Informe sobre el IETF 114

Filadelfia, reunión híbrida

23 al 29 de julio de 2022

El informe ha sido preparado por CENTR y traducido por LACTLD

Agradecemos a Hugo Salgado (NIC Chile) por la revisión de la edición en español

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Contenidos

El DNS sigue siendo un tema de actualidad

Se duplica la asistencia presencial, pero se mantiene el formato híbrido por ahora.

Introducción

La misión del Grupo de Trabajo de Ingeniería de Internet (IETF) es mejorar Internet. Y todo el mundo es bienvenido a participar. Una gran comunidad internacional produce documentación técnica de alta calidad sobre el diseño, el uso y la gobernanza de Internet.

La mayor parte del trabajo del IETF se realiza en línea, mediante listas de correo. Tradicionalmente, la organización también ha celebrado tres reuniones al año, además de ocasionales reuniones intermedias para grupos más pequeños. Sin embargo, la pandemia de COVID 19 tuvo importantes consecuencias para estas reuniones. Entre marzo de 2020 (reunión 107) y noviembre de 2021 (reunión 112), todas las reuniones del IETF fueron completamente virtuales. Toda la participación fue en línea e implicó horas muy poco sociales para algunos "asistentes" remotos.

Desde la reunión 113 (marzo de 2022, Viena), el IETF ha adoptado un formato de reunión híbrido. De los 1.428 participantes en esa reunión, el 22% asistió en persona y el resto virtualmente. En la reciente 114ª reunión (julio de 2022, Filadelfia) la asistencia presencial fue el doble que en Viena, con más del 43% de los 1.427 participantes registrados presentes físicamente. Este aumento ilustra cómo se valora la interacción personal y se considera que favorece una colaboración útil y productiva.

Una reunión del IETF supone una semana repleta de numerosas sesiones de grupos de trabajo dedicadas a una gran variedad de temas, desde la Internet de las cosas hasta los derechos humanos, como la privacidad. Muchos de los procedimientos son relevantes para la comunidad CENTR. Los estándares de Internet, como DNS(SEC), IPv6 y BGP, constituyen un elemento integral e importante de nuestra actividad principal. Por eso, es pertinente resumir lo que se dijo sobre estos temas en la reciente 114ª reunión del IETF.

Breve resumen de la semana:

Actividades informales

Para que todo el mundo se animara, durante el fin de semana previo a los actos principales se celebraron un Hackathon, el IEPG y el HotRFC.

Hackathon

La semana del IETF comenzó el sábado con un hackathon informal. Al fin y al cabo, el lema del IETF es que creemos en el "consenso general y en el código que funciona"[1]. Es bueno que los conceptos teóricos se pongan a prueba en entornos prácticos y que se verifique su aplicabilidad e interoperabilidad. Eso es lo que pretende conseguir el hackathon. Pero también tiene una importante dimensión social. Se forman espontáneamente grupos ad hoc y se realizan todo tipo de experimentos. Un buen ejemplo del hackathon IETF 114 es este: Instalación de pruebas de interoperabilidad L4S (redes de baja latencia).

Otros participantes abordaron temas como IPv6, IPsec / IKEv2, DNSSEC *bootstrapping* y la notificación detallada de errores de DNS, por nombrar solo algunos de una larga lista. Dos días de intenso debate y programación concluyeron con la presentación de los resultados.

IEPG

Ya es tradicional que el domingo de una semana del IETF comience con el IEPG. Se supone que esta reunión informal es para considerar asuntos de relevancia operativa, pero la demarcación es bastante laxa. En el IEPG de Filadelfia hubo presentaciones sobre QUIC, pruebas de cabeceras de extensión IPv6, DANE y medición de validación de origen de rutas (ROV) RPKI. Para esta última presentación, los investigadores configuraron un anuncio de ruta agregado válido y un anuncio de ruta más específico no válido en el contexto de RPKI, como se describe aquí. A continuación, se realizaron una serie de mediciones. La conclusión del estudio es que RPKI ROV no garantiza que el tráfico llegue siempre al destino solicitado. No obstante, la tecnología sigue siendo un medio recomendado para evitar el secuestro de rutas y, sobre todo, los fallos humanos.

En el sitio web de RIPE Labs se puede consultar un informe más detallado.

[1] "Rough consensus and running code"

HotRFC

El domingo concluyó con la llamada "HotRFC", otro evento informal en el que se animó a los candidatos a comentar diversos temas durante breves "charlas relámpago". ¿Tiene una idea, un problema o una propuesta que cree que la gente del IETF debería conocer? ¿Cree que hay algo que el IETF debería abordar, pero cree que sus ideas necesitan más trabajo, o quiere medir el interés antes de seguir adelante? Si es así, la sesión HotRFC es su oportunidad para empezar a trabajar.

Una vez más, se planteó una amplia selección de preguntas, como ¿qué ha hecho el IETF hasta ahora para promover una Internet más ecológica y sostenible y normas de conservación de la energía? ¿Podría el IETF hacerlo mejor? ¿Qué retos se plantean? También se debatieron los retos y las oportunidades asociados a la criptografía post-cuántica. Protocolos como IPSEC, TLS, DNSSEC y otros utilizan la criptografía. ¿Qué seguridad tendrán los algoritmos criptográficos relacionados cuando se utilicen los ordenadores cuánticos? Una de las organizaciones que ha investigado el asunto es el NIST, que ha recomendado una serie de algoritmos que se espera que sigan siendo seguros. Sin embargo, el uso de los algoritmos supone una carga computacional adicional para los servidores. Por tanto, es importante mirar hacia el futuro y evaluar el impacto de la adopción de algoritmos de seguridad cuántica.

Procedimiento formales

La conferencia propiamente tal comenzó el lunes (25 de julio de 2022).

De los muchos temas que se trataron, los siguientes merecen ser considerados aquí.

SAVNET

Junto con el anuncio deliberado o accidental de prefijos de direcciones incorrectos, contra los que RPKI puede proteger, la suplantación de direcciones de origen es otro problema común. El tráfico UDP es especialmente fácil de falsificar sin necesidad de utilizar métodos sofisticados. En consecuencia, los estándares basados en UDP, como NTP, SNMP y DNS, en los que simples consultas de unos pocos bytes generan respuestas mucho más grandes, son vectores atractivos para los ataques DDoS de amplificación.

Hace tiempo que se idearon soluciones a este problema, como el conocido BCP38. Sin embargo, el problema ha persistido, lo que ha llevado a la reciente publicación de un documento complementario, el RFC8704. El Grupo de Trabajo de SAVNET, creado formalmente en la reunión anterior, también está estudiando

esta cuestión. Ha comenzado a explorar varias vías posibles, con el objetivo de tener una RFC lista para su publicación y presentación al proceso del IESG en marzo de 2025.

Descubrimiento adaptativo de DNS (ADD) y DPRIVE

Naturalmente, los miembros del IETF tienen un gran interés en todo lo relacionado con el DNS, y la organización le dedica una atención considerable. Los grupos de trabajo DNSOP, ADD y DPRIVE siguen siendo muy activos, y numerosos desarrollos dentro del IETF son relevantes para nuestro sector.

El Grupo de Trabajo DPRIVE y el Grupo de Trabajo ADD celebraron una sesión conjunta, lo que refleja el solapamiento entre sus ámbitos de actividad. DPRIVE se ocupa del desarrollo de normas destinadas a mejorar la confidencialidad, autenticidad y privacidad del DNS, como el DNS sobre TLS (DoT) y ahora también el DNS sobre QUIC (DoQ). Por su parte, ADD trabaja en el campo del descubrimiento automatizado de estos servicios. Por lo tanto, los dos grupos de trabajo se complementan mutuamente.

Cabe destacar que, si bien las normas mencionadas funcionaban originalmente de forma exclusiva entre el cliente y el resolutor, ahora se están tomando medidas para cifrar la ruta entre el resolutor recursivo y el servidor “autoritativo” (y para utilizar TLS para las actualizaciones de archivos de zona entre pares de servidores autoritativos).

Con el fin de promover la adopción de la encriptación (especialmente DoT y DoQ) entre el cliente y el servidor autoritativo, se ha publicado un borrador que define un método que los resolutores pueden utilizar para comprobar si un servidor autoritativo es accesible utilizando DoT o DoQ. Esto se haría de forma oportunista, con soporte para el uso de un certificado "autofirmado" como certificado TLS. Si se encuentra que un servidor es accesible usando DoT o DoQ, el resolutor podría entonces cambiar de protocolo, por ejemplo, de Do53 a DoT.

Parece que los resolutores de DNS públicos de Google, por lo menos, ya realizan este tipo de sondeo unilateral, lo que tal vez sugiere que este enfoque ganará rápidamente terreno.

Aunque hubo brevemente un grupo de trabajo separado para el DNS sobre HTTPS (DoH) —que por lo tanto no es estrictamente un desarrollo de DPRIVE—, DoH se considera a menudo junto con DoT y DoQ. En consecuencia, hoy en día, el usuario puede elegir potencialmente entre múltiples “sabores” de resolución, así como el DNS tradicional, no cifrado (también conocido como Do53).

Como ya se ha mencionado, el grupo de trabajo ADD está desarrollando mecanismos de descubrimiento que permitan al usuario seleccionar el resolutor

más apropiado automáticamente, en segundo plano. Así, se podría seleccionar un resolutor DoH disponible con preferencia al resolutor Do53 clásico designado. Sin embargo, esto requeriría que el cliente conociera la existencia y la ubicación del resolutor DoH. Por lo tanto, se ha propuesto que el descubrimiento de un resolutor designado sea habilitado por medio de registros DNS especiales.

El sistema funcionaría como sigue. Supongamos que un cliente ha obtenido la dirección IP de un resolutor Do53 de la forma tradicional. Para establecer si un servidor DoH también está disponible, el cliente enviaría una consulta Do53 tradicional para el qtype SCVB y el qname _dns.resolver.arpa. La respuesta DNS asociada podría ser la siguiente:

```
_dns.resolver.arpa.  IN SVCB 1 doh.example.nl (

alpn=h2 dohpath=/dns-query{?dns} )
```

Esto le dice al cliente que, en este caso, hay un resolutor de DoH disponible en https://doh.example.nl/dns-query?dns=[algo].

Además de ese registro SVCB, la "sección adicional" de la respuesta DNS incluiría registros A y/o AAAA para (en este caso) "doh.example.nl" con el fin de evitar la necesidad de una serie de consultas DNS adicionales.

Según el borrador, los resolutores DoT y DoQ (QUIC) podrían descubrirse de forma similar.

Se está desarrollando otro borrador que propondrá un mecanismo para comunicar al cliente información similar sobre los resolutores DoT, DoH y DoQ utilizando la opción DHCP(v6).

DNSOP

Del Grupo de Trabajo del DNSOP (y de otros grupos) siguen saliendo muchas ideas y documentos relacionados con el DNS. No menos de diecisiete borradores activos están siendo considerados por el DNSOP, y hay otros seis borradores caducados que podrían reactivarse en el futuro. Evidentemente, son demasiados para considerarlos en detalle aquí. Sabemos de otros treinta y seis borradores relacionados con el DNS que no están siendo considerados por ningún grupo de trabajo existente. Es posible que haya más, ya que solo hemos contado los borradores con "DNS" en el título.

Con el fin de comprender mejor cómo se relaciona la plétora de propuestas con el DNS, durante esta sesión se propuso el restablecimiento de una Dirección (*Directorate*) del DNS formada por un pequeño número de expertos voluntarios. Se espera una propuesta más sustantiva en el futuro.

Otra novedad digna de mención es que, desde la anterior reunión del IETF, el "draft-ietf-dnsop-nsec3-guidance" se ha convertido en el RFC9276. Para cualquier operador de registro/DNS de TLD que utilice NSEC3, sin duda vale la pena leer esta RFC y considerar sus recomendaciones.

En pocas palabras, los autores aconsejan configurar NSEC3PARAM con cero iteraciones y una sal ("*salt*") vacía, por ejemplo:

tld. IN NSEC3PARAM 1 0 0 –

La RFC explica la razón de este consejo, que algunos TLDs (incluyendo .com y .uk) han implementado desde entonces.

Además, dos notables borradores –'draft-ietf-dnsop-rfc5933-bis' y 'draft-ietf-dnsop-avoid-fragmentation'– han pasado a la fase de "última llamada del GT". Merece la pena leer este último, preferiblemente seguido de 'draft-ietf-dnsop-glue-is-not-optional. Cualquiera que busque un resumen conciso de las RFCs relacionadas con DNSSEC probablemente encontrará muy útil 'draft-ietf-dnsop-dnssec-bcp'. Nuestro último consejo de lectura es 'draft-ietf-dnsop-dnssec-validator-requirements'.

Durante la propia sesión del grupo de trabajo, se presentaron varias ideas nuevas, entre ellas, el 'draft-yorgos-dnsop-dry-run-dnssec'. Este borrador propone un mecanismo que permitiría realizar un "ensayo" de una nueva configuración de DNSSEC, sin poner en riesgo la configuración operativa. Este mecanismo se considera deseable porque es fácil cometer errores, y DNSSEC tiende a ser implacable. Las consecuencias potencialmente graves de los pequeños errores son muy similares a Slack. El mecanismo propuesto en el borrador debería reducir considerablemente la probabilidad de tales incidentes. Se trata de definir un nuevo tipo de resumen (*digest*) para incluirlo en los registros DS, que indicaría a los resolutores que están validando que la prueba está en curso, y que la respuesta no debe considerarse falsa en caso de que haya un problema de validación. No obstante, sería posible informar de estos problemas, por ejemplo, utilizando el método de errores de DNS ampliado.

El proyecto está todavía en desarrollo, pero el concepto es interesante y potencialmente atractivo para su uso futuro en diversas circunstancias, con el fin de minimizar el impacto de los errores de DNSSEC.

IRTF

La mayoría de los grupos de trabajo del IETF se ocupan de la producción de estándares de Internet. Sin embargo, algunos de ellos se dedican a la investigación más general. Estos grupos de trabajo se encuentran bajo el

paraguas del Grupo de Trabajo de Investigación de Internet (IRTF) y cubren regularmente algunos temas interesantes.

Por ejemplo, uno de los temas que estudia el Grupo de Investigación sobre la Internet Descentralizada (DINRG) es la creciente centralización de Internet (y cómo contrarrestarla). Durante la sesión, se presentaron los resultados de un taller anterior sobre el tema. La conclusión central del taller fue que es poco probable que el problema se resuelva por sí solo y que, por tanto, será necesaria la intervención de la comunidad de Internet.

Las sesiones del Grupo de Medición y Análisis de Protocolos (MAPRG) son bien conocidas por la calidad de sus contenidos. En la reunión de Filadelfia, la actualidad de Ucrania ocupó un lugar destacado. Los estudios basados en datos de diversas fuentes han tratado de determinar qué cambios podían observarse en la Internet ucraniana en las primeras semanas tras la invasión rusa del 24 de febrero de 2022. Por ejemplo, hubo aumentos repentinos en el uso de Google Maps y en las visitas a sitios web característicamente ucranianos por parte de usuarios de otros países. Estas observaciones podrían servir para rastrear el flujo de refugiados, por ejemplo.

También se presentaron los resultados de la investigación sobre el uso de la encriptación del DNS (DoT/DoH) y su impacto en el filtrado de Internet. Una de las conclusiones fue que las técnicas de encriptación podrían utilizarse para frustrar a los censores de Internet. No obstante, algunos censores obstinados de Internet han bloqueado los servicios DoT/DoH más conocidos o incluso han impuesto una prohibición general de las conexiones ESNI (o ECH). En el mejor de los casos, esto no debería ser posible sin causar daños colaterales muy considerables, sugieren los investigadores. La adopción generalizada de ESNI o ECH sería ventajosa en ese sentido.

También se presentaron los resultados de la investigación sobre la disponibilidad y los tiempos de respuesta de varios resolutores públicos de DoH conocidos y menos conocidos (y las diferencias entre ellos). Entre los resolutores conocidos, se encuentran los operados por Cloudflare, Google, Quad9, NextDNS, CleanBrowsing y OpenDNS. No es de extrañar que estos resolutores tuvieran tiempos de respuesta más cortos, ayudados, entre otras cosas, por el uso de anycast.

Epílogo

Este documento ofrece un breve resumen de los numerosos temas tratados en la 114ª reunión del IETF. Fue la segunda reunión de este tipo que contó con participantes “in situ” desde la crisis de COVID-19.

En la 114ª reunión del IETF, el número de asistentes en persona fue muy superior al de la 113ª reunión. Se aplicaron estrictas medidas de control de infecciones, como el uso obligatorio de mascarillas durante las sesiones y el acto social. Posteriormente, se notificaron 16 casos de infección, que representan el 2,6% de los asistentes en persona, frente al 2,9% de la reunión anterior.

La intención es que las reuniones del IETF sigan utilizando un formato híbrido por el momento. Esto implica que los participantes remotos puedan participar activamente en las sesiones mediante Meetecho, ya que antes se limitaban a seguir los procedimientos de forma pasiva. Aunque el sistema aún no es perfecto, mejora constantemente.

La próxima reunión del IETF está prevista del 5 al 11 de noviembre en Londres.

Informe realizado por: Marco Davids, SIDN Labs.

La versión en inglés del reporte IETF 114 puede encontrarse acá.