INFORME SOBRE LAS IMPLICACIONES DE SEGURIDAD EN LA IMPLANTACIÓN DE IPv6

INTECO-CERT

Junio 2010

AGRADECIMIENTOS

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) reconoce y agradece a los siguientes colaboradores su inestimable ayuda en la realización del informe. Joao Damas, de la empresa Bondis, Jesús Rodriguez, de la empresa Voztele, Juan Cerezo, de la empresa BT, y Jordi Palet, César Olvera y Álvaro Vives, de la empresa Consulintel.

ÍNDICE

1. MOTIVACIÓN Y OBJETIVOS

Para que Internet siga creciendo y evolucionando se ha revisado uno de sus elementos de base: el protocolo IP. La nueva versión, IPv6[1], esta diseñado para ser el sucesor de IPv4 en Internet solventando muchas de sus deficiencias. IPv6, entre otras ventajas, soluciona el problema del agotamiento de las direcciones IP, aporta funcionalidades de seguridad para el cifrado y autenticación en comunicaciones de extremo a extremo, y permite la creación de nuevos servicios.

Este informe pretende servir de apoyo a responsables de seguridad, administradores de sistemas y técnicos de seguridad, a la hora de plantearse la transición a esta nueva versión del protocolo IP que tanta importancia tiene en los sistemas de información de las organizaciones. Sus objetivos son informar sobre los siguientes aspectos:

- Describir su funcionalidad.
- Detallar los aspectos de seguridad a tener en cuenta.
- Dar un código de buenas prácticas o consejos de actuación.

[1] http://tools.ietf.org/html/rfc2460

2. INTRODUCCIÓN AL PROTOCOLO IP

El protocolo IP es el protocolo más utilizado por los sistemas informáticos para comunicarse. La mayoría de aplicaciones o protocolos de mayor nivel (HTTP, SMTP, P2P, etc.) se apoyan en este protocolo para su funcionamiento.

Los equipos o dispositivos que utilizan el protocolo IP tienen asignado un identificador único llamado dirección IP para encaminar el mensaje entre los distintos nodos de la red de comunicaciones, desde el origen al destino. Este identificador es un número de 32 bits que se suele representar, para su más fácil manejo, mediante 4 números, del 0 al 255, separados por puntos.

2.1. NECESIDAD DEL PROTOCOLO IPv6

Dado que la dirección IP es de 32 bits, se pueden tener unos 4.300 millones de direcciones distintas. Pero, debido principalmente al gran número de dispositivos o equipos que utilizan el protocolo IP, y que por tanto necesitan una dirección IP, el número de direcciones disponibles se está agotando. Aunque se ha tratado de mitigar con soluciones como NAT[2] o CIDR[3], éstas no resuelven el problema de base y, además, introducen limitaciones como la pérdida de conectividad extremo a extremo.

Para solucionar este problema se ha creado una nueva versión de este protocolo llamada IPv6 que utiliza como dirección IP un número de 128 bits, de tal forma que IPv6 tiene 2 ^ 96 veces más direcciones que IPv4. Aunque en realidad, considerando que la subred mínima de IPv6 es de 64 bits de longitud, en IPv6 es más correcto hablar de un espacio total de 2 elevado a 64 subredes con 2 elevado a 64 posibles direcciones en cada una. Además, aprovechando la revisión del protocolo, se han introducido otras mejoras y nuevas funcionalidades:

- Autoconfiguración y reconfiguración automáticas de la dirección IP sin necesidad de servidores (sin estado).
- Soporte nativo y mejorado del direccionamiento multicast y creación del direccionamiento anycast.
- Implementación obligatoria de IPsec.
- Enrutado más eficiente.
- Soporte optimizado de movilidad IP.

[2] Network Address Translation: http://tools.ietf.org/html/rfc3022
[3] Classless Inter-Domain Routing: http://tools.ietf.org/html/rfc1519

- Implementación de etiquetas para QoS[4].
- Implementación de Jumbogramas.

Se espera que los dispositivos IPv4 convivan durante un largo tiempo (difícilmente predecible, pero posiblemente de 10 a 20 años) con los dispositivos IPv6 mediante mecanismos de coexistencia o transición, implementando ambos protocolos simultáneamente o mediante túneles sobre IPv4.

Este gran aumento en el número de direcciones IP disponibles hará posible que un número prácticamente ilimitado de elementos tales como electrodomésticos, automóviles, sensores, etc. se puedan interconectar para ofrecer nuevos servicios.

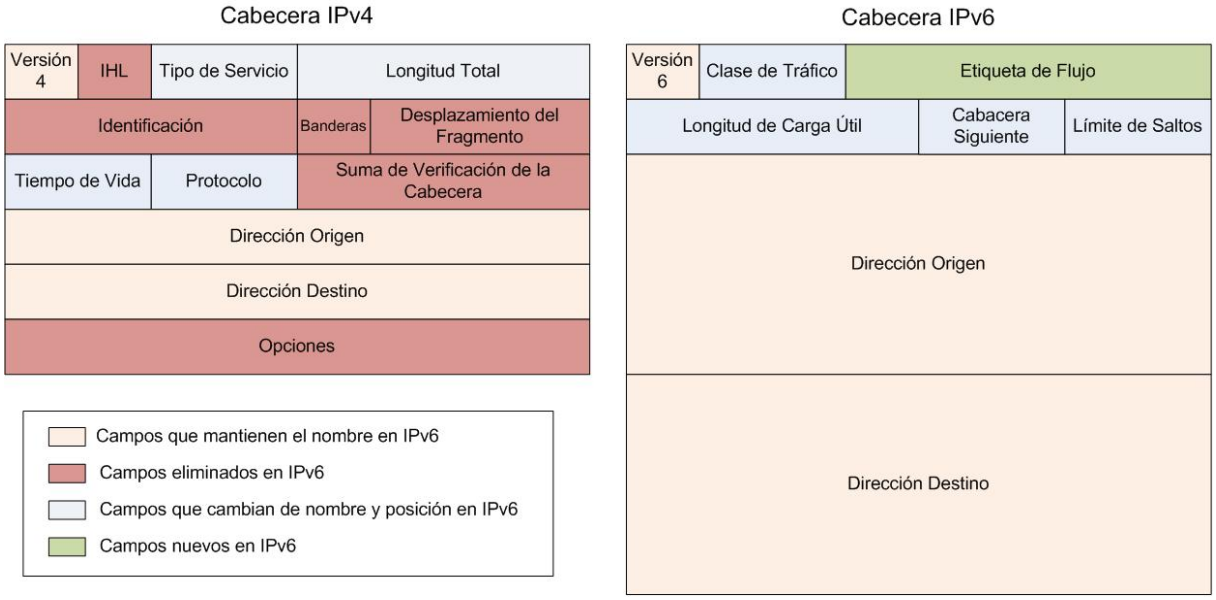

Ilustración 1 - Cabeceras IPv4 e IPv6

[4] Quality of Service: http://tools.ietf.org/html/rfc2990

3. MEJORAS DE SEGURIDAD DE IPv6

3.1. IMPLEMENTACIÓN DE IPSEC

IPv6 incluye explícitamente la posibilidad de utilizar el modelo de seguridad IPsec (Internet Protocol Security) que **proporciona autenticidad, integridad y confidencialidad a las comunicaciones de extremo a extremo**.

IPsec es un conjunto de protocolos abiertos que tienen como fin proporcionar seguridad en las comunicaciones de la capa de red del modelo OSI (a la que pertenece el protocolo IPv6), y de ese modo, a todos los protocolos de capas superiores.

En IPv4 la implementación de IPsec se define en una especificación diferente a la del propio protocolo IPv4, por lo que la inclusión del protocolo se hace con mecanismos definidos fuera del mismo, mientras que en IPv6 la propia arquitectura "extensible" del protocolo permite implementar IPsec de forma natural. Es importante reseñar que IPv6 habilita la posibilidad de usar IPsec, y no los mecanismos de cifrado y autenticación propios de IPsec.

IPsec tiene dos modos de funcionamiento que proporcionan distintos niveles de seguridad:

- Modo Transporte: se cifra y/o autentica la carga útil, o payload, pero las cabeceras no se tienen en cuenta. Tiene como ventaja que se puede utilizar de extremo a extremo pero, por contra, la información de las cabeceras, como la dirección IP de origen y destino, es visible.

- Modo Túnel: una plataforma, o pasarela, encapsula el paquete original en otro paquete. Con ello se cifra y/o autentica el paquete original completo, pero se necesita de una plataforma que realice el túnel.

Además, IPsec tiene dos modos o protocolos de transferencia, que a su vez pueden funcionar en modo túnel o transporte:

- AH (Authentication Header): proporciona autenticación, integridad y un servicio de anti-repetición opcional.

- ESP (Encapsulating Security Payload): además de las ventajas anteriores proporciona confidencialidad.

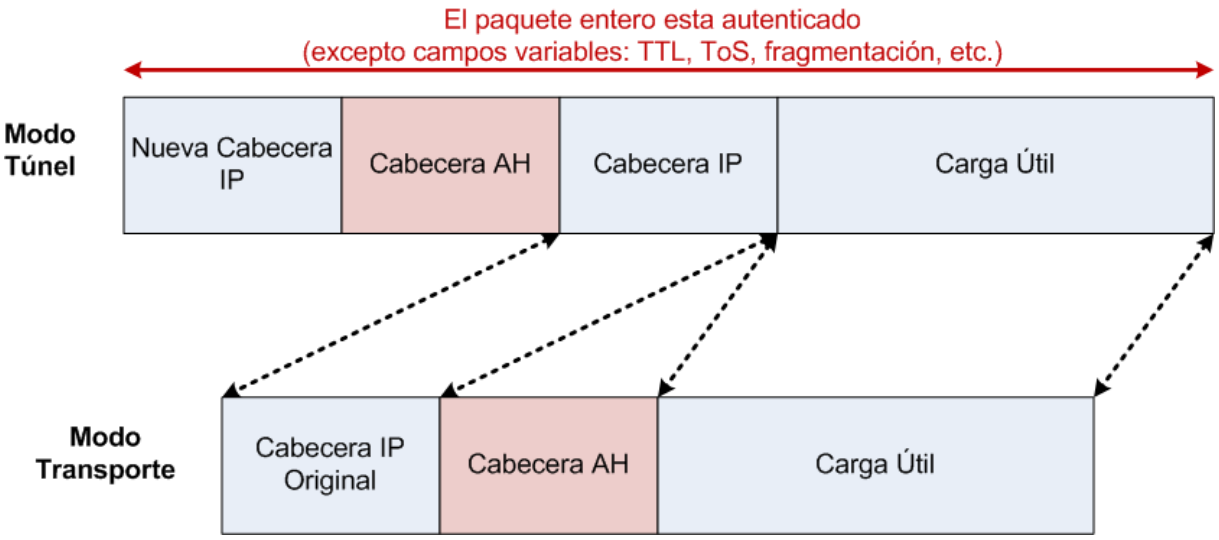

Ilustración 2 - Implementación AH en modo túnel y modo transporte

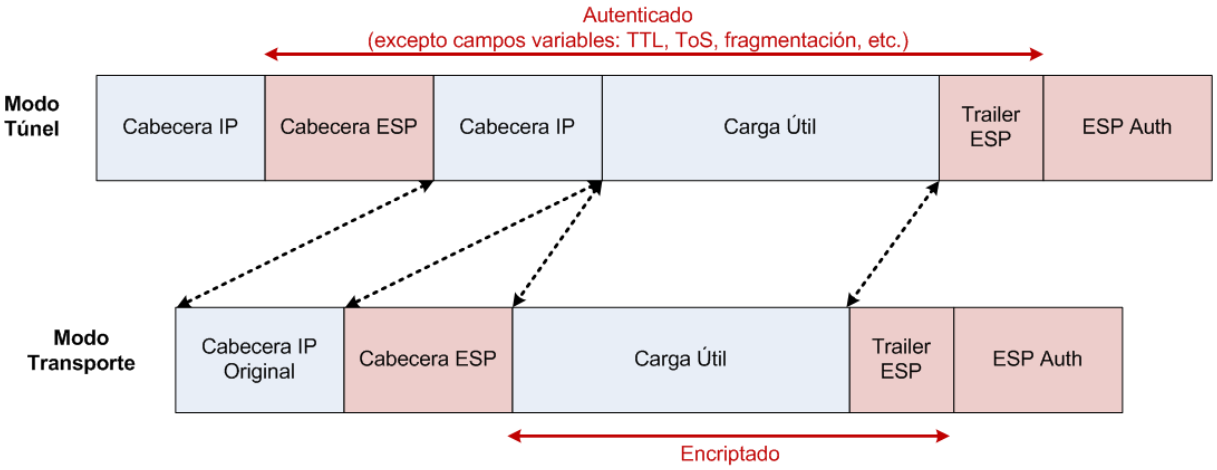

Ilustración 3 - Implementación ESP en modo túnel y modo transporte

En la práctica el uso de IPsec es escaso debido, sobre todo, a la falta de un mecanismo generalizado y global de intercambio de claves. Por esta razón, el uso de IPsec en IPv6 es por el momento similar al de IPv4, para conexiones pre-configuradas como, por ejemplo, las utilizadas en las VPN.

La solución futura para el problema anterior puede que se base en mecanismos externos como certificados transportados por DNS asegurado con DNSSEC[5].

[5] Domain Name System Security Extensions: http://www.icann.org/es/announcements/dnssec-qaa-09oct08-es.htm

3.2. MAYOR FORTALEZA DE LA RED

La nueva versión del protocolo introduce novedades que mejoran la eficiencia del proceso de enrutamiento de los paquetes IP. Lo que permitirá que los elementos de red puedan gestionar mayor número de transmisiones y con mayor rapidez. Los cambios son los siguientes:

- Cabeceras simplificadas y de tamaño fijo.

- No se realiza fragmentación de los paquetes por los elementos intermedios. El tamaño de los paquetes los deberán determinar los extremos de la comunicación. Sin embargo, aunque a largo plazo debería acabar favoreciendo al flujo de datos, esta característica, al ser tan diferente de lo que se hace en IPv4, y al asentarse sobre ICMP, está provocando problemas en la implementación de IPv6, dando lugar a errores de conectividad que están creando la impresión de que IPv6 no funciona completamente bien en la práctica.

- Facilita la agregación en las tablas de enrutamiento debido al uso estricto de CIDR para todos los tipos de direcciones y a la mejor organización de sus asignaciones. Por otra parte, esta mejora es imprescindible debido al gran aumento de direcciones IP que se produce.

- Implementación obligatoria y mejorada del direccionamiento multicast. También se ha creado el direccionamiento anycast, en el que un grupo de servidores que proporcionan un mismo servicio comporten la misma dirección, de tal forma que el servidor seleccionado para dar dicho servicio vendrá determinado por la eficiencia de acceso. Aunque este direccionamiento es difícil de implementar en la práctica y, en su mayoría, es utilizado únicamente por los enrutadores.

- Utilización de etiquetas para QoS en las comunicaciones: el protocolo incluye la posibilidad de etiquetar clases y flujos de comunicaciones para que los enrutadores prioricen unas transmisiones sobre otras.

3.3. OTRAS MEJORAS

- Imposibilidad de exploración de redes mediante "fuerza bruta". Anteriormente, los atacantes o programas maliciosos, como los gusanos, podían encontrar objetivos en una red comprobando todas las direcciones posibles. Pero debido al crecimiento exponencial de su número total, esta exploración es, a priori, inviable.

- Desaparece la necesidad de utilizar NAT. Aunque ha sido una tecnología muy útil, tiene los inconvenientes de que genera una falsa sensación de seguridad y de que se pierde la posibilidad de realizar conexiones seguras de extremo a extremo, incrementando la complejidad y el coste del desarrollo de aplicaciones.

- Se elimina la posibilidad de realizar un ataque DDOS de tipo broadcast o smurf[6] al desaparecer este direccionamiento y al implantarse medidas de seguridad en el multicast.

[6] http://www.cert.org/advisories/CA-1998-01.html

4. CONSIDERACIONES DE SEGURIDAD EN IPv6

Por el momento, el número de problemas de seguridad y ataques sobre IPv6 es pequeño debido a que no está desplegado aún a gran escala. Pero, se espera que la tendencia cambie a medida que los operadores y proveedores de contenidos lo implementen en sus redes y servicios.

En el siguiente apartado se describen los principales aspectos relacionados con la seguridad del protocolo que hay que tener en cuenta desde tres puntos de vista:

- Aspectos técnicos
- Consideraciones de gestión
- Estructura o características propias del protocolo

4.1. ASPECTOS TÉCNICOS

4.1.1. Dispositivos de seguridad que no analizan el protocolo IPv6

Puede que los dispositivos de seguridad, como cortafuegos o IDS, o las herramientas de gestión de red no sean capaces o no estén configurados para analizar los flujos de datos del protocolo IPv6. Si fuera así, se podrían establecer comunicaciones maliciosas desde o hacia equipos de la red que soporten IPv6.

4.1.2. Presencia de dispositivos de los que se desconoce que pueden usar IPv6 y de túneles IPv6

Muchos Sistemas Operativos tienen habilitado IPv6 por defecto, como la mayor parte de sistemas Windows modernos, Mac OS X, Linux y Solaris.

Además pueden existir túneles IPv6. Un túnel es una conexión punto a punto, en la que se encapsulan los paquetes IPv6 en paquetes IPv4, de forma que se pueda transmitir IPv6 a través de una infraestructura IPv4. En el extremo final del túnel, se desencapsula (o extrae) el paquete IPv6 original.

Los dispositivos de seguridad perimetral puede que no estén preparados o configurados para analizar estos flujos de datos, que pueden ser utilizados para comunicaciones no permitidas como, por ejemplo, puertas traseras de C&C (Command and Control) de botnets o de P2P.

La posibilidad de crear túneles IPv6 se encuentra presente en todos los sistemas operativos, como Windows Vista y Windows 7 que tienen habilitado por defecto la tecnología Teredo[7],

[7] http://msdn.microsoft.com/es-es/library/aa965905%28v=VS.85%29.aspx

aunque se deshabilita si detecta que el equipo pertenece a un dominio o tiene soporte IPv6 a través de su red local. Otras formas de implementar túneles que pueden estar presentes son 6to4[8] e ISATAP[9].

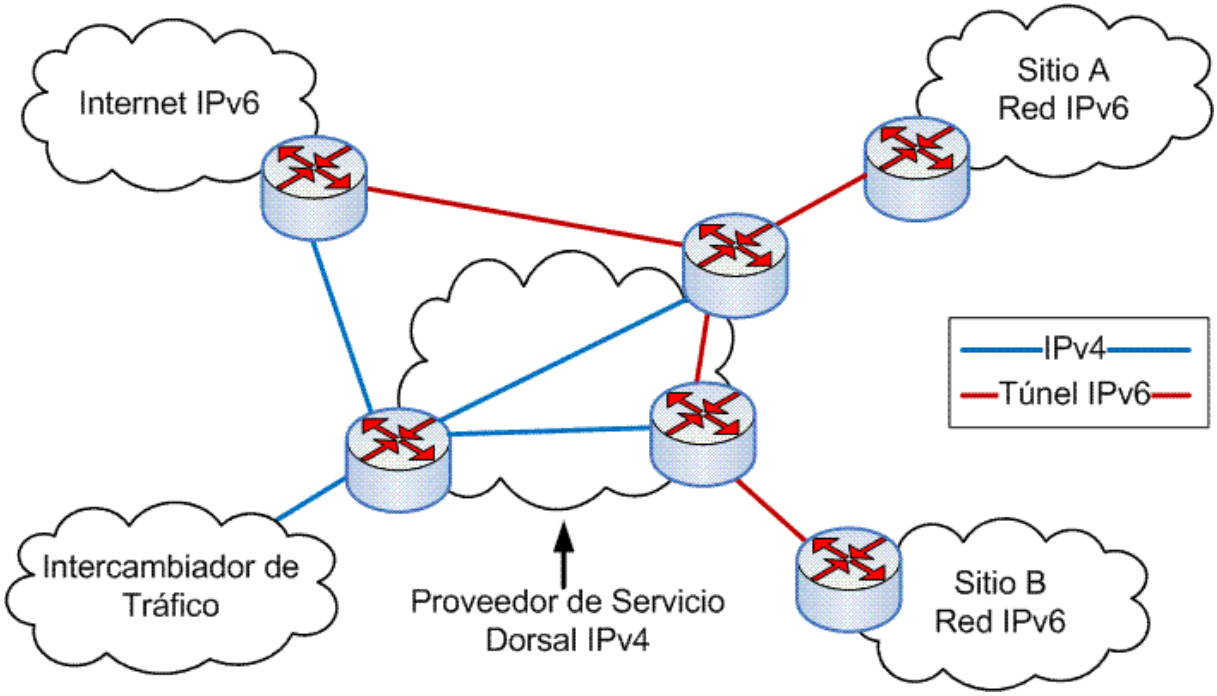

Ilustración 4- Túnel IPv6 en IPv4

4.1.3. Dejar de utilizar NAT

Una consecuencia indirecta del uso de NAT es que se emplea a modo de cortafuegos para proteger los equipos internos de las conexiones externas. Pero ya que IPv6 elimina su necesidad, se deberá modificar la política de los cortafuegos para que, según la política de seguridad, filtre o no las comunicaciones directas a los equipos de la red privada.

4.1.4. Necesidad de multicast e ICMP

Muchos cortafuegos bloquean estos protocolos, aunque ciertas partes pueden ser muy importantes como, por ejemplo, el uso de ICMP para PMTU[10]. En IPv6 son imprescindibles para su funcionamiento; por lo tanto, se deberán modificar las políticas de seguridad para permitir determinadas comunicaciones multicast e ICMP.

[8] http://en.wikipedia.org/wiki/6to4
[9] Intra-Site Automatic Tunnel Addressing Protocol: http://es.wikipedia.org/wiki/ISATAP
[10] Path Maximum Transmission Unit: http://tools.ietf.org/html/rfc1981

4.1.5. Cambio en la monitorización de la red

Debido al gran número de direcciones disponibles será inviable escanear la red por fuerza bruta, por lo que los equipos se inventariarán de otra manera como, por ejemplo, en un servidor DNS.

Sin embargo, posiblemente surjan otras formas de escanear una red: existen direcciones multicast concretas para localizar servicios (por ejemplo FF05::2 All routers, FF05::1:3 All DHCP Servers) y direcciones de link-local, que permiten la comunicación en el segmento de red al que se esté conectado. Un atacante puede utilizar estas direcciones para establecer contacto con equipos o servicios. Aunque, en la práctica, este método no será probable que tenga éxito ya que la mayor parte de los sistemas operativos están configurados para no responder a estas peticiones.

4.1.6. Doble exposición IPv6 e IPv4

Durante años convivirán sistemas con doble pila, que soporten ambas versiones del protocolo, y mecanismos de transición a IPv6, lo que provocará que haya mayores posibilidades de existencia de vulnerabilidades.

Por otra parte, un sistema podrá ser atacado utilizando IPv4, IPv6 o una combinación de ambos, por ejemplo, utilizando IPv4 para detectar el equipo e IPv6 como canal oculto de comunicaciones.

4.1.7. Actualización de protocolos y equipos a IPv6

La gran mayoría de protocolos han sido adaptados para que utilicen direcciones IPv4 e IPv6, como por ejemplo BGP[11] o DNS. La implantación de IPv6 supondrá la instalación y/o configuración de estos protocolos.

Existe el problema de que algunas aplicaciones que trabajan con IPv6 no son actualizadas frecuentemente. También existe actualmente una falta de soporte por parte de algunos fabricantes de enrutadores, switches y cortafuegos, aunque se prevé un mayor impulso a medida que haya una mayor adopción del protocolo.

4.2. CONSIDERACIONES DE GESTIÓN

4.2.1. Curva de aprendizaje

Como con toda adopción de una nueva tecnología, las organizaciones necesitan de tiempo y recursos a la hora de adquirir el conocimiento necesario para implantar y administrar con seguridad el protocolo IPv6.

[11] Border Gateway Protocol: http://tools.ietf.org/html/rfc4271

4.2.2. Implementación de sistemas de doble pila

La implantación de IPv6 supondrá un importante cambio en los sistemas de comunicaciones ya que deberá soportar ambos protocolos y su interoperabilidad. El diseño, implantación y configuración de estos sistemas de doble pila, que implementan IPv4 e IPv6, será un proyecto complejo en el que habrá que evaluar todos los requisitos posibles de seguridad.

4.3. ESTRUCTURA O CARACTERÍSTICAS PROPIAS DEL PROTOCOLO

El uso de IPv4 ha evolucionado con el tiempo, solucionándose los problemas que han surgido debido a su uso generalizado durante muchos años. De este modo se han creado tecnologías como NAT, CIDR o IPsec.

IPv6 puede que sufra un proceso similar, aunque atenuado por la experiencia que se posee con IPv4. Un ejemplo de este proceso de evolución del protocolo, es la decisión de que se rechacen los paquetes que utilizan la cabecera RH0[12], utilizada para definir la ruta de los paquetes, porque se podía utilizar para realizar un ataque de denegación de servicio[13].

Para los puntos descritos a continuación ya hay soluciones disponibles, aunque falta que algunos sistemas operativos las implementen.

4.3.1. Suplantación de identidad en la autoconfiguración de la dirección IP

Una de las novedades del protocolo es la capacidad de una interfaz de generar su dirección IP a partir de su dirección MAC. Durante este proceso el dispositivo pregunta al resto de dispositivos de la red si alguno esta utilizando esa dirección. Además, si el dispositivo está conectado a una red en la que existe un enrutador, recibirá de él el resto de parámetros de configuración como puede ser el prefijo de la red.

Durante este proceso, cualquier dispositivo podría generar de forman continuada una respuesta falsa informando de que la dirección está en uso y provocar que el dispositivo que solicita una dirección no se pueda conectar a la red. También, podría hacerse pasar por un enrutador para realizar un ataque de man-in-the-middle.

El protocolo SEND[14] soluciona este problema, aunque todavía no ha sido implementado en la mayoría de sistemas operativos. SEND es una extensión que mejora la seguridad de protocolo NDP[15], que es el encargado de descubrir otros nodos en la red local, enrutadores, etc. Para realizar sus funciones SEND utiliza encriptación asimétrica y firma electrónica. SEND es una evidente mejora respecto a IPv4 donde no existe nada comparable.

[12] Routing Header tipo 0: http://tools.ietf.org/html/rfc5095
[13] http://www.securityfocus.com/news/11463
[14] Secure Neighbor Discovery: http://tools.ietf.org/html/rfc3971
[15] Neighbor Discovery Protocol: http://tools.ietf.org/html/rfc4861

4.3.2. Privacidad

Al generar un equipo su dirección IP a partir de la dirección MAC, se puede asociar una IP a un equipo de forma unívoca y, a su vez, se puede asociar un equipo a una persona.

Al realizar uso de Internet se deja un rastro de la dirección IP en los distintos servidores o redes con lo que se establece una comunicación. A partir de esta dirección IP se podría saber que servidores web o servicios visitó una persona.

Una solución para este problema consiste en la generación aleatoria de parte de la dirección IP, lo que se conoce como extensiones de privacidad[16]. La gran mayoría de los sistemas operativos soportan las extensiones de privacidad y en algunos incluso están habilitadas por defecto (Windows XP, Vista y 7). Otra posible solución es la asignación temporal de direcciones mediante DHCPv6.

16 Privacy Extensions for Stateless Address Autoconfiguration in IPv6: http://tools.ietf.org/html/rfc4941

5. RECOMENDACIONES DE ACTUACIÓN

5.1. RECOMENCIONES GENERALES

1. Crear políticas de seguridad que tengan en cuenta el protocolo IPv6.

2. Obtener conocimiento de la administración de sistemas IPv6, ya que, aunque en la actualidad se pueda bloquear todo el tráfico IPv6 o se disponga de direcciones IPv4, en el futuro será cada vez más necesario porque los proveedores integrarán sus servicios con IPv6. La mejor forma es hacerlo gradualmente, empezando con pocos servicios muy controlados. Es conveniente comenzar cuanto antes ya que a fecha de Junio de 2010, el espacio disponible de direcciones IPv4 se ha reducido hasta menos del 6%.

3. Disponer de dispositivos de seguridad y herramientas de gestión de red que sean capaces de analizar y, en caso de que sea necesario, bloquear el flujo de datos IPv6 y los túneles o mecanismos de transición IPv6. Seguir, para IPv6, una política de seguridad similar o igual a la usada para IPv4. Por ejemplo, no permitir el paso de un tipo de tráfico para IPv6 cuando no se permite sobre IPv4. Cuando sea necesario permitir el tráfico IPv6, es recomendable, si es posible, definir un subconjunto de reglas y políticas de seguridad diferenciadas para el tráfico IPv6, específicamente para el caso de ICMPv6: como se ha comentado anteriormente, el filtrado de tráfico ICMPv6 puede impactar mucho más directamente en el tráfico permitido y en la conectividad IPv6 de los equipos.

4. Realizar un inventario de los dispositivos con capacidad IPv6 o de realización de túneles IPv6 existentes y deshabilitar esta opción si no es necesaria.

5.2. RECOMENDACIONES EN EL USO DE IPv6

1. En función del grado de control que se quiera dar a cada red se deben usar distintos mecanismos de configuración de direcciones. De menor a mayor control y trazabilidad son:

    - Autoconfiguración Stateless. Existen dos alternativas:

        - Identificador de interfaz mediante números aleatorios (extensiones de privacidad). Esta opción no es recomendable en caso de ser necesario, por razones legales, el tener un registro del uso de la red por parte de cada usuario. Tampoco cuando se necesitan direcciones estáticas, por ejemplo, para aplicaciones Peer-to-Peer (lo que generalmente conlleva el registro de direcciones en DNS.

        - Identificador de interfaz a partir de la dirección MAC.

- Autoconfiguración Stateful utilizando DHCPv6[17].
- Direccionamiento configurado manualmente.

2. Utilizar direcciones no deducibles o previsibles para dificultar la posibilidad de localizar nodos atacables en una red en el caso de direcciones configuradas manualmente.

3. Como norma general se recomienda filtrar tráfico proveniente de prefijos no asignados por IANA o los RIRs[18]. Las direcciones de tipo ULA (Unique Local Address) no deben salir hacia Internet ni entrar a la red ya que son para uso interno. También han de ser filtradas las direcciones correspondientes a la antigua red de pruebas 6Bone y a las direcciones IP de documentación, cuyo prefijo es 2001:0DB8::/32.

[17] Dynamic Host Configuration Protocol for IPv6: http://tools.ietf.org/html/rfc3315
[18] http://www.iana.org/numbers/

6. CONCLUSIONES

Además de solventar la escasez de direcciones IP, el protocolo IPv6 ha sido creado, desde un inicio, con la seguridad y eficiencia como objetivos, medidas como la implantación de IPsec, el nuevo diseño del paquete o la manera de asignar las direcciones IP son la prueba de ello.

No obstante, sustituir un protocolo tan extendido e importante como IPv4 supondrá un desafío de gestión y técnico con implicaciones en la seguridad de los sistemas de información.

Ya que la mayor parte de sistemas operativos tiene la posibilidad de utilizar IPv6, es necesario realizar una política de seguridad que lo contemple y tomar las medidas de seguridad apropiadas para cumplirla.

Debido al agotamiento de direcciones IPv4, a que cada vez existirán más servicios sobre IPv6 y a la aparición de otros nuevos que aprovechan la explosión del número de direcciones IP disponibles, es necesario comenzar a obtener conocimiento y experiencia sobre la implantación y la administración de este protocolo y de los mecanismos de interoperabilidad con IPv4. La mejor forma es hacerlo gradualmente, habilitándolo en unos servicios de manera muy controlada.

7. FUENTES DE INFORMACIÓN

Comisión Europea: http://ec.europa.eu/information_society/policy/ipv6/index_en.htm

ENISA: http://www.enisa.europa.eu/act/res/files/resilience-features-of-ipv6-dnssec-and-mpls/?searchterm=ipv6

SecurityFocus: http://www.securityfocus.com/news/11463

IETF: http://www.ietf.org/rfc/rfc3971.txt

Microsoft: http://technet.microsoft.com/en-us/network/bb530961.aspx

Consulintel: http://www.mundointernet.es/IMG/pdf/ponencia162_1.pdf

NetworkWorld: http://www.networkworld.com/news/2009/071309-ipv6-network-threat.html

Portal IPv6: http://www.ipv6tf.org

IPv6-To-Standard: http://www.ipv6-to-standard.org

[RFC3756] Nikander, P., Kempf, J., and Nordmark, E., “IPv6 Neighbor Discovery (ND) Trust Models and Threats”, May 2004, IETF Request For Comment

[RFC3971] Arkko, J., Kempf, J., Zill, B., and Nikander, P., “Secure Neighbor Discovery (SEND)”, March 2005, IETF Request For Comment

[RFC4193] Hinden, and R., Haberman, B., "Unique Local IPv6 Unicast Addresses", October 2005, IETF Request For Comment

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and Soliman, H., “Neighbor Discovery for IP version 6 (IPv6)”, September 2007, IETF Request For Comment

[RFC4941] Narten, T., and Draves, R., “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, January 2001, IETF Request For Comment

[RFC5095] Abley, J., Savola, P., and Neville-Neil, G., “Deprecation of Type 0 Routing Headers in IPv6”, December 2007, IETF Request For Comment

[RFC5157] T., Chown, “IPv6 Implications for Network Scanning”, March 2008, IETF Request For Comment

Scott Hogg, Eric Vyncke, “IPv6 Security“, Cisco Press, 2008

Daniel Minoli, Jake Kouns “Security in an IPv6 Environment”, Auerbach Publications, 2008