UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

ingeniería civil
telemática
UTFSM

Proyecto final
ELO322 Redes de Computadores I
DNS 1.1.1.1

Integrantes:

-Camila Norambuena

-Ignacio Pérez

-Joselyn Pino

-Alejandro Rodríguez

Profesor: Agustín J. González

Fecha: 24/8/2018

Valparaíso, Chile.

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

ingeniería civil telemática
UTFSM

Resumen

La existencia del sistema de nombre de dominios hace que la navegación en la red sea mucho más fácil y amigable para los equipos terminales.

Si bien, es este el sistema que se ocupa actualmente para la conexión entre dos hosts en la red, no quiere decir que sea perfecto, es más, presenta un gran problema de privacidad para los usuarios, ya que es muy fácil observar el tráfico y el contenido de lo que están haciendo y/o buscando.

El 1 de abril de 2018, diseñado en conjunto por Cloudflare y APNIC, aparece un nuevo sistema: DNS 1.1.1.1, el cual tiene 2 objetivos principales [(1)(2)], mejorar la velocidad de búsqueda en la red y ofrecer seguridad para mantener la privacidad.

Usando las herramientas que vienen incluidas en nuestro dispositivo (Terminal), con el apoyo de otras de herramientas de software (DNS Benchmark, DNS Jumper), se midieron los tiempos y efectividad de este nuevo sistema en comparación con los otros ya existentes. Por otro lado, se realizó una investigación y análisis de las técnicas implementadas que utiliza DNS 1.1.1.1 para brindar la seguridad en la privacidad de los clientes, todo esto con el fin de verificar si realmente cumple con los objetivos propuestos y que tan efectiva puede llegar a ser.

Introducción

La implementación de DNS en 1983 [3] hizo que, mediante un proceso de consultas y respuestas entre servidores DNS, se volviera más fácil y amigable el proceso de traducción de un nombre de host (Ej:“example.com”) a su dirección IP correspondiente (Ej: “255.255.111.1”).

El centro de esta serie de consultas y respuestas, antes que llegue la respuesta final a nuestro dispositivo, es un servidor llamado “DNS Local”. Este es otorgado automáticamente por el ISP cuando es contratado un servicio de Internet, pero los usuarios pueden optar por configurar otros DNS Locales públicos en sus dispositivos que poseen mejor velocidad que el provisto por el ISP (OpenDNS o Google DNS, por ejemplo).

Sin embargo, si bien estos DNS Locales solucionan el problema de la velocidad, no resuelven otro de los temas importantes para los usuarios de hoy en día: “la seguridad de la privacidad”, ya que, en el sistema actual, el ISP o los encargados de otro servicio DNS que esté ocupando, pueden ver todo lo que sus clientes estén buscando; aquí es cuando aparece un nuevo sistema DNS diseñado en conjunto por Cloudflare y APNIC: DNS 1.1.1.1.

DNS 1.1.1.1

Lanzada el 1 de abril de 2018, esta es la nueva versión DNS creada por Cloudflare y APNIC, donde se han añadido diversos protocolos que proporciona mayor seguridad y privacidad para el usuario, además de brindar una de las mayores velocidades de búsqueda. Los protocolos de implementados son:

DNS Query Name Minimisation[3] (RFC 7816):

Al hacer uso de un DNS Local, el usuario es vulnerable a violaciones de privacidad tanto por el ISP mismo o por algún agente externo.

El DNS Query Name Minimisation trabaja bajo el lema de: “Mientras menos información se manda , menos problemas de privacidad se van a tener”,es decir, cuando un DNS Local envía una consulta, solo envía lo que necesita el respectivo servidor DNS destino para realizar dicha búsqueda.

DNS sobre TLS[4] (RFC7858)**:**

Esto consiste en que, el DNS del sistema operativo, establece una conexión TCP con cloudflare-dns.com:853, para así inicializar TLS handshake y presentar el certificado TLS correspondiente. Una vez la conexión TLS se encuentra establecida, el DNS stub resolver puede enviar DNS sobre una conexión completamente encriptada, evitando espiar y manipular la información, ya que, toda consulta hecha por el usuario pasará a través de un canal totalmente encriptado.

DNS sobre HTTPS[5]:

A través de los protocolos UDP/TCP se envían las consultas y respuestas hacia un servidor DNS tradicional, pero estas no suelen ser encriptadas, lo que significa que cualquier persona que escuche paquetes dentro de la red puede saber qué sitios se están visitando y el usuario puede ser vulnerable a una situación de espionaje o falsificación.

El objetivo principal de DNS over HTTPS es aumentar la privacidad y seguridad entre un cliente y un DNS local, los cuales complementan DNSSEC y proporcionan búsquedas auténticas de extremo a extremo por el servidor DNS, evitando el espionaje y la manipulación de los datos.

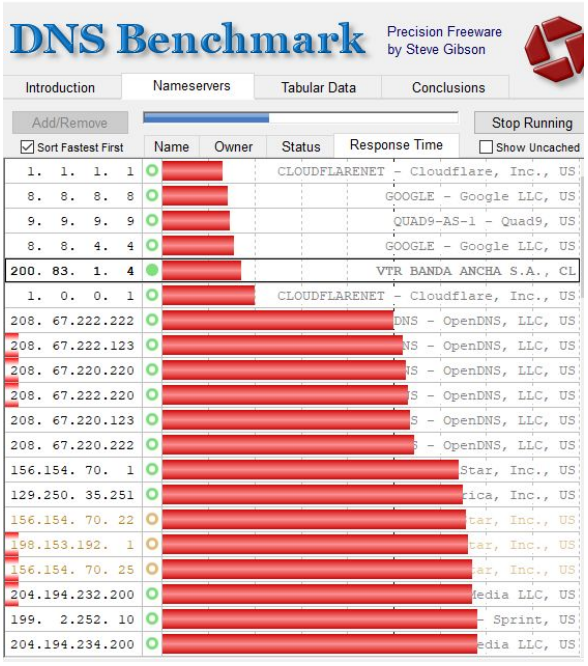
DNSSEC[6]:

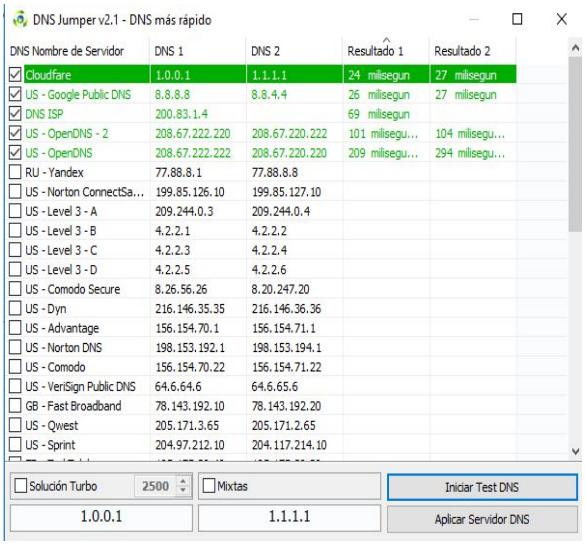
DNSSEC añade una capa de seguridad adicional a los servidores DNS de un dominio. Gracias a ello se previenen una gran cantidad de posibles actividades maliciosas.

DNSSEC añade marcas criptográficas a un registro existente dns. Estas marcas digitales son almacenadas en los servidores dns junto con registros tipo AAAA, MX, CNAME, etc. De esta manera se puede revisar y verificar si algún mensaje pedido por DNS es proveniente de un servidor autorizado.

Demostración :

Para ver las aplicaciones de DNS Query Name Minimisation,DNSSEC, DNS sobre TLS y HTTPS se tendría que correr Wireshark en el DNS Local de Cloudflare. Como no es posible hacer eso, decidimos verificar, mediante el uso de herramientas de software mencionadas anteriormente, si este nuevo DNS es realmente más rápido que los ya existentes.





Como primera herramienta para evaluar el rendimiento del DNS de Cloudflare en comparación a otros, utilizamos DNS Benchmark (Ver Anexo); pulsando sobre “Run Benchmark”, podremos comprobar el nombre, propietario, estado y tiempo de respuesta de todos los DNS locales a los cuales nuestro dispositivo tiene acceso. Dentro de “Tabular Data”, podremos ver información con detalles sobre el tiempo medio de respuesta y velocidad de carga, y otros detalles a tener en cuenta. En la última sección (“Conclusions”) podemos encontrar las conclusiones sobre el análisis hecho a los servidores DNS. Aquí es donde podemos comprobar, que efectivamente DNS 1.1.1.1 es mas rápido que el DNS otorgado por el ISP. Para complementar este análisis, recurrimos a DNS Jumper (Ver Anexo), en el cual, luego de hacer correr su diagnóstico, observamos que la velocidad de respuesta (aunque sea por poco) es menor que los otros DNS, haciéndolo el servicio más rápido al que podemos optar.

Conclusión

Tras el análisis e investigación que anteriormente se realizó durante el transcurso del trabajo, fuimos capaces de evaluar el rendimiento de DNS 1.1.1.1 en contraste con los otros servicios DNS locales que ya existían, tales como, DNS del ISP, OpenDNS o GoogleDNS.

Por un lado, mediante la demostración práctica comprobamos que la velocidad de búsqueda es mayor que los demás DNS locales que podemos ocupar, y por otro, gracias a la investigación sobre DNS Query Name Minimisation, DNSSEC, DNS sobre TLS y HTTPS, somos conscientes de la protección que brinda , proporcionando una mayor seguridad en el usuario al momento de navegar.

DNS 1.1.1.1 es la oportunidad perfecta para eliminar las características principales por las que es criticado el sistema de dominio de nombres (por ser muy lento y por problemas de privacidad), y por ello su proyección hacia el futuro para el futuro se ve bastante comprometedor, asegurando una experiencia agradable para todos los clientes en la red.

Referencias

(1) https://blog.cloudflare.com/dns-resolver-1-1-1-1/

(2) https://www.cloudflare.com/learning/dns/what-is-1.1.1.1

(3) https://tools.ietf.org/html/rfc7816

(4) https://developers.cloudflare.com/1.1.1.1/dns-over-tls/

(5) https://developers.cloudflare.com/1.1.1.1/dns-over-https/

(6) https://www.cloudflare.com/es-es/dns/dnssec/

Anexo.

- DNS raíz: Contiene los dominios de nivel superior (TLD) que aparecen como los sufijos de todos los nombres de dominio de Internet.
- DNS local: Al recibir una consulta, debe remitirse a los servidores DNS que corresponda y luego almacenar la respuesta por si se repite la misma consulta en el futuro.
- DNS autoritativo: Tiene la autoridad final sobre el dominio y es responsable de brindar respuestas a servidores de DNS con la información de la dirección IP.
- DNS Benchmark: Herramienta de software que permite saber qué DNS configurar para que la navegación por internet sea lo más rápida posible. En DNS Benchmark, vienen configurados DNS por defecto (Google, OpenDNS, 1.1.1.1, por ejemplo). El programa hace un benchmark (prueba), para que sepamos cuál es el más rápido para nosotros. Los resultados se muestran de forma continua y actualizada mientras que una gráfica de barras representa la tabla de rendimiento en caché, sin caché y puntocom (Consultas a DNS TLD) de cada servidor de nombres. Estos valores son determinados por cada servidor de nombres para las direcciones IP de los 50 nombres de dominio más populares en internet y también mediante la consulta de dominios inexistentes.
- DNS Jumper: Cuenta con una interfaz básica en la que seleccionamos nuestro adaptador de red y nos permite seleccionar servidores DNS de forma manual. La función de este programa pasa por establecer los mejores DNS para cada conexión.
- OpenDNS: Empresa fundada en 2005, que ofrece un servicio DNS gratuito (para uso privado en el hogar). Actualmente también se enfocan en seguridad de redes
- GoogleDNS: Servidor DNS público de google lanzado el 2009.