XXX aniversario
novática
UPGRADE Revista de la Asociación de Técnicos de Informática

Nº 174, marzo-abril 2005, año XXXI

sumario

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática). ***Novática*** edita también ***UP****GRADE*, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UPENET** (***UP****GRADE* ***E****uropean* ***NET****work*)

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2** y **ASTIC.**

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Ciudad de Granada 131, 08018 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel,
Isla Cartuja 41092 Sevilla, Tlfn./fax 954460779 <secreand@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Asturias-Cantabria <gp-astucant@ati.es>
Redacción ATI Castilla-La Mancha <gp-clmancha@ati.es>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlfn.986581413; fax 986580162 <secregal@ati.es>
Suscripción y Ventas
<http://www.ati.es/novatica/interes.html>,o en ATI Cataluña o ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica.publicidad@ati.es>
Imprenta
Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Antonio Crespo Foix / © ATI 2005
Diseño: Fernando Agresta / © ATI 2005

Monografía del próximo número: *"Ingeniería de Software Libre"*

Estado del despliegue de IPv6 en 2005

Jim Bound
Chief Technology Officer, IPv6 Forum

<Jim.Bound@hp.com>

Traducción: Alberto Cabellos Aparicio (Dept. d'Arquitectura de Computadors, Universitat Politècnica de Catalunya).

Resumen: *el estado del despliegue de IPv6 (*Internet Protocol version 6*) en el año 2005 está caracterizado por redes experimentales repartidas alrededor del mundo aunque están apareciendo en la Internet pública algunos servicios IPv6 en producción. Existen productos IPv6 en el mercado, preparados para ser desplegados, pero se carece de las herramientas de gestión de red, y de las aplicaciones e infraestructuras de seguridad necesarias para un despliegue comercial. Asimismo, empiezan a aparecer planes de transición y de despliegue operacional, y el modelo de negocio está bastante bien definido para algunos mercados concretos, básicamente motivados por las ventajas tecnológicas que proporciona IPv6. Las diferentes zonas geográficas se están preparando para IPv6 a diferentes velocidades y con diferentes grados de compromiso público. Este artículo sólo puede referirse a la parte de despliegue de IPv6 que es de conocimiento público y que surge de información conocida por el autor. Asimismo, este artículo presenta modelos de despliegue actual de IPv6 y en qué contribuirán a una adopción masiva por el mercado de redes IPv6 en producción. Se discutirán estos modelos, partiendo del conjunto de actuales despliegues de IPv6 en el mundo y de lo aprendido en el IPv6 Forum y en sus grupos de trabajo (ver <http://www.ipv6forum.org>).*

Palabras clave: *conectividad extremo a extremo, despliegue de IPv6, implantación de aplicaciones, implantación de seguridad.*

Autor

Jim Bound es *Chief Technology Officer* del IPv6 Forum, <http://www.ipv6forum.com>, y coordinador del Grupo de Trabajo norteamericano de IPv6, <http://www.nav6tf.org>, y trabaja también la empresa Hewlett-Packard como *Fellow*. Contribuye activamente a los trabajos de estandarización que lleva a cabo el IETF (*Internet Engineering Task Force*) y fue miembro del "IP Next Generation Directorate" del IETF que seleccionó IPv6 en 1994 como el protocolo de nueva generación para Internet. Desde 1978 se ha centrado en las redes como ingeniero y arquitecto para desarrollar nuevos productos. Ha sido galardonado con el premio IPv6 Forum Internet Pioneer como "fontanero jefe de IPv6" (I*Pv6 Lead Plumber*). Como CTO del IPv6 Forum está trabajando como SME (*Subject Matter Expert*) en la Internet Society para el proyecto "Security Expert Initiative".

1. Introducción

Inicialmente, los despliegues piloto de IPv6 (*Internet Protocol version 6*) fueron caóticos, centrándose en las características técnicas básicas del protocolo, pero en la actualidad la atención se está empezando a centrar en las diferentes opciones a la hora de implantarlo. La atención se centra ahora en el despliegue de infraestructuras de red, despliegue que está siendo guiado por los proveedores, las empresas, los clientes, los servicios multimedia y las necesidades de movilidad de las redes de nueva generación.

El impulsor del mercado son los servicios multimedia pues los usuarios requieren movilidad cuando usan sus dispositivos multimedia y este requerimiento da lugar a nuevos componentes de infraestructura de red en la redes de proveedores, empresas y clientes (PECN, *Provider Enterprise and Consumer Networks*). Los prototipos de red del 2005 ayudarán a preparar el despliegue de infraestructura de red IPv6 para PECN y definirán un conjunto de modelos de implantación y de transición que podrán ser usados por la industria o por las Administraciones Públicas.

Este artículo explica el estado general actual de los modelos de despliegue y cómo están ayudando a la implantación comercial de IPv6. Para dar soporte a un despliegue comercial con garantías, debe empezarse por la infraestructura de red, aplicaciones, *middleware*, seguridad y gestión de red, tanto para los mercados PECN como para los usuarios.

La planificación y el análisis operativo para un despliegue de IPv6 masivo en una red requieren experimentación y planificación, que no son imprescindibles sin embargo para empezar con el despliegue de la infraestructura de red y, de hecho, el despliegue actual de IPv6 demuestra este axioma.

El despliegue de IPv6 deberá afrontar también algunos retos tecnológicos y de negocio para implementar los modelos descritos en este artículo, basándose en los mismos supuesto que las redes operativas actuales. Los beneficios de mercado de IPv6 se basan en el modelo extremo a extremo, pero éste no es el modelo de la mayoría de las redes actuales, por lo que se requiere una transformación de la tecnología para el nuevo modelo, además de la propia transición hacia IPv6. La estrategia de negocio para determinar los costes y beneficios de desplegar IPv6 es un proceso en curso para los mercados objetivo PECN.

2. Modelos de despliegue

Los mercados PECN se apoyan en el mismo resorte a la hora de afrontar con posibilidades de éxito el despliegue de IPv6: el proveedor. Los despliegues en empresas y clientes requerirán interoperabilidad con un proveedor y además cada uno de ellos puede ser a su vez un proveedor de su entorno. Esto no es obvio cuando se prepara el despliegue de IPv6 y tampoco lo es la razón por la cual muchos de los requerimientos y funciones para dicho despliegue son comunes en todas las PECN.

Un proveedor proporciona prefijos a una empresa y ésta a su vez proporciona prefijos a su Intranet, o el consumidor a los dispositivos de su red doméstica. La asignación de direcciones IPv6 es similar en el conjunto de los mercados PECN. Esto también es aplicable a los modelos de despliegue que están siendo probados en redes experimentales y en implementación de prototipos.

Las redes experimentales están probando diferentes modelos de despliegue, que son el soporte de IPv6 tanto en el núcleo del enrutado Internet, como en la frontera entre proveedor y cliente, y en las redes cliente. Por ello, dentro de este modelo se ofrecen posibilidades tanto de uso disperso o denso para el despliegue IPv6 nodal de Intranet y de subredes.

La transición a IPv6 en la Internet troncal será la parte más compleja de probar. En la Internet troncal inicialmente se entunelarán paquetes, encapsulando IPv6 en IPv4, o bien se usará el protocolo *Multi Protocol Label Switching* (MPLS) para que viajen paquetes IPv6 por el troncal de Internet de una manera transparente a la infraestructura IPv4 desplegada actualmente. Existen redes piloto que hacen la prueba de transportar paquetes IPv6 por el troncal de Internet y otras redes piloto están empezando a

> El despliegue de IPv6 deberá afrontar algunos retos tecnológicos y de negocio

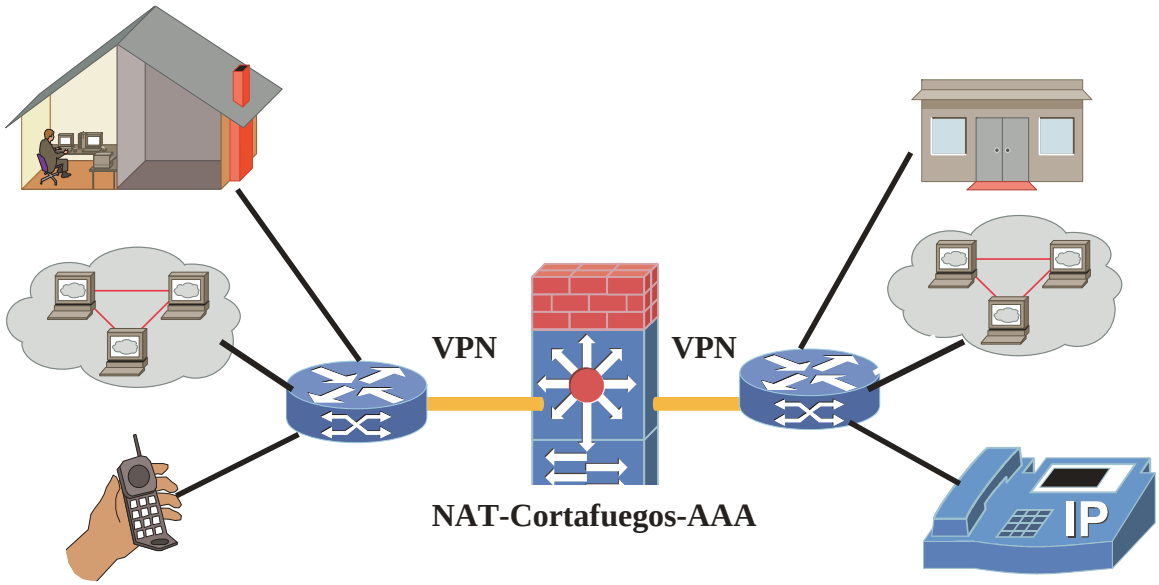

Figura 1. Modelo de seguridad actual.

interconectarse desde diferentes regiones geográficas, lo cual es bueno para poder probar un paradigma de la Internet troncal. En la página web del IPv6 Forum, <http://www.ipv6forum.org,>, se puede ver una lista de redes experimentales en los países que tienen subcapítulos de dicho foro.

En el borde entre proveedor y cliente de las redes experimentales se están probando actualmente paquetes nativos IPv6 y túneles IPv6 sobre IPv4. Cuando no se emplea IPv6 nativo en la Internet troncal, lo que se hace es usar diversos mecanismos de transición a IPv6 para mover IPv6 a través de infraestructuras IPv4 mediante un método de doble pila (*dual stack*).

Esto permite al mercado de PECN poder probar y verificar un modelo de despliegue que se ajuste a su requisito de negocio de dar soporte a una implantación densa o dispersa. El lado proveedor también puede usar IPv6 sobre MPLS con un troncal de Internet que lo soporte (independientemente de si admite IPv4 o IPv6). Esta aproximación se está usando en diversas redes experimentales.

La implementación troncal o a nivel de subred dentro de una red piloto Intranet o PECN se está realizando tomando la *dual stack* tanto para los modelos de despliegue de IPv6 en forma dispersa como densa. En la forma dispersa (*sparse view*) sólo se actualizan los nodos o redes que necesitan funcionar con IPv6; en la forma densa (*wide-use view*) el enrutado IPv6 será predominante frente a IPv4 en los troncales de las Intranet y en las subredes..

3. Despliegue de infraestructura de red

El despliegue actual está verificando la infraestructura de red para dar soporte a la instalación de redes IPv6 en los mercados PECN. Dicha infraestructura incluye el hardware, el software y las aplicaciones necesarias para que una red IPv6 pueda empezar a transmitir datos y dar soporte a la implementación del conjunto de protocolos de Internet en una red y en la red troncal de Internet para comunicaciones extremo a extremo.

El despliegue actual utiliza productos de diferentes fabricantes de diversos países y está demostrando que la infraestructura IPv6 puede proporcionar conectividad e interoperabilidad usando diferentes implementaciones. Se ha verificado la implementación de protocolos de enrutado para IPv6. Las aplicaciones de infraestructura de la red nodal se han utilizado y probado ampliamente así como las comunicaciones nodo a nodo para autoconfiguración, la configuración de parámetros de red para la red y los nodos, la transferencia de ficheros, men-sajería electrónica, acceso a Web y servicios.

También se han verificado y probado las APIs (*Application Program Interfaces*) de IPv6, por lo que los proveedores de aplicaciones pueden migrarlas para dar soporte a IPv6.

También se han implementado mecanismos de transición y han sido probados en redes IPv6, habiendo demostrado su capacidad para soportar diferentes combinaciones de interoperabilidad entre IPv4 e IPv6. Se han usado los modelos de despliegue denso y disperso en diversas redes piloto con interconexión IPv6 nativa (como Moonv6 <http://www.moonv6.org> y <http://www.6net.org>).

El despliegue también ha verificado que los usuarios PECN tendrán una amplia variedad de opciones para la transición y que, dependiendo de su modelo de negocio o de su punto de vista tecnológico respecto a IPv6, podrán utilizar un amplio abanico de mecanismos de transición.

El despliegue de infraestructura de red IPv6 para los mercados PCEN ofrece claramente las siguientes características:

- Existen y de forma comercial productos IPv6 *dual stack*.
- Soporte de comunicaciones IPv6 entre nodos en enlace o subred.
- Los enlaces y subredes IPv6 se pueden intercomunicar a través del troncal de Internet.
- IPv6 da soporte a las aplicaciones de la infraestructura de la red troncal IPv6.

■ Existen mecanismos de transición para soportar interoperabilidad entre IPv4 e IPv6.

Las redes experimentales IPv6 han empezado a desplegar movilidad utilizando IPv6 y a comprobar las ventajas de IPv6 para redes móviles específicas (*Mobile Ad Hoc*) móviles y para movilidad ininterumpida (*Seamless Mobility*).

Así pues, lo anteriormente comentado proporciona una base para un despliegue más amplio de IPv6 que podrá dar soporte al desarrollo de redes de nueva generación en los mercados PECN.

4. Aplicaciones, *middleware* y gestión para el despliegue de IPv6

En general, las aplicaciones y el *middleware* usados para verificar el despliegue de IPv6 han sido software libre y gratuito, y han demostrado que aplicaciones multimedia y servicios web pueden funcionar (y funcionan) eficientemente en una red IPv6. Sin embargo aún no han sido portadas (en el año 2005) aplicaciones de *streaming*, *web proxy caches*, aplicaciones de infraestructura de seguridad como prevención de intrusiones o infraestructura de clave pública, bases de datos, aplicaciones para fabricación y aplicaciones corporativas.

Esto está frenando el despliegue de IPv6, por lo que es absolutamente necesario que para en 2006-2007 todo este conjunto de aplicaciones estén disponibles para los mercados PECN de forma que puedan implementarse operativamente.

Otro requerimiento funcional necesario para IPv6 que aún no ha sido verificado suficientemente son las aplicaciones de gestión de red IPv6 y la interoperabilidad entre IPv4 e IPv6. Se han programado aplicaciones para gestionar redes IPv6 usando SNMP (*Simple Network Monitoring Protocol*) pero no se han integrado con IPv4, algo que será necesario para el despliegue en redes en producción. Las aplicaciones para gestión de red existentes para IPv4 deberán ser portadas para soportar IPv6.

5. Despliegue de seguridad y retos de negocio para IPv6

Hoy en día, los usuarios que acceden a la red utilizan un modelo de seguridad donde la autenticación se hace basándose en un cortafuegos o bien en la implementación del conjunto de protocolos AAA (*Authentication, Authorization, Accounting*). Muchos usuarios están detrás de enrutadores *Network Address Translation* (NAT) que traducen las direcciones origen de la cabecera IP y mantienen el estado de dichas direcciones para comunicarse con nodos y aplicaciones remotas desde su red Intranet. Además, el acceso a la red por algunos usuarios se hace a menudo a través de túneles VPNs (*Virtual Private Networks*) donde la seguridad se localiza en el extremo de la red. En general, los modelos de seguridad de muchos usuarios se basan en que ésta se localiza en el extremo de la red (**figura 1**).

Hoy día los usuarios se conectan a Internet confiando en un tercero, usualmente con un NAT en el extremo de su propia red. Las tecnologías emergentes como el protocolo IPsec (*Secure Internet Protocol*) para comunicación extremo a extremo, o redes *Peer-to-Peer* (P2P) con cifrado, no pueden usarse con NAT, bien porque que estas aplicaciones utilizan la dirección IP como una clave para seguridad de la comunicación o bien porque requieren una dirección IP enrutable globalmente en una red Internet.

El modelo actual no permite el modelo de confianza extremo a extremo, entre dos nodos, usuarios o aplicaciones, ya sean fijas o móviles. Además, NAT no permite que muchas aplicaciones que se basan en tecnología P2P funcionen cuando el nodo sale de la Intranet, impidiendo movilidad ininterrumpida a través de Internet. IPv6 restablecerá la posibilidad de usar aplicaciones en ambos modelos, pero esta misma evolución tecnológica tendrá ramificaciones rompen el modelo de seguridad que la operativa actual de Internet da por supuesto .

Con IPv6 aparece un nuevo modelo que proporciona seguridad extremo a extremo, aunque queda por definir cómo se diseña, se administra, se despliega y se implementa operativamente. La **figura 2** muestra una posible concreción.

El modelo actualizado de la **figura 2** da soporte a las funcionalidades del actual, pero prescinde del NAT para poder dar soporte a la evolución de las aplicaciones P2P así como a la seguridad extremo a extremo. Las VPNs aún están disponibles, pero el Gestor de Seguridad permite un modelo de confianza extremo a extremo para protocolos de seguridad como IPsec.

El modelo actual de cortafuegos proporcionará un entorno de red seguro (dentro de un dominio) en los extremos de la red permitiendo diferentes modelos de seguridad. El Gestor de Seguridad incorporará un sistema de detección de intrusos (IDS, *Intrusion Detection System*) y, si existe un fallo de seguridad en la red, podrá cortar las comunicaciones extremo a extremo y forzar que todas las comunicaciones pasen por el perímetro del cortafuegos como un operación Intranet para las comunicaciones Internet .

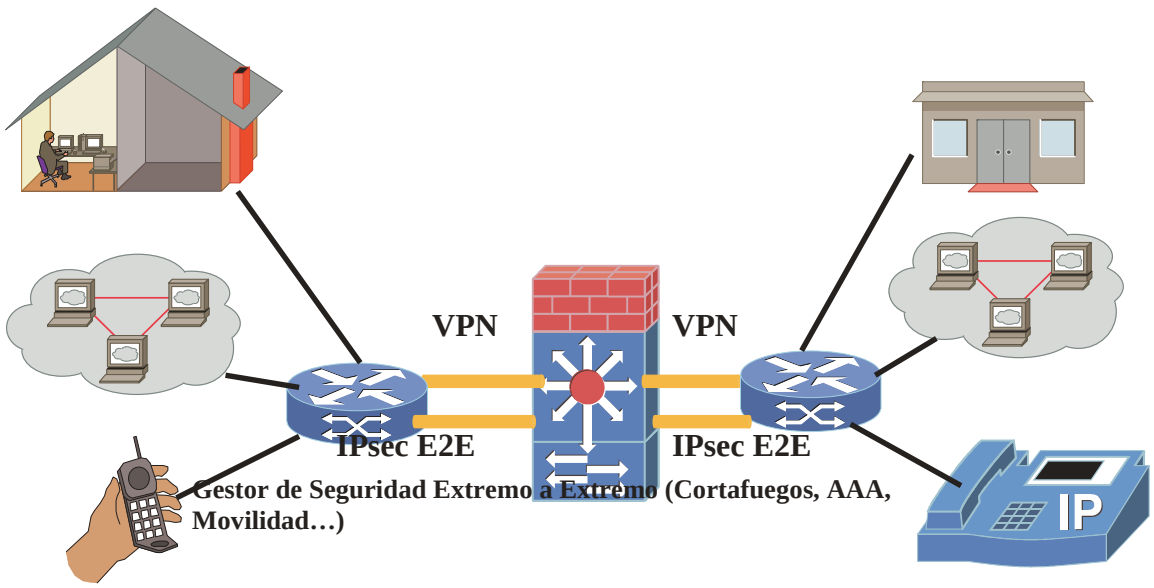

Figura 2. Modelo de seguridad extremo a extremo.

> El modelo extremo a extremo puede dar soporte a la tecnología inalámbrica

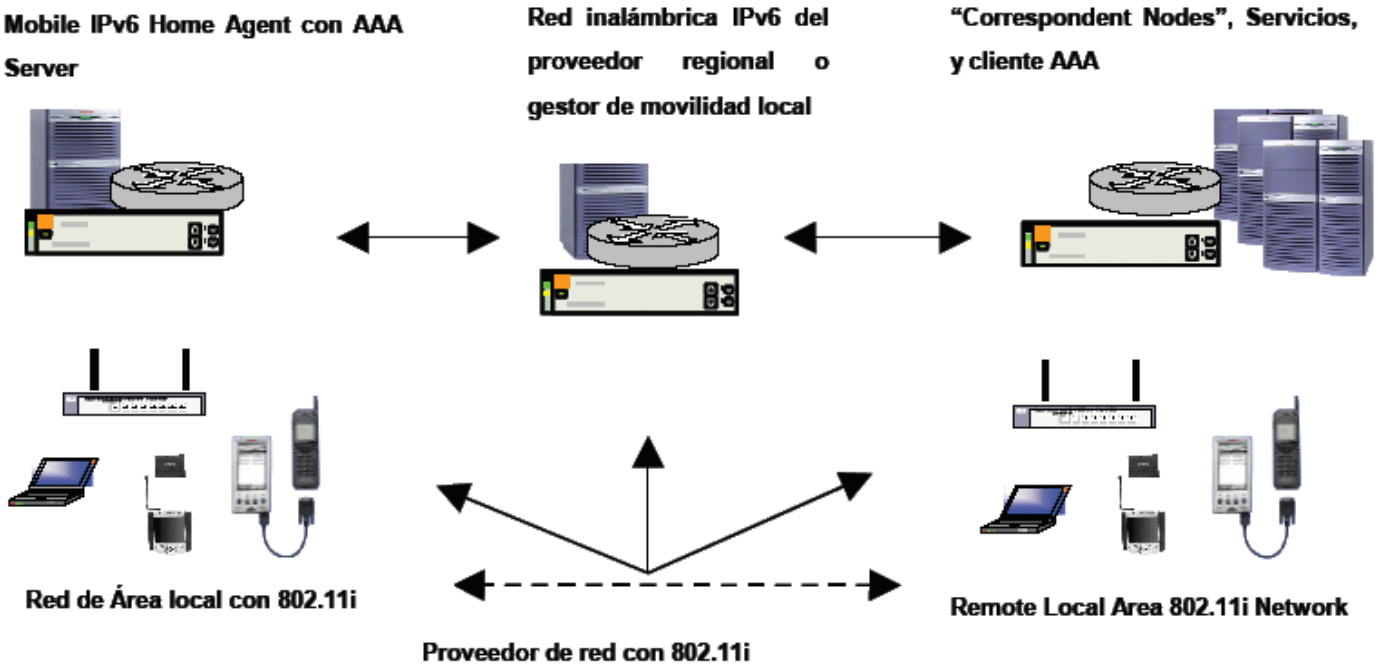

Figura 3. Tecnología inalámbrica y seguridad extremo a extremo.

Este modelo de seguridad considera la red como un todo, y no como un solo punto de entrada, dando soporte a una seguridad centrada en la red.

Este modelo extremo a extremo puede también dar soporte a la tecnología emergente inalámbrica con movilidad ininterrumpida tal y como se muestra en la **figura 3**.

La **figura 3** muestra cómo el Gestor de Seguridad se puede usar con métodos de AAA para permitir el acceso seguro a las redes inalámbricas, además del cifrado soportado por IEEE 802.11i ,que permite el cifrado de los paquetes a nivel 2. El Gestor de Seguridad extremo a extremo con 802.11i dará soporte a movilidad segura conjuntamente con las extensiones de IPv6 móvil a la arquitectura IPv6 que se despliegue.

El trabajo en curso con IEEE 802.11n para proporcionar mayor rendimiento reforzará el método seguro de acceso a redes inalámbricas 802.11i y dará aún mayor efectividad a este método emergente.

La tecnología global necesaria para que las redes permitan un modelo de seguridad extremo a extremo y P2P ya está definida, pero el despliegue de la misma será profundamente disruptivo para el mercado. La evolución tendrá un impacto en los actuales métodos operativos de las redes y en las prácticas de negocio de Internet. Un ejemplo de los retos técnicos a los que nos deberemos enfrentar es que los cortafuegos, filtros e IDS actuales dan por supuesto que pueden acceder a los datos del protocolo de transporte. Sin embargo, según el nuevo modelo éstos no estarán accesibles para las implementaciones cuando los datos se envíen cifrados (por ejemplo con IPsec o 802.11i). Sólo la cabecera IP estará expuesta en los extremos de la red en este modelo. Desde el punto de vista de los negocios, el despliegue y los modelos operacionales actuales para Internet se suelen basar en cifrado en el extremo de la red.

El modelo de seguridad extremo a extremo será disruptivo, pero también proporcionará un modelo superior, más eficiente para las comunicaciones P2P y para las redes que tienen como requerimientos un modelo de confianza extremo a extremo. Este modelo también tiene un mayor rendimiento y ventajas de gestión operativa, una vez que se ha creado la infraestructura para dar soporte a un entorno seguro para aplicaciones P2P, que crecerá guiado por la evolución de la comunicación móvil ininterrumpida, y para la aparición de a una sociedad móvil para los negocios y para la gente en general.

Este nuevo modelo puede ser también un estímulo económico para nuevos negocios, para los que quieran adoptar esta tecnología lo antes posible y para proveedores que proporcionen productos y servicios para la transición hacia un modelo de seguridad extremo a extremo, y los primeros que lo adopten serán los que saquen los mayores beneficios de esta nueva tecnología.

Además, con IPv6 tenemos la posibilidad de hacer descubrimiento de nodos y operaciones de red, facilidades que proporcionarán mayores beneficios para las redes de nueva generación y para la movilidad. No obstante, en una red inalámbrica los nodos y la infraestructura que den soporte a estas nuevas posibilidades deberán también afrontar los nuevos problemas de seguridad de red que conllevan estos mecanismos.

El actual despliegue ha comenzado a probar IPsec extremo a extremo, y el modelo de seguridad comentado anteriormente se está diseñando para ser implantado en diversas redes experimentales. Las aplicaciones de seguridad para IPv4 deberán migrarse a IPv6 para su despliegue masivo en redes de producción.

Agradecimientos

El autor quiere agradecer la información compartida y dar las gracias a los miembros del IPv6 Forum, a los Grupos de Trabajo de IPv6, a empresas, fabricantes, representantes de las Admnistraciones Públicas y personas que le han proporcionado la información sobre el despliegue actual que se presenta en este artículo.