Un viejo mito: IPv6 usa IPsec, y por ésto, es más seguro que IPv4

Uno de los mitos más antiguos relacionados con la seguridad en IPv6 es que por defecto agrega una capa de seguridad con IPsec, lo cual no es cierto.

En este artículo explico por qué pienso que una de las razones para esta creencia radica en la mala interpretación del RFC 4294 «IPv6 Node Requirements» (año 2006) y que, a pesar que en su primera actualización (RFC 6434, año 2011) es más claro que IPsec no es obligatorio en IPv6, aún existen referencias en cursos, blogs y documentación con este error.

Además, expongo por qué nunca debió tomarse como una ventaja, pues IPsec en IPv6 no agrega nada nuevo con respecto a IPv4 y que un análisis rápido de los requisitos de IPsec hacen que al menos hoy utilizarlo para todas las conexiones no es factible ni escalable en la práctica.

La seguridad es clave para el despliegue de IPv6 y asumir una protección que no se tiene, puede ser algo riesgoso.

Existen muchos temas de estudio asociados a la seguridad en IPv6 pero este artículo se enfoca únicamente en lo relacionado con IPsec. Para una visión general de la seguridad en IPv6, recomiendo la lectura del RFC 4942 «IPv6 Transition/Coexistence Security Considerations» y el draft-ietf-opsec-v6-21 «Operational Security Considerations for IPv6 Networks».

Las citas en español son mi propia traducción, para cualquier referencia formal, debe utilizarse el texto original en inglés. Los títulos de los RFCs considero que es mejor conservarlos en inglés.

Interpretación de MUST, SHOULD, MAY

Todo RFC debe ser claro en el ámbito y rigurosidad de sus requerimientos. Para evitar ambigüedades, el RFC 2119 «Key words for use in RFCs to Indicate Requirement Levels» define las palabras clave que deben utilizarse para describir los requerimientos de forma precisa.

Hay cinco palabras clave en el RFC 2119 y estos son sus significados:

- MUST (debe): requerimiento absoluto.
- MUST NOT (no debe): prohibición absoluta.
- SHOULD (debería): recomendado.
- SHOULD NOT (no debería): no recomendado.
- MAY (puede): opcional.

Estas palabras —escritas siempre en mayúscula— deben usarse con austeridad, únicamente cuando sean realmente requeridas, sobre todo, para temas de seguridad.

Un «DEBE» mal interpretado

La sección de seguridad (Sección 8) del RFC 4294 «IPv6 Node Requirements» contiene dos requerimientos absolutos:

> «La arquitectura de seguridad para el protocolo de internet [RFC-4301] DEBE ser soportada»
>
> «ESP [RFC-4303] DEBE ser soportado. AH [RFC-4302] DEBE ser soportado.»

La Sección 8 tiene más requerimientos relacionados con IPsec, pero estos dos son suficientes para sustentar la idea.

Esos requerimientos absolutos (presentados como MUST) hacían que para que un nodo IPv6 se considerara que cumplía con los estándares, debía soportar esos protocolos.

Lo anterior sin embargo nunca significó que el tráfico IPv6 utilizaba por defecto la suite de protocolos de IPsec para autenticar y cifrar los paquetes. Lo único que implicaba era que el sistema operativo de un dispositivo (un servidor, una computadora, un teléfono, un sensor) en su implementación debía tener la capacidad de utilizar IPsec, si quien configuraba este dispositivo así lo deseaba.

Es por esta razón que planteo que fue la mala interpretación de ese «DEBE» en el texto del RFC 4294 la causa de que se difundiera durante años que el tráfico IPv6 hacía uso, de forma automática, de todas las prestaciones de IPsec y sus protocolos relacionados. Fue más que una mala interpretación de un concepto técnico, un error al entender el alcance del requisito.

Escalabilidad

Más allá del error de interpretación comentado antes, conocer cómo opera IPsec debió evitar que se pensara que todo el tráfico de IPv6 tenía IPsec de forma predeterminada pues —al menos con el poder computacional de hoy— no es realizable que todas y cada una de las comunicaciones estén protegidas con IPsec.

Por ejemplo, algunos mensajes necesarios para la operación de ICMP utilizan multicast y utilizar IPsec para esos mensajes, no es factible.

Por otro lado, el manejo de llaves para soportar cada una de las conexiones en Internet, en definitiva no es algo que pueda considerarse fácil de administrar.

Las limitaciones de hardware también son una consideración importante pues pequeños dispositivos como sensores podrían no tener el procesamiento suficiente para el soporte de IPsec.

Y como último ejemplo, el reto del análisis de tráfico cifrado (ETA, Encrypted Traffic Analytics) en los *firewalls*. Los fabricantes de dispositivos de seguridad desarrollan tecnologías que analizan la conducta del tráfico cifrado y mediante técnicas de comportamiento e inteligencia artificial, intentan detectar el tráfico que puede ser malicioso. A pesar de que estas técnicas mejoran cada día, representan una carga adicional al procesamiento del equipo y no son determinantes. Si bien la tendencia es cifrar cada vez más tráfico, para cuando se escribió el RFC 4294 el análisis de tráfico cifrado apenas iniciaba por lo que este es otro argumento para haber descartado desde un inicio que todo el tráfico IPv6 estaría cifrado de forma imprescindible.

De «DEBE» a «DEBERÍA» para un mejor apego a la realidad

Por las limitaciones descritas y otras consideraciones que pueden encontrarse en el RFC 6434 (actualización RFC 4294), el nuevo texto cambió de «DEBE» a «DEBERÍA» el requisito de IPsec en los nodos IPv6, siendo ahora explícito que es una recomendación y no una obligación.

El tema de la seguridad está en la Sección 11 y específicamente en 111 dice:

> «La arquitectura de seguridad para el protocolo de internet [RFC-4301] DEBERÍA ser soportado por todos los nodos IPv6».

Nótese que el cambio no fue para evitar una lectura incorrecta del requisito, sino que fue consecuencia de que no era un requisito realista en la práctica.

Ya no hay entonces espacio para la duda: no debe considerarse IPsec como un requerimiento absoluto en un nodo IPv6 de ahí que no es —ni nunca fue— una ventaja de seguridad sobre IPv4.

Me resulta importante mencionar que hago referencia al RFC 6434 pues fue el documento donde cambió el texto de «DEBE» a «DEBERÍA», pero este ya fue actualizado con el RFC 8504, el cual tiene estatus de mejor práctica, y es el documento vigente para los requerimientos de un nodo IPv6.

¿Tiene IPv6 seguridad en su diseño?

Relacionado con lo expuesto hasta aquí está la creencia que IPv6 tiene la seguridad considerada en su concepción y que por eso, es superior a IPv4 en seguridad desde su diseño, lo cual también es falso.

IPsec no es nuevo y ha trabajado tanto con IPv4 como con IPv6 desde que se estandarizó originalmente en el RFC 2401 «Security Architecture for the Internet Protocol».

La versión vigente (RFC 4301) mantiene el mismo enfoque por lo que cualquier implementación de IPsec en IPv6 no ofrece nada diferente a lo que ofrece en IPv4. La Sección 2 está dedicada a los objetivos de diseño, y arranca diciendo (sección 2.1):

> «IPsec está diseñado para brindar seguridad basada en cifrado que sea interoperable y de alta calidad para IPv4 e IPv6. […] Estos servicios se brindan en la capa IP, ofreciendo protección de manera estándar para todos los protocolos que pueden transportarse a través de IP (incluido el propio IP).»

Además, como lo indica en las suposiciones (sección 2.2):

> «[…] la seguridad que ofrece el uso de estos protocolos depende en última instancia de la calidad de su implementación, que está fuera del alcance de este conjunto de estándares. Además, la seguridad de un sistema informático o de una red depende de muchos factores, incluyendo personal, físico, procedimental, emanaciones comprometedoras, y prácticas de seguridad informática. Así, IPsec es solo una parte de una arquitectura general de seguridad del sistema.»

Es claro que en la propia definición del estándar no hace diferencia entre las dos versiones del protocolo IP y nos recuerda además que la seguridad informática no radica en lo que esté escrito en un estándar sino que es un problema con diferentes consideraciones.

Encabezados de extensión

Un último tema relacionado es el de los encabezados de extensión. IPv6, a diferencia de IPv4, tiene un encabezado de longitud fija por lo que las opciones se colocan en encabezados de extensión entre el encabezado IPv6 y el encabezado de la capa de transporte. IPsec se apalanca en estos encabezados de extensión para realizar sus funciones (por ejemplo, autenticación y cifrado) y podría pensarse que es una implementación más eficiente que en IPv4. En la práctica, con la capacidad de procesamiento actual y con la madurez de IPsec en IPv4, que IPsec esté en los encabezados de extensión en IPv6 no representa ninguna ventaja en cuando a desempeño y eficiencia en el manejo de paquetes.

Conclusiones

En el tema específico de la seguridad que IPsec ofrece a IPv6, no existe diferencia con respecto a lo que ofrece a IPv4. Debido a una mala interpretación del requisito obligatorio de IPsec en los nodos IPv6 (en el RFC original), se asumió que IPv6 tenía una ventaja con respecto a IPv4 al cifrar por defecto todo el tráfico IPv6, lo cual jamás fue cierto y además, conociendo cómo funciona IPsec, debió haberse descartado esta suposición por temas de escalabilidad e implementación práctica. La seguridad que ofrece IPsec depende de la calidad de la implementación y el uso que se le dé al protocolo.

La investigación y la escritura de este artículo se hizo utilizando únicamente software libre y herramientas gratuitas. Pop!_OS ghostwriter

Referencias

- Carter, Earl. «IPv6 Myths». Cisco Blog, febrero de 2011. http://blogs.cisco.com/security/ipv6-myths.
- Caudill, Benjamin. «IPv6 Security: Myths in the Stack». Strategic Blog, https://rhinosecuritylabs.com/network-security/ipv6-security-myths/.
- Grundemann, Chris. «IPv6 Security Myth #2 – IPv6 Has Security Designed In». Internet Society Deploy360, enero de 2015, https://www.internetsociety.org/blog/2015/01/ipv6-security-myth-2-ipv6-has-security-designed-in/.
- Johansson, Olle E. «IPv6 security – the same, but different». IPv6 Friday, marzo de 2012, https://ipv6friday.org/blog/2012/03/ipv6-security-part-one/.
- White, Russ. «IPv6 Security Considerations». CircleID Blog, 1 de octubre de 2018, http://www.circleid.com/posts/20181001_ipv6_security_considerations/.
- Worthman, Ernest. «IPsec Security In IPv6». Semiconductor Engineering, Abril de 2015, https://semiengineering.com/ipsec-security-in-ipv6/.

RFCs

- Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, Marzo 1997, https://www.rfc-editor.org/info/rfc2119.
- Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", BCP 220, RFC 8504, DOI 10.17487/RFC8504, Enero 2019, https://www.rfc-editor.org/info/rfc8504.
- Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, DOI 10.17487/RFC6434, Diciembre 2011, https://www.rfc-editor.org/info/rfc6434.
- Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, Diciembre 2005, https://www.rfc-editor.org/info/rfc4301.
- Loughney, J., Ed., "IPv6 Node Requirements", RFC 4294, DOI 10.17487/RFC4294, Abril 2006, https://www.rfc-editor.org/info/rfc4294.

Autor:
Ing. Luis Carlos Solano López
Miembro de la CIETEL