP dentro de la Internet. Su historia se remonta a la Fuerza de Trabajo en Ingeniería de Internet (IETF o Internet Engineering Task Force) en septiembre de 1981 donde fue nombrado inicialmente como RFC 791.[10]

Este protocolo está orientado hacia datos que se utilizan para comunicación entre redes a través de interrupciones (switches) de paquetes.

El IPV4 se caracteriza por ser un protocolo de un servicio de datagramas no fiable, proporcionando garantía de entrega de datos, pero no proporciona garantía alguna sobre la corrección de los mismos. Este protocolo puede resultar en paquetes duplicados o en desorden y todos los problemas mencionados están inmersos en el nivel superior en el modelo TCP/IP (TCP o UDP).

El IP provee una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4, 294, 967, 295 direcciones únicas. Muchas de estas direcciones están reservadas para propósitos especiales como redes privadas, Multidifusión (Multicast), etc. Debido a esto, se reduce el número de direcciones IP que realmente se pueden utilizar, es esto mismo lo que ha impulsado la creación de IPv6.

IPv6: El crecimiento de la internet ha sido exponencial, tanto los usuarios como las aplicaciones, por ende la aparición del IPv4 lanzada en el año 1981, fue la primera

[9] MINTIC. Valverde R. Santiago J. (2015). Seguridad y Privacidad de la Información. Guía para el Aseguramiento del Protocolo IPV6. 10. 4. TERMINOS Y DEFINICIONES Análisis de riesgos. Bogotá 2015.

[10] Alcance libre. IPV4. Int4oduccion. [En línea]. Tomado de http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4 2016.

versión, la cual fue un gran avance para las comunicaciones dentro de la Red y en esa época se pensaba que sería suficiente.

Posterior a ello nació el Protocolo de Internet versión 5 o IPv5, pero solo fue un protocolo experimental en pro de la mejora del flujo de voz, video y datos.

En 1992 inició la búsqueda de mecanismos para mejorar sus múltiples defectos, dando paso la siguiente generación de protocolos, IPng (Internet Protocol Next Generation) y surgió del IETF (Internet Engineering Task Force), que ha culminado con la especificación de un nuevo protocolo IP, sucesor del actual IPv4, conocido formalmente como la versión 6 del Protocolo Internet o IPv6 el cual fue lanzado en el año 1999[11]. Esta nueva versión es el futuro de las comunicaciones, ya que ayudara a nuevos dispositivos a poder estar conectados.

Protocolo de Comunicaciones: Conjunto de convenciones y reglas a procedimientos que permiten el intercambio de la información entre diferentes elementos de red.

Red: Conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios [12].

RFC (Request For Comments): Solicitud de Comentarios, se compone de una serie de publicaciones de ingenieros expertos que han hecho llegar a la IETF - Engineering Task Force, sus recomendaciones para la valoración por el resto de la comunidad. Describen aspectos técnicos del funcionamiento de Internet y otras redes de comunicaciones, protocolos, procedimientos y comentarios o ideas para clarificar o corregir aspectos técnicos que garanticen buenas prácticas de trabajo.

Redes Privadas Virtuales (VPN): (Virtual Private Network): Es una tecnología de acceso que permite una extensión segura de una red local sobre una red no controlada o pública.

Riesgo Informático: Es definido como un problema potencial que puede ocurrir dentro de la información a proteger. La probabilidad de que una amenaza se materialice, la cual al exponerse conformada por una serie de circunstancias

[11] Becker Francisco & Yañez Rodrigo (2008). Proyecto de Redes de Computadora. IPV6. Pág. 3. 2016

[12] Tanenbaum, Andrew S. (2003). Redes de computadoras (Google Books) (4ª edición). Pearson Educación. 2012

genera pérdidas. Los riesgos informáticos son considerados como atentados dentro de los sistemas de información[13].

Router: Es un dispositivo de interconexión de redes informáticas que admiten y aseguran el enrutamiento de paquetes entre redes o determinan la ruta que debe tomar el paquete de datos. Cuando un usuario accede a una URL, el navegador le consulta al servidor el nombre de dominio, para hallar la dirección IP del equipo deseado.[14]

Este router determinará así el siguiente equipo al que se le enviarán los datos para poder escoger la mejor ruta posible. Para hacerlo, el router cuenta con tablas de enrutamiento actualizadas, que son verdaderos mapas de los itinerarios a seguir en busca de la dirección de destino. Existen numerosos protocolos dedicados a esta tarea.

RPKI (Resource Public Key Infraestructure): Es una certificación de recursos u organismo especializado, cuyo objetivo es la emisión de material criptográfico que permita a sus miembros, asegurar digitalmente sus derechos dentro de las infraestructuras IPv4 e IPv6.

SNMP (Simple Network Management Protocol): Es un protocolo Simple de Administración de Red de capa de aplicación, que concede el intercambio de datos y administración entre dispositivos de red, siendo un componente de la suite de protocolos de internet como se define en la IETF.[15]

TCP: El Protocolo de Control de Transmisión es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, permite administrar los datos y cuando se proporcionan los datos al protocolo IP, son agrupados en datagramas IP. TCP es un protocolo orientado a conexión, permitiendo comunicaciones entre dos o varias máquinas, controlando su estado de transmisión[16].

Vulnerabilidad Informática: Consiste en la debilidad precisa de cualquier tipo dentro de algún sistema, aplicación o cualquier aplicativo de seguridad informática ya sea dentro del diseño e implementación.

---

[13] HISPAVISTA. Galeon.com. Riesgo informático. [En Línea]. Tomado de http://audisistemas2009.galeon.com/productos2229079.html 2016.

[14] CCM. ROUTER. Definición. [En Línea]. Tomado de http://es.ccm.net/contents/299-equipos-de-red-router. 2016

[15] LACNIC. Información general. Quienes somos. Disponible en http://portalipv6.lacnic.net/que-es/. 02 marzo 2016.

[16] CCM. Protocolo TCP. Características. Tomado de http://es.ccm.net/contents/281-protocolo-tcp. 2016

7. MARCO METODOLÓGICO

7.1. METODOLOGÍA DE LA INVESTIGACIÓN

La presente monografía, consta de una construcción académica e intelectual apoyada en **la investigación exploratoria**, ya que es considerada como el primer acercamiento científico a un problema estipulado. Su finalidad describe, analiza y genera una teoría con base a datos objetivos y verificables, partiendo de una "Teoría Fundada", permitiendo la construcción de conclusiones, análisis y pruebas, que ayudan a contextualizar el manejo de un nuevo protocolo. Se utiliza este tipo de investigación cuando aún no ha sido abordado o no ha sido suficientemente estudiado el problema en cuestión y las condiciones existentes no son aún determinantes, lo anterior aplica para nuestro caso ya que la problemática en mención aún no ha sido estudiada completamente, ni tampoco existe una guía que sirva de ayuda para proteger y apoyar a los administradores de redes ante nuevas amenazas. Para el caso específico de la elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO el **enfoque de investigación es cuantitativo,** ya que se pretende hacer la identificación, análisis y mitigación de las vulnerabilidades, amenazas y riesgos en cuanto a la confidencialidad, integridad y disponibilidad de la información en el nuevo protocolo. Por lo tanto, se realiza **una investigación exploratoria con enfoque cuantitativo**, ya que no existen exploraciones en seguridad informática descritas por medio de una guía abierta de fácil acceso e interpretación dentro de los archivos de la UNAD, internet o libros, dirigido a diferentes tipos de público y administradores de redes con capacidad IPv6.

La Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI de la UNAD ha definido líneas de investigación por cada cadena de formación, de acuerdo al tema de estudio de este proyecto se enmarca dentro de la siguiente línea:
CADENA DE FORMACIÓN DE SISTEMAS – Línea 1. Gestión de Sistemas.

7.2. FUENTES DE INFORMACIÓN Y ANÁLISIS DE DATOS

A continuación se menciona las fuentes necesarias para la creación del presente proyecto:

- **Fuentes Primarias**

Para la elaboración de la guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento

dinámico en equipos con plataforma CISCO se utilizaron medios como la entrevista, envío de correos electrónicos a grupos de especialistas vía internet, visita a las bibliotecas de Bogotá y recopilación de información en fuentes de internet. La entrevistas que se llevaron a cabo fue con el Ingeniero y Especialista Alejandro Corletti en España y Mr. Marc Musgrove especialista en redes y IPv6 CISCO en Estados Unidos vía correo electrónicos y Skype. La entrevista solo consta de una única pregunta donde se solicita registros o pruebas sobre IPv6, los cuales pudieran complementar la guía, junto con cualquier aspecto significativo en seguridad aplicado a la protección de datos o mitigación de nuevos riesgo en el actual protocolo. Se realizó solicitud de información a empresas como la empresa CISCO, Optical Networks, Telefónica Perú, LACNIC entre otras y especialista que hayan trabajado en aspectos de seguridad en IPv6.

- **Fuentes Secundarias**

Las fuentes secundarias usadas para el desarrollo del proyecto, comprenden de una revisión documental en la biblioteca más cercana (“Las ferias “y “Virgilio Barco” en Bogotá D.C), consultas a páginas web que proporcionan información al marco teórico del proyecto, normas, estándares y metodologías contemporáneas con la seguridad informática.

Criterios de Exclusión

1. Fuentes subjetivas o no avaladas como investigaciones científicas o comprobables.
2. Páginas web con poca credibilidad.
3. Menciones de seguridad baja o edición ilegal.
4. Información que exceda los tres años de publicación o que se considere como técnica ya obsoleta.

Criterios de Inclusión

1. Fuentes que pertenezca a empresas reconocidas.
2. Fuentes que hayan o estén en proceso de implementación hacia IPv6.
3. Personal profesional que haya trabajado o se encuentre trabajando en sistemas de seguridad informática sobre IPv6.

Análisis de Datos

Posterior la recopilación de datos a través de las respuestas a correos, consultas documentales, visita de campo y búsqueda en páginas web, se da comienzo a la

fase de clasificación y comprobación de los datos relacionados con IPv6 o IPv4, destacando su objetivo de estudio y veracidad.

Se relaciona lo siguiente para el análisis de datos:

- Editar y Validar: En este proceso se verificaron la información proporcionada por las diferentes entidades consultadas y especialistas, la meta de validar es exclusivamente detectar las nuevas técnicas para combatir vulnerabilidades en IPv6 o la generación de consejos útiles para mitigar diferentes tipos de riesgo presentes en la migración o en proceso de aplicación IPv6.
- Codificación: No se efectuó ningún tipo de codificación de la información, sin embargo se traducen múltiples textos a español y se verifican en busca de posibles errores de sintaxis o redacción, tornado la guía a un lenguaje más amigable y no tan técnico para ser interpretado por todo el público.
- Organizar información: Una vez validadas, editadas e interpretada la información, se procede a ser organizada en capítulos, los cuales sean ligados en orden lógico para su consulta, desarrollando siete capítulos numerados para su fácil interpretación y búsqueda.
- Análisis estadísticos: Las estadísticas consultadas, son expresadas junto con sus resultados de manera clara y breve ya que son datos generales mundiales y no representan el objetivo general de la creación de la guía.

Técnicas de análisis

Se utilizaron las siguientes técnicas para el análisis de la información:

- Análisis de componentes y capacidades que usa IPv6.
- Instrumentos existentes en la configuración y mantenimiento seguro de IPv6.
- Verificación de fuentes consultadas encontrando puntos homogéneos en las descripciones
- Numeración de vulnerabilidades. Las vulnerabilidades se identifican y se clasifican como general o específica, con el objeto de determinar su impacto.
- Representación gráfica de los resultados: Para las representaciones graficas de los datos y presentar los resultados se utilizaron las barras.

7.2.1 POBLACIÓN Y MUESTRA

Población: Egresados de la UNAD en seguridad Informática y empresas populares con migración o conocimiento en IPv6.

Muestra: Para el desarrollo del proyecto se tomó como muestra aproximadamente el 10% de personas egresadas de la especialización de seguridad informática, dos especialistas internacionales y cuatro empresas populares con conocimiento en IPv6.

7.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Con el fin de hacer efectiva la recopilación de la información y elaborar la guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO, se llevaron a cabo las siguientes técnicas e instrumentos:

Técnica: análisis de información y documentos en orden cronológico, estadísticas, entrevistas, involucrando los procesos de seguridad informática en el protocolo IPv6 de diferentes empresas reconocidas con énfasis en CISCO y LACNIC.

Instrumentos: para el desarrollo del presente proyecto se utilizaron las siguientes herramientas:

Entrevista: se realizó entrevista vía Skype a diferentes especialistas, quienes tienen experiencia tanto en la migración segura de IPv6 como en técnicas de mitigación de riesgo en el nuevo protocolo.

Visita de campo: Visita programada a la biblioteca pública “Las ferias”, “Virgilio Barco” en Bogotá D.C

Revisión documental: se hace revisión documental de veintiséis (26) RFC de Seguridad en IPv6, página principal de CISCO, entre otros documentos relacionados en las referencias bibliográficas.

Con estos tres instrumentos se recopila la información necesaria para la creación de una guía rápida que determine múltiples vulnerabilidades en IPv6, análisis y tratamiento de mitigación del riesgo, junto con múltiples recomendaciones útiles para los administradores de red.

7.4. DISEÑO METODOLÓGICO

En la elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO, es necesario realizar cuatro fases, pasando por la recopilación de información, diseño, análisis y construcción, tomando los criterios de inclusión y exclusión aplicado a todas las fuentes de información disponibles, con la metodología del ciclo PHVA (Planear, Hacer, Verificar y Actuar).

Este tipo de metodología es ejecutado de acuerdo con lo planteado al cronograma de actividades del anteproyecto y primero se establecieron los recursos e identificación de los procesos necesarios para alcanzar los resultados esperados, llevando al detalle la selección de la información necesaria bajo los criterios de inclusión y exclusión anteriormente mencionados así:

7.4.1 Planear

Se definió en el ciclo PHVA en esta fase de planeación, el alcance, los recursos, fuentes primarias y secundarias, las cuales interactúan como generador inicial de conocimiento a recopilar, refinamiento de los objetivos y la asignación de la línea de acción para cumplir con el primer objetivo trazado, el cual consiste en el análisis, planificación y recopilación de información de múltiples fuentes sobre las principales temáticas relacionadas con IPV6: contexto, origen, vulnerabilidad y amenazas, identificando el contexto tecnológico y organizacional.

A continuación, se describen las siguientes actividades realizadas en esta fase:

- Se identificará la documentación relacionada con el proyecto de grado, para esto se escogieron las bibliotecas de Bogotá (“Las ferias”, “Virgilio Barco Bogotá).
- Se enviará correos a las principales empresas en materia de tecnología como CISCO Latinoamérica, LACNIC, Telefónica Perú, Optical Networks, entre otros, para consultar sobre el nuevo protocolo.
- Se agendará reuniones con los principales especialistas como lo son el especialista Alejandro Corletti en España y Mr. Marc Musgrove especialista en redes y IPv6 CISCO en Estados Unidos.
- Se definirá el modo de recopilación de la información en la web, donde se discriminan por empresas que trabajan actualmente con IPv6 o que se encuentren migrando a él.

- Búsqueda de personal idóneo en la materia, incluyendo egresados de la UNAD, para colaborar como asesores, con el objeto de fortalecer la información y fomentar la doctrina de seguridad en este protocolo.
- Trazar un plan de trabajo para clasificar en cuatro ramas la información recopilada, así: información general sobre IPv6 (características, especificación, tipicidad), información de seguridad en plataforma CISCO sobre IPv6, información de ayuda para solventar problemas con IPv6 y análisis sobre IPv6 en seguridad proporcionado por las diferentes empresas o especialistas.

7.4.2 Hacer

Se desarrollan las siguientes actividades usando el ciclo PHVA que en el Hacer permitieron cumplir con el objetivo de identificar y promover las habilidades necesarias para el funcionamiento de los componentes que usa IPv6, junto con los instrumentos que existen para la configuración y el mantenimiento seguro en una red. Por lo cual, se realizaron las siguientes actividades:

- Reclasificación y validación de la información almacenada, con el objeto de discriminar la veracidad de las fuentes, su tiempo de expedición, aspectos concluyentes concretos, todo esto dentro de los paramentos de inclusión y exclusión anteriormente mencionados.
- Revisión detallada de cada tema, para evitar duplicidad en la información, generando extractos para citas bibliográficas importantes y eliminación de información no específica o poco detallada.
- Identificación de componentes y capacidades que usa IPv6, junto con los instrumentos que existen para la configuración y mantenimiento seguro de IPv6.
- Análisis de las diferentes vulnerabilidades, descartando vulnerabilidades genérales ya sean intencionales y no intencionales, las cuales no apliquen a IPv6 específicamente, como por ejemplo surfing shoulder o ingeniería social entre otros, ya que son aspectos que se aplican a cualquier sistema o protocolo y se pretende concentrar la guía únicamente en IPv6.
- Creación de consejos útiles, conclusiones y recomendaciones tanto como en la implementación de IPv6 de manera segura, como en la sustentación de pruebas de penetración, usando imágenes y fases procedimentales para

visualizar múltiples verificaciones de manera más demostrativa junto con su mitigación del riesgo.

Resultados

No se encontraron registros de investigaciones o proyectos similares.

Existe gran dificultad en la recopilación de la información para la creación de la guía, como material poco actualizado o no verificado, material en otros idiomas e incluso negación de las empresas a participar en la creación de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO, evidenciado en las respuestas de las empresas el deseo por conservar sus derechos pecuniarios o no compartir información de manera académica.

En la visita programada en las bibliotecas más cercanas a la ciudad de Bogotá se encontrando tan solo cuatro (4) libros con información apropiada,

De las solicitudes para entrevistas vía internet con cuatro (4) especialista internacionales, dos (02) de ellos accedieron.

De los veinte (20) correos a diferentes alumnos egresados de la UNAD como especialistas en seguridad, solo dos (02) participaron en el estudio. La mayoría de los especialistas y egresados no contestaron a las citaciones o respondieron los correos

Se realizó búsqueda de información en alrededor de ochenta (80) páginas web y alrededor de treinta (30) páginas web quedaron descartadas por no cumplir con los criterios de inclusión anteriormente mencionados.

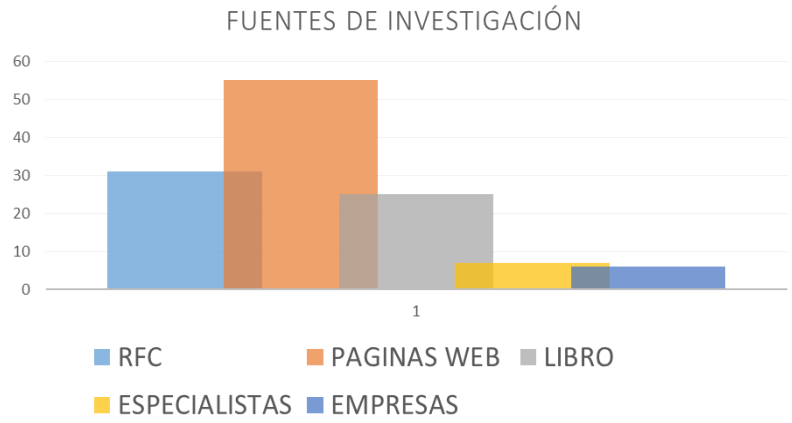
Figura. 1 Fuentes de Investigación 2016

Fuente: Autor

La principal fuente de información de este proyecto está disponible en internet, ya que en Colombia no se ha hecho énfasis en la implementación de IPv6 y menos en el análisis de sus múltiples vulnerabilidades, dando un toque único a este trabajo.

Los resultados a fecha diciembre del 2015 se había recolectado el 70% de lo propuesto, con la selección de la información y a fecha marzo del 2016 hubo un incremento en la información recolectada por páginas web del 15%, descartando el 30% nuevamente, debido a que no cumple con los términos de inclusión de la información, los especialistas y empresas solo incrementan en un punto.

Figura. 2 Fuentes de Investigación 2017



Fuente: Autor

Se crea el primer borrador de la guía con todo el material encontrado bajo parámetros de exclusión e inclusión.

Se organiza la información de manera más acorde, junto con el proceso de validación de manera más ágil.

Se investiga sobre los diferentes tipos de guía para la construcción del presente proyecto descartando sus diferentes tipos, propósitos y formas de construcción. Los tipos de guías responden a objetivos distintos, tales como las guías de Motivación, Aprendizaje, Comprobación, Síntesis, Aplicación, Estudio, Lectura, Guías de Observación: de visita, del espectador, Refuerzo, Nivelación, Anticipación, Guías de Remplazo y demás.

Por lo tanto, se escoge la guía de síntesis y aplicación, para la comprensión y contextualización de la información plasmada.

Estructura de la Guía: pretende con la guía brindar instrucciones claras, con información concisa y bien destacada, que pueda tomar plena conciencia de los términos reactivos, diversidad de información y aplicación del conocimiento.

7.4.3 Verificar

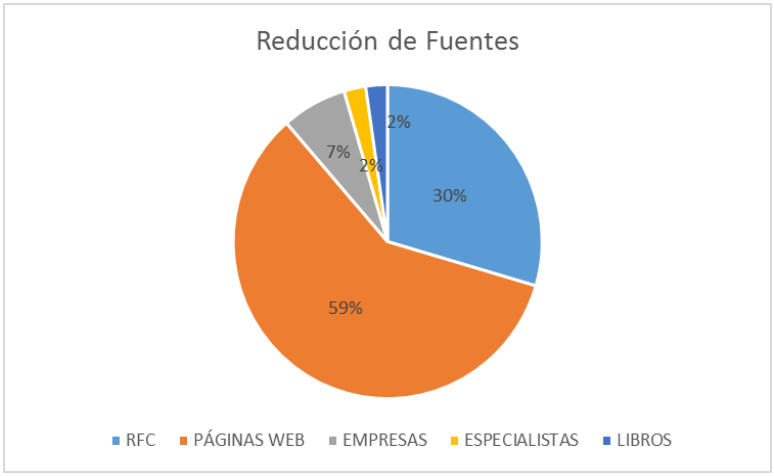
Se realiza el cumplimiento del objetivo tres en esta fase de Verificar del ciclo PHVA, en el que se efectúa el diseño práctico de la guía para la presentación de las investigaciones. Por ende se realizan las siguientes actividades:

- Verificación y trazabilidad de la información, evidencias, hallazgos y porcentajes de cumplimiento.
- Validación de los conocimientos aplicados y previos del anterior protocolo, con el objeto de medir si aquella solución propuesta para cada vulnerabilidad permite contrarrestar el problema detectado.
- Realimentación del diseño práctico de la guía junto con la investigación total, con el objeto de verificar que salió mal, que se puede mejorar, como se analiza e indaga sobre IPv6 y como el análisis puede ser alineado con temáticas de fácil interpretación, manejo y comprensión dirigida para todo el público.

Resultado

Se analiza la guía en busca de falencias para su fácil interpretación, dando como resultado una guía construida por capítulos, ya que de esta manera es más amigable su consulta y corroboración.

Figura. 3 Porcentaje de Información Excluida



Fuente: Autor

Con la exclusión de información no apta según criterios, se procede al análisis de información acorde y publicación en la guía, retomando el siguiente análisis:

Se evidencia disminución de la información encontrada en páginas web, convirtiéndose en un proceso lento para en análisis de la información por encontrarse en otros idiomas. Dos empresas y dos especialistas objetan no proporcionar más información al respecto por ser un tema muy contemporáneo, se continúa con la misma cantidad de RFC revisadas.

7.4.4 Actuar

Para la fase de actuar, se analizan los hallazgos brindados por la fase anterior, desarrollando las correcciones de material e información que no correspondieron a las necesidades de la guía, de esta manera en la fase de actuar se cumple con el objetivo de crear una guía abierta de seguridad actualizada con las recomendaciones que se alleguen por los usuarios de plataforma CISCO. En esta fase del ciclo PHVA se realizan las siguientes actividades:

- Se cambia el tipo de presentación de la guía a modo de aprendizaje y lectura y no como de síntesis y aplicación como se había planteado, ya que esta contienen parámetros técnicos que no son entendible para todo público, el cual es uno de los objetivos trazados.
- Se elimina el capítulo de despliegue de IPv6 para el desarrollo socio económico en América Latina y el caribe, ya que si bien contiene información sobre migración de empresas a IPv6, no se apropia específicamente del tema de seguridad al cual se le está apuntando y se crea otra sección en la guía que habla sobre consejos para implementar IPv6 de forma segura el cual si cumple con lo trazado.
- Se modifica todo el documento general la guía en seguridad IPv6, para corregir errores de redacción, traducción, ortografía y demás, plasmando todas las ideas de manera más organizada y por secciones, se crean las recomendaciones de gestión del riesgo en seguridad informática de acuerdo a lo investigado, junto con observaciones y prácticos consejos, como punto de partida para su apropiación y cautela.

Resultado

Se corrigen imágenes adjuntadas por propias, se actualizan las tablas de contenido, se corrige la guía en redacción nuevamente, se adaptan los anexos y se anexa bibliografía consultada.

7.5. ÁREA DE CONOCIMIENTO

Gestión de seguridad informática.

7.6. ÁREA ESPECÍFICA

Gestión de riesgo informático.

7.7. RECURSOS DISPONIBLES

Los recursos necesarios para la elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet ipv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO son los siguientes:

7.7.1 RECURSO HUMANO

Un investigador en la rama de telecomunicaciones, el cual realiza el diseño practico de la guía, con fácil acceso y consulta, de manera clara y concisa, lo cual de acuerdo a su contenido y fuentes bibliográficas, se podrá compartir en la biblioteca de la UNAD, pretendiendo ser una guía sin ánimo de lucro.

7.7.2 RECURSOS FÍSICOS

Se requiere de computador con acceso a internet, impresora láser, con la cual se pretende llevar a cabo la propuesta de monografía bajo el nombre “Elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet Ipv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO”, se deberá hacer la recolección de información en redes como el internet, magazines y biblioteca local.

7.7.3 RECURSOS TÉCNICOS

Se propone acceder a redes a bases de datos con la CISCO siempre y cuando respondan a las diferentes peticiones particulares vía internet, lo cual puede ayudar a encontrar análisis previos a este, como complemento y anexo bibliográfico.

Posteriormente a la selección de las fuentes bibliográficas más idóneas en la materia, junto con la recolección de la información de alto grado de confiabilidad, se pasa a clasificar los datos recolectados en varias categorías, organizándolos y

sometiéndolos a un análisis bibliográfico y de credenciales, con el objeto de publicar un producto con información clara y específica para la identificación de problemas con el protocolo Ipv6, generando un análisis en la solución de problemas captados actualmente; todo esto con el objeto de crear un medio de fácil acceso, sirviendo como un soporte de alto contenido productivo, académico e intelectual.

No obstante, para el adecuado proceso del proyecto se deben contar con un presupuesto económico y monetario que facilite la elaboración de contenido textual del mismo. Por ende, dicho presupuesto se discrimina de la siguiente forma:

Tabla 1 Costos de Implementación

ÍTEM REQUERIDO	CANTIDAD	COSTO UNITARIO ÍTEM	COSTO TOTAL ÍTEM
Equipos de Cómputo	2	750.000	1.500.000
Provisión de Servicio de Internet	6 Meses	45.000	270.000
Impresora HP Multifuncional 1510	1	240.000	240.000
Papel (Unidades en resmas)	5	8000	40.000
SUBTOTAL		1.950.000	
Gastos de Adicionales	20%	1	390.000
TOTAL			2´440.000

Fuente: Autor

8. IMPACTO Y RESULTADOS

Esta monografía de IPv6 descrita en forma de guía rápida, se desenvuelve como soporte para la interconexión de sistemas operativos, describe las diferentes dificultades y vulnerabilidades encontradas por las fuentes de consulta y promueve esta información útil para la prevención de ataques y minimización de los riesgos de la información sobre el IPv6. A continuación, se menciona los siguientes resultados:

Se requieren guías para la gestión de vulnerabilidad nuevas dadas en IPv6 para orientar en el manejo, revisión, identificación y gestión de riesgos informáticos, dentro de los aspectos de implantación y funcionamiento IPv6.

La creación de la guía nace sobre la falencia de información sobre el tema en Colombia, apoyando a administradores y estudiantes en la mitigación y análisis de riesgos.

Desde los administradores de redes, hasta los alumnos de ingenierías, en especial de sistemas y telecomunicaciones es necesario socializar la información de la guía para ampliar sus conocimientos y en la aplicación de la misma, minimizar la presencia de riesgos, atendiendo a sus criterios, los cuales enriquecerán el contenido de la guía.

Se pudo evidenciar la necesidad de seguir actualizando la guía, ya que este protocolo aún se encuentra mutando y generando más vacíos en cuanto a sus posibles vulnerabilidades, por ende la mitigación del riesgo debe ser evolutiva del mismo modo y tan solo personal comprometido con el manejo de este tipo de protocolo pueden seguirse aportando ideas, dentro de un plan de actualización y mejora continuada.

Se evidencia la necesidad de fortalecer la guía con material general en todas las plataformas, aplicaciones móviles y pruebas sobre las mismas, para la creación de una guía general fortalecida y actualizada.

Se debe generar un procedimiento para estandarización de guías didácticas en el protocolo IPv6, ya que cada entidad cuenta con diferentes técnicas y formatos para las guías.

La guía cuenta con información clara y amigable, de fácil consulta, con imágenes actualizadas para la interpretación objetiva de cada procedimiento, junto con las fuentes referenciadas para validación de la misma.

9. DIVULGACIÓN

La “GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPV6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO”, se adjuntará al material dado por la biblioteca virtual de la UNAD para consulta y actualización, como material pedagógico y de fácil acceso a los estudiantes de especialización en Seguridad en Informática y de ser posible, agregado al módulo de introducción de Seguridad Informática de acuerdo a solicitud de la Universidad UNAD.

BIBLIOGRAFÍA

BECKER FRANCISCO & YAÑEZ RODRIGO (2008). Proyecto de Redes de Computadora. Universidad Técnica Federico Santa María. IPV6. Pág. 3. 10 enero 2016.

BURGOS L. (2013). ¿Preparado para presentar tu proyecto de seguridad informática ante gerencia? [En línea]. Recuperado el 21 de agosto de 2015 de: http://liacolombia.com/2011/02/%C2%BFpreparado-para-presentar-tu-proyecto-de-seguridad-informatica-ante-gerencia/. 4 agosto 2015.

CISCO SYSTEMS, Inc. Definición. [En Línea]. Tomado de http://www.bnamericas.com/company-profile/es/cisco-systems-inc-cisco. 5 enero 2016

CARVAJAL, A. Introducción a Las Técnicas de Ataque e Investigación Forense, un enfoque pragmático. [En línea]. Tomado de http://www.acis.org.co /fileadmin/Artículos/TecnicasAtaqueComputacionForense.pdf. 12 noviembre 2015-

CCM. ROUTER. Definición. [En Línea]. Tomado de http://es.ccm.net/contents/299-equipos-de-red-router. 20 enero 2016

CCM. Protocolo TCP. Características. Tomado de http://es.ccm.net/contents/281-protocolo-tcp. 20 enero 2016.

DATAGRAMA. Definición. [En línea].Tomado de http://enciclopedia_universal. esacademic.com /74779/Datagrama día 26 agosto 2015.

DE LA CRUZ CAMARGO L. IPv6 para los colombianos. [En línea]. Tomado de http://portal.uexternado.edu.co/pdf/derechoDeLasTelecomunicaciones/IPV6-para-los-colombianos.pdf. 8 agosto 2015.

ESCENARIO NORMATIVO PARA LA ADOPCIÓN DE IPV6 EN COLOMBIA. [En línea]. Tomado de http://www.ipv6colombia.com

/index.php/component /content/article/12-noticias/16-escenario-normativo-para- la-adopcion-de-ipv6-en-colombia. 26 agosto 2015.

GÓMEZ MARISOL (2006). Unidades de almacenamiento. [En Línea]. Tomado de http://sol-cowgirl.blogspot.com.co /2006/03/tarea-3-unidades-de-almacenamiento-un.html

HISPAVISTA. Galeon.com. Riesgo informático. [En Línea]. Tomado de http://audisistemas2009.galeon.com/ productos2229079.html 2016.

HUERTA, A. (2002) Seguridad en Unix y Redes. Recuperado el 21 de Agosto de 2015. [En línea]. Sacado de www.rediris.es/cert/doc/unixsec/unixsec.pdf.24 Noviembre 2015.

IPV6. Definición. Internet Protocol versión 6 (IPv6), Características. [En línea]. Recuperado el 20 de Agosto 2015. Sacado de https://es.wikipedia.org/wiki/IPv6

MARTOS N. FERNANDO &NAVARRO E. JOSE L. Gestión de la función administrativa dl sergas. Estándar. Definición. Volumen 4. pág. 411 .2006.

PÉRISSÉ, M. (2001). Proyecto Informático, Una Metodología Simplificada. Recuperado el 21 de Agosto de 2015 [En línea]. Tomado de http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/proyectoinformatico/libro/. 10 enero 2016.

PROTOCOLO DE INTERNET (IP). Definición. [En línea]. Tomado de http://www.monografias.com /trabajos29/modelo-osi/modelo- osi.shtml. 10 enero 2016.

ROUTER. Definición. [En línea]. Tomado de http://es.kioskea.net/contents/299-equipos-de-red-router. 10 enero 2016.

RIOS JULIO. (2013). Seguridad Informática. Importancia de la seguridad Informática. Recuperado el 21 de Agosto de 2015. [En línea]. Sacado de

http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml. 8 agosto 2015.

SERVICIO Y PROTOCOLO. Definición. [En Línea]. Tomado de http://kassandra. udea.edu.co/lms/moodle19/mod/resource /view.php?inpopup=true&id=11095. 8 agosto 2015.

SENYA, Leonardo (2014). Concepto básicos seguridad Informática. Recuperado el 20 de Agosto de 2015. [En línea]. Sacado de https://seguridadinformaticaufps .wikispaces.com/Conceptos+Basicos+Seguridad+Informatica. 8 agosto 2015.

TANENBAUM, ANDREW S. (2003). Redes de computadoras (Google Books) (4ª edición). Pearson Educación. 2012. 10 enero 2016.

ANEXOS

ANEXO A

GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPv6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO.

GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPv6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO

ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA

PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPv6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO

Soñábamos con el protocolo IPv6, ya llego!

Siendo el nivel más actual de protocolo de Internet (IP), desarrollándose como soporte e interconexión de sistemas operativos.

Hoy cuenta con esta guía rápida de consulta para manejo, revisión y gestión de riesgos informáticos en su parte de implantación y funcionamiento, promoviendo la información útil para la prevención de ataques y minimización del riesgo informático.

El tema de seguridad debe ser profundamente analizado dada la alta posibilidad de que se presenten incuestionables debilidades que no son consideradas por los administradores de redes como tal dentro de este nuevo protocolo.

HISTORIAL

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	20/05/16	Borrador
1.1	28/01/17	Edición 1

AGRADECIMIENTOS

A DIOS por su guía y esperanza. Al Ingeniero Salomón González García por su apoyo y guía en el proceso de construcción de ideas. A la Señora Coronel Gutiérrez Nilssen por su dedicación y apoyo ante las tareas propuestas y espacios laborales para el desarrollo del proceso educativos.

Un agradecimiento especial al personal de tutores de la Universidad nacional Abierta y a Distancia, en especial a la Líder de la Facultad de Ciencias Básicas e Ingenierías, Ingeniera Angélica Calderón por su ejemplo y fortaleza, cuya premisa es la de no darse por vencido, Janeth tampoco te olvido!.

Un abrazo y gratitud eterna a mi familia y amigos, que hicieron posible mi crecimiento como profesional y que cada día dieron un aporte invaluable para que este producto fuera posible. Freidy siempre estarás conmigo.

Grossy Sabogal

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

En IPv4 fue lanzado en el año de 1981 como la primera versión del protocolo de Internet implementado de manera extensa, facilitando las comunicaciones entre redes y donde se daba por hecho que la necesidad de más direcciones IP había sido finiquitada. Posteriormente con la migración hacia el IPv5 se pretendía satisfacer otro tipo de necesidad del internet y como protocolo experimental fue orientado únicamente a mejorar el procesamiento de flujo de voz, audio y video.

Posteriormente en el año de 1992, en busca de mejorar y minimizar las fallas de red descubiertas, el IETF (Internet Engineering Task Force), presenta la siguiente generación de Protocolo de Internet o IPng (sucesor del IPv4), conocido como la versión 6 del Protocolo de Internet o IPv6, lanzado oficialmente en 1999 y siendo catalogado como la solución a la interconexión entre dispositivos y el futuro de las comunicaciones.

Debido a las deficiencias en los aspectos administrativos y de seguridad sobre IPv6, a los cuales se encuentran migrando las grandes empresas, ubicándolas por debajo de los estándares necesarios de la globalización y con carencias en la prestación de servicios avanzados que apuntan en el horizonte de la informática; se hace necesaria en la actualidad, toda esta infraestructura de transmisión de alta velocidad, que esté a la vanguardia y que cumpla con las expectativas. Por ende, es grato que se pueda proporcionar una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6, sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO, como respuesta a múltiples interrogantes relacionados con diferentes temas de seguridad y como consulta rápida para aplicativos CISCO; siendo un gran documento pedagógico de consulta amigable, para todo amante de la información de vanguardia.

OBJETIVO GENERAL

Generar una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO despejando dudas a múltiples interrogantes, en cuanto a los diferentes estándares de seguridad y consulta rápida para aplicativos CISCO y un buen artículo pedagógico de consulta ante el personal amante de la información de vanguardia como lo es el nuevo del protocolo IPv6 a implementar en América latina.

DEFINICIONES

Análisis de riesgos: Es un procedimiento que abarca la identificación de activos de información al igual que las vulnerabilidades y/o amenazas a las cuales puede estar expuesta, donde su probabilidad de ocurrencia e impacto se determinan con el ánimo de analizar controles adecuados para minimizar, evitar o transferir la aparición de los mismos.

Confidencialidad: característica de la información para ser accesible únicamente a aquellas personas autorizadas.

DHCPv6 (Dynamic Host Configuration Protocol): Es el Protocolo cliente-servidor, contemplado por la RFC 3315 de la IEFT, el cual proporciona y administra la configuración administrada de dispositivos en redes IPv6.

Direccionamiento IPv6: Es una etiqueta numérica del paquete la cual identifica una interfaz de red, que provee una conexión entre nodos de una red sobre IPv6, esto facilita el enrutamiento de los paquetes de distintos host.[17]

Disponibilidad: característica de la información y servicios, para ser accesibles y utilizables cuando se les requiera.

DNS (Domain Name System): Sistema de Nombres de Dominio que contiene un sistema de nomenclatura jerárquica para equipos de computación, los DNS contienen una base de datos que tienen la función de indicar la IP que está asociada a un nombre de un sitio web (resolución de nombres).[18]

Encapsulamiento: Es un mecanismo usado en los túneles de comunicación hacia Internet que permiten contener paquetes IPv6 dentro de un paquete IPv4 y enviarlo por una red IPv4 o viceversa, ejemplos de esto, es el encapsulamiento 6-en-4 o 4-en-6 .[19]

ICMP (Internet Control Messsage Protocol for IPv6): El protocolo de mensajes de control ICMPv6, es utilizado por los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de internet como el diagnóstico; combina funciones que anteriormente estaban contempladas por varios protocolos tales como ICMP, IGMP y ARP,

[17] MINTIC. Seguridad y Privacidad de la Información. Guía No. 19. Definición Direccionamiento IP. Tomado de http://www.mintic.gov.co/gestionti/615/articles-5482_Guia22_Aseguramiento_IPV6.pdf. 14 Enero 2016
[18] Ibíd., P. 7
[19] Ibíd., P. 7

adicionalmente introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso en el ICMPv4.[20]

IPv6: es la nueva versión del Protocolo de Internet (Internet Protocol -IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90s con el IETF (Internet Engineering Task Force). Al día de hoy el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente maduro para soportar la operación de Internet en substitución de IPv4.[21]

IPsec (IP Security): Protocolo de seguridad definido por el estándar IETF desde 1999 y basado inicialmente en los RFC 2401 y 2412, pero en la tercera generación de documentos nacieron los RFC 4301 y 4309, que le dieron la abreviatura IPsec como hoy en día se conoce; ofrece integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores, actúa como un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad e integridad, es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.[22]

Integridad: características de la información y sus métodos de procesamiento para ser exactos y completos, con el objeto de protegerle por su alto valor para la entidad protectora.

Protocolo de Comunicaciones: Conjunto de convenciones y reglas a procedimientos que permiten el intercambio de la información entre diferentes elementos de red.[23]

RFC (Request For Comments): Solicitud de Comentarios, se compone de una serie de publicaciones de ingenieros expertos que han hecho llegar a la IETF - Engineering Task Force, sus recomendaciones para la valoración por el resto de la comunidad. Describen aspectos técnicos del funcionamiento de Internet y otras redes de comunicaciones, protocolos, procedimientos y comentarios o ideas para clarificar o corregir aspectos técnicos que garanticen buenas prácticas de trabajo.[24]

[20] Ibíd., P. 7
[21] Ibíd., P. 7
[22] Ibíd., P. 7
[23] Ibíd., P. 7
[24] Ibíd., P. 7

Redes Privadas Virtuales (VPN): Es una tecnología de acceso que facilita una extensión segura de la red local, sobre una red pública o no controlada como Internet.

RPKI (Resource Public Key Infraestructure): Es una certificación de recursos u organismos especializados, con el objetivo de emitir material criptográfico que permita a sus miembros, asegurar digitalmente sus derechos dentro de las infraestructuras IPv4 e IPv6 [25].

SNMP (Simple Network Management Protocol): en ella se concede el intercambio de datos y administración entre dispositivos de red, siendo un componente de la suite de protocolos de internet como se define en la IETF[26].

TCP: El Protocolo de Control de Transmisión es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, permite administrar los datos y cuando se proporcionan los datos al protocolo IP, son agrupados en datagramas IP. TCP es un protocolo orientado a conexión, permitiendo comunicaciones entre dos o varias máquinas, que puedan controlar su estado de transmisión.[27]

[25] Ibíd., P. 7

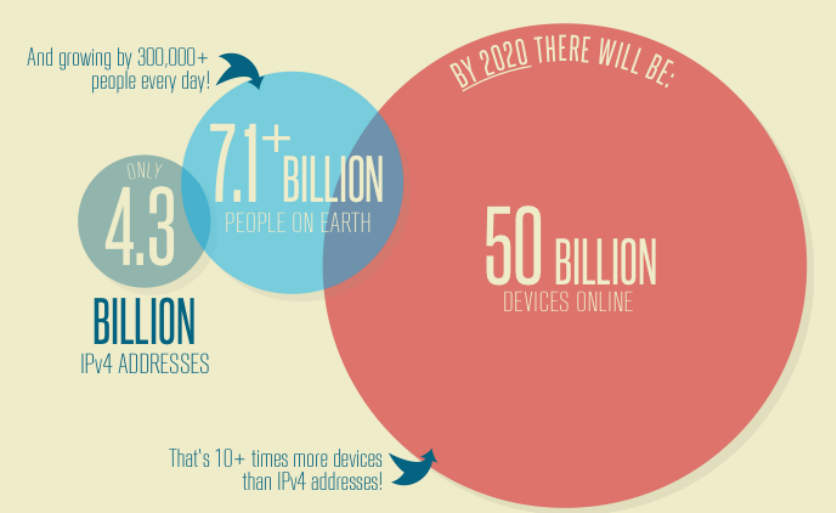
[26] MINTIC. Seguridad y Privacidad de la Información. Guía No. 19. Definición Direccionamiento IP, Disponibilidad, DNS, Encapsulamiento, ICMP, IPv6, IPsec, Integridad, Protocolo de comunicaciones, RFC, VPN, RPKI, SNMP. Tomado de http://www.mintic.gov.co/gestionti/615/articles-5482_Guia22_Aseguramiento_IPV6.pdf. 14 Enero 2016

[27] CCM. Protocolo TCP. Características. Tomado de http://es.ccm.net/contents/281-protocolo-tcp. 2016

1. CISCO & IPV6

Gracias a múltiples predicciones, el IPv6 cuenta con una mayor cantidad de direcciones en comparación con su versión anterior el IPv4, mejorando la capacidad del Internet en numerosos aspectos, como se explica brevemente en esta sección. Por consiguiente, es necesario que todo usuario de internet, en todos sus niveles, empezando por un profesional de TI, fanáticos de la tecnología, ingenieros con objeto empresarial e incluso un gamer en la comodidad de su hogar, conozca y contextualice lo consignado en esta guía, debido a que el IPv6 es el futuro del internet. El IPv6, se encuentra en marcha actualmente e influye considerablemente en el crecimiento de los sistemas, las comunicaciones mundiales y en especial el modo para comunicarnos, vivir, jugar, trabajar y aprender dentro del internet.

Figura. 4 Crecimiento Ipv6

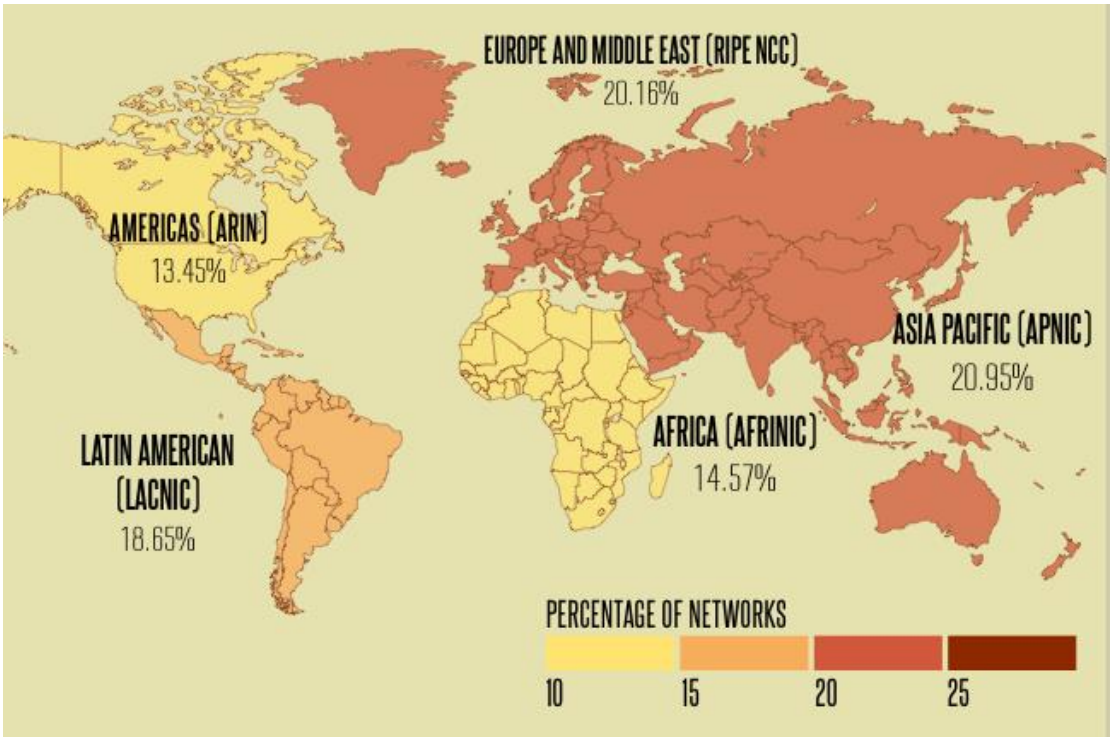


Fuente: http://www.worldipv6launch.org/infographic/

CISCO y sus expertos en la materia Eric Vyncke y Andrew Yourtchenko, explicaron los mitos de seguridad y los problemas de seguridad en el protocolo IPv6 y junto con ellos y otros famosos desarrolladores se explicará en esta guía, los diferentes tipos de problemas de seguridad, instalación y tipicidad de este nuevo protocolo y como ha iniciado en el mundo del internet. Aunque IPv6 sólo está disponible al 3 por ciento de los usuarios de Internet, este número se duplica cada 6 a 9 meses y lo más importante, todos los sistemas operativos de host IPv6 ya vienen activados por defecto. Lo que se explicará en esta guía rápida se centrará principalmente en el propio protocolo de seguridad, aunque también en algunas características del producto. Se espera que los lectores asistentes a esta

guía tengan algún conocimiento de IPv6 y también sobre seguridad de redes en red IPv4.[28]

Figura. 5 Ipv6 redes disponibles por región.



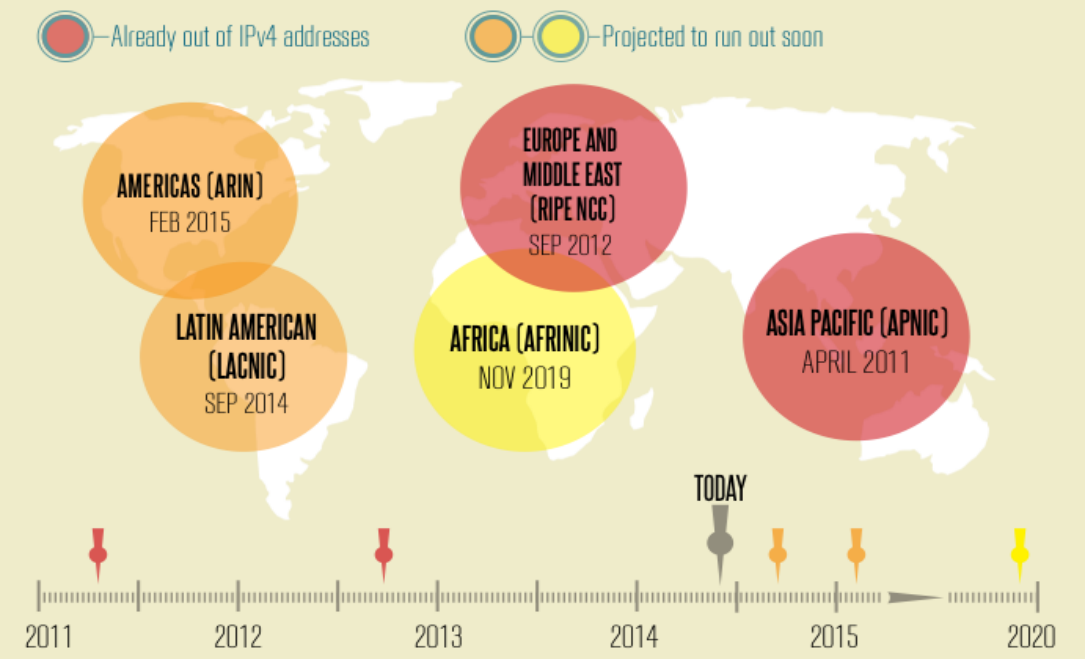
Fuente: http://www.worldipv6launch.org/wp-content/uploads/2014/06/WorldIPv6Launchiversary-2014.png

Según LACNIC, organización no gubernamental internacional establecida en Uruguay en el año 2002, encargada del registro de direcciones de internet para América Latina y Caribe, responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), números autónomos, resolución inversa y recursos para la región de América Latina y el Caribe; muestra en su página como es la proyección de agotamiento de direcciones de IPv4 según sus registros hasta el presente año.[29]

A continuación se muestran algunos extractos de los datos consignados por LACNIC.

[28] IPv6 Security - FAQ from live webcast. Tomado de IPv6 Security - FAQ from live webcast
[29] LACNIC. Definición. Tomado de http://www.lacnic.net/web/lacnic/acerca-lacnic

Figura. 6 IPv6 to the Rescue



Fuente: http://www.worldipv6launch.org/infographic/

1.1 Proyección de agotamiento

Retomando datos estadísticos desde junio del 2014, momento en que se activó esta fase, se analiza el comportamiento de las asignaciones y se grafica a continuación en una proyección con distintos modelados y las posible fechas de agotamiento.

Fecha de ejecución: 2016-04-06

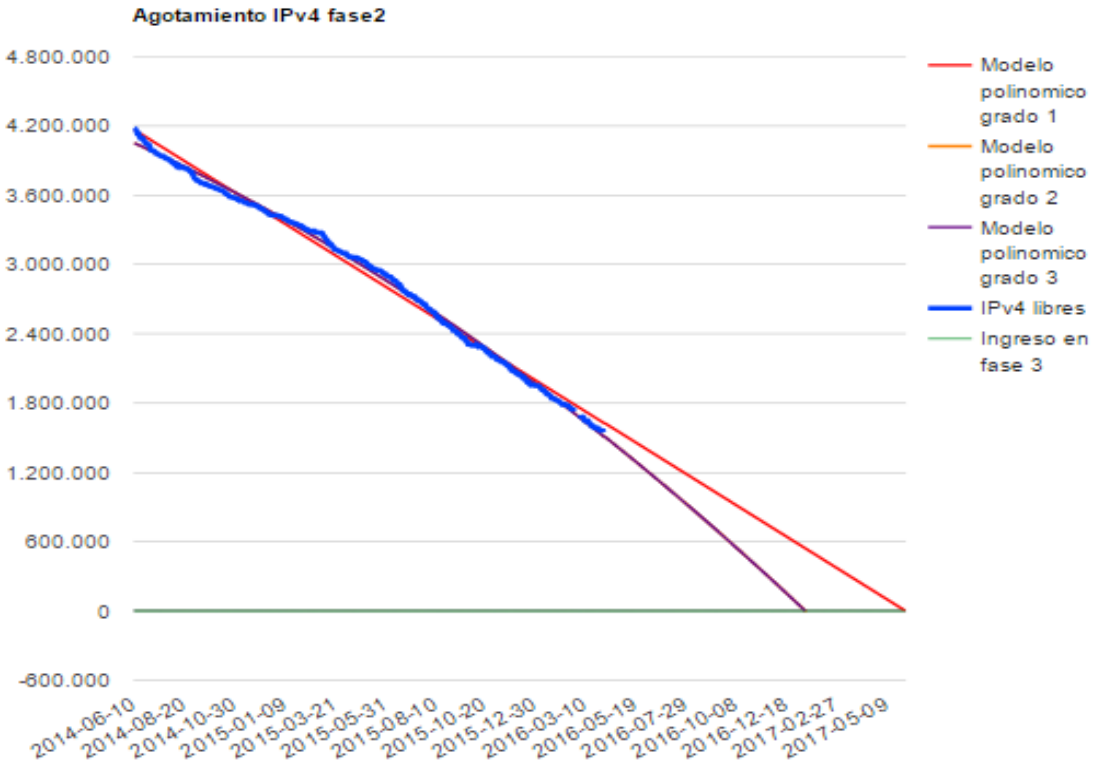
Fin de la fase 2 modelo 1: 2017-06-06 Factor de error: 0.9926022423756221

Fin de la fase 2 modelo 2: 2017-01-16 Factor de error: 0.997683021191912

Fin de la fase 2 modelo 3: 2017-01-15 Factor de error: 0.9976833920119182

Fecha fin ponderado: 2017-03-03

Figura. 7 LACNIC Agotamiento IPv4

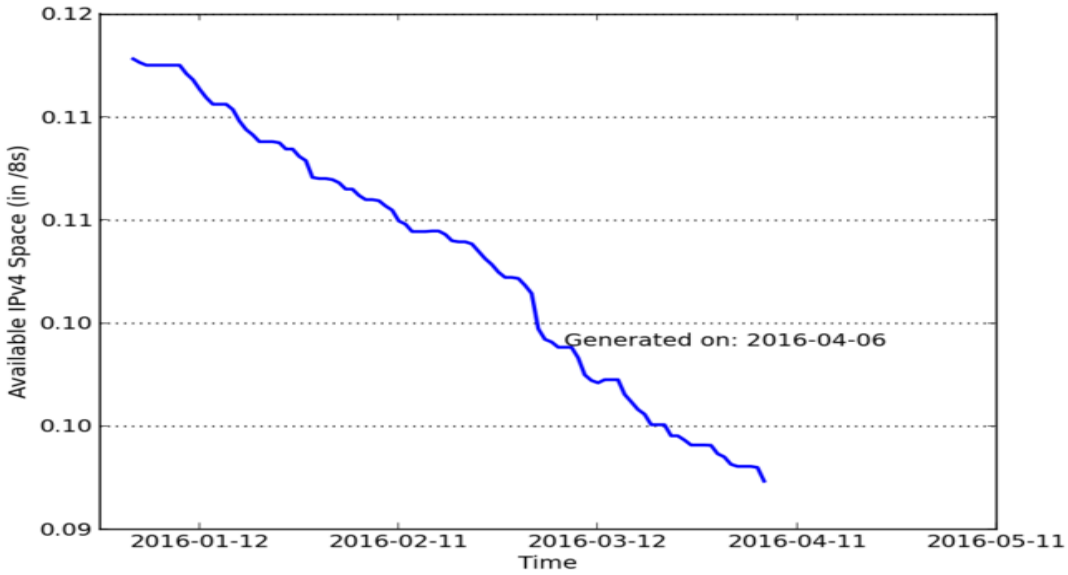


Fuente: http://www.lacnic.net/web/lacnic/agotamiento-ipv4

A pesar de su agotamiento, la adopción de IPv6 no es tan simple, se debe recordar que con un enfoque de adopción como este, se realiza por fases, con una validación y comprobación cuidadosa para evitar prever alguna interrupción de la red IPv4 y la introducción de vulnerabilidades que consigo trae.

Reporte de Direcciones IPv4 154675 - 0.092

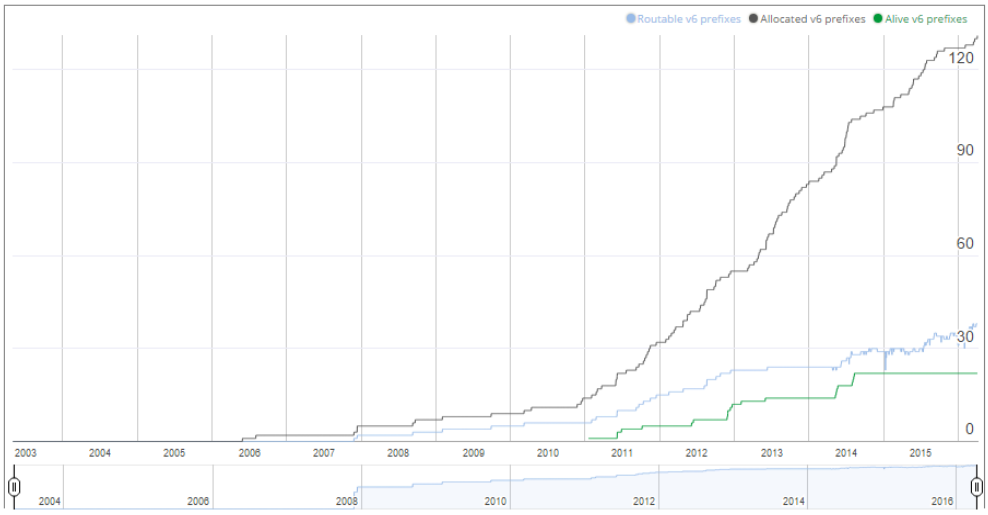
Figura. 8 Reporte direcciones IPv4



Fuente: http://www.lacnic.net/web/lacnic/agotamiento-ipv4

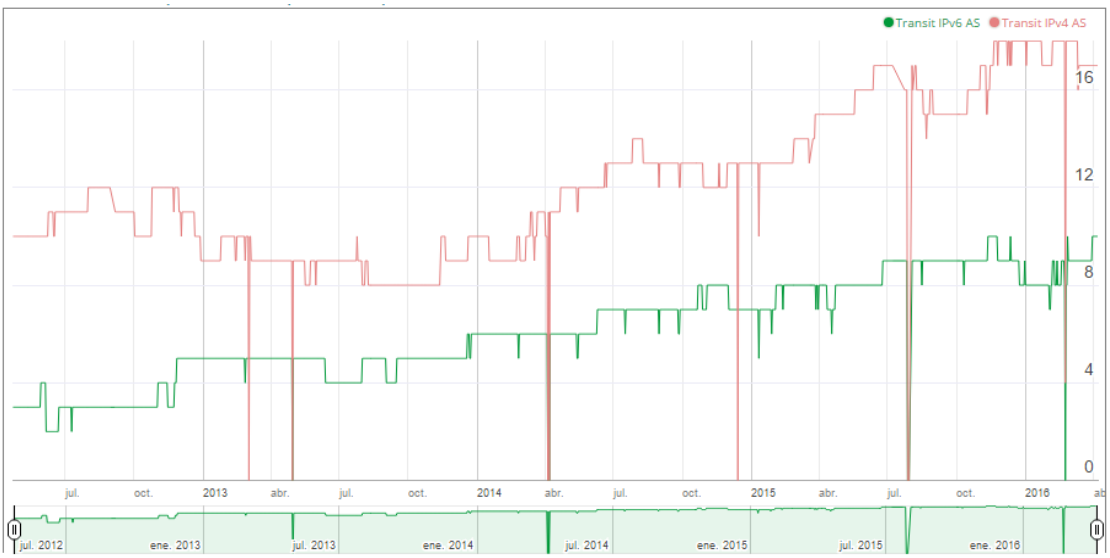
¿En Colombia que ha pasado?, Ahora si bien para Colombia existe la siguiente recopilación de datos que registran el crecimiento y adecuación de la migración de IPv4 a IPv6.

Figura. 9 Display Iv6 Prefixes Data



Fuente: http://6lab.cisco.com/stats/cible.php?country=CO&option=all

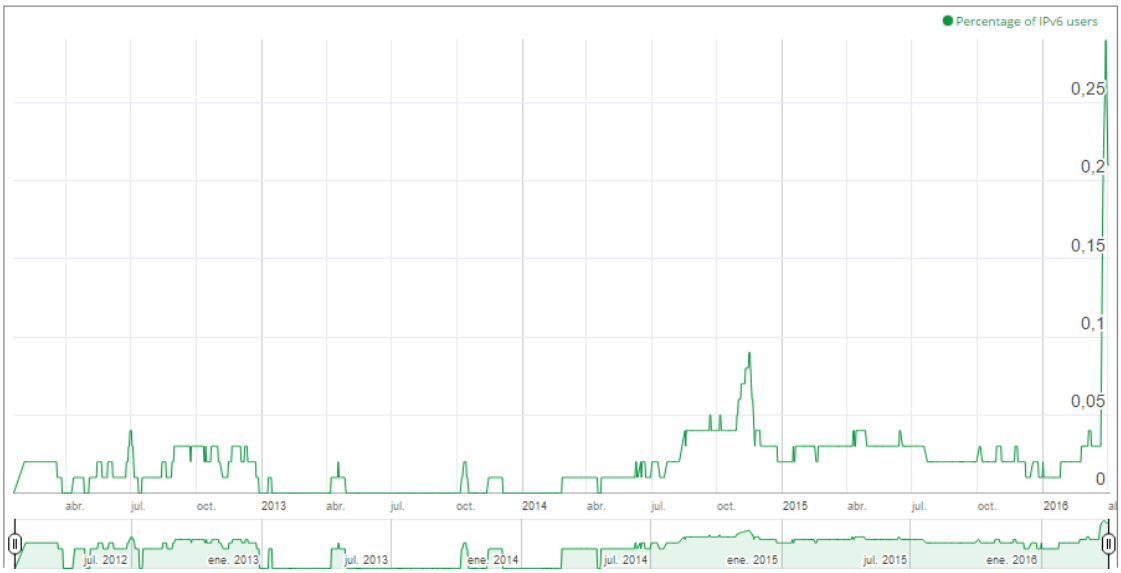
Figura. 10 Historical Expansion of IPv6 and IPv4 transit AS



Fuente: http://6lab.cisco.com/stats/cible.php?country=CO&option=all

IPv6 toma fuerza dentro de las industrias y mercados, donde esta de la mano con la expansión de las redes por fuera de las fronteras convencionales. Se trata no solo de un protocolo, ahora se habla de nuevos modelos de negocios, permitiendo que las empresas puedan conectarse y expandirse a más países en el mundo.

Figura. 11 Display User Data



Fuente: http://6lab.cisco.com/stats/cible.php?country=CO&option=all

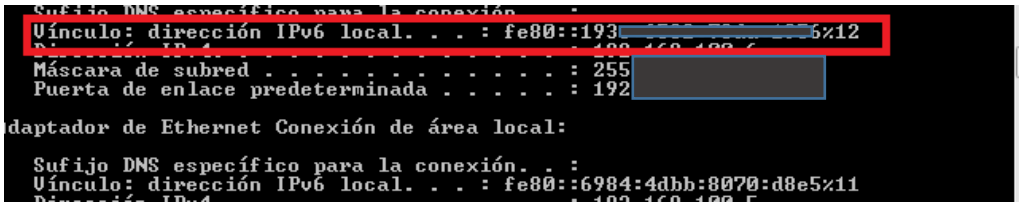
2. SEGURIDAD EN IPV6

2.1 Generalidades

Aunque el IPv6 se encuentra circulando desde hace varios años, existe mucho desconocimiento de sus características y aspectos de seguridad, debido a que las compañías se esmeran en revisar aún sus configuraciones de IPv4, sin denotar realmente que están funcionando en las conexiones SMB, DNS o incluso web de la Intranet, las cuales son parte del protocolo IPv6. Por lo tanto, el conocer sobre el funcionamiento del IPv6 es fundamental para la protección de la información y la misma red, debido a que muchos de los sistemas de protección IDS están configurados para detectar la mayoría de los ataques en redes IPv4, pero no trabajan de manera similar en redes IPv6.

Por consiguiente, se explica en este guía de manera breve las características generales del nuevo protocolo y posteriormente, la exposición de recomendaciones ante posibles ataques, generalidades de implementación y pruebas de vulnerabilidad, sirviendo de soporte para muchos técnicos, que a pesar de conocer mucha información del protocolo, no han entrado en profundidad en lo que a este protocolo se refiere.

Figura. 12 Ipconfig en IPv6



Fuente: Autor

En la anterior imagen muestra una configuración por defecto, característica de una dirección IPv6, la cual está escrita de una forma similar a la IPv4, pero inicia como fe80:123:0000:0000:0000:0000:0000:1ab0. Claro está que no es algo a lo que usualmente se apreciaba en el anterior protocolo, pero no es diferente del todo, debido a que hay 8 grupos de 4 valores hexadecimales. En este protocolo tenemos que el prefijo de Subred, (la máscara de red en IPv4) cambiado así por múltiples inconvenientes con usuarios el uso de subnetting, supernetting y la asignación de máscaras de red del tipo 255.0.124.255; posee la misma función que la máscara, gestiona la visibilidad de red y ha de utilizarse para hacer subnetting y supernetting, pero todos los unos (1) van seguidos y al principio por definición en el estándar, de esta manera podríamos contar con dos direcciones IPv6 sin usar una puerta de enlace en la red, tales como estas:

A: fc00::2000:0001/96

B: fc00::2001:0001/112

Nota: Al hacer un ping en IPv6 de un terminal A a uno B obtendríamos un Time-Out y al hacer un ping en sentido contrario (B a A) obtendríamos una respuesta de Host inaccesible, debido a que A no entra dentro de la misma red que B, pero B si está dentro de la misma red que A.[30]

Direcciones Well-Known en IPv6

Además de las direcciones de enlace o vínculo local, en IPv6 hay una gran cantidad de direcciones que deben ser conocidas, por lo tanto es conveniente describir las más importantes para entender los entornos de ataque:

- ::/128: Es la dirección IPv6 indefinida y con todos los bits a 0.
- ::/0: Es la dirección de red IPv6 la cual describe una ruta por defecto en una tabla de enrutamiento y equivale a la dirección IPv4 0.0.0.0.
- ::1/128: Local host en IPv6 y equivalente a 127.0.0.1 (IPv4).
- fe80::/10: Direcciones de vínculo o enlace local. No son enrutables pero generan una red local efectiva en el rango fe80::/64. La parte de Host se suele calcular a partir de la dirección MAC de la tarjeta.
- ff02::/16: Son direcciones de redes IPv6 Multicast. Equivalentes a las (224.X) en redes IPv4.
- fc00::/7: Son las direcciones para redes IPv6 privadas. Estas direcciones tampoco son enrutables en Internet y son equivalentes a 10.X, 172.16.X y 192.168.X en redes IPv4
- ::ffff:0:0/96: Son direcciones IPv4 pero mapeadas en IPv6. Se utilizan para conversiones e interconexiones de protocolos IPv4 e IPv6.
- 64:ff9b::/96: Son direcciones IPv6 generadas automáticamente a partir de IPv4. Son necesarias para hacer nuevas direcciones IPv6 y se quiera generar a partir de la dirección IPv4 de la máquina.
- 2002::/16: Esta Indica que es una red 6 to 4 esta mapeada y podrá usar la dirección IPv4 192.88.99.X como gateway para la interconexión.

Además de estas direcciones, hay algunas reservadas para propósitos especiales, como son las siguientes:

- 2001::/32: Usado por el protocolo de túneles Teredo que permite hacer tunneling IPv6 sobre redes IPv4 en Internet. Este sistema es el que se utiliza a

[30] UN INFORMÁTICO EN EL LADO DEL MAL. Conceptos básicos IPv6. Disponible http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6.html. 05 mayo 2016

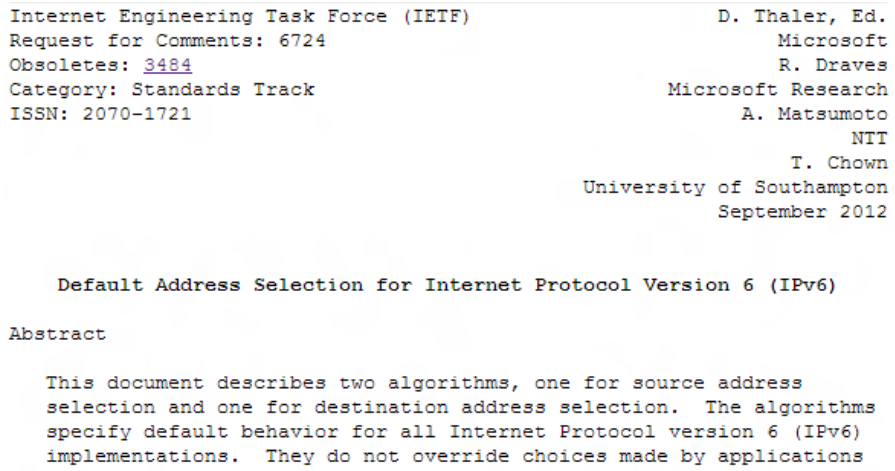
la hora de implementar Direct Access en Windows Server 2008 R2 y Windows 7.

- 2001:2:/48: Asignado a Benchmarking Methodology Working Group (BMWG) para comparativas (benchmarking) en IPv6 (similar a la red 198.18.0.0/15 para comparativas en IPv4).
- 2001:10::/28: ORCHID (Overlay Routable Cryptographic Hash Identifiers). Direcciones IPv6 no-enrutables usadas para identificadores criptográficos Hash.
- 2001:db8::/32: Direcciones utilizadas para documentación o ejemplos IPv6. Similar a las redes 192.0.2.0/24, 198.51.100.0/24 y 203.0.113.0/24 en IPv4.

2.1.1 Como identificar si un computador tiene IPv4 o IPv6

Cada computador debe trabajar con alguno de esos dos protocolos, dependiendo de la configuración que se escoja, sin embargo, ellos conviven juntos, así que el sistema operativo debe elegir siguiendo algunas normas las cuales están regidas por el algoritmo RFC 3484 & RFC 6724 "Default Address Selection for Internet Protocol version 6 (IPv6)", en el cual se explica claramente como son las normas para elegir entre los mencionados.

Figura. 13 RFC 6724



Internet Engineering Task Force (IETF)
Request for Comments: 6724
Obsoletes: 3484
Category: Standards Track
ISSN: 2070-1721

D. Thaler, Ed.
Microsoft
R. Draves
Microsoft Research
A. Matsumoto
NTT
T. Chown
University of Southampton
September 2012

Default Address Selection for Internet Protocol Version 6 (IPv6)

Abstract

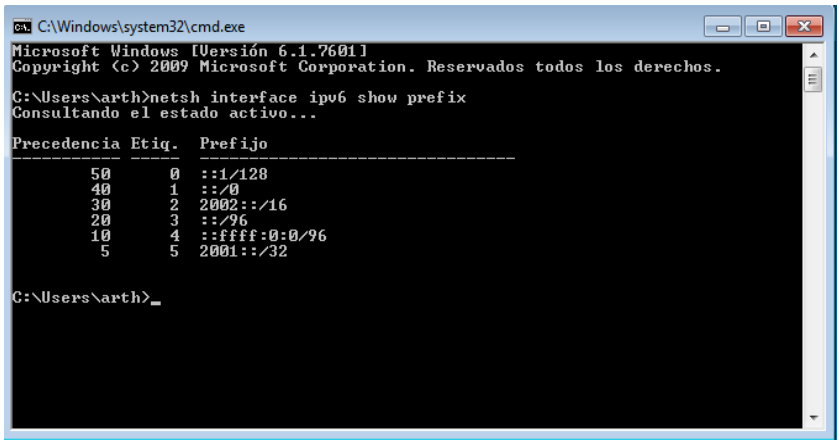
This document describes two algorithms, one for source address selection and one for destination address selection. The algorithms specify default behavior for all Internet Protocol version 6 (IPv6) implementations. They do not override choices made by applications

Fuente: http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6_30.html

Estos algoritmos explican la dirección de origen y la dirección de destino ya sea para escoger un protocolo u el otro, los cuales tienen en cuenta las puertas de enlace, ya que puede darse el caso que el origen como el destino sean IPv4, pero se encuentran en otra red que solo sea IPv6, dando pie para escoger un encapsulado de direcciones IPv4 sobre IPv6 para enrutar el tráfico.

En ciertos sistemas como los de Windows con el comando *netsh interface ipv6 show prefix* no muestra una tabla de prioridades y aunque se puede tomar más comando para modificar estas prioridades, por defecto siempre será la prioridad IPv6 sobre su anterior versión.

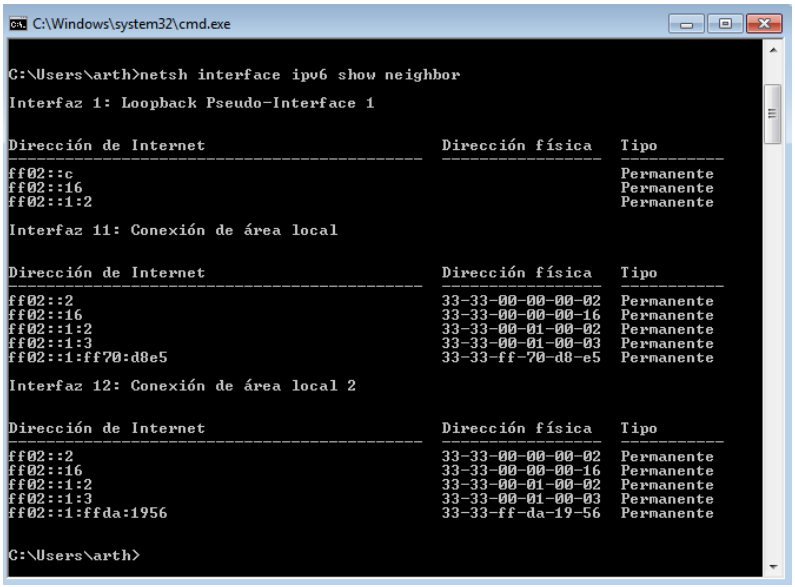
Figura. 14 Algoritmos de prioridades IPv6



Fuente: Autor

Igualmente, gracias al protocolo ICMPv6, junto con sus mensajes Neighbor Solicitation (NA), es posible recolectar información de resolución de una dirección MAC asociada a una dirección IPv6 y NA a la vez, el cual responde con la dirección MAC de la dirección IPv6 que se busca.

Figura. 15 Tabla de Neighbbor IPv6



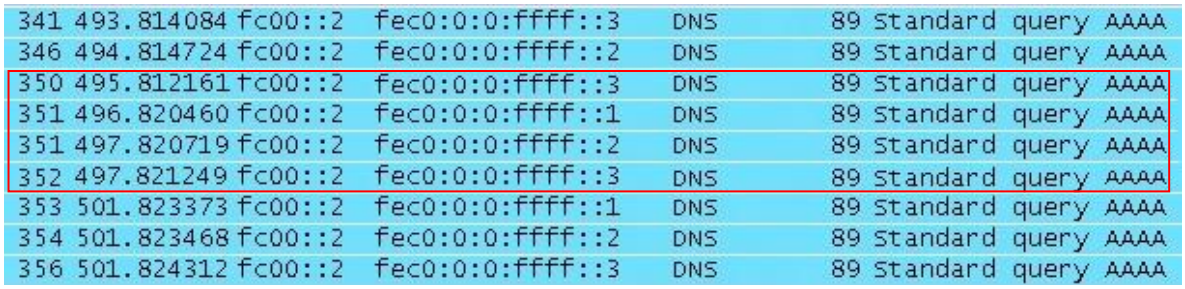
Fuente Autor

Las direcciones MAC asociadas a direcciones IPv6 se almacenan en una tabla de vecinos y se obtiene con el comando *netsh interface ipv6 show neighbor*. Toda esta información es muy importante para cuando se inicien las pruebas y ataques como DoS o Man In the Middle (página 52).

DNS Autodiscovery

Al conectar el equipo a la red IPv6 a través de una configuración SLAAC, se experimenta un problema en configuración de los servidores DNS y todas las peticiones de resolución se reducen a LLMNR de tipo difusión, en busca de posibles servidores en la red de vínculo local. Sin embargo, si el servidor fuera externo, es mandatorio contar con un servicio de resolución de nombres DNS en la red IPv6. Para ello, cuando no se configura ningún servidor en el caso de Microsoft Windows, se inicia una búsqueda automática de direcciones IPv6 establecidas por el estándar IPv6 DNS Autodiscovery.[31]

Figura. 16 Direcciones IPv6 de los DNS Autodiscovery



Fuente: Autor

2.2 Lineamientos de Seguridad para IPv6

2.2.1 Lineamientos Generales

- Para implementar el protocolo IPv6, se debe estructurar, basándose en los esquemas de seguridad de información, contemplando políticas de confidencialidad, integridad y disponibilidad de las entidades.
- Se requiere un plan de contingencia, en el cual se defina un plan de marcha atrás en caso de presentarse inconvenientes de indisponibilidad de servicios, que atenten contra la seguridad de la información y de las comunicaciones de las entidades al momento de implementar el protocolo IPv6.
- En el proceso de transición hacia el nuevo protocolo, se debe revisar la seguridad de información de las infraestructuras de TI, la seguridad de IPv6 y

[31] UN INFORMÁTICO EN EL LADO DEL MAL (2013). Conceptos básicos IPv6. DNS Autodiscovery Disponible http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6.html. 05 mayo 2016

el nivel de impacto de servicios como el Directorio Activo, Sistemas de Nombres de Dominio (DNS), Correo Electrónico, Servicio de Protocolo de Configuración Dinámica de Host – DHCP (Definido en el RFC3315 para DHCPv6), Sistemas Proxy, Servicios de aplicaciones, Servicios Web y Sistemas de Gestión y Monitoreo.

- La documentación es importante, se debe generar la documentación necesaria que contemple los aspectos de seguridad del entorno en los sistemas de comunicaciones, sistemas de información y sistemas de almacenamiento, que surjan del desarrollo de la implementación de IPv6.
- Implementar el IPv6, puede causar conflictos de seguridad de información en los servicios de las entidades; con el objeto de poder detectar estos inconvenientes a tiempo, es necesario hacer un examen detallado que permita encontrar posibles vulnerabilidades y en efecto bajo IPv6, debe ser una labor detallada, debido a que el protocolo se apoya en otros protocolos como IPSec, HTTP, TCP, UDP o SIP.
- Para la infraestructura de TI, se debe segmentar para cada uno de los servicios de una empresa varias zonas lógicas en el firewall, con el objeto de garantizar la mayor protección una vez la red de comunicaciones pueda generar tráfico en IPv6.
- El factor humano, el más importante de todos, se debe disponer del equipo humano idóneo necesario para verificar y monitorear los problemas de seguridad de información que surjan al momento de ejecutar las fases de implementación y pruebas de funcionalidad, cuya labor está bajo la responsabilidad del Director de Seguridad de la Información – CISO (Chief Information Security Officer) o del que haga sus veces y del equipo de trabajo de seguridad de las áreas de TI de cada entidad.
- Los componentes de seguridad diseñados para el protocolo IPv6 deben ser verificados y entendidos plenamente, como la clave para evaluar, monitorear y mejorar el desempeño de los servicios y aplicaciones bajo IPv6 en su desarrollo de generación de tráfico en los canales. El documento “Política para la adopción de IPv6 en Colombia, estructuración y definición de Cintel y Mintic del año 2012”, habla del momento en donde se migra de un protocolo antiguo a uno moderno (IPv4 a IPv6), se mejora las condiciones de seguridad de la información, debido a que el IPv6 facilita las tareas de monitoreo y refuerza los protocolos de seguridad nacional, suministrando a cada usuario en cada terminal móvil, la ventaja de recibir de forma estática, una dirección IP para establecer certeramente la ubicación y origen de la comunicación, dando como resultado la adopción de medidas de seguridad redundantes.

Muchas direcciones no son suficientes, por ello el protocolo IPv6 debido a su gran cantidad de direcciones disponibles no tiene como política manejar direcciones IP públicas o privadas, por lo que elimina toda clase de elementos que permiten "esconder" direcciones IP públicas en la comunicación (como uso de NATs – Traducciones de red), reduciendo los riesgos de intrusión en la red; sin embargo, lo anterior no quiere decir que el protocolo IPv6 sea más seguro que IPv4, pero el IPv6 si obliga a incorporar dentro del paquete IP al protocolo IPsec (eliminando la variedad de protocolos de seguridad existentes en IPv4) y al no requerir NATs, se puede utilizar IPsec, extremo-a-extremo, incrementando los niveles de seguridad en la red."[32]

2.2.2 Sobre el Direccionamiento IP

- En condiciones que se requiera atender solicitudes de servicios HTTP entre nodos IPv6, es necesario el uso de directivas de seguridad del protocolo (IPsec).
- Revisar los segmentos de bloque de las direcciones en IPv6, enfocándose en las necesidades de operación de la empresa, con el fin de, establecer criterios de seguridad apropiados; incluso, aunque estas ya hayan sido revisadas por zonas lógicas de seguridad (DMZ).
- El direccionamiento en IPv6 y su utilización deben ser claros para los usuarios de las empresas, atendiendo políticas de seguridad y privacidad de la información.
- Son criterios básicos en el direccionamiento en IPv6, la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicaciones.
- Cuando inicie la fase de implementación del nuevo protocolo, es recomendable crear VLANs (Redes de Área Local Virtuales), dentro de las redes locales de la empresa, con el fin de usarlas para pruebas de monitoreo, direccionamiento, tráfico y seguridad.
- Un paquete en IPv6 pasa por distintas etapas de enrutamientos, cuyo objeto es mitigar el espacio de búsqueda de posibles atacantes de escaneo sobre la red IPv6. Se recomienda que los administradores de las redes utilicen herramientas de software de monitoreo para controlar posibles patrones de comportamiento de direccionamiento IP, sin importar que sea trafico multicast o se use Neighbor discovery[33].

---

[32] Documento Política para la Adopción del IPv6 en Colombia, estructuración y definición, numeral 12.10, página 72, 73, 2012, Contrato 947 Mintic, Cintel, año 2012.

[33] Más información de este tipo de ataques característicos en el RFC 4941.

- Los paquetes IPv6 contiene cabeceras de autenticación (AH, Authentication Headers) y encabezados de extensión de carga de seguridad encapsulada (ESP, Encapsulating Security Payload), por ende, deben seguir las recomendaciones de seguridad, en la cual el IPsec sede a cualquier nodo de IP la administración de sesiones de seguridad de extremo a extremo.

2.2.3 En La Nube Bajo Ipv6: Con el objeto de mantener una seguridad apropiada y mitigación del riesgo en la nube, se debe responder a una estrategia de análisis para ambientes tanto físicos como lógicos, que permitan a las organizaciones construir políticas adecuadas para su correcta administración e implementación en las infraestructuras de comunicaciones en las entidades; en cumplimiento de estas premisas es preciso conformar un equipo de trabajo de las Oficinas de TI, encargado de dictar lineamientos para el tratamiento de la información en ambientes de comunicación, computación y almacenamiento en la nube, esto con la ayuda o el apoyo de las empresas proveedoras del servicio en la nube.

Ténganse en cuenta los siguientes lineamientos de seguridad a los distintos proveedores de comunicaciones en la nube, así:

- Construcción de un mapa de riesgos y sus implicaciones (Con el apoyo de los proveedores de servicios).
- Implementación de control de identidad de usuarios.
- Acoger normas de protección de información.
- Inspección de esquemas de virtualización (si existen).
- Reconocer la infraestructura del tipo de nube que se requiere implementar para adecuarla a IPv6 (nube híbrida, federada, privada, pública, entre otras).
- Adopción de retención de datos.
- Acuerdos de Nivel de Servicio (ANS) con el proveedor del servicio.
- Conexión a través de Redes Privadas Virtuales - VPNs.
- Utilización de claves complejas.
- Aglomerar de cifrado de la información.
- Evaluación de los estándares de servicio.
- Confirmación por medio de pruebas del servicio, es decir garantía de que los canales y servicios en la nube esté funcionando correctamente.
- El proveedor de servicio a contratar debe ser reconocido, ya que loa información que viaja por la red puede estar circulando por todo el mundo.
- Instaurar acuerdos de confidencialidad de la información.

Recomendaciones antes de subir a la nube:

- Hacer un análisis crítico sobre la información (directorios, cuentas de correo, bases de datos y demás).
- Verificar las condiciones y la calidad del servicio proporcionado por el proveedor de servicios de la nube.
- Definir expresamente el tipo de información a subir a la nube.
- Cerciorarse que la información requerida y almacenada este dentro de una estructura convencional.
- Asegurarse que se haga una contratación de servicios con el proveedor en la nube de buena calidad y experiencia por parte del usuario, el cual apoye la seguridad de la información.

La seguridad en la nube debe estar presente en cada una de las capas de funcionamiento en la nube es decir:

- ❖ Capa de infraestructura.
- ❖ Capa de almacenamiento.
- ❖ Capa de gestión de infraestructura.
- ❖ Capa de aplicación.
- ❖ Capa de servicios.[34]

2.2.4 Actualización de protocolos y equipos a IPv6: El protocolo en cuestión, puede llevar varios años desde su lanzamiento, pero la implementación de aplicaciones que usen IPv6 puede requerir actualizaciones de software e incluso de hardware, así mismo, es posible que no todas las características de IPv6 estén implementadas. En esta sección pasamos a indicar algunos problemas que pueden surgir en diversos sistemas operativos y equipamiento con la implantación de IPv6, la lista no es exhaustiva ni absoluta, por lo tanto se recomienda revisar la información del fabricante en cuestión.

2.2.5 Linux

- Linux en sus sistema de contrafuegos soporta IPv6 usando unos ficheros de arranque y configuración llamados IP6tables (distintos a los de Iptables), pero no todos los módulos a nivel de IPtables están implementados en IPv6, entre los módulos no implementados se encuentra el uLog, comment, Classify, clusterIP y entre estos módulos no implementados esta implementado (en un RedHat 5.5 solamente la mitad de los módulos de Iptables están implementados en IPv6 (59/30).

[34] Capas propuestas por Gartner Group

- La configuración de aplicaciones tales como servidores HTTP, correo-e, hosts.allow, en el caso de existir restricciones de conexión se debe configurar el acceso desde las direcciones IPv6.
- Algunos ataques en la capa de enlace son permitidos por la configuración por defecto de la pila TCP/IP en los sistemas Linux, como puede ser el uso de ICMPv6 para ataques de intermedio, etc. Es conveniente revisar los parámetros del kernel, para evitar este tipo de ataque (www.cibercity.biz).

2.2.6 Correo electrónico: El registro SPF debe incluir las direcciones en IPv6 desde donde se va a enviar el correo, siempre y cuando los servidores de correo soporten IPv6, además se debe contactar con el servicio ESWL de RedIRIS para inclusión de direcciones IPv6 en la lista blanca. Se debe hacer un resalto en el uso de mecanismos como SDF y DKIM desde RedIRIS y su inicio en el despliegue IPV6, con el objeto de evitar inconvenientes que surgen en el SPAM de IPv4.

Las instituciones afiliadas que emplean el servicio Lavadora de RedIRIS, se informa por medio de las listas de coordinación como se pueden emplear un mecanismo de No listing para recibir correo en IPv6 y en servidores de correo de la empresa, desde RedIRIS se está trabajando en SMTP para la generación de una lista de reputación que soporte IPv6 y a su vez proporcione eliminación de todo el spam que se detecte en IPv6[35].

2.2.7 Protocolo IPSec - Internet Protocol Security (IP Security): IPsec es conocido como un protocolo de seguridad definido por el estándar IETF[36] desde 1999 y se basa en el RFC 4301. A continuación, se establecen las siguientes consideraciones con respecto a este protocolo.

Según la IETF, “IPsec está diseñado para proporcionar interoperabilidad, de alta calidad, con seguridad basada en cifrado tanto para IPv4 como para IPv6.

El compendio de servicios de IPsec, incluyen control de acceso, integridad sin conexión, autenticación de origen de los datos, detección y denegación de repeticiones (una forma parcial de integridad secuencial), confidencialidad a través de cifrado y a través de flujo de tráfico limitado.

Estos servicios se proporcionan en la capa 3, brindando protección estándar para todos los protocolos que pueden ser transportados a través de IP.

---

[35] IRIS. Seguridad en IPv6 para Instituciones afiliadas a RedIRIS. 2.2.5 Actualización de protocolos y equipos a IPv6. Correo Electrónico. Disponible en http://www.rediris.es/cert/doc/ipv6seg/#1.7.2

[36] IETF (Internet Engineering Task Force) o Grupo de Trabajo de Ingeniería de Internet, entidad que regula las propuestas y los estándares de Internet, conocidos como RFC

IPsec posee aspectos de control de acceso en la capa IP como especificaciones mínimas de funcionalidad de firewall y cuyas implementaciones son libres de adecuar por medio de mecanismos de firewalls sofisticados y exigidos por mismo IPsec."[37]

A continuación los componentes del IPsec:

- Posee una integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores.

- IPsec es un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad; es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.

- Es un protocolo de obligatorio funcionamiento en IPv6, se usa para asegurar el tráfico entre enrutadores BGP (Boundary Gateway Protocol) para cifrado y autenticación IP y su uso se extiende en protocolo de enrutamiento tipo OSPFv3 (Open Shortest First Path).

- IPsec puede ser usado en diferentes escenarios a nivel de enrutamiento, como por ejemplo con OSPFv3, que utiliza AH, la extensión de encabezados maneja ESP como un mecanismo de autenticación en lugar de la variedad de esquemas de autenticación y procedimientos definidos en OSPFv2; en IPv6 Móvil, esta especificación de protocolo es un proyecto de la IETF propuesto para usar IPSec haciendo obligatoria la autenticación de actualización; en Túneles, en la cual IPSec puede ser configurado entre sitios (enrutadores IPv6) en lugar de que cada equipo utilice IPSec y finalmente, en la cual IPSec se puede utilizar para garantizar el acceso del enrutador para la gestión de la red[38].

2.2.8 Estructura del IPSec: El IPsec incluye protocolos para establecer claves de cifrado, asegurando las comunicaciones del protocolo de Internet (IP) y autenticando y/o cifrando cada paquete IP en un flujo de datos.

El IPSec (Internet Protocol security) está constituido de la siguiente manera:

[37] Security Architecture for the Internet Protocol. 3.3. Where IPsec Can Be Implemented. Pág. 10. Disponible en https://tools.ietf.org/html/rfc4301

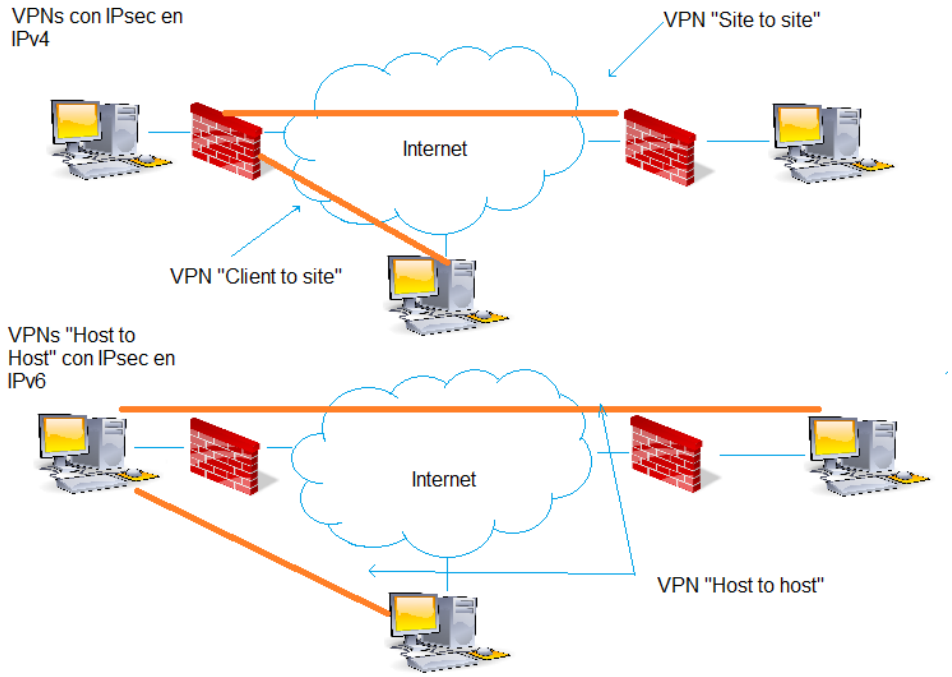
[38] Tomado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

- El IPsec cuenta con una cabecera de autenticación o AH, que brinda protección contra duplicados, protege la integridad de los campos de encabezado IPv6, excepto aquellos que cambian de enrutamiento y adicionalmente el AH autentica el origen por medio de un algoritmo cifrado.

- Los protocolos de IPsec actúan en la capa de red 3 del modelo OSI y es allí donde se permite identificar los nodos finales de una comunicación, es por esto, que los nodos finales no tienen acceso directo uno a otro sino a través de otros dispositivos.

- Un segundo encabezado conocido como Encapsulado de Seguridad de Carga Útil" - IPsec (ESP Encapsulating Security Payload), provee confidencialidad, autenticación, integridad interna y protección contra duplicación.

Figura. 17 IPsec



Fuente: Autor

2.2.9 Revisión de los RFC de Seguridad: Al revisar el RFC 4942 que hace mención a las consideraciones de seguridad para el proceso de coexistencia y transición a IPv6.
En la RFC 6177, en la cual se refiere a una especificación técnica que deben seguir los clientes para solicitar asignación de segmentos de IPv6 en el rango de /48 a /56.

Se revisan los procedimientos de RFC de seguridad para la utilización de equipos de comunicaciones, software de aplicativos, sistemas de cifrado, redes, dispositivos móviles y demás.

Una vez analizado los activos de información de las entidades o empresas, se realiza una matriz de riesgo, clasificando las aplicaciones y determinando los niveles de seguridad de las mismas. Por ende, se revisa los RFCs que hablan sobre las recomendaciones a seguir con respecto a la seguridad en las aplicaciones.[39]

2.2.10 VPN (Redes Privadas Virtuales): Es necesario adaptar varios puntos de red IPv6 para el control de tráfico si dado el caso el diseño de la empresa tiene varias conexiones privadas virtuales extremo a extremo, (intercomunicación entre dos o más redes locales [LAN]); para que la información viaje entre muchos recursos compartidos en una red de amplia cobertura y se garantice la seguridad del tráfico de las comunicaciones a través de redes privadas virtuales usando IPSec.

2.2.11 Monitoreo de IPv6: Este procedimiento no solo se ve en la fase de pruebas de funcionalidad en el modelo de transición de IPv4 a IPv6, sino que igualmente permite establecer el nivel de criticidad y funcionalidad entre redes operativas de IPv6, por lo que el diagnóstico de fallas, la detección, prevención de problemas, determinación de acciones para la solución de problemas de seguridad y plan de contingencias se hace mandatorio.

A continuación se exponen ciertas variables a considerar a la hora de realizar monitoreo de los servicios de red en IPv6:

- Estado de servicios.
- Actividad de los hosts.
- Estado de aplicaciones.
- Medición de tráfico sobre interfaces y dispositivos de red.

Importancia del monitoreo. Existen herramientas como por ejemplo analizadores de tráfico que provean análisis de interfaces de red, monitoreo de librerías de IPv6 y soporte sobre SNMP.[40]

Cada empresa o institución debe estar en capacidad de utilizar libremente las herramientas de monitoreo una vez implementado IPv6, teniendo en cuenta que la

[39] Ver www.mintic.gov.co/ipv6
[40] SNMP: Simple Network Management Protocol, Protocolo Simple de Administración de Red

complejidad de cada una de estas no es lo importante sino los resultados exitosos que arroja el mismo.

2.3 Pilares de la Seguridad de la Información en IPv6

La seguridad del IPv6 se establece de acuerdo al IPsec, regido por las características del mismo y permitiendo que los paquetes IPv6 (de 128 bits) puedan circular en la red de internet completamente cifrados sin interposición de procesos como la traslación de direcciones (NAT) y esquemas de encapsulamiento (túneles), que disminuyen el desempeño de las direcciones IP.

Debido a los múltiples ataques en la comunidad de servicios de internet, la seguridad es importante aplicarla en la gran cantidad de direcciones IPv6 del mismo modo que en IPv4, ya que se basan en los mismos planes básicos de seguridad de información ya conocidos, como son los términos de integridad, confidencialidad y disponibilidad.

2.3.12 Confidencialidad en IPV6: Lo característico de este término consta de la propiedad para evitar o bloquear la divulgación no autorizada de información a estaciones de trabajo o sistemas no autorizados, asegurando el acceso de la información solamente para aquellas personas que posean la debida autorización.

Dentro de la estructura del protocolo IPSec, se entiende que está constituido por dos protocolos a la vez, los cuales son la cabecera de autenticación (AH), encargada de proporcionar autenticidad en los datos, integridad y no repudio. Por el otro lado, está el encapsulado de carga útil (ESP), el cual es el encargado de proporcionar confidencialidad mediante el cifrado de los datos. El ESP (encapsulating Security Payload) utiliza un algoritmo de cifrado encargado de proporcionar integridad, autenticidad y confidencialidad de la información.[41]

EL nodo de origen siempre ha de autenticar en el proceso de envío y recepción de información, este cálculo va de la mano con una comparación de la información de autenticación por parte del nodo de destino en cada datagrama IPv6, por ende el uso de la cabecera de autenticación en estos paquetes IPv6 genera un aumento de latencia en las comunicaciones. Esto hace que la AH y el ESP, se puedan definir como instrumentos para el acceso de datos, influido por la distribución de calves cifradas y flujo de tráfico de paquetes y claves cifradas. Estos métodos permiten trabajar de dos maneras, de modo transporte y modo túnel.

[41] Aseguramiento del Protocolo IPv6. Min TIC. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

2.3.13 Confidencialidad en Modo Transporte: Cuando se genera tráfico de datos existe confidencialidad, pero aun así es posible saber con quién se están comunicando los nodos dentro del flujo de información, es decir, las cabeceras de IP están al descubierto. El siguiente esquema representa el esquema de paquetes IPv6 una vez aplicado el campo de Cabecera de Autenticación AH.

Tabla 2. Flujo de Confidencialidad modo Transporte

Cabecera de Origen	Saltos de paquetes	Cabecera de Autenticación	Destino	TCP	Datos

Fuente: Autor

2.3.14 Confidencialidad en Modo Túnel: En esta condición, existe un cifrado de la cabecera IP y encapsulado (creación de una nueva), con la dirección del enrutador de tal manera que con este elemento se puede identificar la red que envía información, pero no precisamente a que usuarios. A continuación, un breve esquema sobre un paquete IPv6, al cual se le aplica el campo Cabecera de Autenticación AH.

Tabla 3 Flujo Confidencialidad Modo Túnel

Nueva Cabecera	Cabecera de Extensión	Cabecera de Autenticación	Cabecera IP de Origen	Cabecera de Extensión	TCP	Datos

Fuente: Autor

2.3.15 Integridad en Ipv6: La integridad pretende mantener los datos libres de modificaciones no autorizadas. Eso quiere decir que consiste en mantener con exactitud la información tal cual ha sido generada, sin manipulaciones o alteraciones por parte de personas o sistemas no aprobados.

La integridad en el paquete IPv6 relaciona la cabecera de autenticación y el ESP o encapsulado de Seguridad de Carga Útil con la integridad de los datos asegurando la información al momento de generar tránsito de paquetes a través de la red IPv6.

Agregando a la anterior información, el AH proporciona autenticidad e integridad de los datos en la estructura del paquete IPv6, gracias a una función de autenticidad cifrada sobre los datagramas de IPv6, la cual se logra gracias a una autenticación de clave.

Esquema de funcionamiento para proveer seguridad. Este esquema entra en juego cuando el nodo origen procesa la información de autenticidad antes de

enviar el paquete cifrado de IPV6 por la red y el nodo receptor revisa la información autenticada al ser recibida. En el Campo Límite de Saltos (Hop Limit), el cual va inmerso en el paquete IPv6, puede ser omitido en el cálculo de la autenticidad debido a que este evalúa constantemente los números de saltos de ruteo producidos en la red y no el tiempo de vida de los mismos, el cual no afecta la seguridad de los datos.

Los algoritmos de autenticación utilizados en el campo de cabecera de autenticación utilizan cálculos de autenticidad tanto en el nodo de origen como en el nodo de destino (no repudio)[42] y esta característica no es nativa de todos los algoritmos de autenticación que se usan en el campo de AH de IPv6.

2.3.16 Disponibilidad en IPv6: La disponibilidad es el término otorgado a la información que se encuentra a disposición de quien debe acceder a ella, tales como personas, procesos o aplicaciones. Son aquellos datos vacantes y asequibles en los sistemas, para personas autorizadas.

El IPv6 ofrece a los usuarios una alta disponibilidad en servicios y se prevé que estas redes establezcan la compatibilidad de protocolos IPv4 e IPv6, lo cual implica tener configurados los sistemas de enrutamiento para el soporte de manera simultánea, con el fin de mantener la continuidad del negocio empresarial y proteger las inversiones.

2.3.17 Privacidad en IPv6: Con la desaparición de NAT (Network Address Traslation) o la traslación de direcciones de red, lo cual es normal en IPv4, genera otro problema para mantener la privacidad en accesos IPv6, por ende se hace necesario plantear niveles y servicios de privacidad de IPv4 en IPv6.

Dentro del marco de IPv6, es posible la combinación de esquemas de seguridad IP para la transmisión de paquetes, tales como la autentificación y la privacidad. Ahora si bien, de acuerdo al orden de aplicación de servicios nacen diferentes técnicas a usar, tales como:

Cifrado antes de Autenticación

Este procedimiento entra en vigor cuando el paquete IP se transmite y autentica en su totalidad, previo a un esquema de cifrado en los extremos. Inicialmente se aplica la carga de seguridad encapsulada (ESP), a los datos a proteger, para después ser incorporado al texto original en el inicio de la cabecera de autentificación IP.

[42] No repudio es la propiedad que tiene un nodo receptor de ser capaz de verificar que el nodo emisor dice ser el que envió una información, aun cuando el emisor pudiera negar posteriormente haber enviado la información.

Autenticación antes del Cifrado

Adecuada únicamente para el encapsulado de carga útil (ESP), esta técnica en modalidad de túnel, hace que la AH o Cabecera de Autenticación se encapsule dentro del paquete IP interno y se autentique y proteja completando el esquema de privacidad. La tipicidad de este método, trata de que la cabecera de autenticación AH se proteja por la carga de seguridad encapsulada ESP, es muy difícil que los mensajes del paquete sean interceptados o exista modificación en la AH sin ser detectado.

Riesgos a la Privacidad

Los riesgos de seguridad latente comenzaron desde hace mucho, pero su incidencia la marco la desaparición de la traslación de direccionamientos de red o NAT (Network Address Traslation); comúnmente utilizados en IPv4. Dado este caso, ahora surge el riesgo de mantener la privacidad en los servicios de acceso de IPv6, haciéndose obligatorio el planteamiento de niveles superiores en servicios de privacidad y mitigación de riesgos de IPv4 en IPv6.

Servicios Impactados en Seguridad

A continuación, los servicios que impactan en la seguridad de las empresas o entidades al momento de iniciar con el plan de implementación de IPv6:

- Telefonía IP.
- Dominio de red.
- Servicios Proxy.
- Directorio Activo.
- Correo electrónico.
- Video Conferencia.
- Mensajería Instantánea.
- DNS (Domain Name System)
- Aplicaciones y bases de datos.
- Servicio Web y Acceso a Internet.
- Equipos de comunicaciones fijos y móviles.
- Dynamic Host Configuration Protocol - DHCP
- Equipos de seguridad (Firewalls, servidores AAA (Authentication, Authorization and Accounting), NAC (Network Access Control).

En cuanto a los demás aspectos de seguridad que son del entorno de las redes y servicios de comunicaciones, se necesita seguir trabajando con políticas de seguridad informática bien fuertes y mejoradas, tal y como se define actualmente

para el protocolo IPv4; en razón, a la gran cantidad de direcciones disponibles, sobre las cuales ya no son requeridos los mecanismos de NAT (Network Access Traslation) que permiten la optimización de direcciones públicas en forma directa para IPv4 y los mecanismos de encapsulamiento (Túneles) que se manejaban en las direcciones IPv4. La implementación del IPv6 debe hacerse bajo el establecimiento de una conexión extremo a extremo; como se afirma en el documento “Adopción de IPv6 en Colombia , Documento de Política” de Cintel, el cual expresa que “…..debe señalarse que el regreso a la conectividad extremo-a-extremo también redunda en mejoras a la seguridad de la red, toda vez que la implementación del protocolo IPv6 permite incorporar el protocolo IPsec (Seguridad IP) y por el tamaño de las redes IPv6, es mucho más difícil encontrar agujeros de seguridad en una subred, por lo que en principio se reducirá el número de intrusiones en la red.” [43]

[43] Tomado de “Política para la adopción del IPv6 en Colombia, Estructuración y Definición, Mintic, Cintel, Contrato No. 947 de 2012, pág. 12.”

3. PROBLEMAS COMUNES AL UTILIZAR IPV6

Como punto de partida esta la implementación de IPv6 en una red nueva o ya configurada y por otro lado se denota una red ya configurada con previa antelación, cuya diferencia es su implementación por partes, donde supone un importante esfuerzo para su planificación. A continuación, se presentan las tareas principales para configurar IPv6, consejos para problemas generales de red, características y problemas con el IPv6 teniendo en cuenta estas configuraciones y situaciones anteriormente mencionadas.

3.1 Consejos de Resolución de Problemas de Red Generales

La pérdida de comunicación de uno o varios hosts es la primera señal de problemas, debido a que si un host no aparece a la primera vez añadido a la red, el problema puede ser uno de los archivos de configuración. También puede deberse a una tarjeta de interfaz de red defectuosa. Si solo un host genera problemas, puede ser causado por la interfaz de red y si los hosts de una red pueden comunicarse entre sí pero no con otras redes, podría estar la falla en la otra red o en el enrutador.

Puede usar el comando “ifconfig” para obtener información sobre interfaces de red. El comando “netstat” se utiliza para ver las estadísticas de protocolo y tablas de enrutamiento. Existen otros programas de diagnóstico que proporcionan varias herramientas de resolución de problemas.

Los problemas que afectan al rendimiento de la red no son fáciles de identificar y se pueden usar herramientas como “ping” para evaluar problemas como la pérdida de paquetes de un host.[44]

3.2 Comprobaciones de Software de Red Básicas

1. Dentro del sistema local tome el rol de administrador de red o superusuario.
Estas funciones deben incluir comandos con privilegios y autorizaciones.
Nota: Para obtener más información sobre las funciones, consulte *Configuring RBAC (Task Map)* de *System Administration Guide: Security Services*.
2. El comando netstat sirve para ver información de red.
Nota: Sintaxis e información sobre netstat, consulte Supervisión del estado de la red con el comando netstat y la página del comando man netstat (1M).

[44] Consejos De Resolución De Problemas Generales De Red. [En línea]. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipconfig-138/index.html. 14 marzo 2016.

3. La base de datos hosts debe ser comprobada (en Solaris 10 11/06 y versiones anteriores, la base de datos ipnodes, si utiliza IPv6) para comprobar que las entradas estén correctas y actualizadas.

Nota: Para información sobre la base de datos /etc/inet/hosts, se recomienda consultar el siguiente link: Base de datos hosts y hosts (4). Información sobre la base de datos /etc/inet/ipnodes, consulte Base de datos ipnodes y la página de comando man ipnodes(4).

4. Usando protocolo RARP (Reverse Address Resolution Protocol), se comprueba las direcciones Ethernet de la base de datos ethers para verificar que las entradas son correctas y actualizadas.
5. En este paso prosigue el conectarse al host local con el comando telnet.

Nota: para conocer mas sintaxis e información sobre telnet, consulte la página de comando man telnet (1).

6. Comprobación del daemon de red inetd se esté ejecutando.

```
# ps -ef | grep inetd
```

El siguiente resultado verifica que el daemon inetd se está ejecutando:

```
root 57 1 0 Apr 04 ? 3:19 /usr/sbin/inetd –s
```

7. Si IPv6 está activado en la red, compruebe que el daemon IPv6 in.ndpd se esté ejecutando:

```
# ps -ef | grep in.ndpd
```

El siguiente resultado verifica que el daemon in.ndpd se está ejecutando:

```
root 123  1 0  Oct 27 ?  0:03 /usr/lib/inet/in.ndpd
```

3.3 El enrutador IPv4 no puede actualizarse a IPv6

Para solucionar los problemas de actualización de equipos, es posible pensar en la solución de adquirir un equipo más actualizado y preparado para IPV6, ya que aunque suena lógico, a veces equipos obsoletos no son compatibles con el nuevo protocolo.

En ocasiones, algunos enrutadores IPv4 no permiten actualizarse al protocolo más reciente, por ende al conectar un enrutador IPv6 junto con uno de IPv4, soluciona este problema, transmitiendo datos desde un enrutador a otro mediante un túnel.

Nota: Para información sobre tareas relacionadas con la configuración de túneles, se encuentra en Tareas de configuración de túneles para compatibilidad con IPv6 (mapa de tareas).

3.4 Identificar si el Router es Compatible con IPv6

Actualmente los sistemas operativos, servidores web, aplicaciones personales y bases de datos, necesitan pasar a IPv6 para ser compatibles con el resto del mundo; conocer si el router es compatible viene siendo el primer paso de este proceso.

Inicialmente, se ha de constatar que el router es compatible con IPv6 fácilmente visitando *testmyipv6.com*, al ingresar al enlace de “IPv6-only Test”, rápidamente se identifica si el router y todo lo demás están listos para la gran transición. Desafortunadamente, si el PC falla la prueba, no hay manera de saber si el router es el culpable, dentro de las posibilidades cabe que el ISP aún no sea capaz de soportar IPv6.

Si la prueba mencionada no confirma si el modem está listo o no, se revisaran las especificaciones publicadas del router (verificación con el fabricante). Dado el caso que no sea posible encontrar el término IPv6 en las especificaciones del fabricante, se puede asumir que eventualmente será obligatorio el cambio del router.

En el caso de tener previsto la compra de elementos nuevos, se recomienda adquirir un router que ya esté listo para IPv6 con el objeto de ahorrar tiempo y dinero.[45]

3.4.1 Habilitando IPv6 en los Routers: El caso de los routers Juniper ya viene con routing IPv6 habilitado y para el caso de Cisco IOS debemos utilizar los comandos globales.

Comandos Globales

```
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
!
```

Para habilitar IPv6 en una interfaz para un router Juniper:

```
Interface fe-0/0/1 {
unit 0{
family inet6{
address 2001:DB8:C003:1001::1/64;
```

[45] IPV6 MX. ¿Cómo saber si mi router es compatible con IPv6? [En línea]. Disponible en http://www.ipv6.mx/index.php/informacion/ fundamentos/ipv4/100

```
            }
        }
}
```

Para asignar una dirección IPv6 a una interfaz en Cisco IOS:

```
Interface GigabitEhternet1/1
Description Interface de Blackbone
Ipv6 address 2001::DB8:C008:1001::1/64
```
[46]

3.5 Problemas tras la actualización de servicios a IPv6

En la preparación de servicios para que admitan IPv6 puede encontrarse situaciones tales como:

- Algunas aplicaciones, aunque se conviertan a IPv6, no activan IPv6 de manera predeterminada. Es posible que sea necesario configurar estas aplicaciones para activar IPv6.
- La configuración en el servidor se pude presentar cuando se ejecutan varios servicios al mismo tiempo, tales como servicios de solo IPv4 y otros IPv4 e IPv6 simultáneos, causando confusión en el servidor o múltiples errores.

3.6 El ISP actual no admite IPv6

En caso de que el proveedor ISP no ofrezca direcciones IPv6, las siguientes alternativas ofrecen una solución para usar IPv6 sin cambiar de proveedor:

- Una solución algo más costosa es contratar otro proveedor ISP para que proporcione una segunda línea para las comunicaciones IPv6 de su empresa.
- Crear un túnel desde sus oficinas, a través del ISP IPv4, a un ISP virtual, el cual proporciona conectividad IPv6 sin vínculo.
- Usar un túnel 6to4 a través de un ISP hacia otros sitios con IPv6, pero se usa direcciones IPv4 registradas del enrutador 6to4 como sección pública de la dirección IPv6.

[46] CICILEO Guillermo, GAGLIANO Roque, O´FLAHERTY Christian, MOALES Cesar, MARTÍNEZ Jordi, ROCHA Mariela & MARTÍNEZ Alvaro.IPv6 Para Todos. Guía de uso y aplicación de diversos entornos. IPv6 1ª Ed. Buenos Aires: Asociación Civil Argentinos en Internet, 2009,5.3 Configuraciones. Pág. 142

3.7 Consideraciones y Técnicas de Migración IPv6

Teniendo en cuenta que todo el internet se está ejecutando e redes IPv4, la implementación hacia el IPv6 no es tarea fácil, por ende a continuación se presentan algunos de los retos que enfrentamos actualmente como parte de la migración.

- Las bases de clientes de proveedor de servicio actualmente se ejecutan en red IPv4, cualquier nuevo cliente puede estar basada en IPv6. Para ello es necesario que el núcleo SP maneje tanto los clientes IPv4 e IPv6 sin comprometer el rendimiento.

- Las nuevas aplicaciones de negocio se desarrollan en base a IPv6, pero las aplicaciones actuales están basados en IPv4, debido a esto, se requiere que al menos por unos años, la red IPv4 e IPv6 debe coexistir e inter comunicarse sin afectación de rendimiento.

A continuación se nombran técnicas de migración que se pueden utilizar para coexistir entre los diferentes protocolos:

1. Técnica de doble pila.

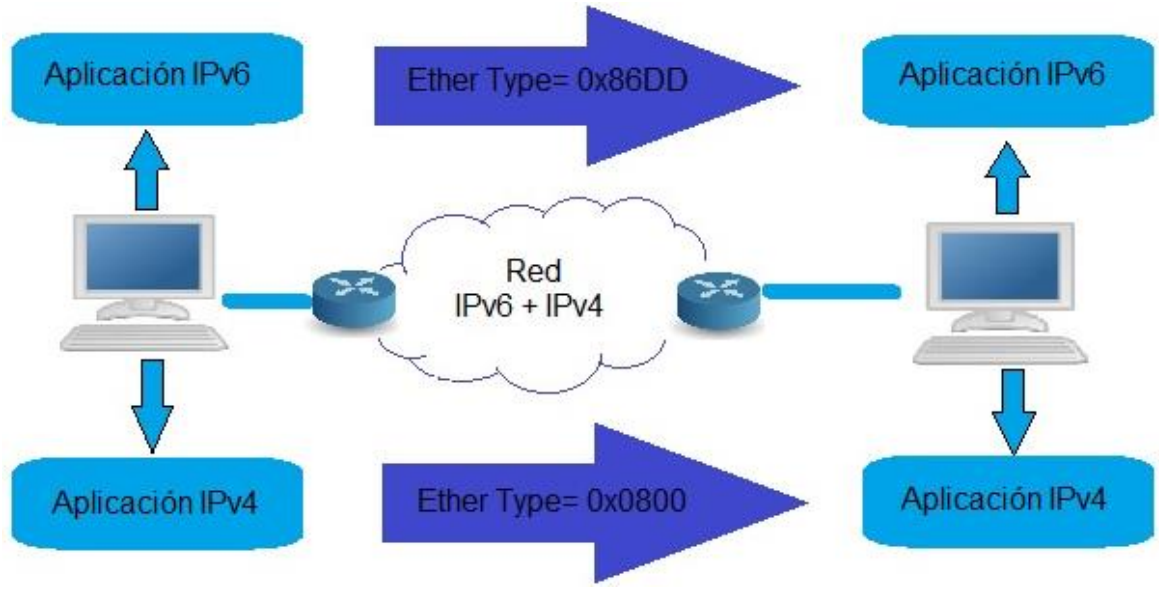
2. Técnica de traducción de protocolo.

3. Técnica de túnel.

3.7.1 Dual Stack Technique (técnica de doble pila): Doble Pila dual es una posible técnica de migración que implica la ejecución de los protocolos IPv4 e IPv6 al mismo tiempo extremo a extremo. Esto implica habilitar todas las aplicaciones para estar al tanto de IPv4 e IPv6 y la pila de protocolos de red de extremo a extremo se ejecuta IPv4 e IPv6 pila de protocolos.

Cualquier comunicación de datos de la aplicación de IPv6 en el host final serán interpretados por el IPv6 pila de protocolos en la capa de red y enviarán con Ether type como 0x86DD. Cada router en la recepción lo entenderá como IPv6 basada en Ether type y será tratado de acuerdo como pila de protocolos IPv6. Lo mismo continúa “end to end” y ambos protocolos IPv4 e IPv6 podrán comunicarse entre sí. La no intercomunicación entre IPv6 e IPv4 es posible con la técnica de doble pila.

Figura. 18 Dual Stack Technique



Fuente: Autor

Gestión del riesgo

Las direcciones de cada equipo aumentan y hablando a nivel de gestión de seguridad hay que considerar que su equivalente son los filtros y medidas que antes aplicaban únicamente para IPv4 habrá que aplicarlas en las direcciones de los equipos IPv6.

Así mismo y teniendo en cuenta que gran parte de los desarrollos en IPv6 fueron creados para ser usados por defecto y dado el caso de no estar disponible, se emplearía su versión anterior, verificando que la información que se mantiene en DNS se encuentre actualizada y junto con todos sus aspectos de seguridad.

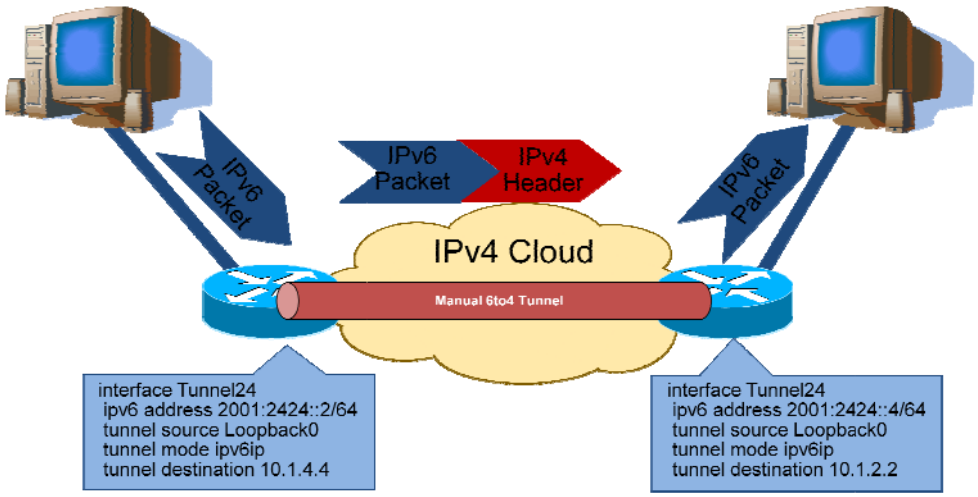
3.7.2 Técnica del túnel: El tunneling básicamente proporciona una forma de usar una infraestructura de nivel de red existente para realizar un protocolo de capa de red diferente. Por ejemplo, IPX a través de la red IPv4, IPv6 sobre IPv4 red.

Túneles en IPv6 es la forma de transporte de paquetes IPv6 sobre IPv4 infraestructura mediante la encapsulación de paquetes IPv6 con cabecera IPv4. Esta técnica de túnel bien puede ser manual o automática. Túneles semiautomáticos también se pueden establecer utilizando aproximación Tunnel Broke. Como parte de la migración, la situación también puede darse en el caso de paquetes IPv4 pueden necesitar ser encapsulados sobre infraestructura IPv6.

En una técnica de visión de túnel más amplio se pueden clasificar como:

Túnel IPv6 sobre infraestructura IPv4.
Túnel IPv4 sobre infraestructura IPv6.

Figura. 19 Tunneling



Fuente: https://supportforums.cisco.com/.../41441-IPv6_Migration.pdf

3.7.3 Técnica de traducción de protocolo (Protocol Translation Technique): Como parte de la migración, es posible afrontar con IPv4 situación en la que el cliente puede tener que comunicarse con los servidores IPv6 y viceversa. Las soluciones anteriormente discutidas pueden ayudar en la migración de IPv4 a IPv6 a la red pero no aborda el requisito de comunicación directa entre dominios IPv4 e IPv6. A continuación, algunas soluciones que se utilizan para la traducción.

NAT-PT es una herramienta traductor de protocolo legado que ayudó a tener una comunicación bidireccional entre dominios IPv4 e IPv6.

NAT-PT router se activará con la regla de conversión, ya sea estática o dinámica programada en el router. La traducción estática necesita una configuración manual de “one to one” traducción de direcciones entre IPv4 e IPv6. Por ejemplo, si un paquete IPv6 pasa a ser enviado al dominio IPv4, el router NAT-PT se mostrará en la tabla y obtendrá la dirección IPv4. Para este caso, es necesario que se configure de forma estática y volver a escribir la misma dirección antes de enviarla al dominio IPv4. Dado que la regla de conversión es bidireccional, cualquier tráfico

inverso puede utilizar la misma regla y volver a escribir con la dirección IPv6 al enviar al dominio IPv6.

La regla de conversión dinámica es mediante la asignación de prefijo IPv6 de 96 bits para el proceso de NAT. Cualquier paquete IPv4 que sea enviado al dominio IPv6 se reescribe con la dirección IPv4 bit prefijo IPv6 96 + embedded, todo debe estar en dirección de IPv4 pero re direccionado como IPv6 de 128 bits.

NAT-PT está desfasada oficialmente por el RFC 4966 debido a problemas operacionales y por lo tanto no se recomienda para cualquier nueva aplicación.

NAT64 es un traductor que permite la comunicación de host IPv6 a Internet IPv4. NAT64 es la sustitución de NAT-PT y actualmente se recomienda para el despliegue y desarrollo. Como parte de la transición a IPv6, a continuación están las cuatro posibles situaciones que requieren traducción de direcciones.[47]

Interoperación entre la red IPv6 e IPv4 red Internet

- Red IPv6 a internet IPv4.
- Internet IPv4 a IPv6 Red

Interoperación entre redes IPv4 e IPv6 Internet

- Red IPv4 a internet IPv6
- Internet IPv6 a la red IPv4

Interoperación entre Internet IPv6 e IPv4 de Internet

- IPv6 de Internet IPv4 a internet
- Internet IPv4 a IPv6 de Internet

3.8 Seguridad en Transmisión de Datos por Medio de Túnel a Enrutador de Reenvío 6to4

En materia de seguridad existe cierta inseguridad dentro de un túnel entre un enrutador 6to4 y un enrutador de reenvío 6to4, debido a que un túnel de este tipo siempre tendrá los siguientes problemas:

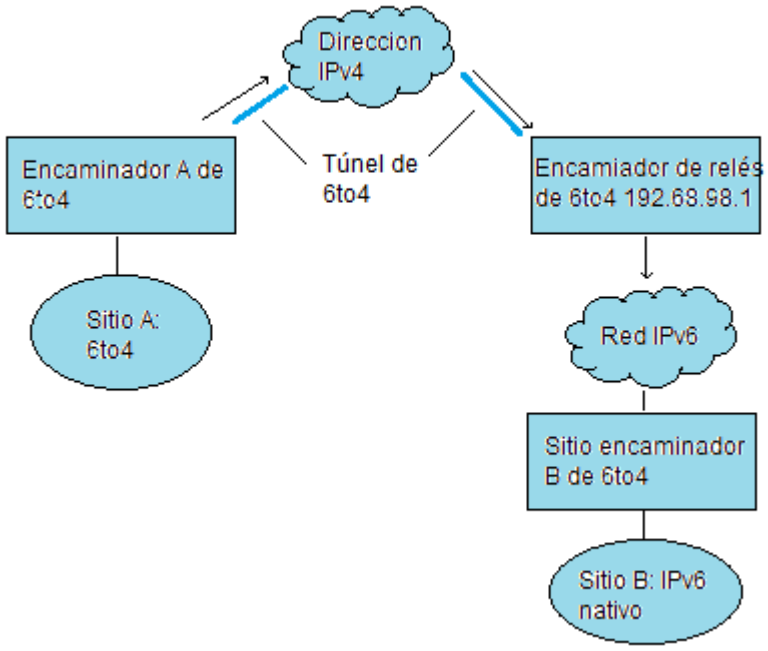
- Los enrutadores de reenvío 6to4 encapsulan y desencapsulan paquetes y a pesar de ello no hay comprobación de los datos que contienen los paquetes.
- Existe el problema de falseamiento de direcciones de los túneles a los enrutadores de reenvío 6to4. El enrutador 6to4 no puede comparar la dirección

[47] IPv6 Migration Document. Técnicas de Migración IPv6. [En Línea]. Pág. 1-15. Disponible https://supportforums.cisco.com/.../41441--IPv6_Migration.pdf

IPv4 del enrutador de reenvío del tráfico entrante con la dirección IPv6 del origen generando esta brecha de seguridad para el falseamiento de la dirección del host IPv6 y la dirección del enrutador de reenvío 6to4.

- Debe existir confiabilidad entre el sitio 6to4 y el destino IPv6, ya que ambos sitios quedan expuestos a un ataque. No existe ningún mecanismo de confianza entre enrutadores 6to4 y enrutadores de reenvío 6to4 de manera automática, por ende un enrutador 6to4 no puede identificar saber si el enrutador de reenvío 6to4 es de confianza, ni determinar si es un enrutador de reenvío 6to4 legítimo.

Figura. 20 Túnel desde una ubicación 6to4 hasta un enrutador de reenvío 6to4



Fuente: Autor

En el documento *Security Considerations for 6to4* hay información más detallada sobre estos problemas anteriormente mencionados y otras cuestiones de seguridad de los enrutadores de reenvío 6to4.

El activar la admisión de enrutadores de reenvío 6to4 solo se recomienda en caso de:

- Intentar comunicarse con una red privada IPv6 de confianza desde su ubicación 6to4. Como por ejemplo, el activar la admisión de enrutadores 6to4 en una red universitaria que consiste en ubicaciones 6to4 aisladas e IPv6 nativas.
- Ubicar de manera apropiada 6to4 por motivos importantes de negocios para comunicarse con ciertos hosts IPv6 nativos.
- Ejecución de comprobaciones y modelos de confianza, para lo cual el documento de Internet *Security Considerations for 6to4* tiene más detalles.[48]

3.9 Problemas comunes con un enrutador 6to4

Las configuraciones 6to4 son afectadas por los siguientes problemas:

- 4709338 - Implementación necesaria de RIPng que reconozca enrutadores estáticos.
- 4152864 – Configuración posible de dos túneles con el mismo par tsrc/tdst .

3.10 Firewalling IPv6 CISCO

Con el soporte de IPv6, el servidor de seguridad CISCO inspecciona ambos paquetes, tanto el IPv4 e IPv6 en los routers con pilas duales y estos routers que pueden inspeccionar los paquetes de ambos protocolos son llamados dual stack routers. Esta característica también proporciona soporte MIB para TCP, UDP, ICMPv6 y sesiones de FTP.

1. Restricciones para IPv6 IOS Firewall: el sistema de detección de intrusiones de Cisco IOS (IDS) no es compatible con IPv6.

2. Información acerca de IPv6 IOS Firewall: la característica de Cisco IOS Firewall proporciona una funcionalidad avanzada de filtrado de tráfico como una parte integral del servidor de seguridad de una red. Cisco IOS Firewall para IPv6 le permite implementar redes IPv6 y puede coexistir con Cisco IOS Firewall para redes IPv4 junto con todos los routers de doble pila.

Entre sus grandes características:

Permite inspección de paquetes fragmentados, el fragmento de cabecera es usado para activar el procesamiento de fragmentos. En Cisco IOS Firewall,

[48] ORACLE. Guía de administración del sistema: servicios IP. El ISP actual no admite IPv6, Problemas comunes con un enrutador 6to4, Cuestiones de seguridad al transmitir datos mediante túnel a un enrutador de reenvío 6to4. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-1/index.html

reensamblaje de fragmentos virtual (VFR), se examinan fragmentos fuera de secuencia y conmuta los paquetes en el orden correcto, examina el número de fragmentos de una sola dirección IP dado un identificador único (denegación de servicio ataque [DoS]) y realiza virtuales remontaje para mover los paquetes a los protocolos de capas superiores.

Existe la mitigación de ataques de denegación de IPv6. Estos procedimientos de mitigación se han implementado del mismo modo que en la implementación de IPv4, incluyendo SYN conexiones medio abiertas.

De inspección de paquetes de túnel, tunelizando paquetes IPv6 termina en un firewall router Cisco IOS, el cual puede ser inspeccionado por el firewall Cisco IOS para IPv6.

Inspección de paquetes, cuya característica proporciona la inspección de estado de paquetes de TCP, UDP, control de mensajes de IP versión 6 (ICMPv6) y sesiones de FTP.

La inspección de estado de paquetes procedentes de la red IPv4 y que termina en un entorno IPv6, esta función utiliza los servicios de traducción de IPv4 a IPv6.

Interpretación o el reconocimiento de la mayoría de la información de cabecera de extensión IPv6. La función proporciona información de encabezado de extensión IPv6 incluyendo enrutamiento de cabecera, encabezado opciones hop-by-hop y el fragmento de cabecera es interpretado o se reconocen.

Mapeo de puerto a la aplicación (PAM). Cisco IOS Firewall para IPv6 incluye PAM.

PAM en Cisco IOS Firewall para IPv6

PAM permite personalizar los números de puerto TCP o UDP para los servicios de red o aplicaciones y utiliza esta información para apoyar los entornos de red que se ejecutan en los servicios que utilizan puertos y que son diferentes de los puertos registrados o conocidos con una aplicación.

Utilizando la información del puerto, PAM establece una tabla de información de asignación predeterminada de puerto a la aplicación en el servidor de seguridad. La información de la tabla PAM permite basarse en el contexto de control de acceso (CBAC) servicios compatibles para ejecutarse en puertos no estándar. CBAC se limita a la inspección del tráfico usando solamente los puertos conocidos o registrados asociados con una aplicación, mientras PAM permite a los administradores de red puedan personalizar el control de acceso a la red para aplicaciones y servicios específicos.

PAM también es compatible con la asignación de puertos o-subred específica en host, lo que le permite aplicar a un único host o subred utilizando ACL estándar. Host o con la asignación de puertos-subred específica se hace uso de las ACL estándar.

Cisco IOS Firewall virtual pistas de auditoría y registro del sistema

Con Cisco IOS Firewall se genera alertas en tiempo real y pistas de auditoría basados en los eventos registrados por el servidor de seguridad. Características mejoradas de seguimiento de auditoría utilizan el registro del sistema para rastrear todas las transacciones de la red; para registrar las marcas de tiempo, fuente de acogida, host de destino y puertos utilizados y para registrar el número total de bytes transmitidos de informes avanzados, basados en la sesión.

Estas alertas en tiempo real envían mensajes de error de registro del sistema para las consolas de administración central cuando el sistema detecta actividad sospechosa. Usando las reglas de inspección Firewall Cisco IOS, puede configurar alertas e información de auditoría sobre una base per-protocolo de aplicación. Por ejemplo, si desea generar información de seguimiento de auditoría para el tráfico TCP, puede especificar la generación de esta información en la regla de firewall Cisco IOS que define la inspección TCP.

Este Cisco IOS Firewall proporciona mensajes de seguimiento de auditoría para registrar los detalles sobre las sesiones inspeccionados. Estas pistas de auditoría son configurables en función de cada aplicación que utilizan las reglas de inspección CBAC. Para determinar cuál es el protocolo fue inspeccionado, utilice el número de puerto asociado con el que responde. El número de puerto aparece inmediatamente después de la dirección.

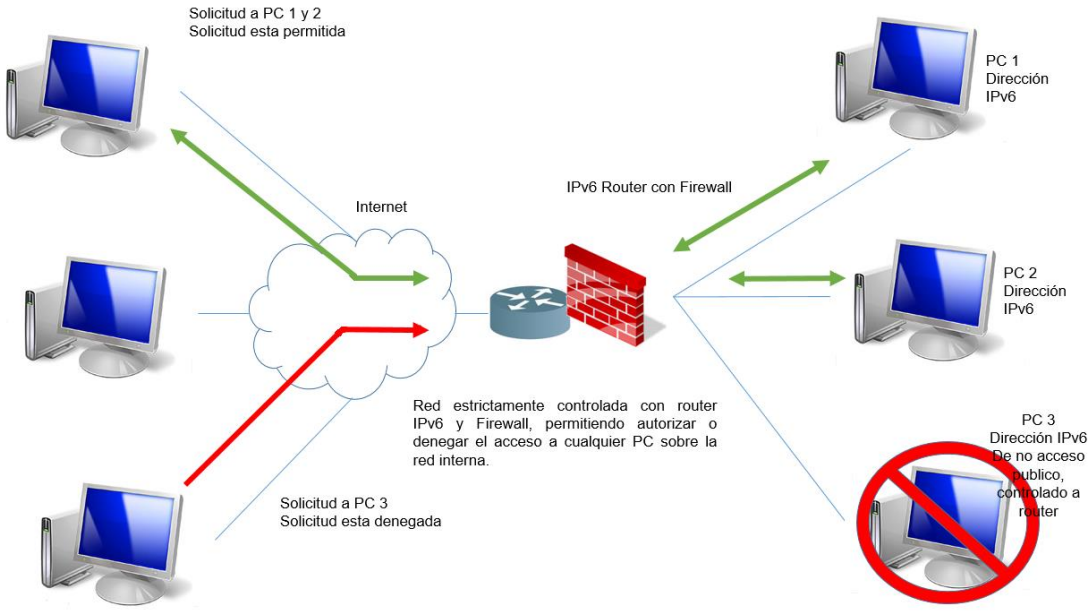
IPv6 Packet Inspection (Inspección de Paquetes): los siguientes campos de cabecera son utilizados para la inspección de IPv6: flow label, payload length, next header, hop limit, and source or destination address. Para más información y descripciones de los campos de la cabecera IPv6, revise RFC 2474.

Soporte de túnel: Los paquetes IPv6 en túnel IPv4 no se inspeccionan. Si un túnel termina en un router y el tráfico IPv6 que va a salir del túnel está sin terminación, entonces se inspecciona el tráfico.

Virtual reensamblaje de fragmentos: cuando se habilita la VFR, este procesamiento comienza después de listas de entrada de ACL, se comparan con

los paquetes entrantes y estos son etiquetados con la información apropiada VFR.[49]

Figura. 21 Red controlada con router IPv6 y firewall.



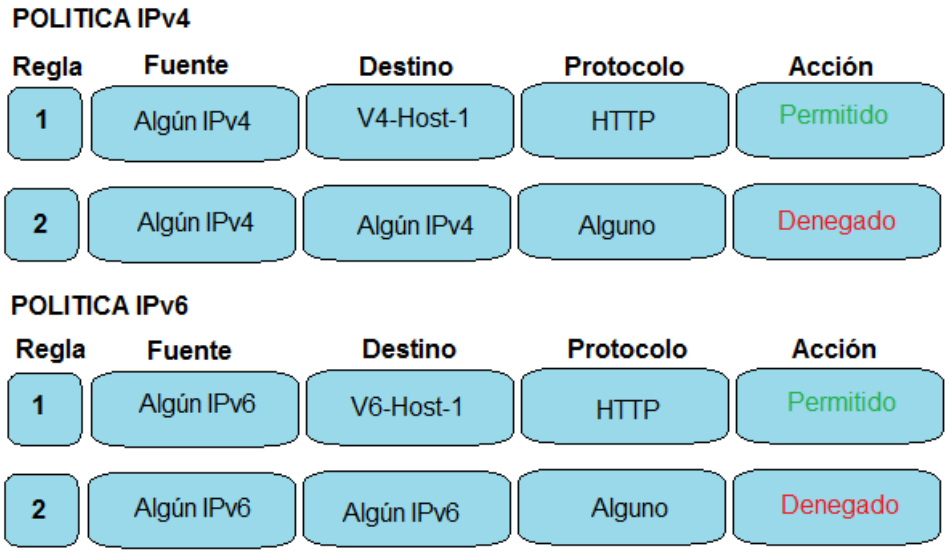
Fuente: Autor

3.11 Políticas de Contrafuegos IPv6

Existe la particularidad de que la mayoría de los servidores de seguridad tienen políticas separadas para IPv4 e IPv6 (esto es cierto para el Cisco ASA). Estos utilizan de forma separada el “ip access-list" y "ipv6 lista de acceso" comandos para definir la política y luego se utiliza "access-group", comandos aplicados para listas IPv4 o IPv6 de acceso a la interfaz y la dirección apropiada. La siguiente figura muestra cómo se ve lógicamente similares y como hay dos políticas separadas. Los objetos IPv4 se usan sólo en la política IPv4 y los objetos IPV6 sólo se utilizan en la política IPv6.

[49] IPv6 IOS Firewall. Restricciones y Características. [En línea]. Disponible en http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_cbac_fw/configuration/15-2mt/ip6-firewall.html. 10 mayo 2016.

Figura. 22 Políticas de contrafuegos IPv4 e IPv6



Fuente: Autor

La ventaja de esta técnica radica en que se puede ver fácilmente cómo su política de IPv6 crece con el tiempo como su despliegue de IPv6 crece. Se puede ver fácilmente los permisos para especificar un host IPv6 y puede estar seguro de que sólo está permitiendo el acceso IPv6 requerido para ese host. Con el tiempo, la política de IPv6 crecerá similar en tamaño a la política de IPv4. Cada una de las dos políticas es "la primera coincidencia" en la naturaleza y para que solamente se pueda ver la lógica de la política sólo IPv6 o políticas de IPv4. Sin embargo, la desventaja de este enfoque es que finalmente tendrá el doble de trabajo para llevar a cabo cualquier nueva adición al entorno. Deberá recordar hacer cambios iguales a las políticas de IPv4 e IPv6, lo cual podría llegar a ser difícil de solucionar si se ha añadido un objeto de dirección IPv4 para un servidor, pero si se olvida añadir el objeto de dirección IPv6 para el servidor y ahora no se sabe porque los paquetes IPv6 están siendo bloqueados.

Hay algunos servidores de seguridad que tienen una sola política combinada que contiene objetos de IPv4 e IPv6 en una lista combinada de reglas. Hosts IP o redes se pueden definir usando cualquiera de las direcciones IPv4 o IPv6. Estos objetos pueden ser también host, convertirse en redes o grupos de otros objetos.

Ejemplos de servidores de seguridad como Check Point y Palo Alto Networks cortafuegos utilizan solo una única política de cortafuegos para IPv4 e IPv6.[50]

La administración de las políticas de Firewall IPv6 y la planeación del despliegue de IPv6 se deben pensar en conjunto, teniendo en cuenta como se adaptara la propia convención de nombre de objeto para objetos IPv6 y cómo se va a crear reglas para hosts o redes IPv6. Un análisis previo se hace necesario antes de la creación de muchas reglas que no puedan organizarse de la manera deseada y tomar decisiones con la cual se va a convivir entre sus redes dentro de los próximos 30 años.

3.12 Discovery and Scanning IPV6

A pesar de que muchas empresas, organizaciones, proveedores de servicios y fabricantes han hecho el cambio hacia el IPv6, este podría ser el año en que cada uno de los que no han tomado la iniciativa de migrar, realmente se puedan quedar sin direcciones de internet, como comienza a presentarse en Asia y Europa.

3.12.4 Descubrimiento a través de direcciones de Multidifusión: El IPv6 no es compatible con el protocolo de resolución de direcciones (ARP) para convertir de direcciones IP a la dirección MAC. En IPv6, la resolución se realiza a través de un proceso de petición de descubrimiento de la red y de descubrimiento de red. El descubrimiento de red (Network Discovery) utiliza ICMPv6 para determinar qué direcciones de enlace local son activos en la subred de la red local.

Mediante el envío de ICMPv6 a la dirección de multidifusión local de enlace, nuestro paquete alcanzará todas las direcciones locales de vínculo activo en la red. La RFC 3513 nos dice que direcciones de multidifusión FF02::1 pueden utilizarse para enviar un paquete a todas las direcciones locales de vínculo activo (link local address). Para enumerar las direcciones locales de vínculo activo, se utiliza PINGv6 como se muestra a continuación.

```
ipv6host ~> ping6 –I eth0 -c 5 ff02::1 > /dev/null 2>&1
ipv6host ~> ip neigh|grep ^fe80
fe80::21e:c9ff:fedb:9fbf dev eth0 lladdr 00:1e:c9:db:9f:bf REACHABLE
```

Van Hauser en su IPv6 Toolkit proporciona una herramienta para encontrar una dirección IPv6 activo llamado alive6. (Hauser, 2008). También se puede utilizar para encontrar las direcciones locales de vínculo activos en la red.

[50] HOGG Scott (2012). Network World. CISCO Subnet. The future of Firewall Policies. 19 junio 2012. Disponible en http://www.networkworld.com/article/2221507/cisco-subnet/cisco-subnet-the-future-of-firewall-policies.html. 10 Mayo 2016

```
./alive6 eth0
Warning: unprefered IPv6 address had to be selected
Alive: fe80::21e:c9ff:fedb:9fbf
Found 1 system alive
```

Con el fin de evitar la enumeración IPv6 dirección de enlace local, se desactiva el IPv6 desde el sistema por completo si no es necesaria. En una red IPv6 única y para evitar que alguien pueda enumerar la dirección local de vínculo activo utilizando ping6, hay que denegar los entrantes de solicitud de eco ICMPv6 (ICMPv6 Tipo 128) (IANA, 2011) destinados a FF02 :: 1 desde el servidor de seguridad de IPv6 en el dispositivo. Por otra parte, la dirección de enlace local IPv6 se puede eliminar manualmente desde el sistema, actualmente no hay manera de desactivar desde la interfaz de forma permanente.

3.12.5 Discovery a través de ICMPv6 Solicitud (ICMPv6): El método de detección anterior, se utiliza para encontrar las direcciones locales de enlace de la red local dentro de una subred. ¿Cómo se puede descubrir la dirección IPv6 de unidifusión global en un host de Internet? THC IPv6 Toolkit, alive6, se puede utilizar para encontrar la dirección IPv6 de unidifusión global, pero está limitada dentro de una subred. Con el fin de descubrir la dirección IPv6 unicast global activa, el método más simple es utilizar ping6 que envía una solicitud de eco ICMPv6. La dirección IPv6 activa, debe responder a ICMPv6 respuesta de eco (ICMPv6 Tipo 129) (IANA, 2011). El desafío consiste en encontrar la dirección IPv6 en el gran espacio de direcciones IPv6 en el prefijo de red IPv6. Por esta razón, tenemos que encontrar otra manera de hacer la enumeración de IPv6 sin necesidad de utilizar el prefijo de red. Otra forma es construir una enorme lista de direcciones IPv6 utilizando script en Perl llamado como buildipv6.pl. Este script Perl es una versión modificada de la herramienta en ipv6-HackIT (Pilihanto, 2010) publicada en SourceForge.

```
#!/usr/bin/perl
#Modification of buildipv6.pl part of ipv6-hackit
# Written for GSEC GOLD certification by Atik Pilihanto | datacomm.co.id
#Save as buildipv6.pl
use strict;
use warnings;
sub str2hex()
{
my($bit) = @_;
my ($bitlo,$bithi);
if($bit =~ /-/){
my @atbit=split('-',$bit);
if(hex($atbit[0]) > hex($atbit[1])){
print "ERR! Hexal value at right of \'-\' must be higher than at left\n";
exit;
```

```
}
$bitlo = $atbit[0];
$bithi = $atbit[1];
}else{
$bitlo= $bit;
$bithi= $bit;
}
return($bitlo,$bithi);
}
if(!$ARGV[0]){
print "USAGE:\n";
print "perl $0 <IPv6 Address Range>\n";
print "Ex=> perl $0 2046:f0af-f0ff:0a0a:c000-c010:0:0:0:1\n";
exit;
}
my ($c1,$c2,$c3,$c4,$c5,$c6,$c7,$c8);
open(IPv6,">ipv6.out");
my @allbit = split(':',$ARGV[0]);
if (scalar(@allbit) !=8){
print "ERR! You have to enter all 128-bit and can not use \'::\'\n";
exit;
}
my ($bit1lo,$bit1hi) = &str2hex($allbit[0]);
my ($bit2lo,$bit2hi) = &str2hex($allbit[1]);
my ($bit3lo,$bit3hi) = &str2hex($allbit[2]);
my ($bit4lo,$bit4hi) = &str2hex($allbit[3]);
my ($bit5lo,$bit5hi) = &str2hex($allbit[4]);
my ($bit6lo,$bit6hi) = &str2hex($allbit[5]);
my ($bit7lo,$bit7hi) = &str2hex($allbit[6]);
my ($bit8lo,$bit8hi) = &str2hex($allbit[7]);
for($c1=hex($bit1lo);$c1<=hex($bit1hi);$c1++){
for($c2=hex($bit2lo);$c2<=hex($bit2hi);$c2++){
for($c3=hex($bit3lo);$c3<=hex($bit3hi);$c3++){
for($c4=hex($bit4lo);$c4<=hex($bit4hi);$c4++){
for($c5=hex($bit5lo);$c5<=hex($bit5hi);$c5++){
for($c6=hex($bit6lo);$c6<=hex($bit6hi);$c6++){
for($c7=hex($bit7lo);$c7<=hex($bit7hi);$c7++){
for($c8=hex($bit8lo);$c8<=hex($bit8hi);$c8++){
printf ("%X:%X:%X:%X:%X:%X:%X:%X\n",$c1,$c2,$c3,$c4,$c5,$c6,$c7,$c8);
printf (IPv6 "%X:%X:%X:%X:%X:%X:%X:%X\n",$c1,$c2,$c3,$c4,$c5,$c6,$c7,$c8);
}
}
}
}
}
}
}
}
close(IPv6);
```

Con el fin de utilizar el script Perl anteriormente mencionado, se ejecuta el script sin pasar ningún argumento en la línea de comandos. Este ejemplo proporciona una guía de cómo crear una lista de direcciones IPv6 que será escrito en el archivo de salida llamado ipv6.out

```
ipv6host ~> perl buildipv6.pl
USAGE:
perl buildipv6.pl <IPv6 Address Range>
Ex=> perl buildipv6.pl 2046:f0af-f0ff:0a0a:c000-c010:0:0:0:0
ipv6host ~> perl buildipv6.pl 2001:44B8:8000-8100:FF00:0:0:0:80
(Edited/cutted)
2001:44B8:80FE:FF00:0:0:0:80
2001:44B8:80FF:FF00:0:0:0:80
2001:44B8:8100:FF00:0:0:0:80
ipv6host ~> ls -l ipv6.out
-rw-r--r-- 1 root root 7453 Aug 30 02:20 ipv6.out
Ipv6host ~>
```

En cuanto a la numeración de la dirección IPv6 que aparece en ipv6.out se puede hacer con ping6, que está disponible por defecto en muchas distribuciones de Linux. Con el fin de enumerar un gran número IP, ping6 se puede llamar desde un script en Perl llamo como isalive6.pl

```
#!/usr/bin/perl
#Taken from isalive6.pl part of ipv6-hackit
# Written for GSEC GOLD certification by Atik Pilihanto | datacomm.co.id
#Save as isalive6.pl
use strict;
use warnings;
use Switch;
use POSIX;
my $LOGFILE = "isalive6.log";
my $MAX_CHILD = 100;
MAIN:
{
my @IPV6LIST;
if(!$ARGV[0]){
print "usage : perl $0 <IPv6 List File>\n";
exit;
}
open(LIST,"<$ARGV[0]") or die();
chop(@IPV6LIST=<LIST>);
my $len = @IPV6LIST;
my $i = 0;
my $j = 0;
while ($j <= $len-1){
switch (fork()){
case (0) { doping6($j,$IPV6LIST[$j]);_exit(0); }
case (-1) { print "Can not fork!\n";_exit(-1); }
```

```
else {
if($i>$MAX_CHILD-2){
wait();
$i--;
}
}
}
$i++;$j++;
}
print "Total Host Scanned : " . scalar(@IPV6LIST) . "\n";
close(LIST);
}
sub doping6
{
my($tid,$ipv6host) = @_;
open(OFILE,">>$LOGFILE");
my @pinglist = `ping6 -c2 -s0 $ipv6host`;
my $result = "@pinglist";
if($result =~ m/8 bytes from/){
print $tid . " : [REACHED] " . $ipv6host . "\n";
print OFILE "[REACHED]" . $ipv6host . "\n";
}else{
print $tid . " : [NOT REACHED] " . $ipv6host . "\n";
}
close(OFILE);
}
```

La razón para crear la secuencia de comandos Perl anteriormente mencionado, es que el *nmap ping* actualmente sólo es compatible con el IPv6 objetivo. Para utilizar este script Perl, se corre desde la línea de comandos de Linux y se proporciona la lista de direcciones IPv6 construido por buildipv6.pl. La salida se guardará en el archivo isalive6.log que contiene la dirección IPv6 activa.

```
ipv6host ~> perl isalive6.pl ipv6.out
32 : [REACHED] 2001:44B8:8020:FF00:0:0:0:80
96 : [REACHED] 2001:44B8:8060:FF00:0:0:0:80
0 : [NOT REACHED] 2001:44B8:8000:FF00:0:0:0:80
1 : [NOT REACHED] 2001:44B8:8001:FF00:0:0:0:80
2 : [NOT REACHED] 2001:44B8:8002:FF00:0:0:0:80
(edited/cutted)
ipv6host ~> ls -l isalive6.log
-rw-r--r-- 1 root root 76 Aug 30 03:04 isalive6.log
ipv6host ~> cat isalive6.log
[REACHED]2001:44B8:8020:FF00:0:0:0:80
[REACHED]2001:44B8:8060:FF00:0:0:0:80
ipv6host ~>
```

Para evitar la enumeración de direcciones IPv6, es necesario deshabilitar IPv6 desde el sistema por completo si no se necesita. Si IPv6 se utiliza en la red de producción, para evitar que alguien enumere la dirección IPv6 activo utilizando ping6, necesitamos negar la *solicitud de eco ICMPv6 de entrada* (ICMPv6 tipo

128) usando el firewall. Muy a menudo, ping6 se utiliza para ayudar en el proceso de resolución de problemas, por lo tanto, debe existir cautela al denegar la solicitud de eco ICMPv6 por razones de seguridad o de tal modo que dé solución al problema de red. Una mejor idea es utilizar un sistema de detección de intrusiones (IDS) para detectar ocurrencias de ping IPv6 barrido en la red.[51]

3.13 Aspectos de seguridad en la implementación de IPv6

En una red ya configurada, no se pretende poner en riesgo la seguridad del sitio al implementar IPv6 durante las fases sucesivas; a continuación se mencionan aspectos relacionados con la seguridad:

- Para los paquetes de IPv6 e IPv4 necesitan la misma cantidad de filtrado.
- A veces los paquetes de IPv6 pasan por un túnel a través de un cortafuego, por ende aplica alguno de los siguientes casos hipotéticos:

    - ❖ Ejecutar el cortafuego para que inspeccione el contenido del túnel.
    - ❖ Colocar un cortafuego de IPv6 con reglas similares en el punto final del túnel del extremo opuesto.
- Establecer mecanismos de transición utilizan IPv6 en UDP a través de túneles de IPv4. Dichos mecanismos pueden resultar nocivos al cortocircuitarse el cortafuego.
- Los nodos de IPv6 son mundialmente asequibles desde fuera de la red empresarial. Si una directiva de seguridad prohíbe el acceso público, se debe establecer reglas más apropiadas con relación al cortafuego, por ejemplo, podría configurar un cortafuego con estado.

Este párrafo informa sobre las funciones de seguridad válidas en la implementación de IPv6.

- La función de IPsec facilita protección criptográfica de paquetes IPv6. Para obtener más información el Capítulo 19 Arquitectura de seguridad IP (descripción general).
- Para la función IKE (Internet Key Exchange, intercambio de claves en Internet) facilita la autenticación de claves públicas para paquetes de IPv6. Para mayor

[51] PILIHANTO Atik (2011). SANS Institute InfoSec Reading Room. A Complete Guide on IPv6 Attack and Defense. Disponible en https://www.sans.org/.../complete-guide-ipv6-attack-defense-339. Pág. 14-20. 20 mayo 2016.

información, existe el Capítulo 22 Intercambio de claves de Internet (descripción general).[52]

3.14 Seguridad IPv6 en Plataforma CISCO

Con el ánimo de administrar el tiempo y los recursos, CISCO contribuye a mejorar estos aspectos dando prioridad a las redes o negocios, escalando más allá de las limitaciones vividas en IPV4. CISCO genera un enfoque mejorado en su plataforma con la adopción de IPv6, como solución por experiencia y capacidades en el ofrecimiento de servicios para el descubrimiento, la planeación, diseño IPv6 y la optimización de servicios de red.

A continuación se describen los problemas de seguridad más comunes y como se solventan teniendo en cuenta las adopciones y mejoras de CISCO.

Configuración de un túnel un protocolo IPv6: teniendo en cuenta el túnel un protocolo IPv6 de información de enrutamiento (RIP) y una red IPv6 Border Gateway Protocol (BGP) y el tráfico a través de una red IPv4 preexistente. Esta técnica le permite conectar los sitios IPv6 a través de la columna vertebral IPv4 existente. Se hace un encapsulado superpuesto de los paquetes IPv6 en paquetes IPv4 para la entrega a través de una infraestructura IPv4. Esto es similar a la forma de crear un túnel de encapsulación de ruta genérica (GRE) para transportar el tráfico de intercambio de paquetes entre redes (IPX) a través de una red IP. En el extremo de la cabeza del túnel, un paquete IPv6 se encapsula en paquetes IPv4 y se envía al destino del túnel remoto. Aquí es donde se elimina la cabecera del paquete IPv4 y el paquete original IPv6 se reenvía además en una nube de IPv6.

Estos son los cinco métodos de tunelización tráfico IPv6:

- Túneles IPv6 manuales
- Los túneles automáticos IPv4-Compatible
- GRE
- Túneles de 6to4
- Dentro de un sitio direccionamiento automático de túnel Túneles (ISATAP) Protocolo

Lo que marca la diferencia entre las técnicas de tunelización, consiste en la manera de seleccionar el método de fuente del túnel y de destino, por

[52] ORACLE. Guía de administración del sistema: servicios IP. Aspectos relacionados con la seguridad en la implementación de IPv6. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-1/index.html

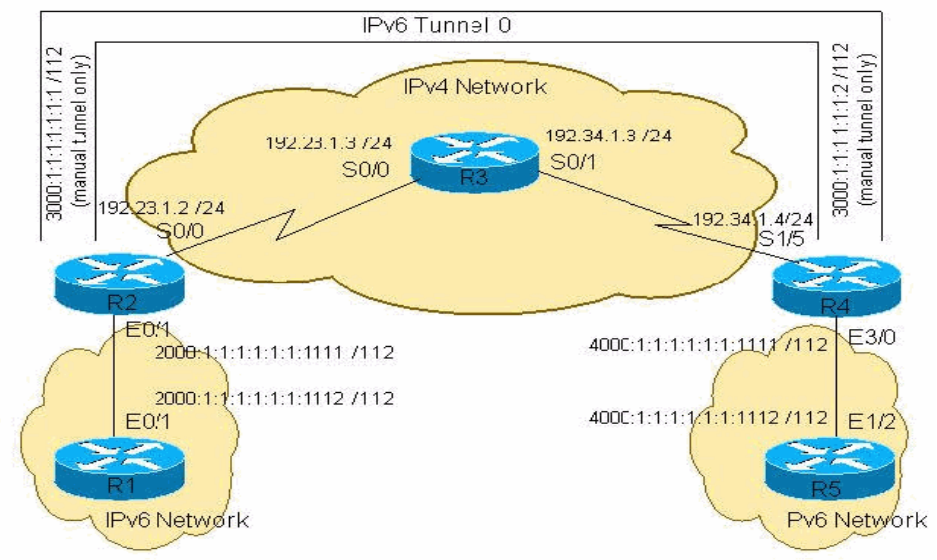
consiguiente, en esta guía mostramos varios tipos de túneles compatibles con IPv6 de manera manual o automática.

Nota: Existen múltiples maneras de creación de túneles para este caso, pero los túneles de superposición reducen la unidad de transmisión máxima (MTU) de una interfaz de 20 octetos. Esto supone que la cabecera básica paquete IPv4 no contiene campos opcionales. Una red que utiliza túneles de superposición es difícil de solucionar. Por lo tanto, túneles de superposición que conectan redes IPv6 aislados no deben ser considerados como una arquitectura de red IPv6 final. El uso de túneles de superposición debe ser considerada como una técnica de transición hacia una red que soporta tanto las pilas de protocolos IPv4 e IPv6 o sólo apilar el protocolo IPv6.

3.14.6 Requisitos previos: La empresa Cisco recomienda que tenga conocimiento de IPv6 antes de intentar esta configuración. Para reforzar este conocimiento es posible consultar la implementación del IPv6 Direccionamiento y la conectividad básica sobre IPv6.

3.14.7 Diagrama de Red: En esta sección se expone esta configuración de la red.

Figura. 23 Diagrama de Red



Fuente: http://www.cisco.com/c/en/us/support/docs/ip/ip-version-6/25156-ipv6tunnel.html#intro

3.15 SSH sobre un transporte del IPv6

SSH en IPv6 e IPv4 funciona lo mismo y ofrece las mismas ventajas. Una de las múltiples características del servidor SSH, es que le permite a un cliente SSH

hacer un seguro y establecer una conexión encriptada a un router Cisco, junto con conexiones encriptadas dirigidas a routers diferentes de esta marca. Una de las mejoras en IPv6 para SSH, consta del soporte para los direccionamientos del IPv6, permitiendo que un router Cisco trabaje sobre un transporte del IPv6 realizando y validando conexiones encriptadas en los nodos remotos del IPv6.[53]

3.16 SNMP sobre un transporte del IPv6

El SNMP o Simple Network Management Protocol, como protocolo de capa de aplicación, proporciona un esquema de mensaje para la comunicación de administradores SNMP y es configurado sobre el transporte del IPv6, de manera que un host de este protocolo realiza las interrogaciones SNMP común y recibe las notificaciones SNMP de un Cisco IOS Software IPv6. Actualmente se ha reforzado este agente SNMP y el MIB para soportar la dirección del IPv6.[54]

Como dato adicional, el AES (Advanced Encryption Standard) se ofrece como la solución para el cifrado del mensaje y el SNMP para el IPv6 proporciona el 3DES.

[53] CISCO. Implementar el IPv6 para la Administración de redes. SSH sobre un transporte del IPv6. (2 agosto 2014). Disponible en http://www.cisco.com/cisco/web/support/LA/111/1116/1116309_ip6-mng-apps.html

[54] CISCO. Implementar el IPv6 para la Administración de redes. SNMP sobre un transporte del IPv6. (2 agosto 2014). Disponible en http://www.cisco.com/cisco/web/support/LA/111/1116/1116309_ip6-mng-apps.html

4. SEGURIDAD DE IPV6 EN LOS CENTROS DE DATOS

Los centros de datos juegan un papel importante en el momento de implementar IPv6 en las organizaciones, al ser los ejes centrales de todas las operaciones tecnológicas de la empresa, por lo tanto tal y como se menciona en muchas organizaciones, donde existen varias formas de operar e introducir IPv6 en Centros de Datos. Una manera es continuando con una operación IPv4 dentro del centro de datos y hacer algún tipo de translación en el borde u otra forma es usar únicamente IPv6 o usar la pila doble.

En síntesis existe:

- Pila Doble: La pila doble está en los que prestan servicios a usuarios o a través todos los servicios del centro de datos. Del mismo modo pueden encontrarse pila doble en el borde mientras que las conexiones internas son IPv4 o IPv6 únicamente.
- Translación de IPv4 en el borde: El centro de datos mantiene su infraestructura interna en IPv4 y hace algún tipo de rotación a IPv6 en el borde.
- Solo IPv6: Es la etapa final de la transición de un centro de datos a IPv6 con todos sus elementos. Se usa la traslación en el borde para ofrecer servicios a los usuarios legados de IPv4.

La utilización de estos contextos no necesariamente es en la forma secuencial descrita anteriormente y tampoco ninguna es la mejor, la correcta o la recomendada, ofrecen diferentes ventajas y desventajas que deben ser examinadas para seleccionar la mejor opción.

La mayoría de las propiedades de seguridad de IPv6 se emplean en los centros de datos[55], sin embargo, un aspecto significativo son los ataques a Neighbor Discovery Protocol (NDP). Este ataque consiste en terminar con la memoria del enrutador provocando la inhabilidad de éste para reenviar paquetes, similar a los ataques de ARP de IPv4 e incluso el atacante puede llenar el caché de host vecinos.[56]

[55] Operational Security Considerations for IPv6 Networks, draft-ietf-opsec-V6. Chittimageni, K., Kaeo, M., And E.Vyncke.2013

[56] Tomado de http://portalipv6.lacnic.net/wp-content/uploads/2015/02/ipv6_operadores_red-tablets.pdf, IPv6 para operadores de red, Alejandro Acosta, Santiago Aggio y otros; Internet Society ISO-AR Capítulo Argentina, pág. 83

5. DIEZ CONSEJOS PARA IMPLEMENTAR IPV6 DE FORMA SEGURA

De acuerdo con la empresa Stonesoft[57], quienes con su credibilidad demostrada dentro del marco de rentabilidad y aplicabilidad, advierten sobre múltiples engaños sufridos a empresas en cuanto a la complejidad que rodea la seguridad en IPv6; se permiten compartir varios consejos de seguridad en IPv6 en despliegue a gran escala para su implementación y mitigación de riesgo.

1. Esbozar una introducción gradual: Manteniendo el control del presupuesto asignado para la larga tarea de implementar el nuevo protocolo y de acuerdo a muchas entidades y administraciones públicas que ya llevan experiencia en IPv6, una completa implementación solo pueda darse al menos por medio de tres fases, las cuales pueden tomar un tiempo promedio de seis años. No es estrictamente necesario tomarse el mismo tiempo que las grandes compañías o incluso el gobierno, pero si introducir gradualmente IPv6 generará el tiempo suficiente para garantizar que el protocolo funcione con el estado similar o mejorado visto en la infraestructura de IPv4.

2. Desactivar capacidades IPv6: Al apagar las capacidades IPv6 cuando no están siendo usadas aumenta el grado de seguridad, dificultando que los sinnúmero de intrusos o programas no deseados ingresen a la red, solo por el hecho de haber sido configurados para trabajar con IPv6 o que tengan el protocolo de encendido por defecto. Es recomendable una revisión de entorno de manera periódica, con el objeto de asegurarse de que IPv6 sólo está disponible cuando realmente se necesite. Otra recomendación sería la instalación de mecanismos con la capacidad de deshabilitar IPv6.

3. Revisar la construcción de estructuras (Sintaxis): La sintaxis IPv6 es muy parecida a la usada por IPv4, pero existen grandes diferencias en su fundamentación. Al conocer la sintaxis es más sencillo de manejar cualquier brecha de seguridad existente o implementación de cualquier medida. Debido a que el IPv6 ya se encuentra rodando en nuestras redes, hay poca información por parte de entes tecnológicos o incluso buenas guías por internet, siendo buen momento para leer esta guía.

4. Adoptar y/o renovar un firewall certificado: La cautela en los anuncios relacionados con la compatibilidad con IPv6 no sobrará, debido a que sin una revisión, es posible que cualquier proveedor haya colocado un generador de

[57] Stonesoft es una empresa que realiza negocios de gestión centralizada a nivel mundial, con agrupamiento de activos en USA, EUROPA y ASIA, la cual vende soluciones de seguridad de red, establecida en Helsinki, Finlandia y fue fundada desde el 2013 con el inicio del protocolo IPv6. Ha trabajado con Intel y McAfee.
https://www.forcepoint.com/product/network-security/forcepoint-stonesoft-next-generation-firewall

tráfico en su producto e informe que trabaja sin problema. Ahora bien, en los productos que hayan sido objeto de certificación por terceras partes, se debe centrar mucho la atención, pues pueden utilizar pruebas prácticas con métodos de evaluación públicamente aceptados para asegurarse de que el usuario sepa clara y precisamente que es lo que es lo que firewall puede manejar.

5. Autenticar: Siendo esto lo más crucial y más complicado a la vez, las grandes empresas como Stonesoft recomienda que se considere el empleo de un proxy HTTP/HTTPS, con el objeto de que los usuarios accedan a internet y una vez establecida para acceder incluso online, se puede decir que se ha disminuido la amenaza de terceros no deseados o sistemas que pretenda ingresar a la red sin aprobación.

6. Inclinación por la doble /pila/apilado: Otra recomendación que no sobra es la de optar por el método de doble apilado en la fase de implementación en IPv6. Este método trae consigo múltiples beneficios, debido a que consta de requerimientos de actualización del router por motivo de lograr las peticiones necesarias de memoria y potencia, junto con la bondad de soportar el funcionamiento simultáneo de IPv4 e IPv6.

7. Rejuvenecer la red existente: Es sinónimo de acicalar la red IPv4, eliminando lo inservible y actualizándola hasta hacerla casi nueva. Depurar y organizar las características desfasadas y desactualizadas, para garantizar que cada aspecto de la red que no esté considerado como competente en su siguiente nivel, quede completamente eficiente a lo largo de su nivel apropiado.

8. Inspección de tráfico y túneles: Las publicaciones como "Directrices para un seguro despliegue del protocolo IPv6", dadas por el Instituto Nacional Americano de Estándares y Tecnología, reflexiona sobre los túneles, los cuales son tratados como un link externo (mucha precaución) y recomienda inspeccionar cada fragmento de tráfico de túnel antes de tolerar datos en la salida o entrada del sistema.

9. Cautela y recelo con lo malicioso: Se ha de continuar con la alerta alta, no se puede descuidar los anuncios y advertencias sobre los peligros latentes en routers o ataques de suplantación, tales como “hombre en el medio” entre otros, ya que los usuarios maliciosos también se están infiltrando en el protocolo IPv6, desde el mismo instante de su creación.

10. Saber decir “si” o “No”: en cualquier red puede presentarse la problemática de visitas de IPv6 no deseado, incluso cuando la red tiene el IPv6 deshabilitado, pero es imperante el conocer como eliminar la amenaza antes de que infecte a

otros asociados de la red. Para ello la compresión de sintaxis IPv6 es de gran ayuda, facilitando la instalación de firewall más eficientes, filtros de tráfico o creación de filtros de acceso para determinar qué es lo que se desea aceptar o que es lo que se desea tener lejos.[58]

[58] MINTIC. Protocolo de Internet Versión 6. Diez consejos para implementar IPv6 de forma segura. Tomado de http://www.mintic.gov.co/portal/604/w3-article-5866.html. 02 febrero 2016.

6. PRUEBAS DE PENETRACIÓN EN REDES IPV6

Lo primero es tener en cuenta las siguientes consideraciones antes de iniciar un proceso de pruebas de penetración sobre redes IPv6:

- Adquirir información: se inicia con la recopilación de información previa y verídica para generar pruebas de penetración exitosas, tales como el direccionamiento IP, dominios de red, cuentas del directorio activo, nombres de personas, infraestructura de las tecnologías de la información, fijación del alcance de las actividades de inspección, obtención de información de la intranet junto con los sitios web, información de corporaciones anexas, grupos de noticias incluyendo las redes sociales o páginas web personales a las cuales aplique, metadatos, entre otros, rescatando que no es necesario seguir este mismo orden.

- Reconocer la red: se debe analizar la red sobre la cual se trabaja y sus múltiples anexos, desde el estudio del manejo de DNS, búsqueda de reversas, hasta la obtención de información pública descuidada a través de herramientas de búsqueda disponibles. Ubicar las rutas de acceso y la topología de la red.

- Recopilación pasiva: es la recopilación de información de fuentes confiables, ya que sería contraproducente para cualquier empresa el no obtener información a través de medios legítimos disponibles en internet, pudiendo afectar su prestigio y veracidad de la información recopilada.

- Obtención de información pública disponible: Página web de la organización, ubicación física, personas de contacto, sucesos, políticas de seguridad, archivos con información legendaria, exfuncionarios descontentos, foros, ofertas de empleo.

- Evocar nombres de dominio en internet: se contempla el direccionamiento IPv6 junto con los parámetros de protocolos y números de puertos.

- Recopilación activa: Ataques de enumeración, fuerza bruta, hacer búsquedas de dominio y subdominios, transferencia de zonas DNS, consulta de servidores DNS existentes, búsquedas inversas de DNS, ingeniería social.

- Mapeo de red: Se puede hacer el mapeo de red a través del descubrimiento de vecinos, direcciones MAC, topología de red, rastreando puertos (TCP, UDP,

ICMP), descubriendo direcciones IP, determinando la rutas que siguen los paquetes apoyado en herramientas como traceroute, entre otras.

- Instauración de los servicios activos: se hace la averiguación sobre los puertos abiertos en el sistema en cuestión y la búsqueda de puertos en estado de “escucha”.

- Escaneo de puertos: Se requiere hacer exploración de TCP ACK, de TCP FIN, de TCP XMAS, TCP Null, de TCP RPC, de protocolo IP, de UDP. Las comprobaciones de conectividad y funcionamiento del equipo es realizada por el scanner, junto con el estado de servicio, revisión de reglas de contrafuegos y análisis de estructura de red.

- Inspección de los sistemas operativos.

- Evidenciar vulnerabilidades: se requiere actualizar el software a usar, para posterior pasar a la verificación de puertos, puertas traseras y modo de comunicación de túneles.

- La información que arrojen las resultados de las pruebas de penetración, deben manejarse en forma confidencial, para posterior análisis, interpretación y socialización si es el caso.

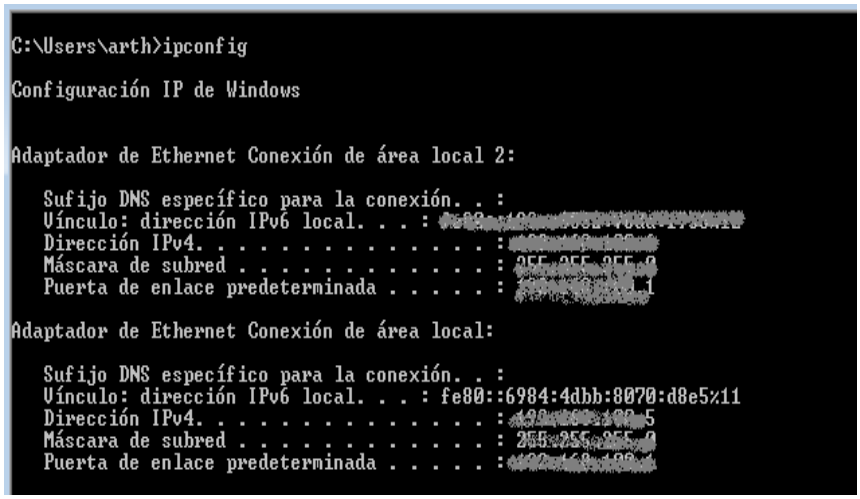
- Se fija un alcance para las pruebas, junto con la puntualización de los recursos asociables y alternativos.

6.7 Seguridad Por Defecto En IPv6

La IPv6 está en todo lados y aun así nadie la conoce del todo, siendo casi todos los Windows vinculados a él, tales como servidores Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2 y Windows Server 2012 viene configurado por defecto con IPv6, por ende con una demostración sencilla, la guía desea mostrarles el trabajo de concientización de riesgo en este protocolo.

Fase 1: Se inicia un Ipconfig en una máquina, Windows o ifconfig si es Ubuntu, para ver que si sale una dirección IPv6.

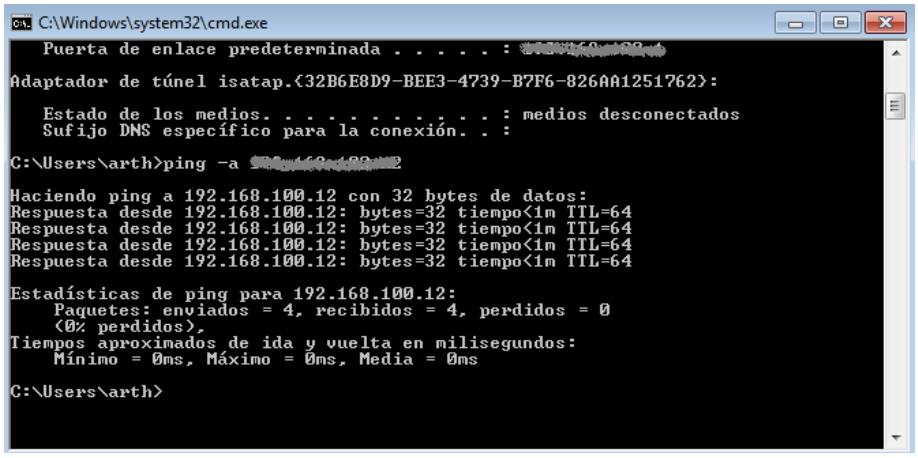
Figura. 24 Ipconfig IPv6 por defecto



Fuente: Autor

Fase 2: Ahora se pasa a un ping -a dirigido a una dirección de cualquier equipo en la red del mismos segmento físico (dato importante) disponible, por ende se aprecia que por defecto el IPv6 no viene configurado con default Gateway, eso se debe efectuar después con un DHCPv6 o RA para atacar a toda la red.

Figura. 25 Ping -a

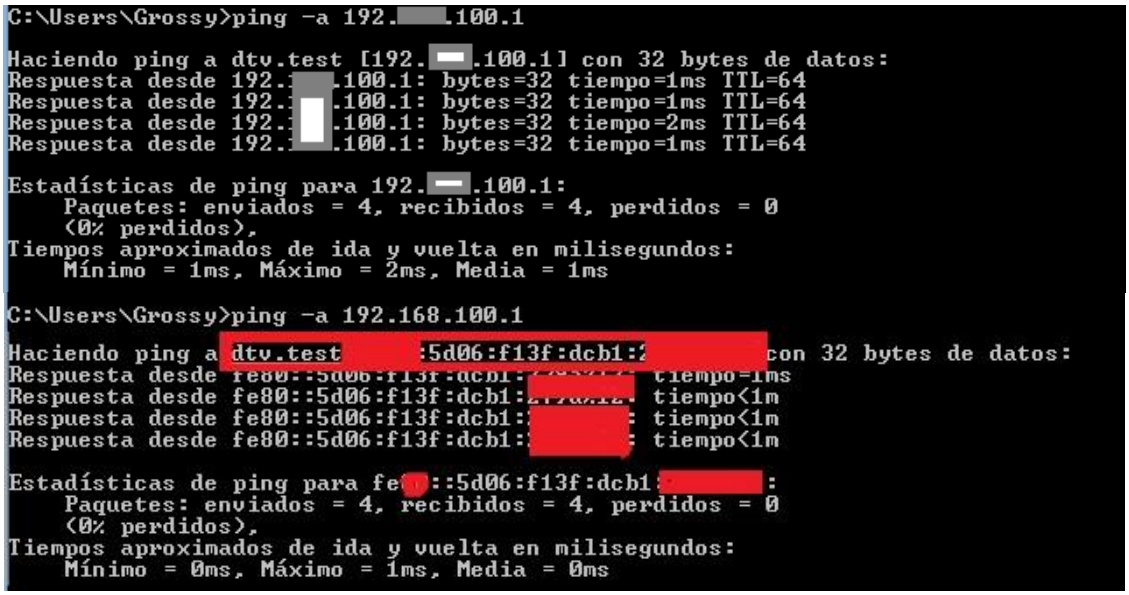


Fuente: Autor

Fase 3: se pasa a realizar un ping al nombre NetBIOS del equipo que ha salido. Preferiblemente no escoger FQDN, por si solo existe un DNS en la red IPv4, esto provoca que el protocolo LLMNR inicie una búsqueda en toda la red sobre todas las direcciones IPv4 e IPv6 asociadas con este nombre, buscando registros A y AAA haciendo uso de los dos tipos de registros en los dos servidores DNS en IPv4

e IPv6. Un resultado positivo sería cuando conteste el equipo en cuestión pero desde la dirección IPv6.

Figura. 26 Ejemplo Ping al nombre del servidor IPv6



Fuente: Autor

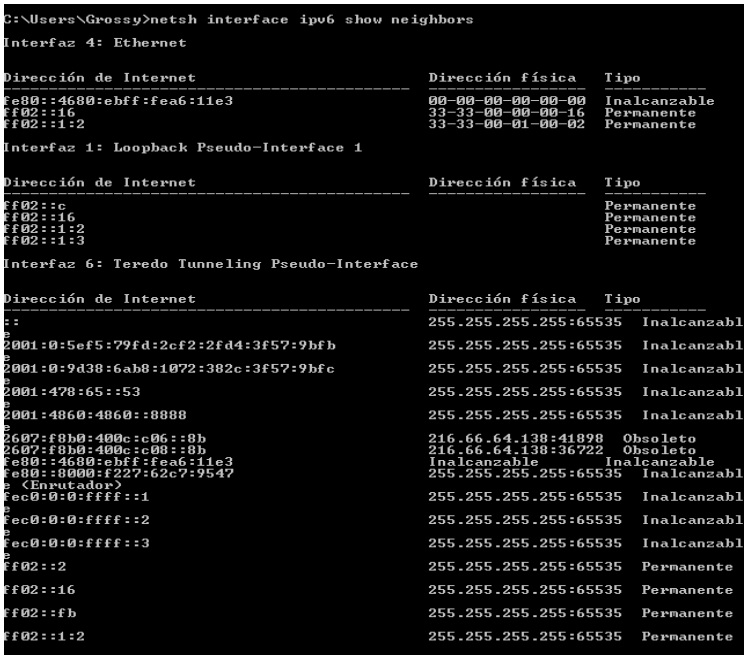
Si en el ordenador esto ha sido posible, entonces se puede apreciar un ataque de Neighbor Spoofing en IPv6 que podrá ser utilizado para robar ficheros SMB y en este caso no es útil monitorear la tabla ARP con arp -a, ya que todo el ataque tiene efecto en la lista de vecinos que puedes ver con *netsh interface ipv6 show neighbors*.[59]

Ahora bien, con este método la red pasa a estar preparada para ser víctima de un ataque, en donde el victimario puede usar un Rogue DHCPv6, DNS AutoDiscovery y SLAACD con el objeto de apoderarse de toda la infraestructura disponible. Por consiguiente, se puede hacer un *route print* para comprobar que no existe ningún Gateway en la tabla de enrutamiento del protocolo IPv6.

Cabe aclarar para quien no este familiarizado que la puerta de enlace se caracteriza con la dirección ::0.

[59] UN INFORMÁTICO EN EL LADO DEL MAL (2013). Disponible http://www.elladodelmal.com/2013/02/te-van-hackear-por-ipv6-por-pensar-que.html. 05 mayo 2016

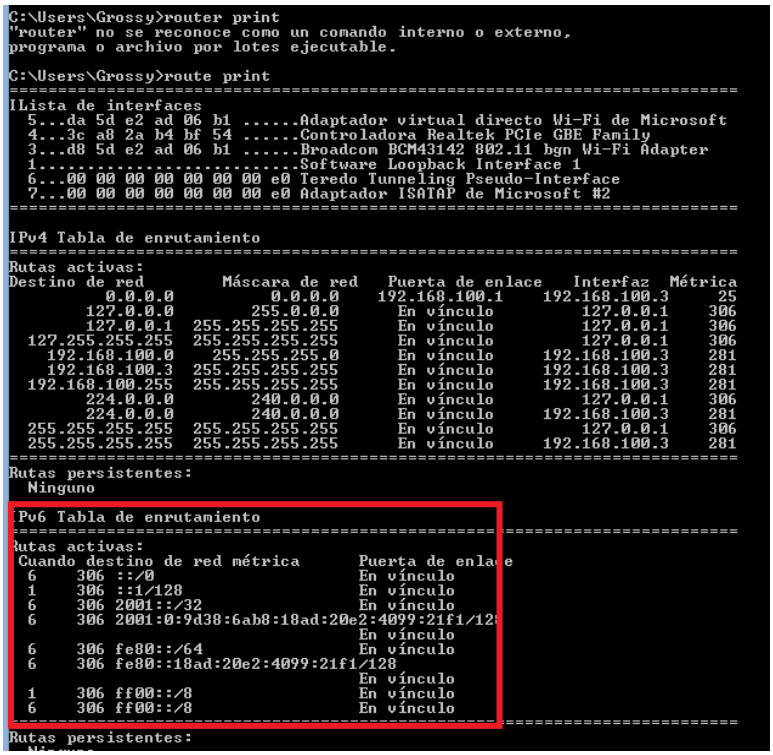
Figura. 27 Comando netsh interface IPv6 show neighbors



```
C:\Users\Grossy>netsh interface ipv6 show neighbors

Interfaz 4: Ethernet

Dirección de Internet                          Dirección física   Tipo
---------------------------------------------  -----------------  -----------
fe80::4680:ebff:fea6:11e3                      00-00-00-00-00-00  Inalcanzable
ff02::16                                       33-33-00-00-00-16  Permanente
ff02::1:2                                      33-33-00-01-00-02  Permanente

Interfaz 1: Loopback Pseudo-Interface 1

Dirección de Internet                          Dirección física   Tipo
---------------------------------------------  -----------------  -----------
ff02::c                                                           Permanente
ff02::16                                                          Permanente
ff02::1:2                                                         Permanente
ff02::1:3                                                         Permanente

Interfaz 6: Teredo Tunneling Pseudo-Interface

Dirección de Internet                          Dirección física   Tipo
---------------------------------------------  -----------------  -----------
::                                             255.255.255.255:65535  Inalcanzabl
e
2001:0:5ef5:79fd:2cf2:2fd4:3f57:9bfb           255.255.255.255:65535  Inalcanzabl
e
2001:0:9d38:6ab8:1072:382c:3f57:9bfc           255.255.255.255:65535  Inalcanzabl
e
2001:478:65::53                                255.255.255.255:65535  Inalcanzabl
e
2001:4860:4860::8888                           255.255.255.255:65535  Inalcanzabl
e
2607:f8b0:400c:c06::8b                         216.66.64.138:41898  Obsoleto
2607:f8b0:400c:c08::8b                         216.66.64.138:36722  Obsoleto
fe80::4680:ebff:fea6:11e3                      Inalcanzable       Inalcanzable
fe80::8000:f227:62c7:9547                      255.255.255.255:65535  Inalcanzabl
e (Enrutador)
fec0:0:0:ffff::1                               255.255.255.255:65535  Inalcanzabl
e
fec0:0:0:ffff::2                               255.255.255.255:65535  Inalcanzabl
e
fec0:0:0:ffff::3                               255.255.255.255:65535  Inalcanzabl
e
ff02::2                                        255.255.255.255:65535  Permanente

ff02::16                                       255.255.255.255:65535  Permanente

ff02::fb                                       255.255.255.255:65535  Permanente

ff02::1:2                                      255.255.255.255:65535  Permanente
```

Fuente: Autor

Figura. 28 Tabla de enrutamiento IPv6 sin puerta de enlace



```
C:\Users\Grossy>router print
"router" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Grossy>route print
===========================================================================
ILista de interfaces
  5...da 5d e2 ad 06 b1 ......Adaptador virtual directo Wi-Fi de Microsoft
  4...3c a8 2a b4 bf 54 ......Controladora Realtek PCIe GBE Family
  3...d8 5d e2 ad 06 b1 ......Broadcom BCM43142 802.11 bgn Wi-Fi Adapter
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
  7...00 00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #2
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0    192.168.100.1     192.168.100.3     25
        127.0.0.0        255.0.0.0       En vínculo         127.0.0.1    306
        127.0.0.1  255.255.255.255       En vínculo         127.0.0.1    306
  127.255.255.255  255.255.255.255       En vínculo         127.0.0.1    306
    192.168.100.0    255.255.255.0       En vínculo     192.168.100.3    281
    192.168.100.3  255.255.255.255       En vínculo     192.168.100.3    281
  192.168.100.255  255.255.255.255       En vínculo     192.168.100.3    281
        224.0.0.0        240.0.0.0       En vínculo         127.0.0.1    306
        224.0.0.0        240.0.0.0       En vínculo     192.168.100.3    281
  255.255.255.255  255.255.255.255       En vínculo         127.0.0.1    306
  255.255.255.255  255.255.255.255       En vínculo     192.168.100.3    281
===========================================================================
Rutas persistentes:
  Ninguno

Pv6 Tabla de enrutamiento
===========================================================================
Rutas activas:
 Cuando destino de red métrica      Puerta de enla e
  6     306 ::/0                    En vínculo
  1     306 ::1/128                 En vínculo
  6     306 2001::/32               En vínculo
  6     306 2001:0:9d38:6ab8:18ad:20e2:4099:21f1/12
                                    En vínculo
  6     306 fe80::/64               En vínculo
  6     306 fe80::18ad:20e2:4099:21f1/128
                                    En vínculo
  1     306 ff00::/8                En vínculo
  6     306 ff00::/8                En vínculo
===========================================================================
Rutas persistentes:
```

Fuente: Autor

6.8 Neighbor Spoofing

Con la migración eventual para IPv6, ARP se está eliminando, esto hace que ARP Spoofing tienda a desaparecer, pero no es del todo cierto, ya que IPv6 pone su confianza en ICMPv6 para muchas de las operaciones realizadas a través de ARP en el campo de IPV4.

El Neighbor Spoofing en redes de datos IPv6 es muy sencillo junto con su impacto, pero debe tenerse en cuenta ya que su funcionamiento es muy parecido al ARP Spoofing y también permite realizar man in the middle.

Básicamente este ataque consiste en enviar mensajes de Neighbor Advertisement (NA) a dos equipos víctimas, poniendo a ambos la dirección IPv6 del otro y la dirección MAC de quien haga las veces de atacante.

Fase 1: se pretende ejecutar es un spoofeando usando una dirección IPv6 de origen de paquetes, simulando un mensaje que viene de un equipo víctima, pero para ambos casos es necesario usar la dirección MAC del atacante, con el objeto de obligar al switch de comunicaciones enviar todos los mensajes a la maquina designada como man in the middle.

Al enviar un mensaje de Neightbor Solicitation (NS) con destino una dirección multicast, se pretende que este establezca una comunicación IPv6 respondiendo al mensaje con un mensaje unicast de Neighbor Advertisement (NA) junto con su dirección física MAC, la cual será almacenada por el receptor en la tabla de vecinos junto con la dirección IPv6 asociada.

Es posible enviar de primero un mensaje NA sin haber recibió el NS, y hacer que en la cache se guarde el registro.

6.9 Man in the Middle IPv6

El protocolo Stateless Address Automatic Configuration (SLAAC), se encarga de la configuración de direcciones IPv6, no por medio del envío de mensajes desde un servidor DHCPv6 como usualmente se hace, sino desde el router de conexión. Por consiguiente, se pretende que en un equipo con una dirección IPv6 de vínculo local no se pueda enrutar su tráfico si no tiene una dirección IPv6 de sitio o global, y es por eso que los routers envían mensajes RA (Router Advertisement) diciéndole a los equipos cómo configurarse para obtener comunicación entre ellos.

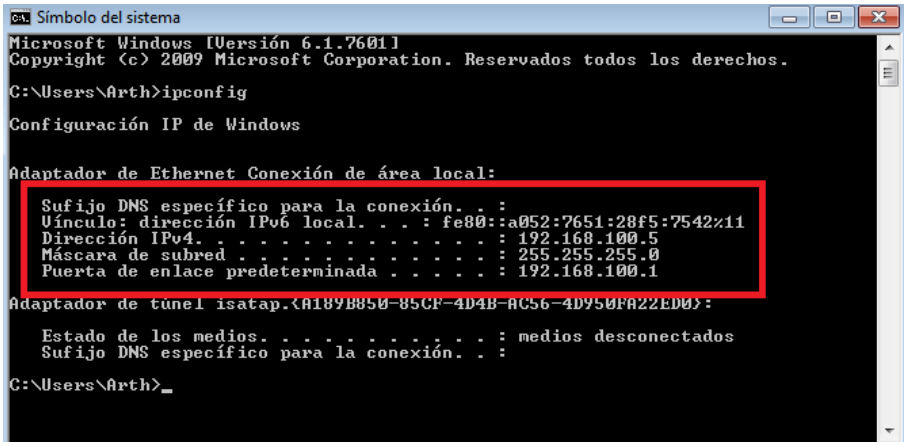
Existe un riesgo que se está implementado como un sistema de Bridging HTTP (IPv6) a HTTPs (IPv4) para poder realizar ataques de man in the middle el cual afecta lugares web en los que supuestamente solo funcionaban bajo HTTPs. Con los mismos principios manejados en el ataque SLAAC, esto funciona en el proceso de autenticación de las redes sociales como Facebook, Twitter o de Tuenti. En esta sección se ejecuta un ejemplo con el login de Tuenti.

Fase 1: El ataque con la Evil FOCA

Este ataque con Evil FOCA no varía mucho de sus anteriores versiones, ya que envía un paquete SLAAC para que el equipo configure la dirección del atacante como puerta de enlace IPv6. Para que esto funcione, es necesario evitar la configuración vía DHCP en el protocolo IPv4 y se ordena con direcciones de vínculos locales.

Utilizando una máquina de W7, se usa el comando ipconfig para determinar nuestra IP, la cual es de IPv4 pero se va a configurar de manera remota a IPv6.

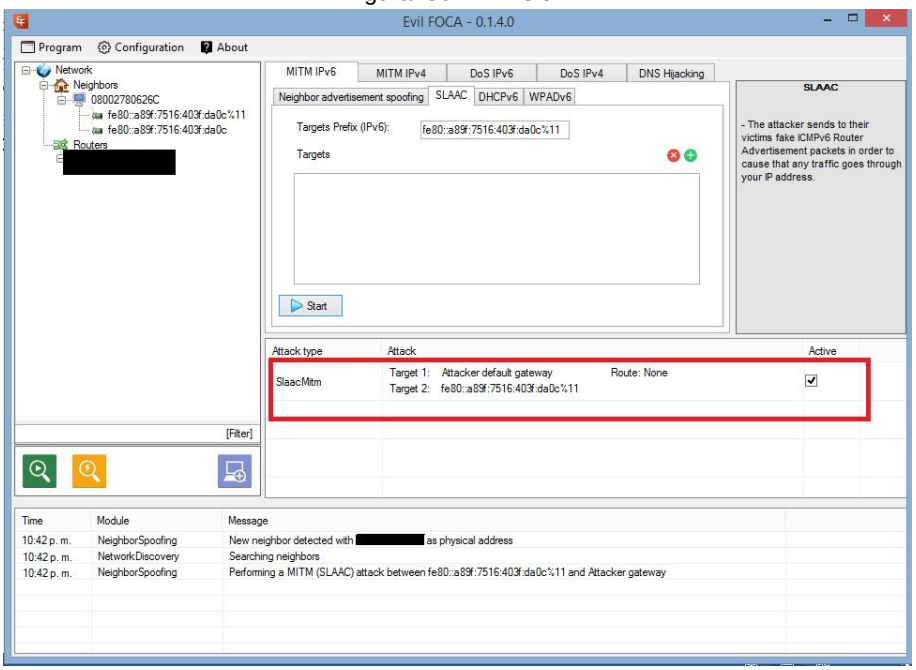
Figura. 29 IP Máquina Virtual



Fuente: Autor

Usando Evil FOCA, se configura el protocolo a IPv6 y en él se puede apreciar que reconoce el protocolo en la red asociado a la máquina virtual previamente configurada y su IP es identificada.

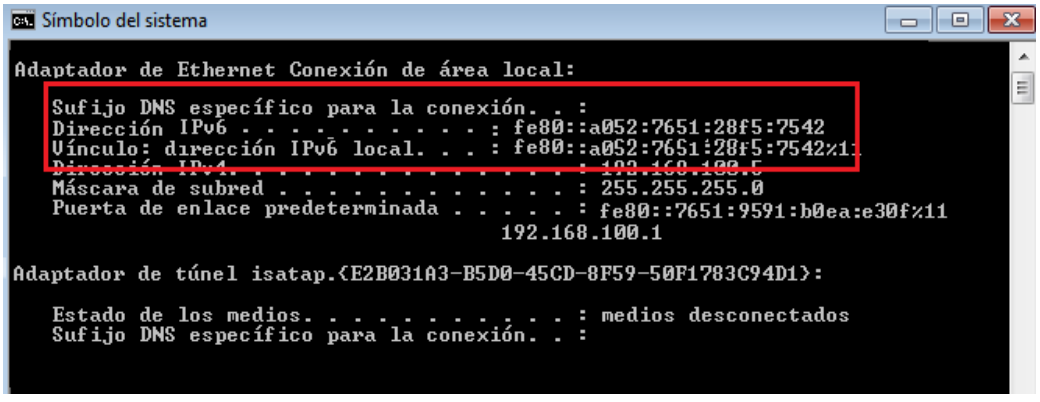
Figura. 30 Evil FOCA



Fuente: Autor

Una vez hecho el ataque con Evil FOCA, es suficiente con observar la configuración proporcionada por la víctima, detectando que posee una configuración de vínculo local en IPv4, configuración de IPv6 de vínculo local y la dirección IPv6 en la tarjeta generada con SLAAC con comunicación con la puerta de enlace, que es la dirección IPv6 del atacante.

Figura. 31 Cambio a IPv6



Fuente: Autor

Debido a que los servidores DNS AutoDiscovery fueron configurados por defecto en IPv6, el Evil FOCA genera una dirección con este protocolo nuevo, haciéndola visible ante las peticiones de resolución por parte del equipo victimado. Se recuerda que para este ejemplo se usa el dominio de www.tuenti.com, pero se puede recurrir a cualquier otro.

Fase 2: Obstaculización de títulos

Evil FOCA data desde la misma creación que el CAIN para protocolo IPv4, pero actualmente se ha centrado en IPv6. Este programa hace el resto del trabajo de manera automática y cada enlace HTTPs, que viene en las páginas HTML de respuesta, sufre un sslStrip, es decir, se le quita la "s", debido a que los vínculos entre quien ataca y quien es la víctima se hacen con HTTP. Así que la negociación de las credenciales de Tuenti irá en claro.

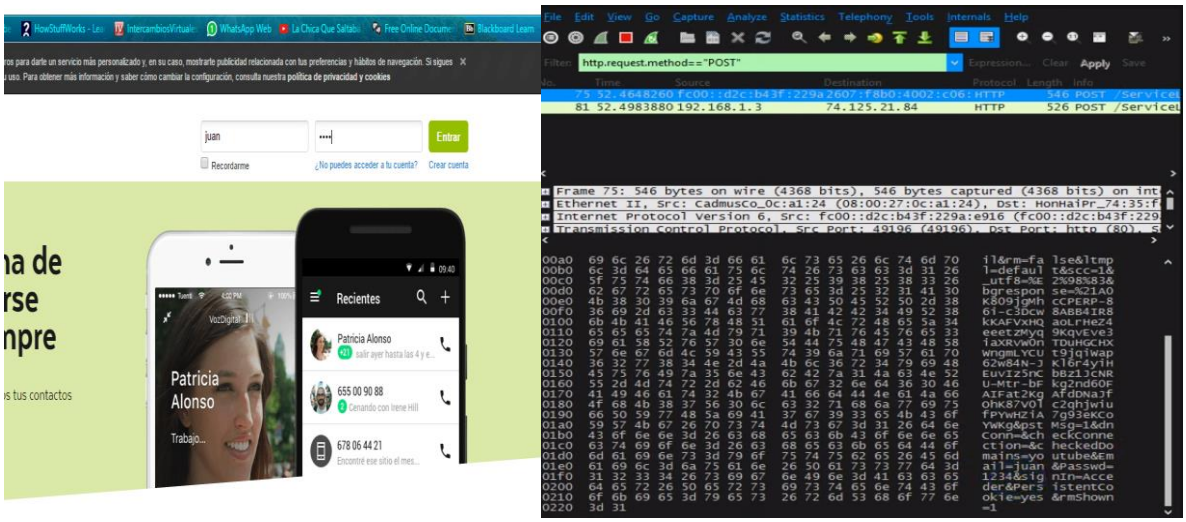
Figura. 32 Ingreso a Navegador Victima

Fuente: Autor

En la web principal se puede ver como Evil FOCA ha entregado la página de login bajo HTTP en lugar de bajo HTTPs.

El uso de Wincap facilita el uso de programas de registro de periféricos y paquetes (sniffer), tales como el Wireshark con el objeto de generar ataques en este protocolo nuevo.

Figura. 33 Resultados Spoofing



Fuente: Autor

Ahora bien, cuando la víctima incautamente haga una solicitud HTTP para el login, Evil FOCA se comunicará con el servidor, pero dado el caso que no exista respuesta y la única salida de comunicación sea por HTTPs, el Evil FOCA hará una nueva petición con HTTPs. Todo el tráfico del victimado se irá bajo HTTP, asi como se muestra en la anterior imagen de Wireshark, donde aparecen las credenciales.

Como dato adicional, se recuerda el uso de sniffers con su respectivos filtros con el objeto de revisar solo los paquetes que se desea (http.request.method==”POST”.)

Fase 3: Análisis

En la captura se aprecia como el contrato existe sobre IPv6, utilizando una URI bajo HTTP, donde se pone en exposición el usuario y la contraseña, con lo que el hombre en medio podrá ver todos los datos, mientras que para la desprevenida víctima, estará en un proceso de navegación común y corriente.

Hasta el día de hoy, los ataques con Evil FOCA son efectivos en la mayoría de lugares web y se están depurando algunos sitos que hacen algunas verificaciones extras, pero Twitter, Facebook y Tuenti funcionan ya en este entorno.

Si la victima instalara un programa anti man in the middle, no lo detectaría porque esta trabaja con ARP y acá la tabla de SLAAC es la que ha sido Spoofiada y no la de ARP.

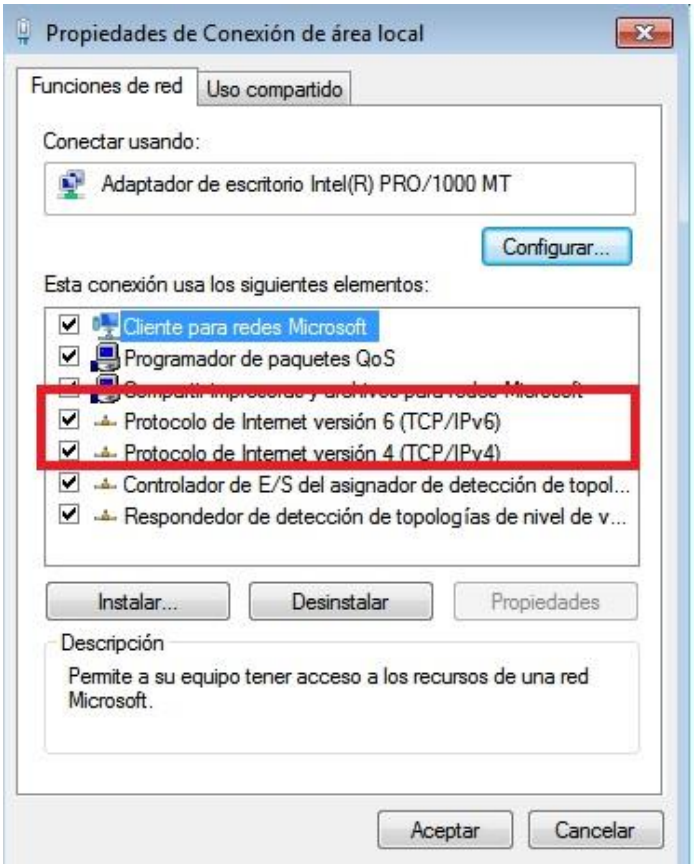
Solución y Recomendaciones

El bloquear el descubrimiento de routers por SLAAC en IPv6 suele ser la mejor recomendación para estos casos, junto con el uso de comandos de bloqueo tales como:

netsh interface ipv6 set interface "Nombre NIC" routerdiscovery=disabled

Por consiguiente esto evita el ataque *mitm* SLACC, y el D.O.S. de *flood* RA, pero en IPv6 aún existe el riesgo de envenenamiento hacia los sistemas aledaños que estén funcionando sobre direcciones IPv6 de vínculo local (incluye los rouge DHCP); al no usar IPv6 es mejor inhabilitarlo.

Figura. 34 Conexión de Área local IPv6



Fuente Autor.

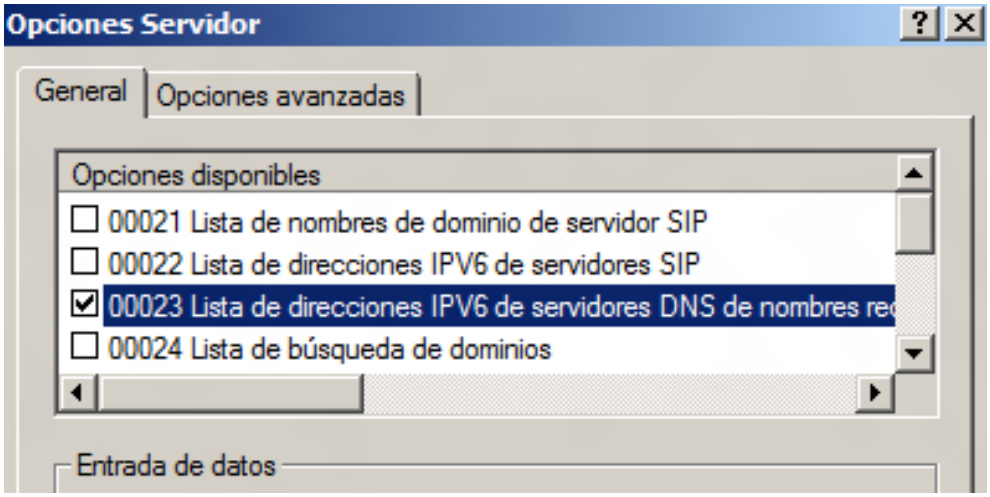
6.10 Man in the Middle IPv6 sobre redes IPv4

Se inicia deshabilitando IPv4 en las propiedades de área local, con el objeto de que el algoritmo de precedencia haga el resto y se reenvíe el tráfico por la conexión IPv6.

Fase 1: se anula IPv4 y partiendo del hecho que no existan protecciones tipo PatriottNG y Marmita en el ordenador afectado, se envía un paquete ARP que configure una dirección falsa MAC a la dirección IP del gateway en el cliente, dejando el equipo sin conectividad con el Gateway, dejando al sistema en entredicho para que evalúe la posibilidad con IPv6.

Fase 2: se pasa a configurar IPv6 en el cliente con Rogue DHCPv6, para después establecer en el cliente una configuración útil (en IPv6). Si hay disponibilidad de un servidor Rogue DHCPv6 es posible que el cliente obtenga todo lo necesario de este esquema de ataque, como lo es una dirección IPv6 valida, una dirección IPv6 de un gateway para la red IPv6 y las direcciones de los servidores DNSv6.

Figura. 35 DHCPv6



Fuente: Autor

Para servidores Windows Server 2008 o Windows Server 2008 R2 o de clases parecidas es permitido configurar un servidor DHCP para IPv6 y preparar la configuración apropiada para el equipo víctima con el ánimo de realizar el ataque.

Paso 3: por consiguiente se hace la configuración IPv6 en el cliente con SLAAC e IPv6 DNS AutoDiscovery o también puede ser usando el servicio SLAAC para

configurar la dirección IPv6 y la dirección del gateway, lo cual hace que el tráfico IPv6 sea dirigido hacia la máquina del atacante, (recomendación: el protocolo SLAAC no permite configurar valores como los servidores DNS), por ende complica mucho al usuario conectado a internet usando nombres de dominios mientras el servidor DNS esta anulado, al igual que la red IPv4.

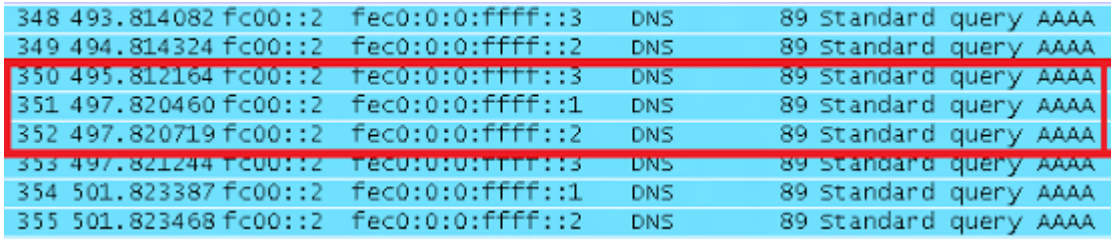
Se recuerda que un servicio de IPv6 implementado en máquinas con Windows (IPv6 DNS AutoDiscovery) propuesto por el Network Working Group del IET (aún no se registra datos de haber sido probado en Linux) se espera que serán muy parecidos, donde se direccionaran varias peticiones hacia otras direcciones fijas con el objetivo de encontrar servidores DNS en redes IPv6.

Figura. 36 Equipo Anulado IPv4 - Ping a sitio no existente

Fuente: Autor

Con el objeto de comprobar lo mencionado, se procede a realizar un ping a un nombre en la red IPv6 para interceptar el tráfico en el gateway, mostrando como en una máquina en la que se anula IPv4, continua lanzándose peticiones DNS a direcciones IPv6 fijas y reservadas, sin importar que no están configuradas en el cliente.

Figura. 37 Peticiones DNS a servidores IPv6 fijados

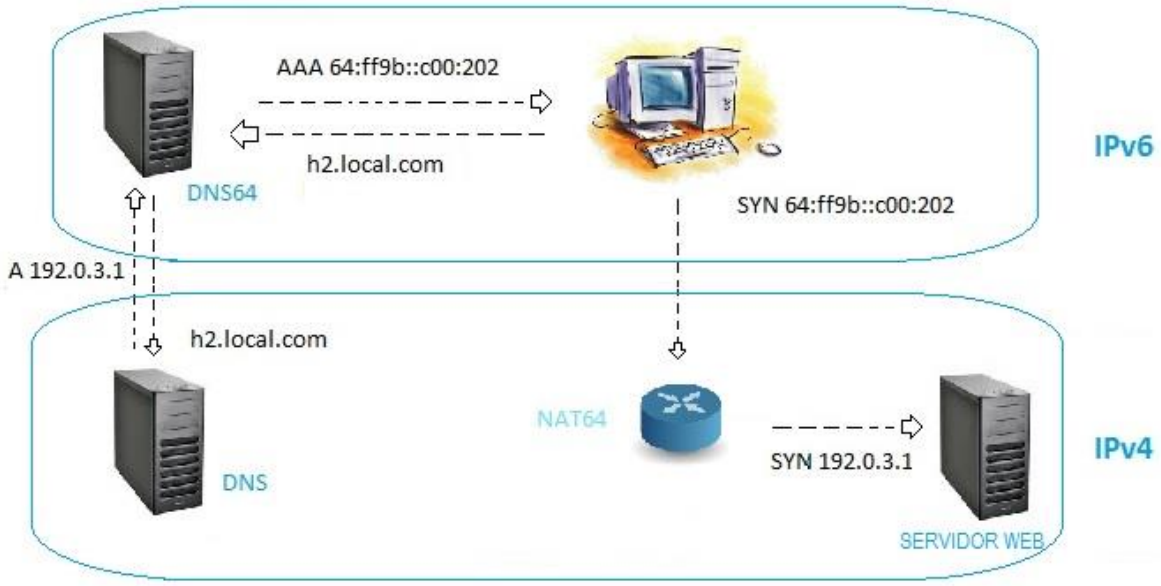


Fuente: Autor

Se deben escoger las direcciones (en la gráfica se usan algunas ya spoofeadas) para que apunten a las maquinas del atacante.

Fase 4: Enrutar el tráfico IPv6 a IPv4 e IPv4 a IPv6 y para lograr que el cliente envíe todo su tráfico con IPv6, se debe lograr que toda la resolución de direcciones se haga en formato IPv6, siendo necesario contar con un servicio DNS64, (un servidor DNS que escuche por IPv6), solicite las tramas recursivas por IPv4 y devuelva las respuestas en formato de direcciones IPv4 en IPv6.

Figura. 38 Enrutamiento de tráfico IPv4 a IPv6 controlando DNS y Gateway en IPv6



Fuente: Autor

La anterior figura muestra como las direcciones de servidores IPv4 tendrán formato IPv6 y se envían al gateway IPv6, donde el atacante configura un servicio NAT64 para enrutar el tráfico por internet usando un router IPv4 de la propia red.

7. RECOMENDACIONES PARA MITIGAR RIESGOS EN IPv6

Dentro del proceso de transición del IPv4 al IPv6 en su fase de diagnóstico, es imperativo la identificación de los riesgos de seguridad, para posterior dar paso a las siguientes fases de implementación y monitoreo, ya que sin la primera parte es muy difícil garantizar el éxito de esta migración. A continuación se hace un sobrevuelo concluyente y múltiples recomendaciones para la mitigación de riesgos en IPv6.

Planificación y conocimiento

La implementación de IPv6 abre posibilidades a diferentes tipos de ataque, por lo tanto la información y mitigación debe ser constante, los profesionales de seguridad necesitan información/preparación en IPv6, teniendo en cuenta que la clave del éxito en IPv6 y su seguridad va desde el impacto sobre la networking y capacitación del personal, como a nivel de servidores, aplicaciones y dispositivos. Las configuraciones y migraciones mixtas son las más atractivas para los atacantes debido a que estas vulnerabilidades aumentan en la etapa de transición cuya realidad es que esta etapa nada que termina.

Riesgo de las configuraciones de Doble Pila

Esta configuración trata de la admisión simultánea de los protocolos IPv4 e IPv6, por ende cualquier configuración por parte de los controles de seguridad, reglas de firewalls o cualquier otro encargado de detener el tráfico no deseado, puede funcionar en IPv4 pero cabe la posibilidad de que no sean tan efectivos para IPv6. Debido a esto las empresas necesitan controles de seguridad y tecnología paralela, con el ánimo de no comprometer la seguridad al hacer uso de algún dispositivo o prácticas poco seguras no detectadas.

DNS en IPv6

Dentro de la administración de redes, está dado que los DNS internos contengan la información de todo los host dentro de la red, siendo esta la información más deseada por los posibles atacantes, declarando los servidores DNS como objeto de ataque constante, donde se le facilita a un intruso el evitar la información de toda la red cuando todo está en el DNS, siendo un atajo para el problema de la cantidad de direcciones en la red, convirtiéndose en un problema de seguridad a nivel software. Por ende, la implementación de IPv6 refuerza la necesidad de seguridad a nivel interior, siendo un problema más visto por las entidades.

Deshabilitación y bloqueo de IPv6

Un buen consejo siempre será, desactivar lo que no se está usando, tal es el caso de desactivar todos los protocolos de red innecesarios. Dentro de las políticas de

seguridad de una empresa es posible encontrar dispositivos o cualquier tipo de hardware habilitado para usar IPv6, ya que vienen configurados por defecto. Es buena idea que los dispositivos que son llevados al trabajo o los asignados por el gobierno, se configuren para bloquear todo el tráfico IPv6 no deseado en las redes inalámbricas.

Traducción de direcciones de red

Es una práctica de redes IPv4 (NAT) cuyo efecto segundario permitía una capa de protección frente a los dispositivos habilitados para este mismo protocolo, el cual permitía ocultarlos ante las redes externas, pero inevitablemente con la desaparición de NAT en IPv6, podría estar ahora desprotegido, en especial en redes domésticas, donde no hay controles de seguridad perimetral. Para mitigar esto, se recomienda que cualquier dispositivo que ejecuta IPv6 esté protegido por un software de firewall en el equipo de la red misma para el bloqueo de tráfico no entrante no deseado.

Ataques en ambientes IPv6

Existe la probabilidad de generar riesgos al ejecutar IPv6, tales como:

- Si existe un desarrollo defectuoso del software, puede presentarse un fallo en la implementación del protocolo, permitiéndose usar para un fin maligno.
- Algún fallo en la especificación puede hacerlo propenso a ser aprovechado por los Hackers. Por lo tanto, haciendo uso de componentes del mismo protocolo para realizar ataques, es recomendable realizar revisiones con el fin de eliminar fallos.

Multicast en IPv6

El local multicast siendo una dirección especial que nos permite identificar grupo de host en la red, como lo pueden ser servidores, router, switches entre otros, dan un mundo de posibilidades de ataque, ya que una dirección no da acceso a todo un grupo, generando esos ataques de tipo tradicional como el Denial of service DoS o el Port scanning.

Riesgos de Túneles de IPv6 a IPv4

IPv6 utiliza como protocolo de protección el IPsec, en el caso de que este no existiera, cabe la posibilidad de riesgos potenciales. Claro está, que una de las técnicas de transición en IPv6 son los túneles de tráfico de IPv6 a IPv4 permitiendo encapsular un protocolo en otro, pero al general disminución en el control del tráfico puede crearse una “puerta trasera” en el protocolo, es decir, el riesgo de tener acceso a un programa o sistema sin autorización, debido a, que las configuraciones de seguridad del IPv6 se encuentran anuladas.

Se recomienda el uso de mecanismos de transmisión extremo a extremo, también usado en IPv6, debido a sus múltiples ventajas de desempeño con mejores tiempos de respuesta en los sistemas de información y comunicaciones. Debido a que este protocolo no cuenta con procesos NAT, existe el riesgo en las terminales finales, por su exposición desde cualquier punto extremo de la red, cuya solución es el uso de un buen firewall.

Escaneo en Redes ipv6

Gracias a las técnicas de escaneo se realizan los ataques más comunes en las redes de comunicaciones, entre ellos existe los nodos con puertos activos, servidores DHCP con identificación de la estructura de red; para el caso de IPv4 se utiliza una máscara de subred de 24 bits que genera un grupo no superior a 254 nodos por red, facilitando el escaneo para identificar redes TCP o UDP. En cuanto a IPv6 se refiere, los ataques como el anterior no sería tan viables debido al gran espacio de direccionamiento que este ofrece (128 bits), ya que tardaría más tiempo sobre la red del estimado, por ende este ataque quedaría descartado.

CONCLUSIONES

En IPv6 ya no es necesario el uso de servidores DHCP ni su configuración manual de las direcciones IP, tampoco el uso de proxy, especialmente usadas en aplicaciones como videoconferencias y telefonía IP, pero ante ello ya existen toolkits de ataques que aprovechan vulnerabilidades de estas características, esto quiere decir que a medida que se difunde el IPv6, sus vulnerabilidades se convierten inmediatamente en un objetivo para un atacante.

Esta monografía de diseño y elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO, utiliza como recurso fuentes confiables de internet, consultas a especialistas de redes CISCO y personal internacional de Perú y España, junto con LACNIC, como organización no gubernamental de registro de direcciones de internet para América Latina y Caribe.

Por medio de este trabajo, se aprecian vulnerabilidades presentadas en la implementación y desarrollo del protocolo IPv6 como protocolo guía, ya que a pesar de que se encuentra circulando desde hace buen tiempo en la red y diseño de equipos, aún no se puede constatar de una implementación total por parte de entidades Colombianas dentro de sus redes el IPv6. Debido a las vulnerabilidades encontradas en este nuevo protocolo y sus similitudes con su anterior versión, se hace necesaria una gestión de vulnerabilidades, para mitigar los riesgos y evitar cometer los mismos errores pasados. Sin embargo este protocolo contiene aspectos de mejora en la seguridad, junto con el manejo de diferentes técnicas de administración, provocando que el administrador de red esté en la obligación de conocer aquellos esquemas para implementarlos, manejarlos e identificar posibles vulnerabilidades, aumentando los márgenes de seguridad en un protocolo poco aplicado y con poca experiencia en cuanto a seguridad de la información se trata.

Este trabajo es generado por medio de la investigación y consulta de fuentes externas y confiables en IPv6, tales como empresas internacionales que ya han trabajado con este protocolo, que conocen su implementación y desarrollo, junto con el aporte de profesionales titulados, quienes han experimentados ciertas vulnerabilidades del protocolo o han identificado riesgos latentes en IPv6.

En esta guía se centra toda la evidencia recolectada, para su consulta, estructuración y administración de riesgos. Por otro lado, se realizan pruebas para explicar las soluciones a las vulnerabilidades identificadas y se emiten recomendaciones para el manejo de las mismas.

Se espera alcanzar el máximo nivel de comprensión en los temas propuestos en la guía, que respondan a las necesidades de los diferentes estudiantes o administradores de red, para iniciar con el proceso de migración hacia IPv6, detección temprana de posibles amenazas o simplemente sea de carácter pedagógico, como modelo para la implementación y manejo de seguridad en IPv6.

BIBLIOGRAFÍA

ACOSTA Alejandro & AGGIO, Santiago Aggio. (2014). Descargado content/uploads/2015/02/ipv6_operadores_red-tablets.pdf, IPv6 para operadores de red, Internet Society ISO-AR Capítulo Argentina. Tomado de http: //portalipv6.lacnic.net/wp-, pág. 83

CCM. PROTOCOLO TCP. Características. Tomado de http://es.ccm.net/contents/281-protocolo-tcp. 01 febrero 2016

CICILEO Guillermo, GAGLIANO Roque, O´FLAHERTY Christian, MOALES Cesar, MARTÍNEZ Jordi, ROCHA Mariela & MARTÍNEZ Alvaro.IPv6 Para Todos. Guía de uso y aplicación de diversos entornos. IPv6 1ª Ed. Buenos Aires: Asociación Civil Argentinos en Internet, 2009,5.3 Configuraciones. Pág. 142.

CONSEJOS DE RESOLUCIÓN DE PROBLEMAS GENERALES DE RED. [En línea]. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipconfig-138/index.html. 14 marzo 2016

CIPRIAN, P., (2006). Deploying IPv6 Networks, Cisco System. ED 1ª. Pag. 142. Consultado 22 diciembre 2015.

DE LA CRUZ CAMARGO L. IPv6 para los colombianos. [En línea]. Tomado de http://portal.uexternado.edu.co/pdf/derechoDeLasTelecomunicaciones/IPV6-para-los-colombianos.pdf. 8 agosto 2015.

DE LEON Gianni. (2014). SLAAC Spoofing. Evil FOCA. Disponible https://www.youtube.com/watch?v=PvJfgqIF7XY. [10 marzo 2016].

FUNDAMENTOS IPv6. [En línea]. Definición. Disponible en http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6. 1 diciembre 2015.

HOGG Scott (2012). Network World. CISCO Subnet. The future of Firewall Policies. 19 junio 2012. Disponible en

http://www.networkworld.com/article/2221507/cisco-subnet/cisco-subnet-the-future-of-firewall-policies.html. 10 mayo 2016

IETF (Internet Engineering Task Force) o Grupo de Trabajo de Ingeniería de Internet, entidad que regula las propuestas y los estándares de Internet, conocidos como RFC

INTERNET SOCIETY. Deploy360 Programme Disponible en http://www.internetsociety.org/deploy360/ipv6/ . 05 mayo 2016

INTERNET SOCIETY. IPv6. Internet2 IPv6 Working Group. IPv6 Knowledge Base: General Information. IPv6 Testing Consortium. From the University of New Hampshire InterOperability Laboratory, the “IPv6 Consortium is focused on offering testing services that reduce the time to market for our participants, and accelerate the adoption of IPv6 technology.” Disponible en http: //www.internetsociety.org/what-we-do/internet-technology-matters/ipv6, Includes links to guides, publications and workgroups. 05 mayo 2016.

IPv6 Security - FAQ from live webcast. Tomado de IPv6 Security - FAQ from live webcast.

IPV6 MX. ¿Cómo saber si mi router es compatible con IPv6? [En línea]. Disponible en http://www.ipv6.mx/index.php/informacion/ fundamentos/ipv4/100

IPV6 IOS FIREWALL. Restricciones y características. [En línea]. Disponible en http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_cbac_fw/configuration/15-2mt/ip6-firewall.html. 10 Mayo 2016.

IRIS. Seguridad en IPv6 para Instituciones afiliadas a RedIRIS. Correo Electrónico. Disponible en http://www.rediris.es/cert/doc/ipv6seg/#1.7.2. 22 De mayo 2016.

MARCO Gabriel (2011). IPsec. Disponible en http://es.slideshare.net/jarvel/ seguridad-en-ipv6. Diapositiva 15. 1 Mayo 2016

MINTIC. Protocolo de Internet Versión 6. Tomado de

http://www.mintic.gov.co/portal/604/w3-article-5866.html 30 Abril 2015.

MINTIC. Pruebas de penetración en IPv6. [En Línea]. Tomado de http://www.mintic.gov.co/gestionti/615/articles-5482_Protocolo_IPV6.pdf pág. 30-31. 02 mayo 2016

MUR, P., (2000). Seguridad a nivel de IP: IPSec, Estudiante de la ETSETB, UPC. Ramas de estudiantes del IEEE, recuperado del sitio web de la Universidad Politécnica de Cataluña Barcelona: https://upcommons.upc.edu/ revistes/bitstream/2099/9944/1/Article00 5.pdf

LACNIC. Información general. Quienes somos. Disponible en http://portalipv6.lacnic.net/que-es/. 02 marzo 2016.

Revisión de los RFC de Seguridad. Definición. Consejos para IPv6. Disponible en www.mintic.gov.co/ipv6. 14 Octubre 2015.

Operational Security Considerations for IPv6 Networks, draft-ietf-opsec-V6. Chittimageni, K., Kaeo, M., And E.Vyncke.2013

ORACLE. Guía de administración del sistema: servicios IP. El ISP actual no admite IPv6, Problemas comunes con un enrutador 6to4, Cuestiones de seguridad al transmitir datos mediante túnel a un enrutador de reenvío 6to4. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-1/index.html

ORACLE. Guía de administración del sistema: servicios IP. Aspectos relacionados con la seguridad en la implementación de IPv6. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-1/index.html

PAZ Alvaro. (2005). Gurú de la informática. Herramientas para realizar MITM (man-in-the-middle) en SLL. Disponible en http://www.gurudelainformatica.es/2014/01/ herramientas-para-realizar-mitm-man-in.html 06 mayo 2016.

PILIHANTO Atik (2011). SANS Institute InfoSec Reading Room. A Complete Guide on IPv6 Attack and Defense. Disponible en https://www.sans.org/.../complete-guide-ipv6-attack-defense-339. Pág 14-20. 20 Mayo 2016.

Security Architecture for the Internet Protocol. 3.3. Where IPsec Can Be Implemented. Pág. 10. Disponible en https://tools.ietf.org/html/rfc4301. [10 marzo

2016].

SERVICIOS IPV6 DE CISCO. [En línea]. Disponible en http://blog-cisco-spain.com/2012/05/29/documento-cisco-servicios-ipv6-para-escalar-su-empresa-mas-alla-de-las-limitaciones-de-ipv4/. [10 marzo 2016].

SERVICIOS IPV6 DE CISCO. [En línea]. Disponible en http://blog-cisco-spain.com/2012/05/29/documento-cisco-servicios-ipv6-para-escalar-su-empresa-mas-alla-de-las-limitaciones-de-ipv4/. [10 marzo 2016].

TOWNSLEY Mark (2013) .Blog CISCO Latinoamérica. [En línea] Disponible en http://gblogs.cisco.com/la/desmitificando-ipv6/ [10 marzo 2016].

UN INFORMÁTICO EN EL LADO DEL MAL. Conceptos básicos IPv6. Disponible http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6.html. 05 mayo 2016

APENDICES

APÉNDICE 1
RFC de Seguridad en Ipv6 [60]

Lista de RFC que aplican a la seguridad en IPv6:

- ✓ RFC 5619: Software Security Considerations, Agosto 2009
- ✓ RFC 5269: FMIP Seurity Distributing a Symectric Fast Mobile IPv6 (FMIPv6)
- ✓ RFC 4942: IPv6 Transition/Coexistence Security Considerations
- ✓ RFC 4218: Threats Relatiing To IPv6 Multihoming Solutions
- ✓ RFC 4891: Using IPsec To Secure IPv6 Tunnels
- ✓ RFC 4890: Recommendations For Filtering ICMPv6 Messages in Firewalls
- ✓ RFC 4864: Local Network Protection For IPv6
- ✓ RFC 4843: An IPv6 Prefix For Overlay Routable Cryptographic hash Identifiers (ORCHID)
- ✓ RFC 5213: Proxy Mobile IPv6
- ✓ RFC 4835: Cryptographic Algorithm Implementation Requeriments for Encapsulatiing Security Payload (ESP) and Authentication Header (AH)
- ✓ RFC 4487: Mobile IPv6 And Firewalls: Problem Statement
- ✓ RFC 4449: Securing Mobile IPv6 Route Optimization Using a Static Shared Key
- ✓ RFC 4303: IP Encapsulating Security Payload (ESP)
- ✓ RFC 3756: IPv6 Neighbor Discovery (ND) Trust Models Threats
- ✓ RFC 4301: Asociaciones de seguridad (SA). Security Architecture for the Internet Protocol. Soporte para IPsec-V2. (Hace obsoleto el RFC 2401)
- ✓ RFC 2401: Security Architecture for the Internet Protocol (Actualizado por RFC 3168), Soporte para IPsec-V2.
- ✓ RFC 4302: IP Authentication Header (Hace obsoleto RFC 2402)
- ✓ RFC 4303: IP Encapsulation Security Payload
- ✓ RFC 5282: Using Authenticated Encription Algorithms with the encrypted
- ✓ Payload of the internet key Exchange Versión 2 (IKEv2) Protocol.

[60] Para mayor información consultar en http://www.mintic.gov.co/portal/604/w3-article-5938.html

- ✓ RFC 5996: Internet Key Exchange (IKEv2) Protocol
- ✓ RFC 4877: Mobile IPv6 Operation with IKEv2 and the revised IPSec Architecture
- ✓ RFC 4581: Cryptographically Generated Addresses (CGA) extention field format (Actualiza el RFC 3972)
- ✓ RFC 4982: Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGA). (Actualiza el RFC 3972 errata)
- ✓ RFC 3414: User – Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
- ✓ RFC 4807: IPSec Security Policy Database Configuration – MIB.

APÉNDICE 2

Libros de consulta:

Presentación de Hack In The Box 2006: Scapy and IPv6 networking.

Disponible en http://void.gr/kargig/ipv6/scapy-IPv6_HITB06.pdf

Libros de Ataques en redes de datos

Disponibles en IPv4 & IPv6 http://0xword.com/es/

Comunidad de foros de CISCO

Disponible en https://supportforums.cisco.com/community/5531/ipv6-integration-and-transition

ANEXO B

RESUMEN ANÁLITICO RAE

Título de Documento.	Guía Abierta para la Administración de Riesgos de Seguridad en de Protocolo de Internet IPv6 Sobre Estándares de Enrutamiento Dinámico en Equipos con Plataforma Cisco.
Autor	SABOGAL Ortiz, Arth Grossy (2017).
Palabras Claves	Análisis de riesgos, Confidencialidad, DHCPv6, Direccionamiento IPv6, Disponibilidad, DNS, Encapsulamiento, ICMP, IPv6, IPsec, Integridad, Protocolo de Comunicaciones, RFC, Redes Privadas Virtuales, RPKI, SNMP, TCP.
Objetivos	**General** Estructurar las técnicas y mejoras para la administración de seguridad sobre estándares de enrutamiento dinámico ejecutado en equipos con plataforma CISCO, mediante la elaboración de una guía abierta de seguridad basada en el análisis de riesgo en el protocolo de internet IPV6. **Específicos** • Recopilar información de los múltiples resultados de las investigaciones actuales sobre el IPv6, amenazas, vulnerabilidades, identificando sus antecedentes de creación, contexto tecnológico y organizacional. • Identificar y promover las habilidades necesarias para el funcionamiento de los componentes que usa IPv6, junto con los instrumentos que existen para su configuración y mantenimiento seguro en una red establecida bajo dichos parámetros. • Realizar un diseño práctico de guía para la presentación de las investigaciones que serán objeto de publicación. • Generar una guía abierta de seguridad con las recomendaciones que se alleguen por los usuarios de plataforma CISCO, con el fin, de actualizar la información suministrada por este a medida que se presenten modificaciones o novedades.
Contenidos	Introducción. Objetivos y Definiciones. • Capítulo 1. CISCO & IPv6. • Capítulo 2. Seguridad en IPv6. • Capítulo 3. Problemas comunes al utilizar IPv6. • Capítulo 4. Seguridad de IPv6 en los centros de datos. • Capítulo 5. Diez consejos para implementar IPv6 de forma segura. • Capítulo 6. Pruebas de penetración en redes IPv6.

	• Capítulo 7. Recomendaciones para mitigar riesgos en IPv6. Conclusiones y Bibliografía.
Descripción del Problema de Investigación La monografía es creada haciendo énfasis en la seguridad en IPv6, como el nivel más reciente del protocolo de Internet (IP), desenvolviéndose en parte como soporte y parte interconexión de sistemas operativos, descrita en forma de guía rápida para la consulta, manejo, revisión y gestión de riesgos informáticos, dentro de los aspectos de implantación y funcionamiento de IPv6, promoviendo la información útil para la prevención de ataques y minimización de riesgos informáticos. El tema de seguridad debe ser profundamente analizado dada la alta posibilidad de que se presenten incuestionables debilidades en un protocolo tan nuevo, las cuales no son consideradas por los administradores de redes por su poca socialización e información disponible. Se realizó la investigación para esta monografía remitiéndose a fuentes de internet (Redes CISCO, LACNIC, Optical Networks, CES), especialistas (Marc Musgrove especialista en redes y IPv6 CISCO, Corletti Alejandro, Universidad de Madrid), desarrolladores (CISCO Latinoamérica), programadores, empresas nacionales (CISCO Colombia), internacionales (Telefónica Perú), Monografía aplicada para personal en seguridad de redes y seguridad informática cuyo objetivo es evaluar las múltiples vulnerabilidades y complicaciones presentadas en el manejo, implementación y socialización del protocolo Ipv6 en las nuevas redes, como guía inicial para incrementar el margen de seguridad del nuevo protocolo y socialización de las nuevas vulnerabilidades a un protocolo necesario en el futuro de la internet.	
Fuentes Bibliográficas	• LACNIC. Información general. Quienes somos. Disponible en http://portalipv6.lacnic.net/que-es/. 02 Marzo 2016. • Revisión de los RFC de Seguridad. Definición. Consejos para IPv6. Disponible en www.mintic.gov.co/ipv6. 14 Octubre 2015. • Operational Security Considerations for IPv6 Networks, draft-ietf-opsec-V6. Chittimageni, K., Kaeo, M., And E.Vyncke.2013. • ORACLE. Guía de administración del sistema: servicios IP. El ISP actual no admite IPv6, Problemas comunes con un enrutador 6to4, Cuestiones de seguridad al transmitir datos mediante túnel a un enrutador de reenvío 6to4. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-1/index.html • ORACLE. Guía de administración del sistema: servicios IP. Aspectos relacionados con la seguridad en la implementación de IPv6. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-1/index.html. • SERVICIOS IPV6 DE CISCO. [En línea]. Disponible en http://blog-cisco-

	spain.com/2012/05/29/documento-cisco-servicios-ipv6-para-escalar-su-empresa-mas-alla-de-las-limitaciones-de-ipv4/. [10 marzo 2016]. • DE LA CRUZ CAMARGO L. IPv6 para los colombianos. [En línea]. Tomado de http://portal.uexternado.edu.co/pdf/derechoDeLasTelecomunicaciones/IPV6-para-los-colombianos.pdf. 8 agosto 2015.
Referentes Teóricos y Conceptual	• CCM. Protocolo TCP. Características. Tomado de http://es.ccm.net/contents/281-protocolo-tcp. 01 Febrero 2016 • Consejos De Resolución De Problemas Generales De Red. [En línea]. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipconfig-138/index.html. 14 marzo 2016. • Documento Política para la Adopción del IPv6 en Colombia, estructuración y definición, numeral 12.10, página 72, 73, 2012, Contrato 947 Mintic, Cintel, año 2012. • Fundamentos IPv6. [En línea]. Disponible en http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6. 01 diciembre 2015. • IPV6 MX. ¿Cómo saber si mi router es compatible con IPv6? [En línea]. Disponible en http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4/100 • MINTIC. Protocolo de Internet Versión 6. Tomado de http://www.mintic.gov.co/portal/604/w3-article-5866.html 30 Abril 2015.

Resume

La guía abierta comprende análisis bibliográficos, investigaciones prácticas e información disponible sobre ¿Cómo podemos mejorar y estructurar los niveles de seguridad y administración en IPv6 sobre estándares de enrutamiento dinámico ejecutado en equipos con plataforma CISCO entre otros?; siendo pieza fundamental para entender el protocolo IPv6, capacitando a los administradores de este tipo de redes, generando conciencia sobre las vulnerabilidades del mismo y planteando que posibilidades existen sobre este protocolo IP.

En esta guía se estructuran las técnicas y mejoras para la administración de la seguridad sobre estándares de enrutamiento dinámico ejecutado en equipos con plataforma CISCO, basadas en el análisis de riesgo en el protocolo de internet IPV6; se recopila información de los múltiples resultados de las investigaciones actuales sobre el IPv6, amenazas, vulnerabilidades, estudios previos, adecuación por parte de desarrolladores, empresas en proceso de migración a nivel internacional, apoyo a la red CISCO entre otros, donde se identifica sus antecedentes de creación, contexto tecnológico y organizacional. Posteriormente, se identifican y promueven las habilidades necesarias para el

funcionamiento de los componentes que usa IPv6, junto con los instrumentos que existen para su configuración y mantenimiento seguro en una red establecida bajo dichos parámetros.

Metodología

La presente monografía, consta de una construcción académica e intelectual apoyada en **la investigación exploratoria**, ya que es considerada como el primer acercamiento científico a un problema estipulado. Para el caso específico esta monografía el **enfoque de investigación es cuantitativo,** ya que se pretende hacer la identificación, análisis y mitigación de las vulnerabilidades, amenazas y riesgos en cuanto a la confidencialidad, integridad y disponibilidad de la información en el nuevo protocolo. Por lo tanto, se realiza **una investigación exploratoria con enfoque cuantitativo**, ya que no existen exploraciones en seguridad informática descritas por medio de una guía abierta de fácil acceso e interpretación dentro de los archivos de la UNAD, internet o libros, dirigido a diferentes tipos de público y administradores de redes con capacidad IPv6.

Conclusiones

- Este documento presenta descripciones de nuevas características proporcionadas por el protocolo de Internet versión 6 (IPv6). Promoviendo una visión en profundidad de las nuevas características de seguridad en IPv6, analizando desde las vulnerabilidades latentes, como el uso de la autenticación de cabecera, carga de seguridad encapsuladora (ESP) entre otros problemas de adaptación y configuración.
- La guía abierta examina cómo las características del IPv6, pueden ayudar a prevenir ciertos tipos de ataques de red, que se producen actualmente a través de Internet y promueve el debate de ciertos temas pendientes con los elementos de seguridad de IPv6 de los cuales no se tiene mucha información en Colombia.
- En IPv6, la mencionada seguridad IP (IPsec), hace parte del conjunto de protocolos obligatorios, siendo un conjunto de especificaciones de seguridad escritas de modo original como una especificación de IPv6 y nacida de la gran necesidad de seguridad en la Internet actual con el IPv4.

Resultados

La creación de la guía promueve un largo camino evolutivo, tanto de la familiarización con el protocolo nuevo, como la mutación de las amenazas, por ende, se recomienda que la guía sea actualizada de manera periódica, siendo consignada en medio magnético y administrada por la Universidad para su uso, actualización, consulta y complemento constante.

ANEXO C

Solicitud información CISCO sobre IPv6

Cisco Latinoamérica

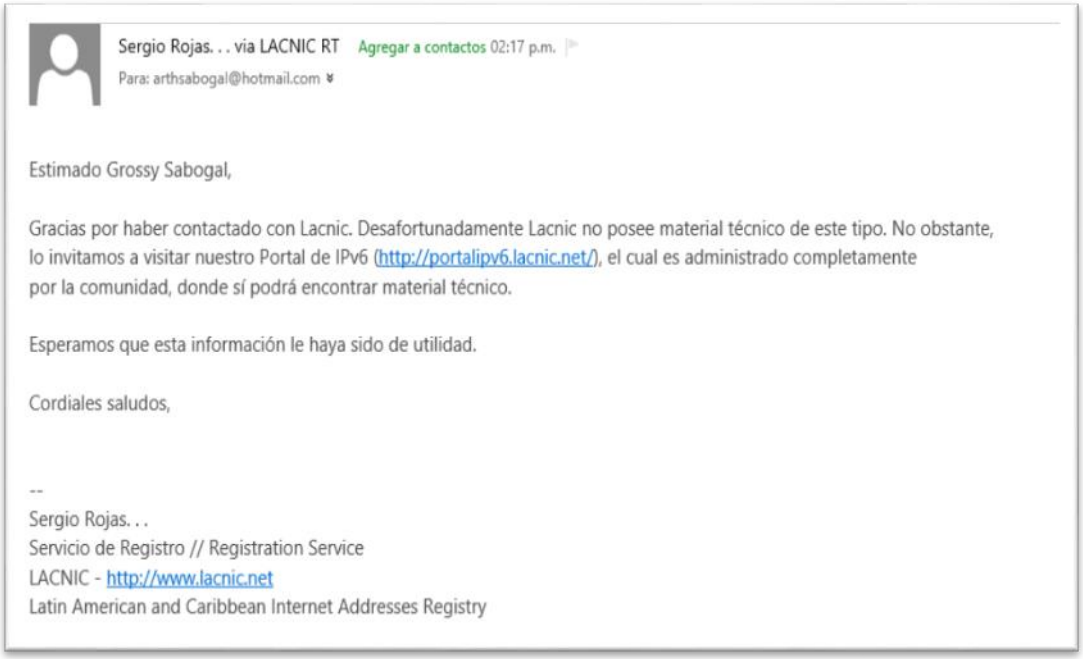
¡Buenos días, Grossy! Gracias por contactarnos. Te invitamos a investigar y encontrar material de apoyo en nuestra página web, blog y documentos de slideshare. A continuación encontrarás nuestra información: http://gblogs.cisco.com/la/desmitificando-ipv6/ http://gblogs.cisco.com/la/escalar-su-empresa-mas-alla-de-las-limitaciones-de-ipv4/ http://es.slideshare.net/ciscolatinoamerica/i-pv6-serviceoverview http://www.cisco.com/c/en/us/solutions/ipv6/overview.html y http://www.cisco.com/c/en/us/tech/ip/ip-version-6-ipv6/index.html ¡Saludos y feliz semana!

Blog Cisco Latinoamérica » Desmitificando IPv6

La versión 6 del protocolo de Internet (IPv6) es un habilitador f…

gblogs.cisco.com

Solicitud ante LACNIC



Sergio Rojas. . . via LACNIC RT Agregar a contactos 02:17 p.m.

Para: arthsabogal@hotmail.com

Estimado Grossy Sabogal,

Gracias por haber contactado con Lacnic. Desafortunadamente Lacnic no posee material técnico de este tipo. No obstante, lo invitamos a visitar nuestro Portal de IPv6 (http://portalipv6.lacnic.net/), el cual es administrado completamente por la comunidad, donde sí podrá encontrar material técnico.

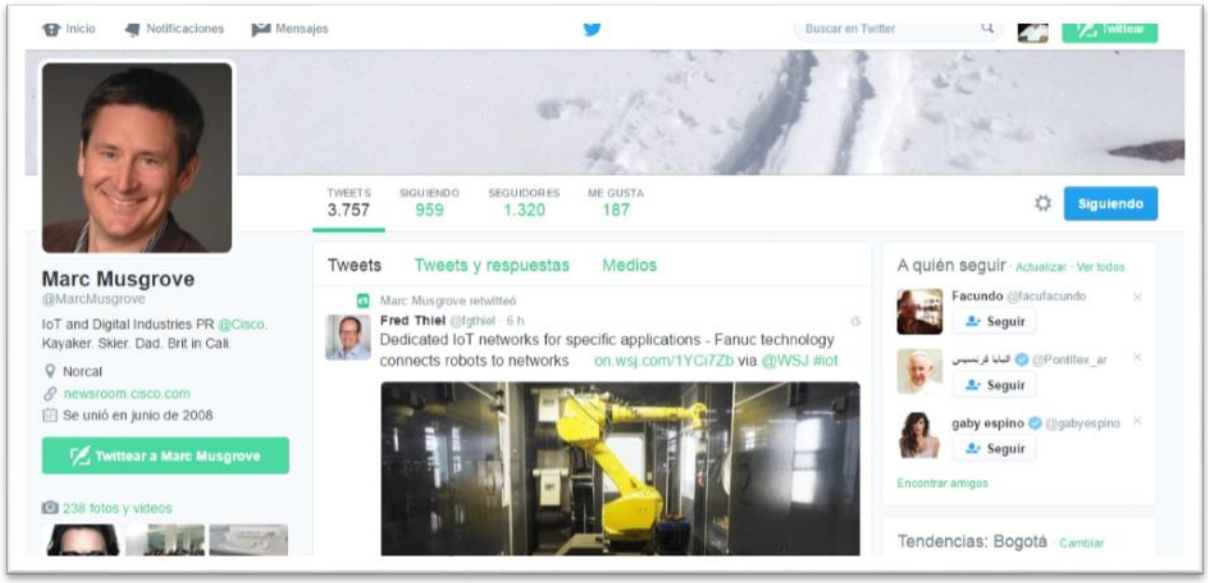
Esperamos que esta información le haya sido de utilidad.

Cordiales saludos,

--
Sergio Rojas. . .
Servicio de Registro // Registration Service
LACNIC - http://www.lacnic.net
Latin American and Caribbean Internet Addresses Registry

ANEXO D

Solicitud ante Mr. Marc Musgrove especialista en redes y IPv6 CISCO.



ANEXO E

Solicitud Aspectos de seguridad Especialista Alejandro Corletti

RE: Solicitud Aspectos de Seguridad Ipv6

alejandro corletti (acorletti@hotmail.com) Agregar a contactos 09:28 a.m.
Para: Grossy Sabogal

Hola Grossy,

Yo vengo trabajando con IPv6 en las empresas del Grupo Telefónica, que en el core de sus redes ya está funcionando hace tiempo pero como comprenderás se trata del Core de redes muy grandes y trabajando con routers cisco y juniper de máxima capacidad que hace tiempo soportan OPv6, así que problemas sobre estos dispositivos no hemos tenido ninguno.

en cuanto a ayuda, cuenta con lo que te pueda ser útil, pero necesito dudas muy concretas sobre las que te pueda ayudar, e igualmente te pido disculpas si me demoro en las respuestas, pues la verdad es que tengo muchos mails por día y aveces no doy abasto con todos,

un saludo
alejandro corletti

From: arthsabogal@hotmail.com
To: acorletti@wanadoo.es; acorletti@hotmail.com
Subject: Solicitud Aspectos de Seguridad Ipv6
Date: Mon, 25 Apr 2016 09:30:04 -0500