UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

EVALUACIÓN DE RENDIMIENTO Y SEGURIDAD DEL ACCESO FIJO A INTERNET MEDIANTE LA EXTENSIÓN DNS CHAINQUERY PARA LA VALIDACIÓN DNSSEC

TESIS PARA OPTAR AL GRADO DE
MAGÍSTER EN CIENCIAS DE LA INGENIERÍA, MENCIÓN ELÉCTRICA

JEISSON STEVEN SÁNCHEZ MAHECHA

PROFESOR GUÍA:
SANDRA LORENA CÉSPEDES UMAÑA, Ph.D

MIEMBROS DE LA COMISIÓN:
JAVIER BUSTOS JIMÉNEZ , Ph.D
NÉSTOR BECERRA YOMA, Ph.D

Este trabajo ha sido financiado parcialmente por NIC Chile Research Labs

SANTIAGO DE CHILE
2020

RESUMEN DE LA TESIS PARA OPTAR
AL GRADO DE MAGÍSTER EN CIENCIAS DE LA INGENIERÍA, MENCIÓN ELÉCTRICA
POR: JEISSON STEVEN SÁNCHEZ MAHECHA
FECHA: 2020
PROF. GUÍA: SANDRA LORENA CÉSPEDES UMAÑA

EVALUACIÓN DE RENDIMIENTO Y SEGURIDAD DEL ACCESO FIJO A INTERNET MEDIANTE LA EXTENSIÓN DNS CHAINQUERY PARA LA VALIDACIÓN DNSSEC

La correcta función del sistema de nombres de dominio DNS es fundamental en rendimiento y la seguridad en Internet. Basados en el incremento de demanda de Internet, actualmente la cabecera del protocolo DNS se ha extendido con nuevas características denominadas EDNS0. Sin embargo, no existen investigaciones del despliegue y funcionalidad de una gran parte de esas extensiones a nivel operacional en Internet. Por ese motivo en esta tesis se propone un algoritmo para analizar el actual estado de EDNS0; principalmente se evalúa el contexto de seguridad y rendimiento de la extensión *DNS ChainQuery* para la validación DNSSEC en clientes. En cada prueba se realizan solicitudes DNS, evaluando la respuesta desde los servidores recursivos. Para la evaluación se establecen 3 escenarios de prueba analizando tiempos de respuesta, número de bytes y cantidad de paquetes por solicitud DNS. Los resultados de la muestra en estudio revelan una baja implementación a nivel operacional de cada extensión, incluyendo un 68 % de configuraciones incorrectas en DNSSEC. También se determina que la correcta configuración *DNS ChainQuery* obtuvo mejores resultados en 2 de las 3 métricas de análisis, aumentando el nivel de seguridad sin afectar el uso de CPU en el cliente, lo que se resume en una mejora del rendimiento global en Internet.

A Dios todopoderoso por guiarme y brindarme tantos momentos grandiosos durante estos años académicos.

A mis padres por su apoyo incondicional y dar su vida entera por mi bienestar. Este logro va enmarcado en su honor y gran ejemplo que siempre me han dado.

A Amy Valentina por ser mi mayor motivación.

A Diana por el apoyo y soporte como pareja y Madre de mi hija en esta etapa de vida.

Agradecimientos

Agradezco inmensamente a Sandra Céspedes y a Javier Bustos por darme la oportunidad de ingresar a sus grupos de trabajo y apoyarme 100 % en cada paso durante la realización de este estudio. Gracias por la confianza.
Agradecimientos totales a los compañeros del grupo de investigación Winet, en especial a Pablo Ortega, Adriana Arteaga y Diego Londoño. También a los compañeros de lucha del NicLabs quienes son maravillosas personas.

Siglas

ASN Número de Sistema Autónomo, Autonomous System Number por sus siglas en inglés

AXFR Zona de transferencia autoritativa, Authoritative Transfer por sus siglas en inglés

CDN Content Delivery Network

DDoS Ataque de denegación de servicio distribuido, Distributed Denial of Service por sus siglas en inglés

DMZ Zona desmilitarizada, Demilitarized Zone por sus siglas en inglés

DNS Sistema de Nombres de Dominio, Domain Name System por sus siglas en inglés

DNSOP Domain Name System Operations

ECS EDNS subred de cliente, EDNS Client Subnet por sus siglas en inglés

FQDN Nombre de dominio completo, Fully-Qualified Domain Name por sus siglas en inglés

gTLD Dominio de nivel superior genérico, en inglés Generic Top Level Domain

IANA Internet Assigned Numbers Authority

IETF The Internet Engineering Task Force

ISC Consorcio de sistemas de Internet, Internet Systems Consortium por sus siglas en inglés

ISP Proveedor de servicios de Internet, Internet Service Provider por sus siglas en inglés

IXFR Autoridad de la zona, Start of Authority por sus siglas en inglés

MSS Tamaño del segmento máximo, Maximum Segment Size por sus siglas en inglés

NTP Protocolo de hora en red, Network Time Protocol por sus siglas en inglés

PDU Unidad de datos de protocolo, Protocol Data Unit por sus siglas en inglés

RFC Request for Comments

RR Registro de Recursos,Resource Records por sus siglas en inglés

RTT Round Trip Time

SDN Redes definidas por software, Software Defined Networks por sus siglas en inglés

SOA Autoridad de la zona, Start of Authority por sus siglas en inglés

TCP Transmission Control Protocol

TLD Dominio de nivel superior, Top Level Domain por sus siglas en inglés

UDP User Datagram Protocol

UIT-T Unión Internacional de Telecomunicaciones - sector de estandarización de telecomunicaciones

Tabla de Contenido

Índice de Tablas

Índice de Ilustraciones

Capítulo 1

Introducción

1.1. Antecedentes Generales

Las primeras actualizaciones como mecanismos de extensión del protocolo DNS fueron presentadas en 1999. En 1999 se publicó la *Request for Comment* RFC 2671 [70], la cual ha sido actualizada y detallada en extensiones individuales hasta el día de hoy. Estas extensiones se definen como modelos para implementar nuevas características y aumentar la capacidad de obtener información adicional a través de la resolución de solicitudes DNS. Sin embargo, la implementación de los mecanismos de extensión en los diferentes elementos de la jerarquía no ha sido la adecuada. Esto se debe a factores que dificultan la implementación correcta descrita en la RFC, entre eso la variedad de software DNS desplegado a nivel mundial y los administradores DNS.

Para una correcta resolución DNS que incluya los mecanismos de extensión se han configurado soluciones temporales o se ha optado por configurar respuestas sin las extensiones. Pero el mayor problema de las soluciones temporales es que pueden aumentar la latencia en la red global de Internet e incluyen la dificultad de desplegar más características del protocolo [60]. Debido a esto, la comunidad de investigación y operación DNS se ha propuesto en remover dichas soluciones temporales y ha aumentado su interés en estudiar la implementación correcta de las extensiones DNS a partir del 1 de Febrero de 2019. No obstante estos esfuerzos inicialmente están enfocados en un nivel alto de la jerarquía DNS, es decir en servidores autoritativos.

Basado en el conocimiento del estado en la última milla de resolución DNS y como parte de la colaboración de la comunidad DNS, en esta tesis se presenta un estudio de la configuración actual de las extensiones DNS en servidores recursivos (los más cercanos al cliente). Este estudio permite generar un mapa de conocimiento de fallas de resolución DNS con extensiones, mediante la ejecución de un algoritmo, que puede ser replicado en cualquier ambiente para dar soluciones en producción. De acuerdo al código de respuesta y algunas banderas de los mecanismos de extensión, el algoritmo genera un reporte de clasificación del estado de la zona DNS con detección de fallas EDNS0, precauciones de una correcta operación EDNS0 y una correcta operación con controles preventivos en los servidores recursivos. Además, el

estado del despliegue de las extensiones DNS además permite analizar el acondicionamiento de los estándares y mejores prácticas en el mundo real de la resolución DNS.

Principalmente, mediante este trabajo se analiza la implementación de un nivel de seguridad en el cliente a través de la extensión cadena de solicitudes en DNS, *DNS ChainQuery*. Esta extensión es descrita en la RFC experimental 7901 [74] para ser implementada en servidores de validación de llaves de seguridad y a su vez configurados como servidor de reenvío de solicitudes. Su función principal es el reenvío de una única consulta, donde se solicita una ruta de validación completa junto con la respuesta de consulta regular DNS. Esto permitiría reducir la cantidad de consultas y además la latencia global debido a la espera de validación de llaves de seguridad por cada consulta.

1.2. Justificación

La continuidad de la correcta operación del protocolo DNS depende de una configuración adecuada de sus mecanismos de extensión. Un factor es la configuración de los servidores por parte de los administradores DNS, lo que puede generar una correcta resolución DNS con soporte EDNS0 o generar una respuesta fallida, incluyendo el reenvío a otros servidores y generando latencia en alcanzar la respuesta. Esto incluye no solo los servidores de más alto nivel en la jerarquía DNS sino a los elementos intermedios que permiten una resolución desde el cliente.

Una parte fundamental de la resolución DNS se encuentra en el correcto funcionamiento de los servidores recursivos [30], por este motivo son un objeto de estudio en esta tesis. Basado en que la mayoría de las extensiones DNS se complementan para optimizar su funcionamiento y alcance, se requiere una investigación del estado EDNS0 en servidores recursivos de las principales extensiones, el cual es desconocido. Para ello se deben planear estrategias de análisis de respuestas DNS fallidas e identificar patrones del comportamiento en distintos escenarios. Por eso es de gran relevancia desarrollar un algoritmo para analizar las respuestas DNS de los servidores recursivos a solicitudes EDNS0. Aunque no existe formalmente una recomendación para realizar pruebas sobre los servidores recursivos basado extensiones DNS, se utiliza como guía el documento en borrador "*A Common Operational Problem in DNS Servers - Failure To Respond*", el cual se encuentra en su versión 12 [7].

Como parte del estudio de las extensiones, se realiza un análisis más exhaustivo sobre la extensión *DNS ChainQuery* a nivel operacional en el cliente. Actualmente, no existen estadísticas del comportamiento de los servidores recursivos a solicitudes DNS con la extensión *DNS ChainQuery*. Un requisito básico del funcionamiento de *DNS ChainQuery* es la configuración de la extensión de seguridad DNSSEC descrita en las RFC 4033 [9], 4035 [10] y la optimización de su función mediante la extensión de cookies para el protocolo de transporte UDP descrita en la RFC 7873 [3] o la opción de conexión TCP Keepalive descrita en la RFC 7828 [62]

Aunque *DNS ChainQuery* es una extensión DNS experimental que puede agregar un nivel de seguridad al cliente final mediante la implementación de la validación DNSSEC, no se ha

medido su impacto mediante métricas de rendimiento de red. Por eso se debe establecer las condiciones en las que se debería implementar una cadena de solicitudes confiable siguiendo las mejores prácticas en la operación DNS. Para ello se requieren escenarios de implementación para una cadena de solicitudes DNS y así evaluar el rendimiento de la resolución DNS.

1.3. Definición del problema

DNSSEC es una extensión de seguridad del protocolo DNS, y su despliegue se realiza en 5 etapas: experimental, anunciado, parcial, firmado por delegación en raíz y operacional [36]. Actualmente en Latinoamérica existen 11 países en la etapa operacional incluyendo a Chile. Sin embargo, en Chile solo hay un 5.39 % de validación de la extensión DNSSEC [8]. Por otro lado del 90 % de TLD con firma en la raíz a nivel mundial, solo un 13 % de los clientes realiza validación DNSSEC [1]. Debido a estas cifras, mediante la implementación de los nuevos mecanismos de extensión DNS se proyecta mejorar el despliegue de DNSSEC y a su vez los tiempos de respuestas en sistemas de validación de llaves de seguridad.

La validación DNSSEC en el cliente es una solución para evitar fugas de información y ataques de denegación de servicio mediante falsificación de direcciones IP. A través de las cifras menores al 10 % de validación DNSSEC en clientes, se determina que existe algún obstáculo para su implementación de manera masiva. Aunque existen mecanismos como la extensión *DNS ChainQuery* especificada para la validación de llaves DNSSEC en el cliente sin afectar el rendimiento de red mediante las aplicaciones que requieran una resolución DNS, aún no se ha realizado pruebas de su despliegue.

Un punto esencial para el despliegue operacional de la extensión *DNS ChainQuery* es la respuesta DNS que generan los servidores recursivos al cliente siguiendo los estándares planteados por la *Internet Engineering Task Force* (IETF). Sin embargo, no existen estudios previos del estado de configuración de los servidores recursivos para responder a consultas EDNS0 como la extensión *DNS ChainQuery*.

1.3.1. Hipótesis

¿Existe algún mecanismo confiable en el protocolo DNS que permita reducir el procesamiento y tiempos de respuesta de consultas para la validación DNSSEC desde el lado del cliente en al menos un 10 %?

Actualmente los clientes que requieran una resolución DNS en un contexto de seguridad DNSSEC requieren obtener toda la información necesaria para realizar la validación de las llaves de seguridad de toda la cadena de confianza. En términos de latencia en la resolución DNS, la validación DNSSEC en el cliente aumenta tiempos de respuesta para la resolución DNS debido a que utiliza más recursos de procesamiento y almacenamiento de caché. Sin embargo, debido a la importancia de la validación DNSSEC existe un mecanismo experimental que propone crear una cadena de solicitudes DNS que incluya la ruta de validación

completa en una sola consulta desde el cliente. Esto se realiza agregando la función de reenvío a servidores recursivos con mayor capacidad de procesar toda la cadena de validación paso a paso, evitando que el cliente realice esta tarea. No obstante, se hace necesario analizar si la distribución de carga de trabajo efectivamente reduce, y en que proporción, los tiempos de respuesta en la última milla de resolución DNS.

1.4. Objetivos

Es de gran importancia abordar los objetivos para responder las preguntas de investigación planteadas, los cuales se centran en un objetivo general y objetivos específicos:

1.4.1. General

Evaluar de manera experimental el estado operacional de los mecanismos de extensión DNS en servidores recursivos y analizar el impacto de la implementación de la extensión *DNS ChainQuery* en la operación DNS.

1.4.2. Específicos

- Caracterizar el grado de adopción e implementación de los mecanismos de extensión DNS en los servidores recursivos mediante el código de respuesta y las banderas DNS.
- Diseñar un algoritmo de evaluación de las respuestas DNS de los servidores recursivos para clasificar el estado de adopción e implementación de los mecanismos de extensión DNS.
- Analizar los resultados del algoritmo de clasificación para determinar qué servidores recursivos cumplen las condiciones mínimas requeridas para la implementación de la extensión *DNS ChainQuery* descrita en la RFC 7901.
- Evaluar, en un conjunto de escenarios de estudio representativos, el rendimiento de la resolución DNS y validación DNSSEC en un cliente, comparando la implementación de la extensión *DNS ChainQuery* con la actual validación DNSSEC sin el uso de la extensión *DNS ChainQuery*.

1.5. Metodología y herramientas

1.5.1. Metodología

En esta sección se describe la metodología empleada para lograr los objetivos mencionados en la sección 1.4.

1.5.1.1. Caracterización del grado de adopción e implementación de los mecanismos EDNS0

Inicialmente se realizan consultas a los servidores para determinar el soporte EDNS de acuerdo a la metodología [49] y presentada en el I-D "*A Common Operational Problem in DNS Servers - Failure To Respond*" [7]. Las pruebas se realizan en tres fases.

En la fase A se obtiene las características básicas de los servidores como el servidor del dominio, versión del software DNS del servidor, así como el número de sistema autónomo (ASN) adjunto, ubicación del país y la empresa a cargo del ASN. En esta misma fase se estudia si soporta EDNS y se analizan las respuestas de acuerdo a la versión 1 EDNS.

La fase B es una etapa de análisis de características EDNS como las respuestas con sección opcional EDNSOPT, respuestas truncadas, respuestas recursivas con EDNS, configuración de la negociación EDNS para discriminar ataques con solicitudes diferentes a EDNS0 y finalmente el soporte DNSSEC.

En la fase C se realizan las pruebas a cada una de las extensiones y las características básicas de EDNS. Las extensiones evaluadas en la fase C son *Client Subnet* [13], DNSSEC [9], *EDNS Cookies* [3], *EDNS expire option* [6], *Edns-tcp-keepalive* [62] y la extensión *DNS ChainQuery* [74].

1.5.1.2. Diseño del algoritmo de clasificación del estado de los mecanismos EDNS0

Posteriormente se procesan las respuestas a cada solicitud DNS para evaluar y clasificar el estado de cada servidor en cumplimiento con los estándares propuestos para EDNS. La clasificación se basa en las banderas activas, soporte DNSSEC, soporte EDNS0, versión/proveedor del software DNS y códigos de respuesta.

Mediante la clasificación de los *resolvers* se establece un banco de pruebas para nuevas implementaciones como la extensión *DNS ChainQuery*, la cual requiere el descubrimiento de los servidores recursivos que soporten su código de opción para optimizar su despliegue a nivel operacional.

Como resultado del algoritmo se genera un reporte final con 3 estados definidos del servidor recursivo: *ALL OK*, *WARNINGS* y *NO SUPPORT*.

1.5.1.3. Análisis de los resultados de algoritmo de clasificación del estado de los mecanismos EDNS0

La evaluación de las respuestas DNS permite generar un análisis del impacto de la implementación de los mecanismos EDNS0 en la resolución DNS. El enfoque principal se basa en analizar el cumplimiento de las condiciones mínimas de implementación de la extensión *DNS ChainQuery* descritas en la RFC 7901 [74]. A través del resultado final, se determina si es

factible su despliegue a nivel operacional y que servidores recursivos actualmente pueden ser los pioneros para cumplir este objetivo.

1.5.1.4. Evaluación de la implementación de la extensión *DNS ChainQuery*

La extensión *DNS ChainQuery* presenta las consideraciones de seguridad para evitar ataques distribuidos de denegación de servicios basados en suplantación de direcciones IP y la sobrecarga en el cliente para realizar la validación DNSSEC. Por este motivo se realizan las pruebas de evaluación comparando parámetros de operación como el uso de almacenamiento de caché en escenarios de la actual validación DNSSEC, como los protocolos de transporte.

La evaluación se realiza mediante métricas de rendimiento de red como la longitud de la cola de bytes recibidos, cantidad de paquetes recibidos y tiempos de respuesta al finalizar la validación DNSSEC en un cliente con el uso y no uso de la extensión *DNS ChainQuery*. La diferencia se comprueba mediante la disminución de solicitudes de validación DNSSEC en un analizador de protocolos.

1.5.2. Herramientas

Las herramientas utilizadas en la investigación de este tesis son de código libre y actualmente usadas en la operación de ciertas zonas DNS.

- **Dig:** es la herramienta más popular para realizar consultas DNS. Dig tiene comandos adicionales de configuración para extraer información de un servidor mediante su dirección IP, realizar búsqueda reversa (encontrar un dominio mediante la dirección IP), versión de servidor DNS, establecer el protocolo de transporte o de seguridad, algoritmos de encriptación, entre otros [37].
- **delv:** es una herramienta especificamente diseñada para realizar consultas DNS y validar los resultados de DNSSEC. La herramienta desarrollada por los proveedores de software DNS de BIND emplea la misma lógica de resolución y validación que "named". delv además muestra las características DNSSEC relevantes de una resolución DNS, como lo son los códigos de respuesta a fallas de resolución, firmas del conjunto de registro de recursos (RRSIG) y la cadena de validación [42].
- **Stubby:** Stubby en un servidor DNS sobre TLS instalado de manera local en el cliente. Stubby encripta las solicitudes DNS desde el cliente hasta un servidor recursivo dedicado para aumentar la privacidad. Es una aplicación de código abierto y se puede ejecutar como un demonio [65].

1.6. Alcances

Esta tesis realiza el estudio de la resolución DNS de 19061 servidores recursivos en Chile bajo pruebas experimentales, las cuales pueden fluctuar entre cada una de ellas. El principal

aporte del estudio es proveer un algoritmo de evaluación del estado operacional de los servidores en zonas DNS y determinar el impacto de implementar la validación DNSSEC en clientes aumentando los niveles de seguridad en transacciones DNS. El estudio genera experimentos replicables bajo las condiciones descritas como respuestas esperadas para cada prueba.

Para ello se realizan múltiples pruebas en escenarios estables. Los escenarios establecidos contemplan la misma red de comunicación desde donde se realizan las pruebas, horarios de bajo tráfico y conexión segura y el mismo *stub resolver*. Esta tesis no incluye una evaluación práctica de la extensión chain query debido a las limitaciones de despliegue en código e implementación en los software DNS desarrollados hasta hoy en día. Esta tesis no incluye en la evaluación servidores autoritativos ni sistemas de seguridad intermedios en la resolución DNS como cortafuegos.

Capítulo 2

Sistema de Nombres de Dominio

Hoy en día el protocolo DNS es parte fundamental del rendimiento y funcionalidad de las aplicaciones Web y arquitecturas de red como Named Data Networks (NDN). En este capítulo se describen los conceptos más importantes para generar un contexto del problema a resolver con este trabajo. El soporte principal de este trabajo es el seguimiento de buenas prácticas y estándares de Internet desarrollados por entes de estandarización de Internet como lo es la Fuerza de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés) y la Unión Internacional de Telecomunicaciones UIT-T.

Los Sistemas de Nombres de Dominio, (DNS por sus siglas en inglés) actualmente son una parte fundamental en la infraestructura de Internet por su uso en distintas aplicaciones y nuevas tecnologías. Fue estandarizado en 1983 por la RFC 882 (Domain names: Concepts and facilities) [52], RFC 883 (Domain names: Implementation specification) [53] y en 1986 por la RFC 973 (Domain System Changes and Observations) [54]. Sin embargo, fue solo hasta 1987 en que los sistemas de redes de comunicación tienen una serie de estándares consolidados para la implementación del protocolo DNS. Estas actualizaciones fueron establecidas mediante la RFC 1034 [55] y la RFC 1035 [56], que presentan el funcionamiento, conceptos, los diferentes formatos de los mensajes DNS y una descripción de su implementación a los diferentes niveles de la jerarquía DNS. La función principal es asociar una dirección IP a un nombre de dominio solicitada por un usuario en Internet.

2.1. Arquitectura del protocolo DNS

La arquitectura del protocolo DNS es distribuida y además de tipo jerárquica [27] como se puede observar en la Fig. 2.1. La consulta proveniente desde el navegador web queda almacenada en caché del servidor Stub del sistema operativo del cliente y luego esa consulta es enviada al servidor recursivo Fig. 2.1(1). El servidor recursivo realiza diferentes consultas iterativas para resolver la consulta DNS, iniciando por el servidor raíz Fig. 2.1(2). Posteriormente el servidor raíz genera la respuesta correspondiente y la transfiere al servidor gTLD (“.com” en el ejemplo de la Fig. 2.1). Al ser una arquitectura distribuida, los servidores au-

toritativos pueden delegar la autoridad de respuestas de un dominio a otros servidores de nombre. Luego el servidor recursivo envía la consulta al servidor gTLD, recibiendo referencia al servidor que contiene el dominio Fig. 2.1(3). Finalmente el servidor del nombre de dominio genera la respuesta al servidor recursivo Fig. 2.1(4) y esta es enviada al cliente Fig. 2.1(5).

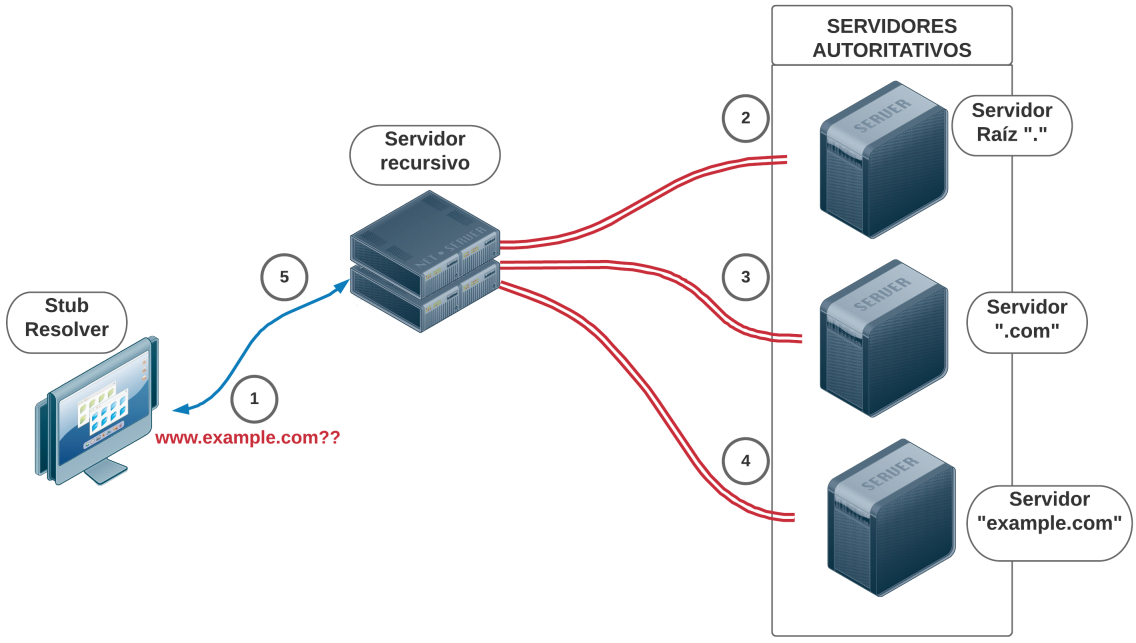

Figura 2.1: Arquitectura del protocolo DNS

Las respuestas de los servidores autoritativos no solo contienen la dirección IP sino registros de recursos, que describen el tipo de información en un Sistema de Nombres de Dominio. Adicionalmente, durante el proceso de resolución DNS existen múltiples consultas entre los distintos niveles de servidores de nombre para encontrar los recursos del dominio solicitado. Actualmente existen diferentes tipos de servidores, los cuales ayudan a mantener un equilibrio entre resiliencia y rendimiento de la red basado en la cantidad, prioridad y recursividad de las consultas.

Servidor Stub: está configurado por defecto en la máquina del cliente y reenvía la solicitud a los servidores recursivos.

Servidor recursivo: descritos también como resolvers, el servidor recursivo aunque puede estar configurado para distintas funciones, su operación consiste en recibir las solicitudes del servidor Stub y empezar a enviar distintas consultas hasta encontrar la respuesta para el cliente. Este tipo de servidores se encuentran físicamente más cercanos al cliente según la topología DNS (principalmente proveedores servicio de internet, registradores de dominio, administradores de hospedaje servicios de internet) y establecen comunicación constante desde el servidor raíz y los servidores gTLD para empezar a crear la resolución DNS [56].

Servidor autoritativo: se encargan de responder a una solicitud en su zona responsable, esto hace una resolución fácil y eficiente. Siempre tiene un rol de servidor y no de cliente, lo cual requiere una respuesta completa a la solicitud o puede delegar a un servidor de nombres para completar la resolución.

Servidor caché: es el servidor primario de contacto para el servidor Stub del cliente, permite resolver una consulta del cliente almacenando sus resultados en caché. Esto se realiza para evita el envío de solicitudes iterativas a otros servidores y pasar por la cadena completa de resolución DNS cuando se ha realizado previamente la misma consulta. Una ventaja de este tipo de servidores es el acceso eficiente a consultas recientemente realizadas. No necesariamente almacenan consultas del dominio completo, sino también pueden almacenar registros de recursos, claves de seguridad, respuestas de un solo servidor de nombres, entre otros.

Servidor reenvío *(Forwarding)*: su función principal es reenviar solicitudes DNS recibidas desde la última milla en la cadena de resolución DNS hacía servidores recursivos (públicos) o servidores caché con más recursos para la resolución DNS. Esto se realiza para evitar congestión en los servidores de alto tráfico y para segmentar tráfico privado o público [5]. Este tipo de servidores se encuentran físicamente en la zona desmilitarizada, posterior a los sistemas de seguridad de la red interna del usuario como firewall.

Servidor de validación DNSSEC: es un servidor DNS configurado para validar la extensión DNSSEC de manera automática o manual. Este tipo de servidor avisa al cliente el soporte de validación DNSSEC mediante el contenido de la bandera AD (Authenticated Data) y un nuevo registro de recursos con la firma de validación RRSIG con el mismo nombre que el registro A [9], [10]. Este tipo de servidores son configurados a nivel de software en servidores recursivos y su ubicación física esta basada en la ubicación física de los servidores recursivos.

De acuerdo a la segmentación de tráfico, el uso de servidores públicos o servidores privados aumenta el nivel de seguridad. Por lo que se puede realizar una combinación de estos tipos de servidores dependiendo el escenario en el que se requiera la resolución. Este es el caso de implementación de la extensión *DNS ChainQuery*, en el que primordialmente se configura un servidor de reenvío de solicitudes y un servidor de validación DNSSEC.

Por otro lado la extensión de seguridad DNSSEC que antes tenía un grupo de trabajo propio dentro de la arquitectura del área de seguridad de la IETF, actualmente se encuentra en un marco de interés de diferentes grupos de trabajo como DNSOP [33] del área de gestión y operaciones. DNSOP es el encargado de desarrollar guías para la operación de software DNS y servicios para las zonas DNS, consolidando en distintos documentos la información técnica para proveedores o administradores DNS en general.

En la línea de tiempo estos documentos han sido modificados o en su defecto reemplazados de acuerdo al crecimiento masivo de tráfico en la red de Internet, lo cual ha afectado la capacidad de la cabecera del protocolo DNS. El primer documento estandarizado fue la RFC 2671 ″Extension Mechanisms for DNS (EDNS0)” [70] para así incrementar la capacidad de los campos fijos de la cabecera DNS con el fin de generar redes resilientes. Posterior fue publicada la RFC 2673 ″Etiquetas binarias en el sistema de nombres de dominio” [20] que quedó obsoleta[1] mediante la RFC 6891 conocida como los "Mecanismos de extensión para DNS (EDNS0)"[24], donde el valor 0 representa la versión en la que se encuentra este estándar.

[1]Mediante los documentos de la IETF el término *obsoleto* hace referencia a una re-definición del protocolo descrito en el estándar previo, lo cual es reemplazado por un nuevo documento. Mientras que la definición de *actualización* mantiene la implementación del protocolo con términos nuevos o complementos al documento actual de la RFC.

2.2. Revisión de Literatura

2.2.1. Mecanismos de extensión DNS 0

Los mecanismos de extensión DNS también denominados EDNS0, por sus siglas en inglés y versión, son mecanismos de expansión compatibles con las versiones anteriores del protocolo DNS. El requerimiento de desarrollar nuevos mecanismos se debe al incremento del flujo de datos en múltiples servicios que incluyen al protocolo DNS, ya que el rango de los campos fijos de la cabecera del protocolo no permitía agregar nuevas características como información adicional del estado del cliente a los resolvers, entre otras consideraciones de seguridad y resiliencia.

Inicialmente, la resolución DNS mediante UDP se limitaba a paquetes de 512 bytes de carga útil [56]. Sin embargo, mediante la implementación de ENDS0 se obtuvo información adicional contenida en los Registros de Recursos (RR) y esto se debe al espacio extra en la cabecera DNS [24]. Dentro de la información relevante para este trabajo están las banderas adicionales y códigos de respuesta (RCODEs) de los servidores. Otras ventajas de EDNS0 son la inclusión de direcciones IPv6 y de firmas de seguridad como DNSSEC [32].

También existen ventajas de la implementación de EDNS0 como la disminución de la efectividad de ataques de denegación de servicios mediante extensiones DNS [58], [60], por ejemplo con las DNS Cookies definida en la RFC 7873 [3]. No obstante, la efectividad de la seguridad EDNS0 se complementa con la configuración de elementos como *middleboxes* o cortafuegos [59] para que no bloqueen paquetes DNS de acuerdo a su longitud. Principalmente porque esto genera fragmentación y así vulnerabilidades frente a ataques de tipo DNS-poisoning [28], [47],[72]. Finalmente, estas vulnerabilidades no solo permiten generar ataques sino que limitan el despliegue de extensiones como EDNS Cookies, cuya función permite reducir ataques distribuidos de denegación de servicio masivos DDoS [61] y respuestas de dominio inexistente, "NXDOMAIN", lo que se resume en el aumento de latencia en la red en general por reenvío de solicitudes para la resolución DNS [16].

A pesar de que EDNS0 es una mejora al protocolo DNS, en la actualidad la resolución DNS con extensiones no se realiza de una manera correcta, lo cual genera un problema que concierne a toda la comunidad de Internet [40], [68], incluyendo a proveedores de servicio de internet ISP, registradores DNS, proveedores de software DNS e inclusive clientes finales.

Debido a la cantidad de software y versiones de DNS, existen inconsistencias en la resolución a solicitudes DNS con extensiones [26]. Este tipo de resoluciones se realizan mediante soluciones provisionales o simplemente se resuelven negando las respuestas DNS. Por esta razón, los cuatro fabricantes de software DNS más conocidos, BIND(ISC), KnotResolver(CZ.NIC), PowerDNS(PowerDNS.COM BV) y Unbound(NLnetLabs) eliminan todos las soluciones provisionales que están habilitadas de forma predeterminada para las principales implementaciones de servidores DNS [60].

2.2.2. DNS FlagDay 2019

A partir del 1 de Febrero de 2019 los retardos de red y la dificultad de implementar nuevas extensiones DNS fueron controladas mediante la implementación de software actualizado DNS. Hasta antes de esa fecha, la resolución de solicitudes EDNS0 retornaba códigos de respuesta incorrectos o se descartaban paquetes con estas características. La solución provisional consistía en realizar la resolución simple DNS sin extensiones. Esto se realizaba mediante los tiempos de espera agotados en una resolución, lo cual desactivaba la respuesta EDNS0. Como parte de esta tesis se realiza el análisis de las respuestas antes y después del DNS Flag day para determinar el estado de resolución EDNS en diferentes servidores.

El impacto esperado de los cambios en el "DNS Flag day" era la negación de resolución de un dominio que antes podía ser resuelto sin extensión o por las soluciones provisionales. Aunque no es obligatorio que los servidores respondan a solicitudes EDNS0, estos sí deben generar una respuesta cumpliendo con la sección 7 y 8 de la RFC 6891 [24] donde se describen las consideraciones de transporte y seguridad.

Uno de los mayores contribuyentes a este cambio positivo es el Consorcio de Sistemas de Internet ISC, desarrollador y distribuidor del software DNS BIND [41]. Actualmente, BIND es el software DNS más usado en Internet [43]-[69]. Además el ISC desarrolló una plataforma Web "EDNS compliance Tester" [39] para realizar pruebas que determinan si un dominio cumple con los estándares EDNS0. Mediante esta herramienta, los administradores DNS pueden analizar un dominio hospedado en uno de sus servidores y comprobar las respuestas generadas. Por otro lado, los desarrolladores de software DNS deberán configurar los tiempos de espera para responder acorde a las solicitudes EDNS0. Para investigadores del protocolo DNS existen las estadísticas de compatibilidad EDNS generadas por la herramienta Web como serie de reportes. Finalmente, hay un escáner de código libre [22] desarrollado por el registrador de la República Checa, NIC.cz, para evaluar toda una zona DNS y clasificar la cantidad de dominios que cumplen los requisitos EDNS.

2.2.3. Investigación sobre extensiones DNS

Uno de los principales motivos de crear las extensiones DNS fue el de optimizar la operación DNS, por lo que cada una de las extensiones puede ser estudiada de manera independiente. Sin embargo, aunque EDNS aumenta las capacidades de carga útil en el protocolo UDP y así mejora la escalabilidad del DNS, esto pretende evitar el uso generalizado de TCP para el transporte DNS (ver [24], numeral 3).

Basado en los objetivos de esta tesis, a continuación se presenta una revisión de literatura con trabajos relacionados a las extensiones DNS y optimización de rendimiento DNS desde diferentes perspectivas, principalmente tiempos de respuesta en DNS como factor de impacto decisivo en la latencia global de red [12]. Una de las principales extensiones de estudio es DNSSEC, ya que proporciona seguridad a distintas vulnerabilidades en DNS [10].

2.2.3.1. *Domain Name System Security Extensions - DNSSEC*

Las extensiones de seguridad del sistema de nombre de dominios (Domain Name System Security Extensions) son mecanismos de seguridad para certificar que los datos provienen de fuentes seguras y no son modificados durante la comunicación entre los nodos de la red [9]. En la jerarquía DNS existen dos funciones DNSSEC básicas, firma y validación que pueden ser realizadas de manera independiente.

Un dominio es firmado por el operador de servicios DNS, un proveedor de servicios Web "*Web hosting*", el operador de los servidores autoritativos de operación DNS o un registrador DNS que ofrezca *DNS hosting*. La información de la firma DNSSEC es enviada al registrador del dominio y luego hasta el registro del dominio de nivel superior [10].

La validación de las llaves criptográficas es realizada en el servidor recursivo. En la Fig. 2.2 se puede observar el proceso de validación DNSSEC completo entre el servidor recursivo y servidores autoritativos, así como la información de validación DNSSEC entre el servidor recursivo y el cliente mediante la bandera DNSSEC OK y la bandera de datos autenticados AD, Authenticated Data por sus siglas en inglés.

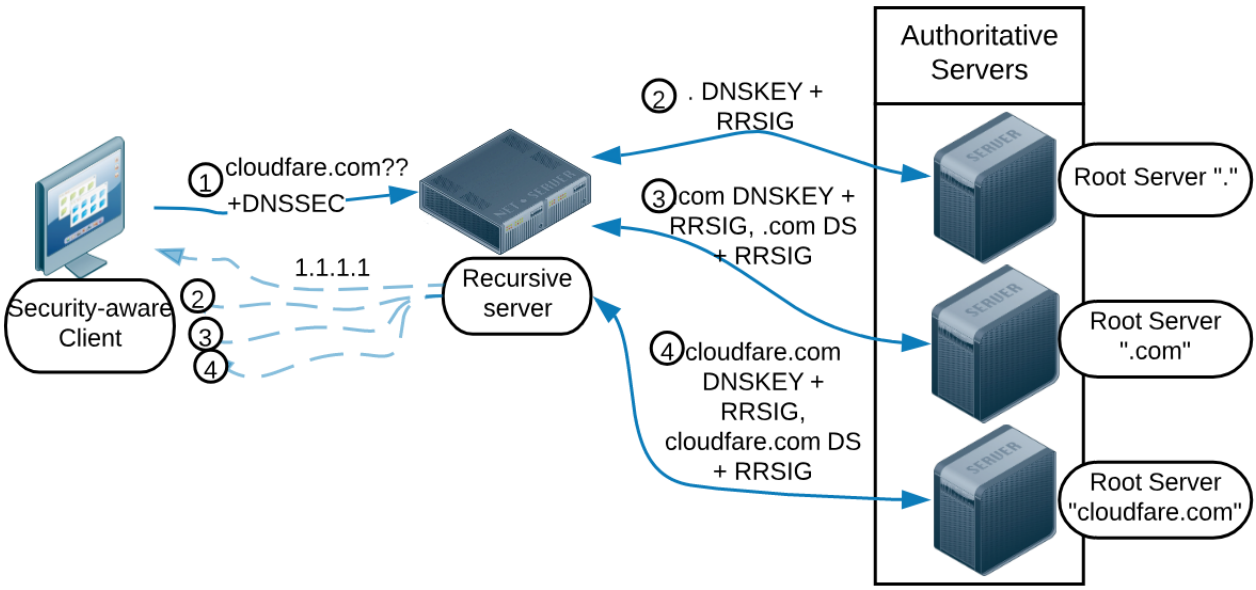

Figura 2.2: Arquitectura de validación DNSSEC

El servidor recursivo se puede encontrar en el borde de la red local o inclusive puede ser un servidor DNS público. También se puede realizar la validación a nivel de software como en servidores de correo o en el navegador web [38]. Los servidores recursivos públicos como el resolver DNS de Google (8.8.8.8) han incrementado su popularidad [67], [2], [30]. Sin embargo, estos servidores tienen desventajas debido a que comprometen la privacidad de las consultas DNS por medio de ataques de escucha no deseada (eavesdropping) [47]. Adicionalmente, existen ataques como DNSChanger, un *malware* que re-direcciona los servidores recursivos a terceros de manera malintencionada [51] y que puede ser detectada mediante la validación DNSSEC.

La implementación de EDNS0 permite la agregación de información DNSSEC como las llaves DNSKEY y registros RRSIG, debido al aumento en los tamaños de respuesta de DNS. No obstante, las respuestas negativas basadas en solicitudes DNS con registro de recursos erróneos son almacenadas en caché, lo cual genera vulnerabilidades ante ataques DoS o DDoS [71]. Zheng et al. presentan un mecanismo eficiente de almacenamiento en caché negativo, para servidores ajenos a DNSSEC, basado en el espacio de nombre de los registros NSEC/NSEC3. Esos registros se pueden reutilizar para demostrar la inexistencia de cualquier subdominio o dominio en su rango de nombres por lo que se mejoran tiempos de respuesta.

Una parte fundamental de esta tesis es la evaluación comparativa de la extensión *DNS ChainQuery* con el escenario donde no se usa esta extensión, para la validación de claves DNSSEC. Hoy en día existen una serie de métodos que permiten establecer si las llaves recibidas entre cada elemento de red son confiables. Dado que los clientes utilizan los resultados de validación de cadenas de resoluciones completas DNS y DNSSEC, se aumenta la complejidad de validación obteniendo errores de falla o de tiempo de espera agotado. Para ello, en [44] los autores han desarrollado un sistema de validación adaptativo basado en el cliente con mecanismo de alerta, considerando un tiempo de espera mínimo. Este mecanismo permite prevenir o corregir las fallas en la validación DNSSEC basado en las alertas al usuario.

2.2.3.2. *DNS ChainQuery*

La extensión *DNS ChainQuery* es un mecanismo para crear una cadena de solicitudes DNS específicamente entre clientes y servidores en un contexto de validación de llaves DNSSEC, definida en la RFC 7901 de tipo experimental [74]. Con la implementación de la RFC 7901 se podrían reducir los tiempos de respuesta (*round trip time* - RTT) gracias a la simplificación de enviar múltiples solicitudes a la vez, lo que concluye en disminuir la latencia en la red por la resolución DNS con el grado de seguridad que DNSSEC le brinda al cliente.

La función principal de *DNS ChainQuery* es configurar un servidor de reenvío desde el lado del cliente para enviar una sola consulta hacia el servidor recursivo, y recibir una ruta de validación completa junto con la respuesta de la consulta DNS regular, como se ilustra en la Fig. 2.3. La ruta de validación completa es denominada "cadena de confianza" y contiene la información intermedia de validación al cliente, desde el servidor raíz hasta el servidor recursivo.

Además este proceso puede ser resuelto en 2 RTT, inclusive en 1 RTT si se configura junto con la extensión "The edns-tcp-keepalive EDNS0" definida en la RFC 7828 [62]. Por este motivo se hace necesario el análisis del estado de implementación y adopción de las diferentes extensiones EDNS0 en los servidores recursivos.

Actualmente la extensión *DNS ChainQuery* describe que se debe hacer uso del protocolo de transporte TCP o el protocolo de transporte UDP con la inclusión de la extensión Cookies, para una correcta implementación. Esto debido a que el conjunto de solicitudes sobre el protocolo UDP no garantizan que se obtengan todos los registros requeridos para la validación DNSSEC, generando posteriormente el reenvío de solicitudes adicionales para completar la cadena de confianza.

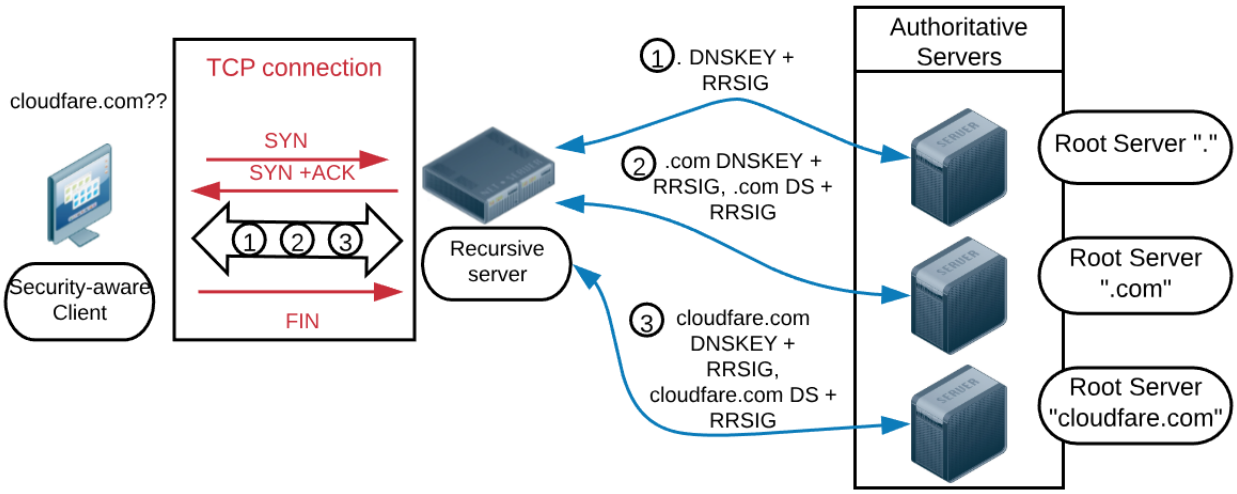

Figura 2.3: Arquitectura de configuración de red para la extensión *DNS ChainQuery*, RFC 7901 [74].

El reenvío de solicitudes adicionales en enlaces de alta latencia es crítico, como por ejemplo la resolución del dominio de acceso a servidores Network Time Protocol (NTP) en proyectos de redes satelitales. Para estos casos se realiza una propuesta del uso de servidores de validación DNSSEC públicos para que los clientes finales ubicados en zonas desmilitarizadas (DMZ) accedan a la resolución DNS de los servidores NTP sin ser expuestos a fallas por DDoS [19].

De acuerdo a estudios previos [29], el despliegue de *DNS ChainQuery* puede generar ataques de amplificación DNS debido a que genera respuestas muy grandes. Este tipo de ataques se denominan "Ataques de amplificación" en DNS, un tipo de ataque DDoS. La vulnerabilidad permite a los atacantes usar una dirección IP falsificada y usar una cadena de validación para enviar un gran volumen de datos en la respuesta. El factor de amplificación es el parámetro de medición de la respuesta amplificada respecto a una respuesta convencional, incluso en servidores con altos niveles de seguridad. Respecto a esta vulnerabilidad, diferentes mecanismos basados en los patrones de tráfico DNS han sido configurados en los elementos de seguridad en una red, para controlar y crear protección en los servidores DNS. Adicionalmente, mediante redes definidas por software (SDN) se han modelado patrones para diferenciar paquetes de ataque DNS con tráfico normal y así bloquear los ataques de amplificación DNS en escenarios específicos sin generar sobrecarga adicional en la transmisión [45].

En resumen, la implementación de la extensión *DNS ChainQuery* podría disminuir el uso de recursos de hardware como memoria, CPU y batería en el cliente gracias al envío de varias solicitudes UDP simultáneamente en aplicaciones y servicios en Internet. Además, la correcta configuración de la RFC 7901 garantizaría completar la cadena de validación DNSSEC en las primeras consultas, reduciendo posiblemente la latencia en la red. Finalmente, varios estudios indican la necesidad de un método de seguridad para mitigar las vulnerabilidades que aparecen con la implementación de la extensión, como los ataques de amplificación.

2.2.3.3. *Client Subnet in DNS Queries*

Desde la creación de los mecanismos EDNS y las soluciones provisionales que mantenían el funcionamiento parcial del protocolo DNS, no existía un interés de desplegar dichos mecanismos EDNS como se describía en las RFC. Sin embargo, esto cambió con el desarrollo de la extensión EDNS0 Client Subnet (ECS) en solicitudes DNS, descrita en la RFC experimental 7871 [13]. La extensión ECS, bajo la promesa de un "Internet más rápido" [46], permite a los servidores recursivos proveer información de las direcciones de red del cliente a los servidores autoritativos DNS.

ECS ha permitido desarrollar sistemas de distribución geo-localizada de solicitudes a servidores de redes de distribución de contenidos CDN de manera óptima. Esto mejora los tiempos de respuesta del lado del cliente basados en la redirección más precisa del cliente al contenido en un servidor CDN cercano. El despliegue de ECS inclusive ha superado a la técnica de Anycast hasta en 80 % de efectividad de una correcta distribución, basado en el análisis de resultados de emulación de escenarios reales y métricas estadísticas como el cuartil Q1 y mediana de la latencia [15]. Así mismo se ha generado una serie de estudios de distribución geo-localizada y se han realizado estudios del impacto de este tipo de distribuciones [14], [66].

En otro escenario se ha probado la efectividad de la extensión ECS en la estimación de distancia en la red entre nodos finales mediante la construcción de rutas de réplicas CDN [25]. La creación de sistemas de asignación de clientes subyacente mediante ECS permite realizar una construcción de rutas de replicas CDN para estimar distancia entre nodos remotos, esto libre de infraestructura de medición o administración.

También existen trabajos relacionados con el diseño e implementación de ECS en sistemas de seguridad como cortafuegos. Mediante ECS se pueden cambiar de manera dinámica las políticas basadas en reglas de acuerdo con la dirección IP de procedencia de la información [59]. Sin embargo, aunque la implementación de ECS mejore el rendimiento, también tiene un costo a nivel de privacidad para el cliente que realiza la solicitud DNS. Las debilidades de privacidad han sido analizadas como los ataques de envenenamiento de caché y vigilancia no deseada por parte de terceros [46]. El estudio presentado en [46] establece una serie de recomendaciones para evitar ataques masivos por medio del uso de la extensión ECS, la cual estaba configurada por defecto. Esto permite concluir que hay que establecer escenarios donde exista un equilibrio de rendimiento y seguridad en las extensiones DNS.

2.2.3.4. *Padding*

La carga útil es un problema creciente a medida que el DNS evoluciona para mejorar la seguridad en la red. El impacto del aumento de carga útil en la transmisión de paquetes DNS permite el despliegue de nuevos mecanismos de seguridad como DNSSEC. Actualmente, un 75 % de los sitios web ubicados en la lista TOP 1000 de *Alexa* responden con al menos 738 bytes, lo cual no es soportado sin EDNS a menos que exista fragmentación a nivel IP y esto aumenta los riesgos de seguridad [75]. *Padding* es una solución a este obstáculo. Actualmente descrita por la RFC 7830, este estándar describe un proceso para agregar espacio (octetos) a los mensajes de solicitud o respuesta, en clientes y servidores.

Capítulo 3

Evaluación y análisis del estado EDNS0 de los servidores recursivos

En este capítulo se describe el desarrollo de un algoritmo para clasificar el estado de un servidor recursivo respecto a la resolución DNS y sus extensiones. El algoritmo propuesto se prueba experimentalmente sobre 19061 servidores recursivos, donde un 60 % pertenecen a la zona de Chile y el 40 % restante son consultados mediante transacciones DNS recurrentes en la zona de Chile[1]. El análisis está basado en el comportamiento de las repuestas de los servidores a consultas EDNS0, haciendo un énfasis a las respuestas de *DNS ChainQuery*. Además, se evalúa el rendimiento de la implementación de la extensión *DNS ChainQuery* en la resolución DNS.

3.1. Algoritmo de clasificación del estado de resolución EDNS en servidores recursivos

Para el desarrollo del algoritmo de clasificación se considera el seguimiento del Internet-draft "*A Common Operational Problem in DNS Servers - Failure To Communicate*" [7]. El borrador, a la fecha de escritura de este documento, se encuentra en su versión 13 y presenta una guía para detectar fallas en las respuestas a las solicitudes DNS más comunes. No obstante, aunque está dirigido a cualquier servidor DNS en la jerarquía, en este estudio se descarta el uso de la bandera `+norec`. Esto se debe a que esta bandera deshabilita la recursividad en la búsqueda de la respuesta DNS, lo cual es el objetivo principal de este trabajo para analizar el comportamiento de servidores recursivos y así evitar códigos de respuesta tipo *REFUSED*.

Las pruebas experimentales se realizan en 3 fases que son ilustradas en la Fig. 3.1. En la fase A se obtienen datos básicos de los servidores recursivos y se estudia si soporta EDNS, con el fin de identificar posibles fallas en la configuración como el espacio en buffer o simplemente

[1]Los datos correspondientes a los servidores recursivos son fuente del registrador oficial de la zona de Chile, NIC Chile.

falta de soporte de EDNS. En esta misma fase se analiza la configuración de la versión 1 de EDNS, la cual consiste en un conjunto de nuevas versiones del sistema EDNS para reservar un campo a futuras características que no se acoplen a la versión 0.

Posteriormente, en la fase B se mide el desempeño EDNS con diferentes opciones, la negociación EDNS entre cliente/servidor, evaluación de banderas desconocidas y la extensión más importante de seguridad DNSSEC.

Finalmente en la fase C se realiza la evaluación del estado de las extensiones: *EDNS TCP keepalive*, *DNS ChainQuery*, *Client Subnet*, *EDNS Cookies* y *EDNS Expire option*.

3.1.1. Fase A del algoritmo de clasificación

Las primera prueba consiste en analizar la versión del software DNS de los servidores mediante los registros DNS en texto plano de la clase ***CHAOS***. La clase ***CHAOS*** derivada de la red local *Chaosnet* [57], permite obtener información sobre el sistema DNS y en la actualidad se usa mediante el software *BIND*.

Aunque esta información puede ser oculta o modificada en la configuración del servidor para prevenir exponer las vulnerabilidades de la versión del software DNS, la información del software DNS permite detectar fallas en las pruebas EDNS basado en la implementación o modificación de las características en cada versión, como se observa en la Tabla 3.1. Los valores observados en la Tabla 3.1 hacen referencia a la versión estable de cada característica EDNS, por ejemplo, aunque DNSSEC es soportado desde una versión BIND 9.2, no esta configurado por defecto. Para el soporte DNSSEC en esta versión es necesario agregar a la configuración el software OPENSSL para comunicaciones seguras y aún así no provee todas las opciones de configuración DNSSEC como las versiones actualizadas de BIND.

Adicionalmente, en esta fase se puede detectar la inexistencia del soporte EDNS mediante el código de respuesta rCODE NOTIMP como advertencia en la sección de respuesta, lo cual reduce tiempo de evaluación de las siguientes pruebas. El comando utilizado para obtener la versión del software DNS en los servidores recursivos es:

```
dig +short @1.2.3.4 version.BIND TXT CH
```

Un ejemplo de la respuesta a la solicitud de la versión del software DNS es:

```
9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6\_5.1
```

La versión del software esta representada por 9.8.2, luego se puede observar el sistema operativo *RedHat* y finalmente se observan las actualizaciones a la versión mediante los lanzamientos 9.8.2-0.23.rc1.el6_5.1. Aunque no todas las respuestas contienen los mismos parámetros, la versión si se puede interpretar como parte esencial de esta tesis.

La segunda prueba consiste en asociar información extra del resolver como el Número de Sistema Autónomo (ASN) asignado, compañía a cargo de los servidores y geolocalización de los servidores de nombre. Esta información permite realizar un diagnóstico del estado de una

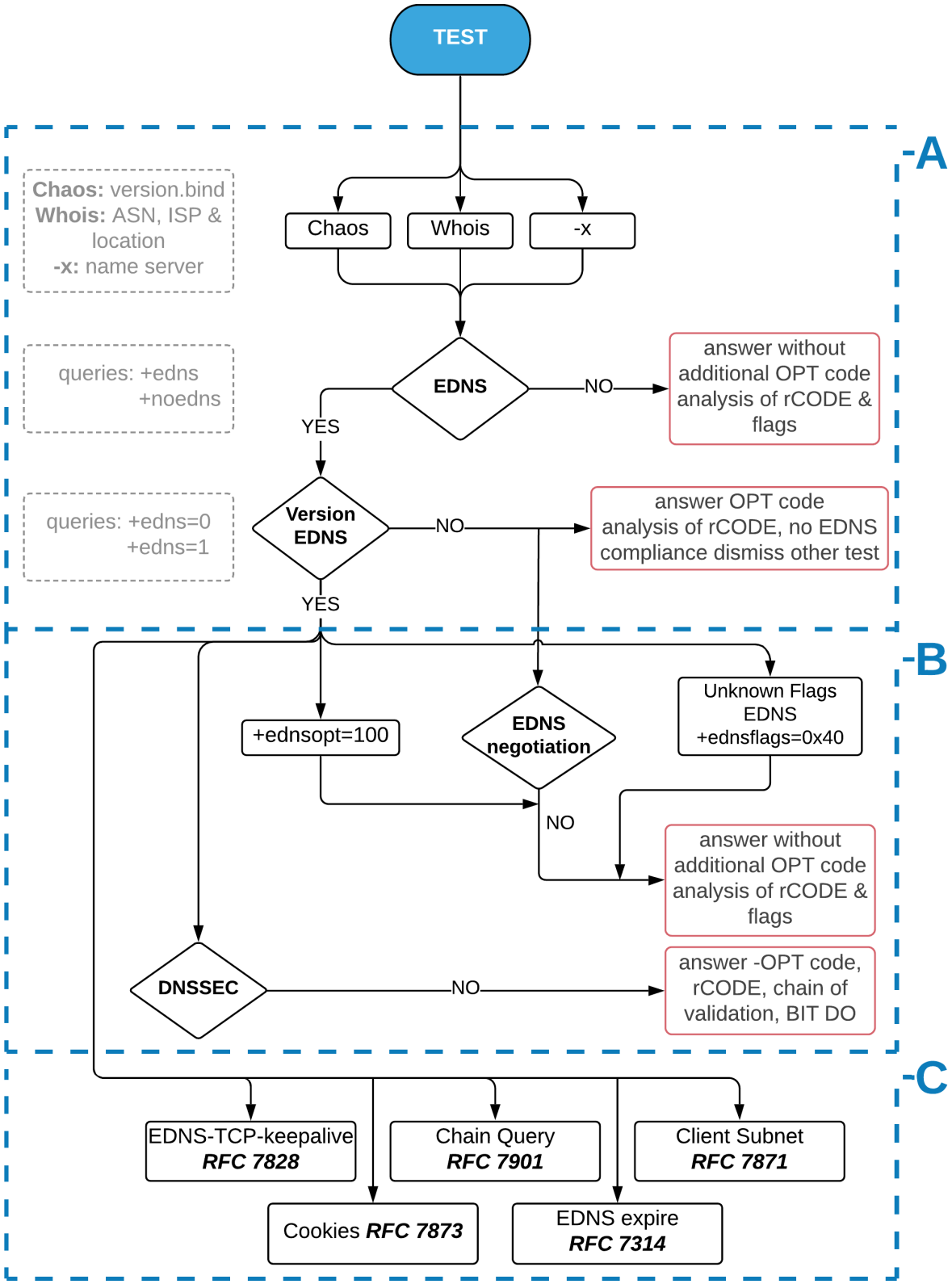

Figura 3.1: Diagrama de bloques de pruebas para el análisis del estado de cumplimiento EDNS en resolvers de la muestra.

Característica EDNS	Descripción	Versión BIND
EDNS versión 0 (RFC 6891)	El servidor reconoce la opción EDNS	9 en adelante
Soporte GeoIP	Geolocalización de la dirección IP	9.9-S
DNSSEC (RFC 4033, 4035,7646)	Soporte de la extensión de seguridad DNSSEC y Negative Trust Anchor	9.6-S1
EDNS Client-Subnet ECS (RFC 7871)	Soporte de la extensión ECS para resolvers	9.10-S, 9.11-S, 9.12 (9.11 no stable no soporta)
EDNS EXPIRE option (RFC 7314)	Soporte de la extensión ECS para servidores	9.10.1, 9.10-s, 9.11, 9.11-S, 9.12
EDNS Padding option (RFC 7830)	Soporte de la extensión Padding para resolvers	9.10.5-S1, 9.11-s y 9.12
EDNS TCP keepalive (RFC 7828)	Soporte de mejora de rendimiento sobre sesiones TCP en cliente o servidor	9.10-S, 9.11-S, 9.12 (9.11 no stable no soporta)
Pipelined TCP queries	Soporte de mejora de rendimiento para servidores	9.10-S, 9.11, 9.11-s, 9.12
TCP connection sharing	Soporte de mejora de rendimiento para actualizar el estado de reenvío	9.11, 9.11-S, 9.12

Tabla 3.1: Características EDNS soportadas en las diferentes versiones de software DNS

zona DNS, por ejemplo si existen pruebas fallidas o servidores recursivos inalcanzables de un mismo operador de servidores de nombre o ASN. Adicionalmente, en esta fase se obtienen los datos de geolocalización del servidor recursivo mediante las bases de datos de acceso público ***Whois***, esto con el fin de mapear fallas masivas en el estado de resolución DNS en la zona del servidor recursivo mediante el comando:

```
whois -h whois.cymru.com -v
```

Un ejemplo de la respuesta a la solicitud Whois es:

AS | CC | Registry | AS Name
15169 | US | arin | GOOGLE - Google LLC, US

En la columna AS se representa el número asignado por la IANA, en este ejemplo es 15169. La columna CC representa el código de país, Registry representa el registrador *ARIN* del ASN y AS Name indica el nombre público del ASN.

La tercera prueba se basa en realizar solicitudes DNS de manera reversa para encontrar los dominios y nombres de host asociados a la dirección lógica IP de los servidores recursivos. Esta prueba realiza un diagnóstico de fallas directas a los dominios para respuestas rápidas de configuración en los servidores de nombre. Esta prueba fue de gran utilidad para el trabajo realizado el día DNS Flag Day 2019. El comando utilizado para la búsqueda DNS reversa es:

```
dig +noall +answer -x @1.2.3.4
```

Un ejemplo de la respuesta a la solicitud DNS reversa es:

```
1.2.3.4.in-addr.arpa.      36000 IN    CNAME
rev-c41-10.gnu.org.        300     IN      PTR
                    www.gnu.org.
```

En la respuesta se puede observar la dirección IP consultada con el nombre de dominio especial *in-addr.arpa* que apunta al nombre de host asociado a la dirección IP. Posteriormente aparece el tiempo de vida útil por defecto en 36000 segundos. El valor IN CNAME hace referencia al registro de nombre canónico (CANONICAL NAME en inglés), utilizado para asignar un alias a un nombre de dominio auténtico o canónico. Finalmente, se observa la respuesta del servidor rev-c41-10.gnu.org que contiene un tiempo de vida útil de 300 segundos y un registro PTR *Pointer* que resuelve el nombre de dominio completo FQDN.

Parte esencial de esta tesis para lograr el primer objetivo de caracterizar la adopción e implementación EDNS, es el estudio actual del estado EDNS en servidores recursivos basado en el seguimiento del estándar RFC6891 [24].

EDNS es un mecanismo que mejora la escalabilidad del protocolo DNS mediante el uso del protocolo de transporte UDP para enviar mensajes más extensos de los 512 bytes, proporcionando espacio adicional para nuevas características. El mecanismo tiene como prioridad mantener compatibilidad con las versiones anteriores del protocolo sin afectar la operación DNS, lo cual fue logrado a través de la opción de registro de recursos *OPT*. Esta opción es incluida en la respuesta como *OPT PSEUDOSECTION* entre todos los elementos de la jerarquía DNS para notificar el soporte EDNS. Un ejemplo de la respuesta, donde se muestra la versión EDNS, las banderas activas y el tamaño del paquete UDP por defecto de 4096 bytes es:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: aa,rd,do; udp: 4096
```

El algoritmo propuesto tiene como objetivo analizar las banderas y códigos de respuesta para clasificar el estado EDNS. Las banderas y códigos de respuesta especificados en [56], [10] y [24], así como su descripción se pueden observar en la Tabla 3.2 y son definidos por la Entidad de Supervisión de Asignación de Direcciones IP IANA [35].

Para el análisis del soporte EDNS se consulta la versión 0 sin configuración de banderas DNS o EDNS, además de opciones EDNS. La prueba se realiza a cada una de las IPs de los 19061 servidores existentes en la muestra en estudio, para determinar el estado de configuración EDNS. El comando usado para la consulta es el siguiente:

```
dig +edns=0 +noad soa @1.2.3.4
```

En un consulta con registro SOA de una zona en la que el servidor está nominalmente configurado para servir y sin autenticación de datos, la expectativa en la respuesta es un código de respuesta NOERROR, un registro EDNS (0) en la sección PSEUDOSECTION y las banderas *AA* de ser autoridad para la consulta realizada, *RA* si está configurado la

Banderas de la cabecera DNS y EDNS	Descripción	Código de respuesta	Descripción
QR- Query	indica si es el mensaje es una solicitud (0) o una respuesta (1)	0 - NoError	no hay condición de error
AA- Authoritative Answer	específica si el servidor de nombres es una autoridad para el dominio consultado	1 - FormErr	el servidor de nombres no puede interpretar la solicitud
TC - TrunCation	indica mensaje truncado debido a la longitud máxima permitida por el canal de transmisión	2 - ServFail	el servidor de nombres no puede procesar la solicitud debido a un problema con el servidor
RD - Recursion Desired	especifica que la consulta sea recursiva, opcional si el servidor de nombres lo soporta	3 - NXDomain	indica que el dominio solicitado no existe
RA - Recursion Available	indica que el servidor de nombres soporta recursividad	4 - NotImp	el servidor de nombres no soporta este tipo de solicitudes
Z	reservada para futuro uso	5 - Refused	el servidor de nombres se niega a realizar la operación especificada por políticas de configuración
CD - Checking Disable	indica que acepta una respuesta sin necesidad de la validación de las firmas DNSSEC, deshabilita la validación	16 - BADVERS	no existe la versión del registro OPT solicitado
AD - Authentic Data	especifica que el conjunto de registros de recursos DNSSEC obtenidos en las secciones de respuesta y autoridad son auténticos	16 - BADSIG	Fallo de la firma TSIG
DO - DNSSEC OK	indica que el resolver soporta una resolución con los registros de recursos DNSSEC y que el servidor de nombres puede autenticar la respuesta mediante los registros SIG, KEY or NXT	17 - BADKEY	no se reconoce la llave utilizada por el cliente

Tabla 3.2: Banderas y códigos de respuesta de la cabecera DNS/EDNS.

recursividad en el servidor y *QR* en todas las respuestas basado en que es una consulta DNS. No debe existir registro de la bandera de datos autenticados *AD*.

Basado en la respuesta de soporte EDNS se prosigue a evaluar la versión EDNS. La versión EDNS1 está reservada para futuros cambios de la versión EDNS0 y se evalúa mediante el siguiente comando:

```
dig +edns=1 +noednsneg +noad soa @1.2.3.4
```

Basado en la expectativa de respuesta solo para la versión EDNS1 se habilita la opción `+noednsneg` la cual instruye al servidor no establecer la negociación EDNS, ya que *dig* la soporta por defecto en las consultas de la versión EDNS0. En la sección de respuesta se espera como resultado un código de respuesta BADVERS, un registro EDNS (0) en la sección *PSEUDOSECTION*, además de la ausencia de las banderas AA, AD y el registro de la autoridad de la zona DNS SOA. Las banderas y códigos de respuesta están descritos en la Tabla 3.2. Con esta prueba se finaliza la fase A del monitoreo del estado de compatibilidad EDNS de los servidores.

3.1.2. Fase B del algoritmo de clasificación

La fase B consiste en evaluar el desempeño EDNS con diferentes opciones, la negociación EDNS entre cliente/servidor, evaluación de banderas desconocidas y finalmente la extensión más importante de seguridad DNSSEC. Basado en la respuesta de la versión EDNS0, si es correcta se analiza el comportamiento del servidor respecto a diferentes códigos OPT, correspondiente a la prueba *+ednsopt=100* de la Fig. 3.1, y se realiza mediante el siguiente comando:

```
dig +edns=0 +noad +ednsopt=100 soa @1.2.3.4
```

El comportamiento del servidor respecto a EDNS con códigos OPT desconocidos se determina por el análisis de los códigos más usados y establecidos por la IANA. El código usado es el 100 ya que no está asignado actualmente, como se puede observar en la Tabla 3.3.

En una consulta con el registro SOA de una zona en la que el servidor está nominalmente configurado para servir, sin autenticación de datos y un código OPT, la expectativa de los resultados es un código de respuesta NOERROR, un registro EDNS (0) en la sección PSEUDOSECTION, registro OPT en la sección adicional y las banderas AA de ser autoridad para la consulta realizada Esta respuesta se espera para un caso donde se consulta el registro SOA de una zona en la que el servidor está nominalmente configurado para servir sin bits de marca de DNS establecidos. Además en la respuesta no debe existir registro del código OPT=100 y tampoco de la bandera AD de datos autenticados.

La siguiente prueba permite analizar la negociación EDNS entre los servidores recursivos y clientes o servidores autoritativos en un proceso de resolución DNS. Esta corresponde a la prueba *EDNS negotiation* de la Fig. 3.1. La solicitud se realiza sin banderas activas, consultando la versión EDNS1, debido a que la herramienta *dig* admite la negociación EDNS0 entre los nodos DNS por defecto. La finalidad de la prueba es analizar las políticas de negociación configuradas para los servidores recursivos a través del siguiente comando:

```
dig +edns=1 +noednsneg +noad soa @1.2.3.4
```

La expectativa de respuesta cuando se consulta el registro SOA de una zona en la que el servidor está nominalmente configurado para servir sin bits de marca establecidos para la negociación EDNS, es un código de respuesta BADVERS, un registro EDNS (0) en la sección PSEUDOSECTION y un registro OPT en la sección adicional. No deben existir registros de banderas, ni registro SOA en la sección de respuesta.

La siguiente prueba evalúa la respuesta del servidor cuando se realizan consultas por el registro de autoridad de la zona configurada SOA con banderas EDNS desconocidas. Las banderas asignadas en los campos del registro OPT son DO y Z descritas en la Tabla 3.2(sección 6.1.4 de [24]). La especificación indica que el transmisor debe configurar la bandera Z en 0. Una de las opciones de configuración de las banderas EDNS del registro OPT descrita en la documentación de la herramienta dig [37] es `+ednsflags=`. El valor indicado es *Must Be Zero* (MBZ) y puede establecerse mediante codificación octal, decimal o hexadecimal. La

Código OPT EDNS0	Nombre	Descripción
0	Reservado	Definido para la opción EDNS (0), RFC 6891 [24]
1	DNS Long-Lived Queries - LLQ	Propuesta en versión borrador que permite al cliente conocer cambios sin sondear el servidor, útil para DNS Service Discovery y DNS Push Notifications [17]
2	Dynamic DNS Update Leases - UL	Propuesta en versión borrador, método para extender la Actualización de DNS Dinámico para que contenga una vida útil de la actualización de la licencia [18]
3	DNS Name Server Identifier Option - NSID	Identificador único del servidor de nombres para determinar el servidor que responde una solicitud en particular [63]
4	Reservado	
5 6 7	Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC) DAU, DHU y N3U	Métodos DAU, DHU y N3U para indicar los algoritmos hash y firmas digitales que soportan los servidores consultados [21]
8	Client Subnet in DNS Queries EDNS ECS	Mecanismo para generar información de la subred del cliente desde los servidores recursivos [13]
9	Extension Mechanisms for DNS (EDNS) EXPIRE Option EDNS Expire	Es un mecanismo para que los servidores secundarios respeten el campo SOA EXPIRE como si siempre se transfiriera desde un servidor primario [6]
10	Domain Name System (DNS) Cookies DNS Cookies	Mecanismo ligero de seguridad para transacciones DNS que proporciona protección limitada contra ataques DoS, amplificación, falsificación o envenamiento de caché [3]
11	The edns-tcp-keepalive EDNS0 Option EDNS TCP Keepalive	Mecanismo que permite a los servidores DNS indicar un tiempo de espera de inactividad variable fomentando el uso de TCP en sesiones de larga duración [62]
12	The EDNS(0) Padding Option Padding	Mecanismo que permite a servidores y clientes DNS rellenar los mensajes con un número variable de octetos [50]
13	CHAIN Query Requests in DNS DNS ChainQuery	Mecanismo que permite a un servidor en contexto de seguridad utilizar un servidor de reenvío para solicitar la cadena completa de validación DNSSEC en una solicitud mediante una sesión TCP [74]
14	Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC) EDNS Key Tag	Mecanismo que especifíca dos formas para que los servidores indiquen cuales son las llaves que pertencen a la cadena de confianza DNSSEC [73]
15	Sin asignación	
16 17	DNS EDNS Tags EDNS Client Tag EDNS Server Tag	Propuesta versión borrador, mecanismo mediante el que clientes y servidores pueden transmitir un campo de datos sin sentido semántico más que el acordado entre cliente y servidor [11]
18-65535	Sin asignación, reservado para uso experimental o futura expansión	

Tabla 3.3: Resumen de códigos OPT disponibles y asignados para los mecanismos EDNS0

bandera configurada para la consulta en codificación hexadecimal es `0x40`, en decimal es `64` o en octal se define `/100` y se realiza por el siguiente comando:

```
dig +edns=0 +noad +ednsflags=0x40 soa @1.2.3.4
```

Los resultados esperados cuando se consulta el registro SOA de una zona en la que el servidor está nominalmente configurado para servir, sin datos autenticados y banderas EDNS desconocidas, son un código de respuesta NOERROR, un registro EDNS (0) en la sección *PSEUDOSECTION*, un registro SOA en la sección de respuesta, un registro OPT en la sección adicional y las banderas AA si es autoridad para la zona consultada, RA y QR. No debe existir registro de banderas EDNS presentes en la respuesta como MBZ, respecto a la bandera desconocida en la consulta debe ser ignorada por el receptor DNS.

Finalmente en la fase B se analiza la extensión de seguridad con mayor trayectoria, DNS-

SEC. DNSSEC se define en [9] y [10]. Esta prueba es esencial debido a que la falla en la validación algún proceso relacionado con DNSSEC puede terminar en una resolución DNS fallida.

En la prueba se consulta el registro de autoridad de la zona configurada SOA, la cual no requiere estar firmada por DNSSEC. El proceso de firma y validación DNSSEC será explicado más adelante. La opción para solicitar que la zona consultada esté firmada es `+dnssec`. El comando para analizar la respuesta del servidor respecto a una consulta firmada con DNSSEC es:

```
dig +edns=0 +noad +dnssec soa @1.2.3.4
```

La respuesta esperada cuando se consulta el registro SOA de una zona en la que el servidor está nominalmente configurado para servir solicitando la cadena DNSSEC, es un código de respuesta NOERROR, la bandera AA presente si es autoridad para la zona y QR. Si el servidor recursivo soporta DNSSEC, la bandera AD debe estar configurada en la respuesta, de lo contrario no debe aparecer. Basado en que son servidores recursivos, la bandera RA puede aparecer como advertencia de que la recursividad está disponible. Previamente a las banderas mencionadas no deben existir banderas EDNS activas, excepto la bandera EDNS DO (DNSSEC OK). La bandera DO inicialmente fue definida en la RFC 3225 [23] para indicar que el servidor recursivo soporta DNSSEC. El bit de la bandera DO debe ser 1.

3.1.3. Fase C del algoritmo de clasificación

Las fases A y B evalúan el estado EDNS en general para los servidores recursivos, generando resultados de gran utilidad para el despliegue de las extensiones de seguridad u optimización de resolución DNS. La primera extensión de prueba es *EDNS TCP keepalive*. La prueba se basa en mantener una sesión TCP abierta para futuras transacciones DNS y se realiza por medio del siguiente comando:

```
dig +tcp +time=15 +edns=0 soa @1.2.3.4
```

La opción `+tcp` indica al servidor a realizar la solicitud mediante el protocolo TCP y la opción `+time` establece el tiempo de espera de la sesión en 15 segundos para la consulta, el cual por defecto es de 5 segundos mediante la herramienta *dig*.

La respuesta esperada incluye el registro SOA para la zona consultada en la sección de respuesta, un código de respuesta NOERROR, la bandera AA presente si es autoridad para la zona y QR. En la sección adicional se espera como resultado los campos del formato para la extensión como se observa en la Fig. 3.2.

Los campos tienen 2 octetos cada uno, el código OPT asignado es el 11. La longitud de la opción (OPT-LENGTH) con valor 0, se interpreta como una sesión TCP normal sin tiempo de espera y el valor 2 indica que existe un tiempo de espera para establecer la conexión TCP de manera definida. El campo de tiempo de espera (TIMEOUT) se define en milisegundos.

La segunda extensión de prueba es *DNS ChainQuery*. El descubrimiento del soporte de

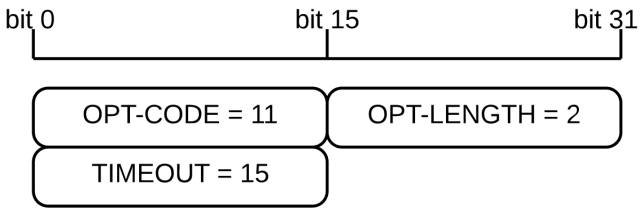

Figura 3.2: Formato de opción de la extensión EDNS TCP keepalive [62]

DNS ChainQuery se realiza mediante el envío de la opción CHAIN de longitud cero en la solicitud. En este caso el cliente es un servidor de reenvío que puede utilizar cualquier protocolo de transporte para generar la solicitud. Si el servidor recursivo soporta *DNS ChainQuery* mediante un protocolo de transporte seguro[2], este responde con una opción CHAIN de longitud cero tal como fue recibida en la solicitud.

La solicitud se genera mediante el siguiente comando con la herramienta *Pydig* y la opción `+chainquery` contenida en la librería *edns.py*:

```
pydig +tcp +chainquery soa @1.2.3.4
```

La respuesta esperada al consultar el registro SOA de una zona en la que el servidor está nominalmente configurado para servir mediante el protocolo TCP es: el registro SOA para la zona consultada en la sección de respuesta, un código de respuesta NOERROR, la bandera AA presente si es autoridad para la zona y QR. Si el servidor recursivo no reconoce la opción *CHAIN*, el código de respuesta debe ser FORMERR. En la sección adicional se espera como resultado los campos del formato para la extensión, como se observa en la Fig. 3.3.

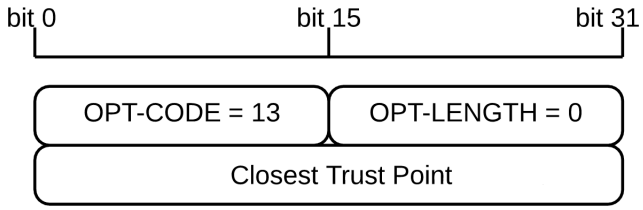

Figura 3.3: Formato de opción de la extensión cadena de solicitudes DNS [74]

Los campos de código (OPT-CODE) y longitud de la carga útil de la opción (OPT-LENGTH) tienen 2 octetos cada uno, mientras que el punto de confianza más cercano tiene 4 octetos debido a que está basado en un nombre de dominio completo (FQDN) de longitud variable. El código OPT asignado es el 13 y el punto más cercano es la entrada de la cadena de solicitudes DNS, la cual es inspeccionada en caché incluyendo los registros de la llave DNSKEY y la delegación que firma DS.

La tercera extensión de prueba es *Client Subnet*. Una opción de uso activo para señalar la información de red desde donde fue generada la solicitud y la información de la red donde la respuesta fue almacenada en caché. Esta opción puede ser iniciada por un servidor de reenvío o un servidor stub. En la sección adicional se espera como resultado los campos del formato para la extensión, como se observa en la Fig. 3.4.

[2]Transporte seguro: TCP o UDP con cookies

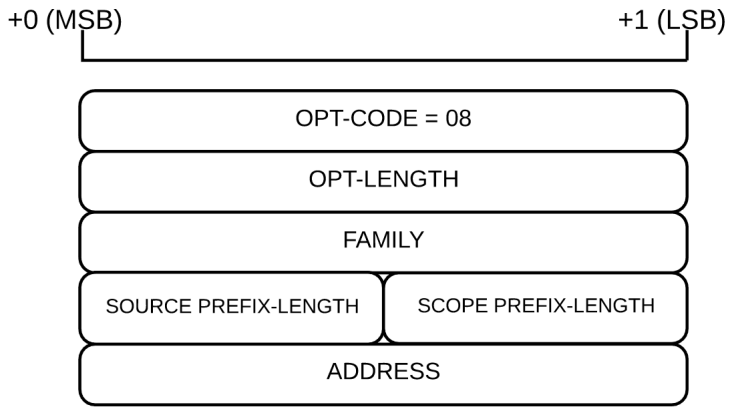

Figura 3.4: Formato de opción de la extensión EDNS Client Subnet [13]

Los campos de código (OPT-CODE), la longitud de la carga útil de la opción (OPT-LENGTH) y familia (FAMILY) de dirección IP tienen 2 octetos cada uno. El código (OPT-CODE) asignado para ECS es 8. Actualmente la familia (FAMILY) está definida por la IANA como el tipo de dirección IP y de manera operacional está IPv4 con el número 1 o IPv6 con el número 2 [34]. La longitud (OPT-LENGTH) del prefijo de origen (*SOURCE PREFIX-LENGTH*) está conformada por un octeto que representa los bits más significativos de la dirección que se utilizarán para la consulta, este valor en las respuesta es el mismo que la consulta. La longitud del prefijo de destino (*SCOPE PREFIX-LENGTH*) está conformada por un octeto y representa los bits más significativos de la dirección IP para generar la respuesta, este valor en el caso de la consulta debe ser cero. La dirección es representada por IPv4 o IPv6 dependiendo la familia, el cual debe ser truncado al número de bits indicado por el campo *SOURCE PREFIX-LENGTH* y rellenado con ceros hasta completar el último octeto.

La solicitud es generada mediante la misma librería *edns.py* de la herramienta *Pydig* con la opción `+subnet=addr`. El comando para realizar la consulta de soporte para *Client Subnet* es:

```
pydig +subnet soa @1.2.3.4
```

La respuesta esperada al consultar el registro SOA de una zona en la que el servidor está nominalmente configurado para servir y la configuración de consulta de subred es: incluye el registro SOA para la zona consultada en la sección de respuesta, un código de respuesta NOERROR. Sin embargo, el código de respuesta debe ser FORMERR si el servidor recursivo emplea demasiados o muy pocos octetos para la dirección IP, o que tiene bits distintos de cero establecidos más allá del campo *SOURCE PREFIX-LENGTH* como una señal para arreglar su implementación en la configuración del software del servidor. La bandera activa AA dependiendo si es autoridad para la zona consultada y RD basado en las pruebas de servidores recursivos.

La cuarta extensión de prueba es *EDNS Cookies*. Una extensión de seguridad basada en el mecanismo ligero de seguridad para transacciones DNS, cookies. Es un mecanismo de gran acople a nivel operacional debido a que funciona con la técnica de *Anycast* y en la sección

adicional se espera como resultado los campos del formato para la extensión como se observa en la Fig. 3.5 y la Fig. 3.6.

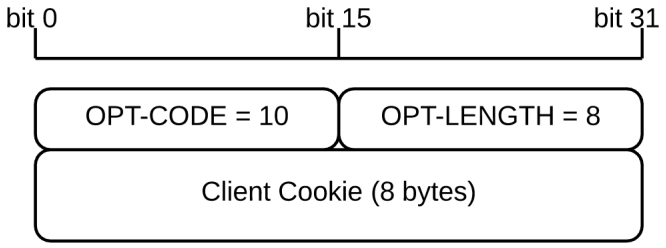

Figura 3.5: Formato de opción de la extensión DNS Cookies para cookie del cliente [3]

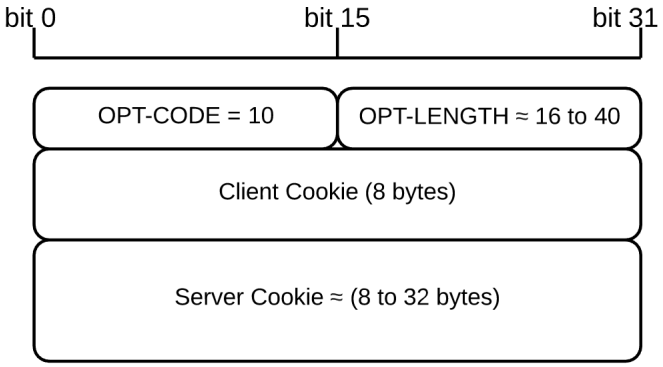

Figura 3.6: Formato de opción de la extensión DNS Cookies para cookie conocida del servidor [3]

En la Fig. 3.5 se observa los campos del formato de opción (OPT-CODE) para cuando el cliente no conoce la cookie del servidor, el código (OPT-CODE) asignado es 10 y la longitud (OPT-LENGTH) es fija de valor 8. La figura 3.6 representa el caso cuando el cliente tiene almacenada la cookie del servidor en su caché y la longitud (OPT-LENGTH) es variable siendo la mínima de 16 y máxima de 40, esto corresponde a la longitud de ambas *Cookies*.

La solicitud se genera con el siguiente comando de la herramienta *Pydig* mediante la opción `+cookie[=xxx]` contenida en la librería *edns.py*:

```
pydig +cookie soa @1.2.3.4
```

La respuesta esperada al consultar el registro SOA de una zona en la que el servidor está nominalmente configurado para servir y la opción de consulta del mecanismo de seguridad *Cookies* es: el registro SOA para la zona consultada en la sección de respuesta, un código de respuesta NOERROR, la bandera AA presente si es autoridad para la zona y QR. Sin embargo, el código de respuesta puede ser FORMERR debido a que no reconoce la opción en la consulta, la opción es demasiado corta para contener una cookie del cliente, si la opción es más extensa en longitud que la cookie del cliente (8 bytes) pero es menor que la longitud de la cookie del cliente y servidor juntas (16 bytes) o si supera el máximo valido de la longitud de la opción (40 bytes). Adicionalmente, se puede generar un código de error *BADCOOKIE* (Bad/missing Server Cookie) si el servidor no puede validar la cookie.

La quinta extensión de prueba es *EDNS Expire option*, donde se propone un método para que los servidores DNS secundarios respeten el registro *SOA EXPIRE* como si siempre estuvieran transfiriendo desde el primario. Esta opción es común en consultas de tipo SOA, zonas de transferencia autoritativa AXFR y zonas de trasnferencia de incremento IXFR aunque puede ser agregada a cualquier consulta mediante el envío de la opción *EDNS EXPIRE* de longitud cero. En la sección adicional se espera como resultado los campos del formato para la extensión como se observa en la Fig. 3.7.

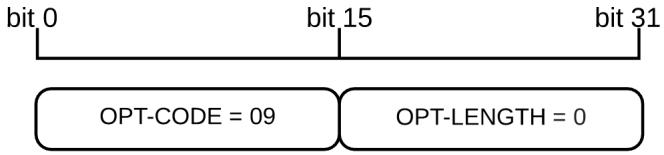

Figura 3.7: Formato de opción de la extensión EDNS EXPIRE [6]

El código (OPT-CODE) asignado es 9. El descubrimiento del soporte de la extensión expire se realiza mediante el envío de la opción con longitud (OPT-LENGTH) cero en la solicitud. La consulta es generada a través del siguiente comando:

```
pydig +expire soa @1.2.3.4
```

La respuesta esperada al consultar el registro SOA de una zona en la que el servidor está nominalmente configurado para servir y la opción de consulta *+expire* es: el registro SOA para la zona consultada en la sección de respuesta y un código de respuesta NOERROR. Además cuando la solicitud está dirigida al servidor primario de la zona la longitud OPT el valor es de 4, conteniendo el valor del campo *SOA EXPIRE*, en segundos y orden de bytes de red. Si la solicitud es hacia el servidor secundario la longitud, el campo OPT es de 4 conteniendo el valor del temporizador de caducidad en ese servidor en segundos y orden de bytes de red. Si el servidor es autoritativo para la zona debe estar presente la bandera AA y debe agregar la opción *EXPIRE* en la respuesta, de lo contrario no debe realizarlo.

3.2. *DNS ChainQuery* para validación DNSSEC en clientes

En la sección 3.1.1 se realizaron las pruebas del estado EDNS en una muestra de cerca 20000 mil servidores recursivos DNS con el fin de identificar su comportamiento respecto a las extensiones DNS y poder evaluar el impacto de la implementación de una de las extensiones de prueba, la extensión *DNS ChainQuery* [74]. La evaluación de las otras 4 extensiones se debe a que complementan la funcionalidad de *DNS ChainQuery*, que es la validación DNSSEC en un cliente mediante la cadena de solicitudes DNS. Basado en los costos de recursos que requiere un servidor para verificar cada recurso DNSSEC, se analiza el impacto de la implementación de la extensión *DNS ChainQuery* para reducir latencia en red durante la validación DNSSEC en la última milla de resolución DNS. La extensión *DNS ChainQuery* fue propuesta para ser configurada entre un stub resolver y servidores recursivos, no hacia servidores autoritativos.

Para el análisis de *DNS ChainQuery* es necesario configurar los requerimientos de red de acuerdo a la RFC 7901 [74]. Inicialmente se configura un *Stub resolver* en el lado del cliente como servidor DNS de reenvío y se habilita la validación DNSSEC. Para esto se instala *Stubby* [65] como *Stub resolver*. Stubby es una aplicación que funciona como demonio para encriptar todas las transacciones DNS a través de la dirección loopback (127.0.0.1, ::0).

Stubby permite configurar el tipo de resolución del servidor en modo Stub, el protocolo de transporte TCP, dirección IP y puerto por el que se recibe las solicitudes DNS, el tiempo de espera de la sesión basado en la extensión EDNS TCP Keepalive y finalmente los servidores recursivos a los que se reenviará las solicitudes DNS. Además de habilitar la validación DNSSEC. El archivo de configuración se puede observar en la Fig. 3.8. Para más opciones de configuración de *Stubby* se puede visitar el proyecto de privacidad en DNS [64].

```
########################## BASIC & PRIVACY SETTINGS ############################
resolution_type: GETDNS_RESOLUTION_STUB  # Stub resolver mode
dns_transport_list:
  - GETDNS_TRANSPORT_TCP                 # TCP as transport protocol for queries
edns_client_subnet_private : 1           # ECS activated
idle_timeout: 10000                      # Idle timeout in (ms) for keepalive
listen_addresses:
  - 127.0.0.1
  -  0::1
port:53                                  # Default port for TCP or UDP
dnssec: GETDNS_EXTENSION_TRUE            # DNSSEC validation true
appdata_dir: "/var/cache/stubby"         # Directory for storing trust-anchor
                                         # files

round_robin_upstreams: 0                 # Use only listed upstreams servers
upstream_recursive_servers:
## NIC Chile (self-signed cert)          # Upstream server
  - address_data: 200.1.123.46
```

Figura 3.8: Archivo de configuración "stubby.yml"para la extensión cadena de solicitudes en DNS

Las métricas de evaluación son el número de bytes en la respuesta, tiempos de respuesta y la cantidad de paquetes en el caso de la segmentación en el uso del protocolo TCP. Posterior a la configuración del servidor stub se realizan 5 pruebas para cada dominio consultado para los diferentes escenarios propuestos. Principalmente, se realizan esta cantidad de pruebas basado en la métrica de tiempos de respuesta para estabilizar los resultados de prueba de acuerdo a la varianza. Además la muestra utilizada de servidores recursivos fue reducida para las pruebas en las que se utiliza un servidor recursivo recurrente de Google y un servidor recursivo de NIC Chile.

Por otra lado las pruebas realizadas de los escenarios TCP y UDP se realizan de manera experimental, mientras que el escenario *DNS ChainQuery* se analiza de manera teórica ante la inexistencia de implementaciones que permitan hacer las pruebas sobre servidores reales.

3.2.1. Escenarios de prueba

El primer escenario es el uso de UDP como protocolo de transporte para la solicitud de un registro de recurso DNSSEC por una solicitud DNS hasta completar las cadena de

confianza DNSSEC. El segundo escenario es el uso de TCP como protocolo de transporte para la solicitud de un registro de recurso DNSSEC por una solicitud DNS hasta completar las cadena de confianza DNSSEC. El tercer escenario es el uso de TCP como protocolo de transporte solicitando todos los registros de recurso DNSSEC mediante una solicitud DNS que usa la función de la extensión *DNS ChainQuery* propuesta en la RFC 7901 [74].

3.2.1.1. Escenario User Datagram Protocol (UDP)

Actualmente la resolución DNS se realiza por defecto sobre el protocolo de transporte UDP. Las características de UDP incluyen ser un protocolo simple, no orientado a conexión y de cabecera sencilla, lo que permitiría obtener tiempos de respuesta más eficientes para realizar la validación DNSSEC. La cabecera UDP tiene 3 campos fijos contenidos en la respuesta DNS: la cabecera Ethernet definida en la RFC 894 [31] que contiene 14 bytes, la cabecera IP que contiene 20 bytes y el datagrama UDP que contiene 8 bytes, para un total de 42 bytes.

Las pruebas se basan en el siguiente comando para emular la solicitud DNS desde un cliente mediante el protocolo UDP consultando todos los registros DNSSEC. Dicha solicitud se reenvía a un servidor *up-streaming* que realiza la validación DNSSEC a los servidores autoritativos, como se observa en la Fig. **??**. Además este proceso se realiza sin las características de la extensión *DNS ChainQuery*:

```
dig @localhost +dnssec A example.com DNSKEY example.com
    DS example.com DNSKEY com. DS com. DNSKEY .
```

Hoy en día la validación DNSSEC se realiza en 8 pasos basados en que se encuentra almacenado en el servidor recursivo la llave pública de la zona raíz.

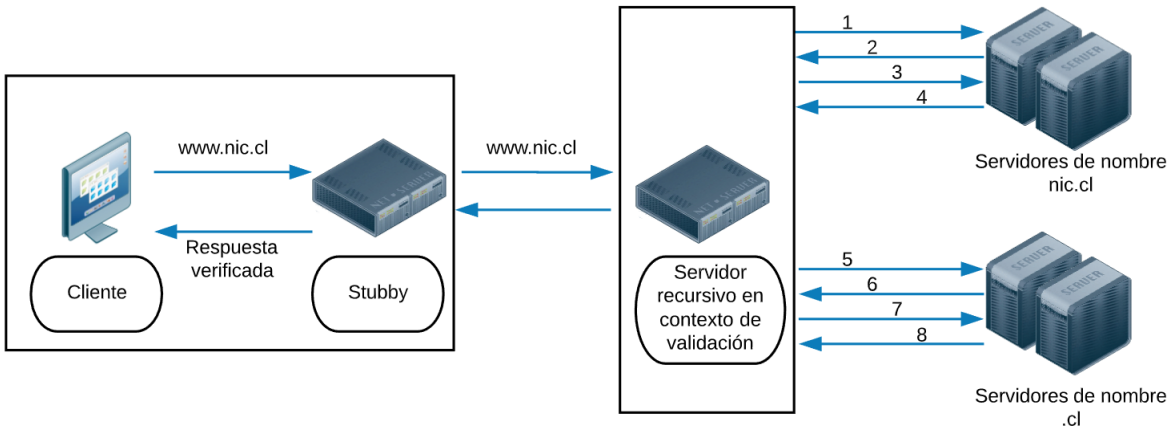

Figura 3.9: Proceso de validación DNSSEC con el punto de confianza (.cl)

1. El servidor recursivo consulta al servidor de nombre NIC.cl por el recurso tipo A *www.nic.cl*.
2. El servidor de nombre NIC.cl responde a la consulta del recurso tipo A con su respectiva firma *RRSIG*.
3. El servidor recursivo solicita al servidor de nombre NIC.cl por la llave *DNSKEY*.

4. El servidor de nombre NIC.cl responde a la consulta de la llave *DNSKEY* con la respectiva firma del recurso *RRSIG*.
5. El servidor recursivo consulta por el recurso *DS* de *nic.cl* al servidor de nombre .cl.
6. El servidor de nombre .cl responde a la consulta con el recurso *DS* y su respectiva firma *RRSIG*.
7. El servidor recursivo solicita la llave *DNSKEY* al servidor de nombre .cl.
8. El servidor de nombre .cl responde a la consulta con la llave *DNSKEY* y su respectiva firma *RRSIG*.

En la consulta se solicita el registro tipo A de un dominio firmado contenido en un servidor de nombres con cada recurso DNSSEC. Por eso es necesario determinar dominios que están firmados y los servidores que soportan DNSSEC.

3.2.1.2. Escenario Transmission Control Protocol (TCP)

El escenario TCP tiene 12 bytes adicionales del segmento TCP respecto a la cabecera UDP, para un total de 54 bytes. TCP tiene el proceso *three-way handshake*, el cual genera una comunicación fiable entre cliente y servidor. Sin embargo, dicha señalización genera una carga en la respuesta DNS, 66 bytes de sincronización, 66 bytes de sincronización + reconocimiento y 44 bytes de reconocimiento como respuesta. Además, TCP agrega 2 bytes al tamaño de la unidad de datos de protocolo PDU, lo que representa la longitud de la carga útil DNS. Los 2 bytes agregados permiten una completa compilación del mensaje DNS antes de ser analizado.

Las pruebas se basan en el siguiente comando para emular la solicitud DNS con todos los registros DNSSEC mediante el protocolo TCP, de un cliente al servidor *Stubby*. Dicha solicitud se reenvía a un servidor *streaming* que realiza la validación DNSSEC a los servidores autoritativos. Este proceso es realizado sin las características de la extensión *DNS ChainQuery*:

```
dig @localhost +tcp A example.com DNSKEY example.com DS example.com
                    DNSKEY com. DS com. DNSKEY
```

En la consulta se solicita el registro tipo A de un dominio firmado contenido en un servidor de nombres con cada recurso DNSSEC.

3.2.1.3. Escenario *DNS ChainQuery*

En el escenario *DNS ChainQuery* se realiza un análisis teórico basado en los 54 bytes de la cabecera TCP generados en la consulta y los 176 bytes del proceso *three-way handshake*. El análisis teórico se hace debido a la inexistencia de comandos para construir la cadena de confianza DNSSEC mediante *DNS ChainQuery* y el alcance a un servidor recursivo que reconozca la solicitud con el código OPT asignado para realizar la operación de validación completa. La principal diferencia con los escenarios previos radica en que la solicitud de todos

los registros de recurso DNSSEC se hace mediante una única solicitud DNS, como se observa en la Fig. 2.3.

3.2.2. Servicio de caché en DNS

En cada escenario, después de la primera consulta, el dominio consultado queda almacenado en la caché del servidor. Basado en esto se realizan las pruebas para comparar los RTT con la caché en frío y con almacenamiento en caché de los registros DNS consultados. Para analizar la validación DNSSEC con caché en frío, se desactiva la función de almacenamiento en caché o se borra cada vez que se consulta el dominio a comparar en los diferentes escenarios.

Para controlar el servicio de caché se instaló el demonio *Name Service Cache Daemon (NSCD)* [48]. El archivo de configuración *nscd.conf* ubicado en la carpeta etc permite habilitar o deshabilitar la caché mediante el comando **enable-cache**. Las líneas de comandos para borrar la memoria caché y dejarla en frío son:

```
\$ sudo /etc/init.d/nscd restart
\$ service nscd restart
\$ service nscd reload
```

El servicio de caché permite establecer el punto de anclaje del inicio de la cadena de confianza DNSSEC. El servicio de caché de los proveedores de software DNS establece el punto mínimo de acuerdo a la raíz, como la llave *root.key*, la cual almacena el "." del dominio en la zona consultada.

3.2.3. Métricas de análisis de rendimiento e implementación de cadena de solicitudes DNS

Las métricas de evaluación permiten cuantificar las mejoras de rendimiento mediante la implementación de la extensión de cadena de solicitudes en DNS. Las métricas de evaluación son: 1) la cantidad de bytes transmitidos adicionales a la carga útil del mensaje DNS, basados en la cabecera de cada escenario; 2) los tiempos de respuesta DNS en la recepción de toda la cadena de confianza DNSSEC en el cliente; y 3) y la cantidad de paquetes en la segmentación TCP. Además en las métricas planteadas se utiliza un índice que describe la cantidad de pasos de la validación DNSSEC, en el caso de las pruebas se realizan en 12 pasos emulando la solicitud de la zona raíz (.). Sin embargo, las métricas decriben el índice en 8 evaluando la mayoría de los sistemas operacionales actuales, como se puede observar en la Fig. 3.9.

3.2.3.1. Cantidad de bytes para la validación DNSSEC con *DNS ChainQuery*

La métrica *Bytes of Chain Query - BCQ* es propuesta como parte de esta tesis para representar la cantidad de bytes totales que se consumen para completar la validación DNSSEC

mediante la implementación de la extensión *DNS ChainQuery*. *BCQ* se define en la ecuación 3.1 y se calcula de acuerdo al total de bytes al final de la transacción DNS definido como *Tb* menos el total de bytes ahorrados con *DNS ChainQuery* definido como *Saved with ChainQuery - SCQ*. *Tb* se compone por los bytes de la consulta y respuesta DNS, más la cantidad fija de 54 bytes correspondiente a los bytes de la cabecera. *SCQ* se calcula en la ecuación 3.2. Por último, *i* representa el número de pasos para completar la cadena de confianza como se observa en la Fig. 3.9, iniciando por el registro DNSKEY de la raíz almacenada en el servidor del cliente.

$$BCQ = \sum_{\mathrm{i}=1}^{8} Tb(\mathrm{i}) - SCQ(\mathrm{i}) \tag{3.1}$$

SCQ se compone por *Qb* que representa los bytes de cada consulta. Finalmente, no se considera la primera consulta *Qb(i=1)* debido a que es necesaria como base para iniciar la cadena de confianza de solicitudes DNS, independiente de si se está usando o no *DNS ChainQuery*.

$$SCQ = \left[\sum_{\mathrm{i}=1}^{8} Qb(\mathrm{i})\right] - Qb(\mathrm{i}=1) \tag{3.2}$$

3.2.3.2. Tiempos de respuesta para validar DNSSEC con *DNS ChainQuery*

La métrica Response Times of Chain Query - RTCQ propuesta en esta tesis, evalúa los tiempos de respuesta consumidos en la validación de los registros DNSSEC con la implementación de *DNS ChainQuery*. Además, un proceso estocástico modela los resultados de acuerdo a las condiciones de red en cada prueba, por ejemplo latencia global de red o tráfico de red durante la prueba, por este motivo se realizan múltiples pruebas. Finalmente se extraen los datos con menor varianza de 5 pruebas. La ecuación del modelo de pruebas se resume en 3.3 *RTCQ* se calcula en la ecuación 3.3 y se compone por el total de los tiempos de respuesta *TRT* al final de la transacción DNS, menos el total de los tiempos de respuesta ahorrados con *DNS ChainQuery* definidos como *TSCQ*.

$$RTCQ = \sum_{\mathrm{i}=1}^{8} TRT(\mathrm{i}) - TSCQ(\mathrm{i}) \tag{3.3}$$

Por otro lado *TSCQ* se define en la ecuación 3.4. La ecuación define los tiempos de respuesta de cada transacción DNS, es decir cada paso descrito en la Fig. 3.9. Los cálculos de tiempo de respuesta se realizan mediante la marca de tiempo en la respuesta de la transacción inicial *TrAns* y la marca de tiempo en la consulta de la siguiente transacción *TrQry*. Finalmente, en los tiempos de repuesta ahorrados no se considera el tiempo de respuesta de la primera consulta debido a que es necesaria como base para iniciar la cadena de confianza de solicitudes DNS.

$$TSCQ = \sum_{\mathrm{i}=1}^{8} TrAns(\mathrm{i}) - TrQry(\mathrm{i} > 1) \tag{3.4}$$

3.2.3.3. Cantidad de paquetes para validar DNSSEC con *DNS ChainQuery*

La métrica *Packets of Chain Query - PCQ* permite analizar la cantidad de paquetes transmitidos en el proceso completo para la validación DNSSEC y se determina por la ecuación 3.5. La evaluación consiste en la segmentación de paquetes TCP de acuerdo al número de bytes obtenidos en la ecuación 3.1 y el tamaño del segmento máximo MSS de la sesión TCP que equivalen a 1460 bytes, sin incluir los bytes de la cabeceras.

$$PCQ = BCQ/MSS \tag{3.5}$$

Adicionalmente se considera el paquete de la primera consulta, el paquete final para cerrar la sesión TCP y la carga útil en la respuesta dentro del termino .

Capítulo 4

Resultados

Los comandos ejecutados en este trabajo difieren a los mostrados en el Internet-Draft "A Common Operational Problem in DNS Servers - Failure To Communicate" en la opción de configuración *+norec*. Esta opción elimina la recursividad para completar el proceso de resolución DNS, lo que en la gran mayoría de pruebas se obtiene como código de respuesta *REFUSED*. Una de las causas asociadas a un código de respuesta *REFUSED* es el mensaje "*WARNING: Message has 23 extra bytes at end*", el cual es observado en todas las pruebas realizadas. No obstante, existen otras causas como el bloqueo de paquetes por parte de dispositivos físicos en la red, lo cual es difícil de identificar en las pruebas.

4.1. Resultados de la fase A del algoritmo de clasificación EDNS

La primera prueba de la fase A consiste en determinar la versión del software DNS de los 19061 servidores. En la Tabla 4.1 se muestran los resultados de las pruebas, en la columna 2 se observan los resultados previos al DNS Flag day y en la columna 3 los resultados posteriores al DNS Flag day. Las versiones basadas en el nombre propietario o de la compañía hace referencia a las compañías que están a cargo de los servidores como los registradores DNS o municipalidades en Chile. En la clasificación *Sin respuesta* hace referencia a resultados nulos en la sección de respuesta o resultados con valores *WARNING: EDNS query returned status NOTIMP - retry with '+noedns'*, *WARNING: Message has 23 extra bytes at end* o cuyas *Cookies* aparecen en esta sección sin una versión del software DNS.

Previamente al DNS Flag day aproximadamente 60 % (11436 servidores) revelan la versión de software DNS, mientras que el 40 % (7625 servidores) restante equivale a respuestas con tiempo de espera agotado o no existe respuesta por parte del servidor. Basado en el 60 % del total de servidores, aproximadamente el 83 % (9482 servidores) utilizan el software BIND 9 [41]. Teóricamente, de acuerdo a las características EDNS soportadas según la versión Bind 9 presentadas en la Tabla 3.1, un 100 % del total de los servidores soportan EDNS versión 0, las opciones y negociación EDNS. Sin embargo, cumpliendo los estándares solo un 93 %

Proveedor/Versión software DNS	**Servidores antes del DNS Flag Day 2019**	**Servidores después del DNS Flag Day 2019**
Bind 9.2.	77	12
Bind 9.3.	504	262
Bind 9.4.	22	10
Bind 9.5.	18	11
Bind 9.6.	16	30
Bind 9.7.	165	129
Bind 9.8.	4565	2318
Bind 9.9.	3838	4223
Bind 9.10.	256	1375
Bind 9.11.	24	2197
Bind 9.12.	2	5
Bind 9.13.	1	3
dnsmasq	155	189
connection timed out no servers could be reached	1570	1281
Configuración administrador	“get lost”: 113 “none”: 270 “DNS”: 55 “BIND”: 69 “la que estoy utilizando”: 24 “unknown”: 78 “surely you must be joking”: 7 Otros: 84	“get lost”: 113 “none”: 270 “DNS”: 55 “BIND”: 69 “la que estoy utilizando”: 24 “unknown”: 78 “surely you must be joking”:7 Otros: 91
Nombre propietario/compañía	267	358
i-MSCP DNS Server	8	8
SOA hostmaster	139	139
Microsoft DNS	397	405
Name Server Daemon (NSD)	57	57
PowerDNS recursor 3.7.4	225	690
Sin respuesta	6055	4652

Tabla 4.1: Resultados de la versión del software DNS de los servidores, antes y después del DNS Flag day 2019

(8867 servidores) soportan las características DNSSEC y finalmente las extensiones EDNS como Client Subnet, Padding, entre otras, son soportadas por un 4 % (283 servidores).

Posterior al DNS Flag day, la cantidad de servidores con tiempo de espera agotado y sin respuesta disminuye a un 31 % (5933 servidores). De acuerdo al 69 % (13128 servidores) que revela la configuración por defecto o modificada de la versión del software DNS, un 80 % (10575 servidores) están configurados con Bind 9. Como análisis de los avances colectivos que se obtienen durante este tipo de jornada DNS a nivel global, del 80 % teóricamente un 100 % soporta EDNS y sus características básicas, un 97 % (10280 servidores) soporta las características DNSSEC y aproximadamente un 34 % (3580 servidores) soporta las extensiones

EDNS mencionadas previamente.

En resumen se puede observar la actualización de las versiones del software DNS en la Fig. 4.1, con un 30 % del total de servidores en una versión Bind 9.9 o superior, lo cual indica un soporte de los servidores a consultas con extensiones EDNS incluyendo la extensión *DNS ChainQuery*.

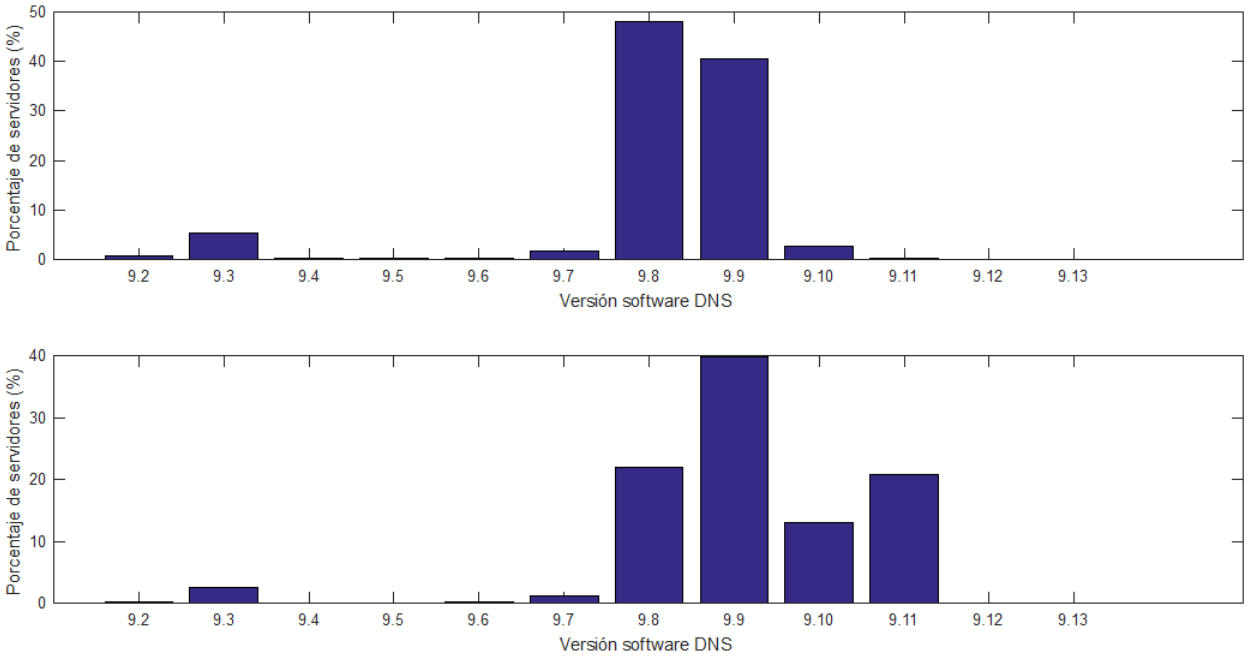

Figura 4.1: Clasificación del estado de los servidores, antes (superior) y después (inferior) del DNS Flag day 2019

Posteriormente se presentan los resultados del estado de los servidores para la prueba EDNS antes y después del DNS Flag day. Los resultados representan la clasificación *ALL OK* de acuerdo al cumplimiento total de la respuesta esperada, *WARNINGS* cuando el resultado es parcial y *NO EDNS* con el incumplimiento basado en un código de respuesta erróneo o no soporte de EDNS. en la Fig. 4.2 se observan los porcentajes de los resultados posteriores al DNS Flag day representado por el círculo externo y los resultados previos al DNS Flag day representados por el círculo interno.

En esta prueba no existen restricciones de las banderas en la respuesta, por lo que se considera esencial el código de respuesta. Previamente al DNS Flag day se obtiene respuesta del 81 % (15439 servidores) del total de servidores y basado en ese porcentaje de servidores que responde, aproximadamente un 67 % (10344 servidores) tienen compatibilidad con EDNS y se clasifica en *ALL OK*, un 27.5 % (4246 servidores) se clasifica en *WARNINGS* con códigos de respuesta *REFUSED* y *NOTIMP* con el registro EDNS (0) en la sección PSEUDOSECTION y el 5.5 % restante se clasifica *NO EDNS* como servidores no compatibles con EDNS.

Se observa que posterior al DNS Flag day se aumenta la cantidad de servidores con un resultado *ALL OK* a un 75 % (13008 servidores) de los 17345 servidores. Esto confirma que las actualizaciones de software así como configuraciones bajo los estándares ayudan a mejorar la resolución DNS. Lo anterior se debe a que no hay desvío o generación de una nueva consulta,

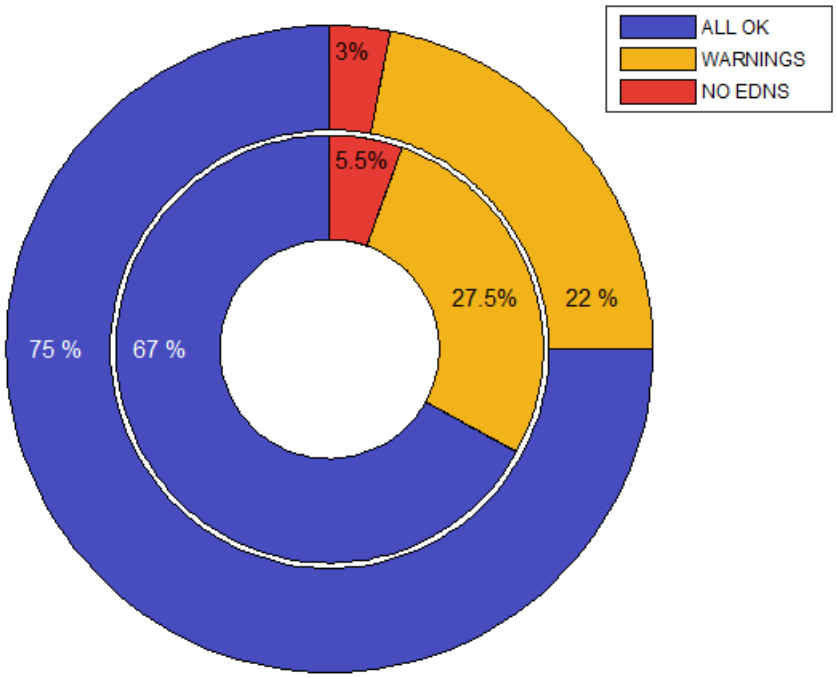

Figura 4.2: Clasificación del estado EDNS de los servidores, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

disminuyendo tiempos de respuesta. Una de las mejoras observadas como resultado del DNS Flag day fue la configuración de reglas en los dispositivos físicos para evitar descartar paquetes EDNS. Esto se ve reflejado mediante la disminución del código de respuesta NOTIMP y el mensaje en la sección de respuesta *WARNING: EDNS query returned status NOTIMP - retry with '+noedns'* en el 1.7 % (293 servidores) a aproximadamente 0.9 % (147 servidores).

Finalmente los resultados de clasificación de la prueba EDNS versión 1 se observan en la Fig. 4.3. Los porcentajes de los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, se observa que un 63 % (12008 servidores) responde a la prueba y 37 % (7053 servidores) son respuestas con tiempo de espera agotado y código de respuesta *REFUSED*. Basado en el 63 % de los servidores que responde a la solicitud EDNS versión 1, aproximadamente un 54 % (6483 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 13 % (1561 servidores) se clasifica en *WARNINGS* debido a la presencia de la bandera AA y registro SOA, y un 33 % (3964 servidores) se clasifica en *NO EDNS1* basado en códigos de respuesta erróneos, con un 19 % (2281 servidores) *NOERROR* y 14 % (1683 servidores) *NOTIMP*.

Posterior al DNS Flag day, se observa que un 78.99 % (15058 servidores) responde a la prueba y el 21.01 % restante entrega respuestas con tiempo de espera agotado y código de respuesta REFUSED. Basado en el 79 % de los servidores que responde a la solicitud EDNS versión 1, un 71 % (10691 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento

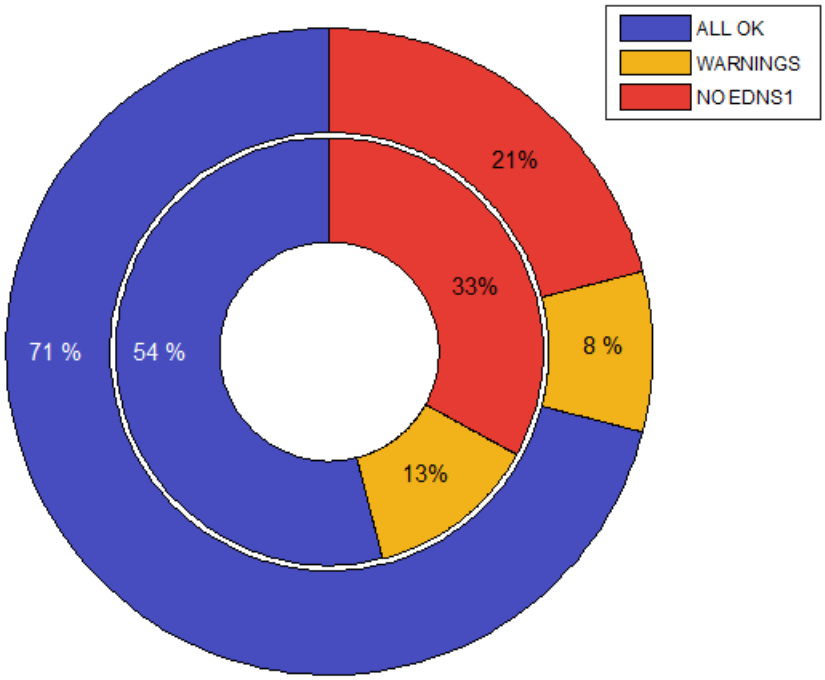

Figura 4.3: Clasificación del estado de los servidores para la prueba EDNS1, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

de la respuesta esperada en la prueba, un 8 % (1204 servidores) se clasifica en *WARNINGS* debido a la presencia de la bandera AA y un 21 % (3163 servidores) se clasifica en *NO EDNS1* basado en códigos de respuesta erróneos, con un 13 % (1957 servidores) *NOERROR* y un 8 % (1206 servidores) *NOTIMP*.

4.2. Resultados de la fase B del algoritmo de clasificación EDNS

Los resultados de la primera prueba de la fase B corresponde a la verificación del estado de los servidores para la evaluación de las opciones EDNS antes y después del DNS Flag day. en la Fig. 4.4 se observan los resultados posteriores al DNS Flag day representado por el círculo externo y los resultados previos al DNS Flag day representados por el círculo interno.

Antes del DNS Flag day un 61 % (11627 servidores) responde a la prueba y 39 % (7434 servidores) son respuestas con tiempo de espera agotado. Basado en el 61 % de los servidores que responde a la solicitud EDNS opción 100, un 57 % (6628 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 4 % (465 servidores) se clasifica en *WARNINGS* debido a la presencia de la opción OPT=15 (incluso con un código de error *NOERROR*) y un 39 % (4534 servidores) se clasifica en *NO EDNS OPT*, basado en códigos de respuesta erróneos con un 33.5 % (3894 servidores) *REFUSED*, un 3 % (349 servidores) *FORMERR*, un 1.5 % (175 servidores) *NOTIMP* y un 1 % (116 servidores) *SERVFAIL*.

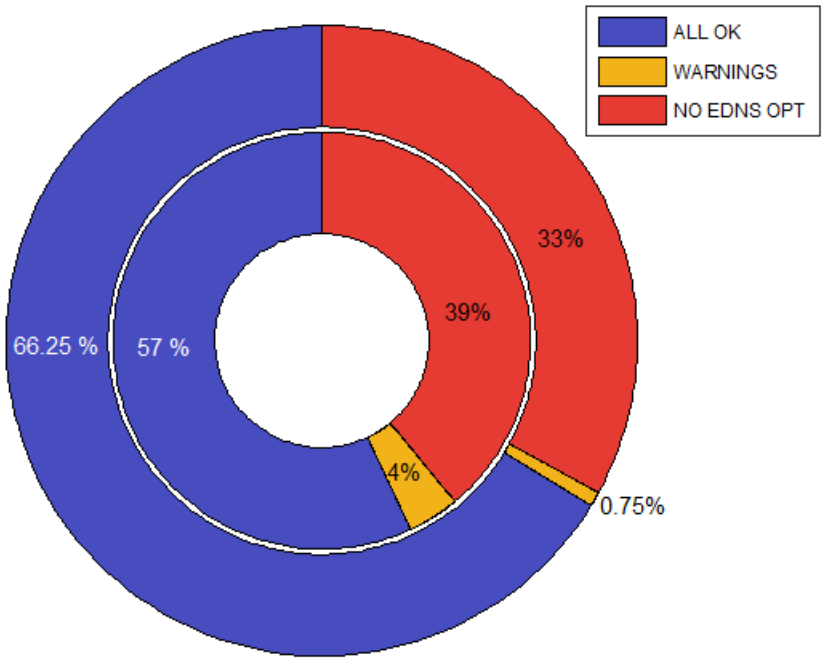

Figura 4.4: Clasificación del estado de los servidores para la prueba EDNS OPT, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

Posterior al DNS Flag day se observa un 75.02 % (14300 servidores) responde a la prueba y el 24.98 % restante son respuestas con tiempo de espera agotado. Basado en el 75 % de los servidores que responde a la solicitud EDNS opción 100, un 66.25 % (9474 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 0.75 % (107 servidores) se clasifica en *WARNINGS* debido a la presencia de la opción OPT=15 en la sección PSEUDOSECTION y un 33 % (4719 servidores) se clasifica en *NO EDNS OPT*, basado en códigos de respuesta erróneos con un 30 % (4290 servidores) *REFUSED*, un 2.2 % (314 servidores) *FORMERR*, un 0.3 % (43 servidores) *NOTIMP* y un 0.5 % (72 servidores) *SERVFAIL*.

En total, después del DNS Flag day, 2790 servidores más cumplen con los requerimientos EDNS para esta prueba, siendo esencial para realizar las pruebas con los códigos correspondientes de cada extensión EDNS. Basado en la clasificación de los servidores, se determina que un máximo de 9474 servidores de la muestra pueden responder correctamente a las pruebas de la fase C del algoritmo.

Los resultados de la prueba del estado de los servidores para la evaluación de la negociación EDNS, antes y después del DNS Flag day se muestran en la Fig. 4.5. Los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, se observa que un 57.99 % (11054 servidores) responde a la prueba y un 42.01 % (8007 servidores) generan respuestas con tiempo de espera agotado y código de respuesta *REFUSED*. Basado en el 58 % de los servidores que responde, aproximadamente un 35 % (3869 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la

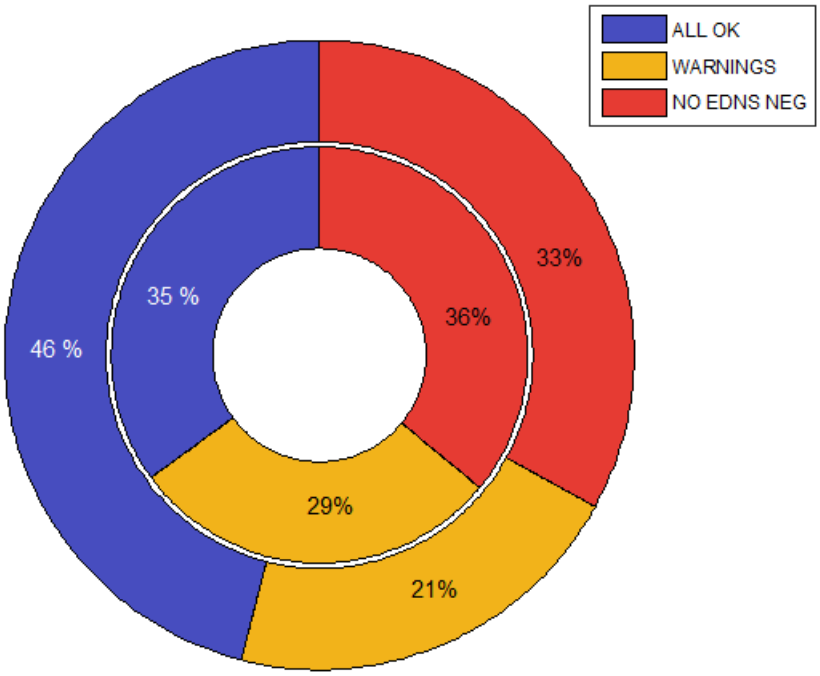

Figura 4.5: Clasificación del estado de los servidores para la prueba de negociación EDNS, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

respuesta esperada en la prueba, un 29 % (3205 servidores) se clasifica en *WARNINGS* debido a la presencia de banderas EDNS y registro SOA, y un 36 % (3980 servidores) se clasifica en *NO EDNS NEG*, basado en códigos de respuesta erróneos con un 25 % (2764 servidores) *NOERROR*, un 1 % (111 servidores) *FORMERR* y 10 % (1105 servidores) *NOTIMP*.

Posterior al DNS Flag day, un 59.99 % (11436 servidores) responde a la prueba y un 40.01 % genera respuestas con tiempo de espera agotado y código de respuesta REFUSED. Basado en el 60 % de los servidores que responde a la solicitud, un 46 % (5260 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 21 % (2401 servidores) se clasifica en *WARNINGS* debido a la presencia de banderas EDNS y un 33 % (3775 servidores) se clasifica en *NO EDNS NEG*, basado en códigos de respuesta erróneos con un 28 % (3202 servidores) *NOERROR*, un 0,75 % (86 servidores) *FORMERR* y un 4,25 % (487 servidores) *NOTIMP*.

Los resultados de la prueba del estado de los servidores para la evaluación de banderas desconocidas EDNS antes y después del DNS Flag day se pueden observar en la Fig. 4.6. Los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, un 62 % (11818 servidores) responde a la prueba y un 38 % (7243 servidores) genera respuestas con tiempo de espera agotado. Basado en el 62 % de los servidores que responde, un 32 % (3782 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 4.5 % (532 servidores) se clasifica en *WARNINGS* debido a la presencia de la bandera MBZ aún con un código de respuesta *NOERROR*, y un 63.5 % (7504 servidores) se clasifica en *NO UNKNOWN FLAGS*

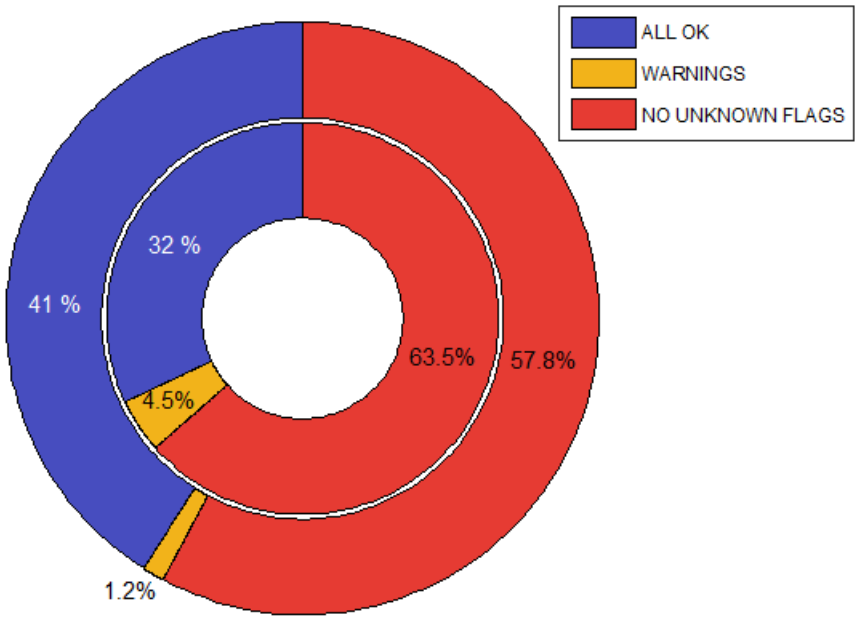

Figura 4.6: Clasificación del estado de los servidores para la prueba de banderas desconocidas EDNS, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

basado en códigos de respuesta erróneos con un 56.7 % (6701 servidores) *REFUSED*, un 3,6 % (426 servidores) *SERVFAIL*, un 0,9 % (107 servidores) *NXDOMAIN*, un 2 % (233 servidores) *FORMERR* y un 0,3 % (37 servidores) *NOTIMP*. Anexo a los códigos de respuesta erróneos, existe un 4.5 % (532 servidores) en el que aparece la bandera MBZ.

Posterior al DNS Flag day, un 64 % (12200 servidores) responde a la prueba y un 36 % (6861 servidores) genera respuestas con tiempo de espera agotado. Basado en el 64 % de los servidores que responde a la solicitud, un 41 % (5002 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 1.2 % (146 servidores) se clasifica en *WARNINGS* debido a la presencia de la bandera MBZ aún con un código de respuesta *NOERROR*, y un 57.8 % (7052 servidores) se clasifica en *NO UNKNOWN FLAGS*, basado en códigos de respuesta erróneos con un 49 % (5978 servidores) *REFUSED*, un 4,2 % (512 servidores) *SERVFAIL*, un 2,6 % (317 servidores) *NXDOMAIN*, un 1.7 % (207 servidores) *FORMERR* y un 0.3 % (38 servidores) *NOTIMP*. Anexo a los códigos de respuesta erróneos, existe un 3.9 % (476 servidores) en el que aparece la bandera MBZ.

La última prueba de la fase B es la extensión de seguridad DNSSEC. La clasificación del estado de los servidores se observa en la Fig. 4.7, donde los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, un 67 % (12770 servidores) responde a la prueba y un 33 % (6291 servidores) genera respuestas con tiempo de espera agotado. Basado en el 67 % de los servidores que responde, un 26 % (3320 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, aproximadamente 68 % (8682 servidores) se clasifica en *WARNINGS* debido al código de respuesta REFUSED con la bandera DO y

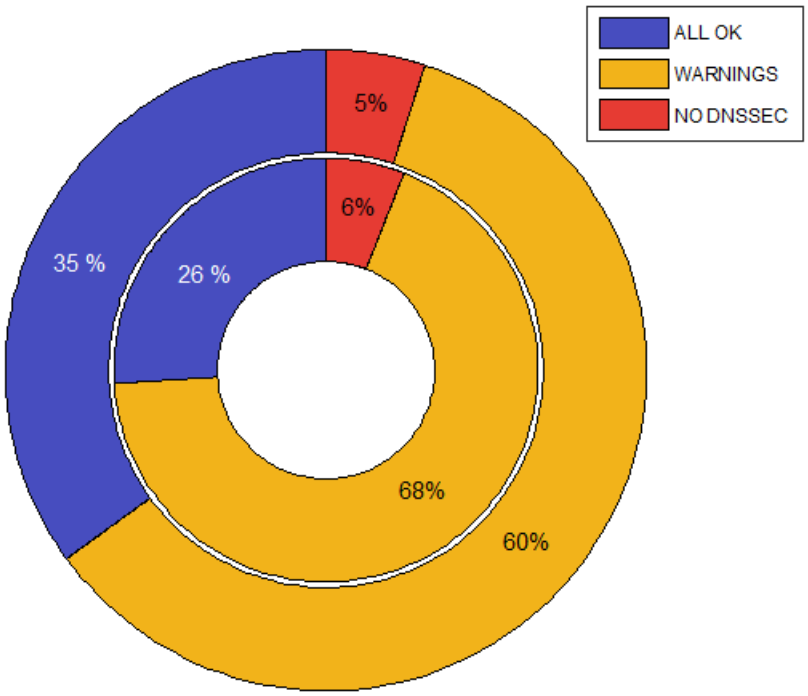

Figura 4.7: Clasificación del estado de los servidores para la prueba DNSSEC, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

AD, y un 6 % (768 servidores) se clasifica en *NO DNSSEC*, basado en códigos de respuesta erróneos con un 0.3 % (38 servidores) *NOTIMP*, un 3.6 % (460 servidores) *SERVFAIL*, 0.9 % (115 servidores) *FORMERR* y 1.2 % (155 servidores) *NXDOMAIN*.

Posterior al DNS Flag day, un 73 % (13915 servidores) responde a la prueba y el 27 % restante genera respuestas con tiempo de espera agotado. Basado en el 73 % de los servidores que responde a la solicitud, un 35 % (4869 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 60 % (8349 servidores) se clasifica en *WARNINGS* debido al código de respuesta REFUSED con la bandera DO y AD, y un 5 % (697 servidores) se clasifica en *NO DNSSEC* basado en códigos de respuesta erróneos con un 0.2 % (28 servidores) *NOTIMP*, un 3.2 % (446 servidores) *SERVFAIL*, un 0.6 % (84 servidores) *FORMERR* y un 1 % (139 servidores) *NXDOMAIN*.

4.3. Resultados de la fase C del algoritmo de clasificación EDNS

Los resultados de clasificación del soporte de la extensión EDNS TCP Keepalive se observan en la Fig. 4.8, donde los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

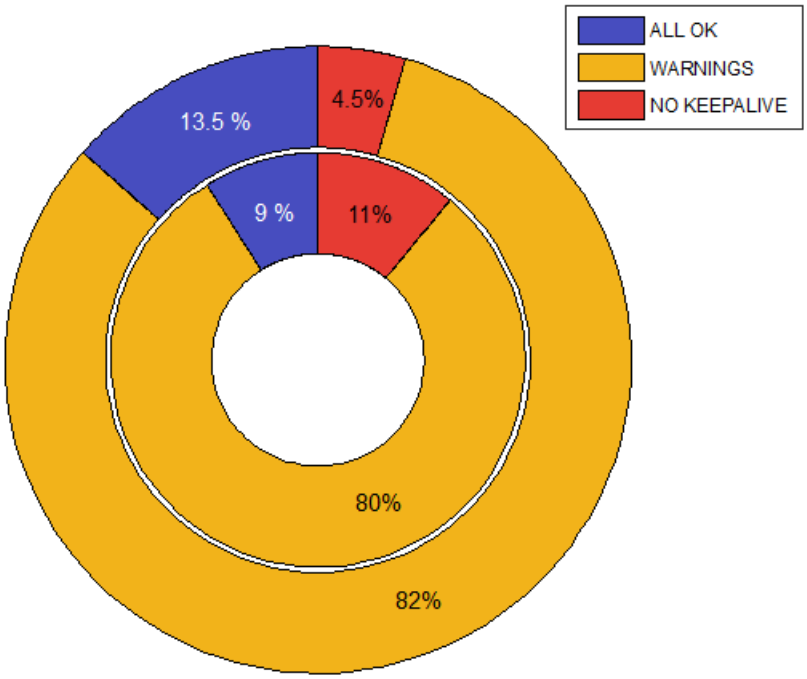

Figura 4.8: Clasificación del estado de los servidores para la prueba TCP Keepalive, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

Antes del DNS Flag day, un 52 % (9911 servidores) responde a la prueba y 48 % (9150 servidores) genera respuestas con tiempo de espera agotado. Basado en el 52 % de los servidores que responde, un 9 % (892 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 80 % (7928 servidores) se clasifica en *WARNINGS* debido al código de respuesta REFUSED aún con el código OPT en la sección adicional, y un 11 % (1091 servidores) se clasifica en *NO Keepalive*, basado en códigos de respuesta erróneos con un 6.6 % (654 servidores) *SERVFAIL*, un 2.3 % (228 servidores) *FORMERR*, un 1.2 % (119 servidores) *NOTIMP* y un 0.9 % (90 servidores) *NXDOMAIN*.

Posterior al DNS Flag day, un 58 % (11056 servidores) responde a la prueba y 42 % (8005 servidores) genera respuestas con tiempo de espera agotado. Basado en el 58 % de los servidores que responde, un 13.5 % (1492 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 82 % (9065 servidores) se clasifica en *WARNINGS* debido al código de respuesta REFUSED aún con el código OPT en la sección adicional, y un 4.5 % (499 servidores) se clasifica en *NO Keepalive*, basado en códigos de respuesta erróneos con un 2.8 % (310 servidores) *SERVFAIL*, un 1.3 % (144 servidores) *NXDOMAIN* y un 0.4 % (45 servidores) *FORMERR*.

La segunda extensión en prueba es *DNS ChainQuery*, la cual es parte esencial de este trabajo y los resultados de clasificación se observan en la Fig. 4.9, donde los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, un 73 % (13533 servidores) responde a la prueba y 27 % (5528 servidores) genera respuestas con tiempo de espera agotado. Basado en el 73 % de los servi-

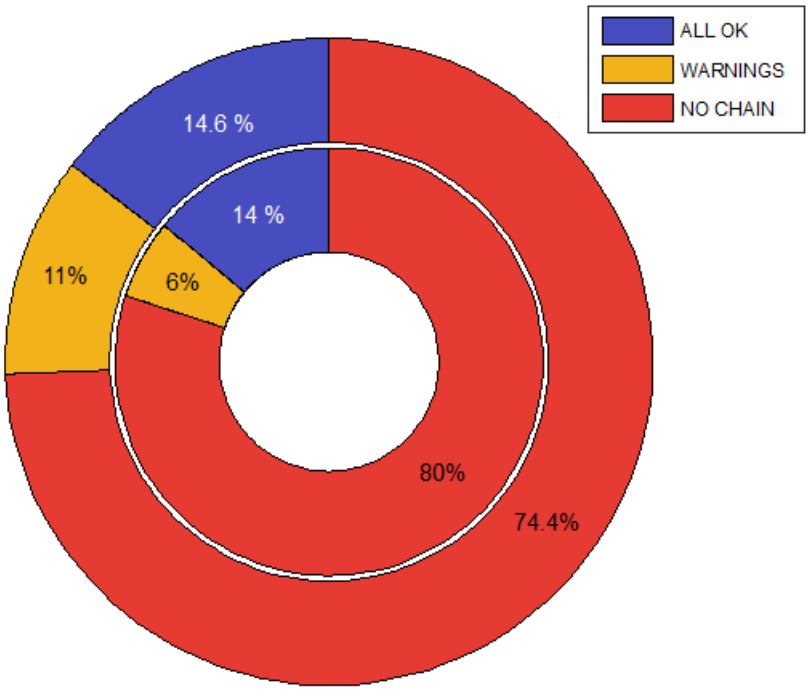

Figura 4.9: Clasificación del estado de los servidores para la prueba *DNS ChainQuery*, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

dores que responde, aproximadamente un 14 % (1895 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 6 % (812 servidores) se clasifica en *WARNINGS* debido al código OPT 13 en la sección adicional con un código de respuesta diferente a *NOERROR* y *FORMERR*, y un 80 % (10826 servidores) se clasifica en *NO CHAIN*, basado en códigos de respuesta erróneos con un 74 % (10014 servidores) *REFUSED*, un 2.4 % (325 servidores) *SERVFAIL*, un 1.9 % (257 servidores) *NXDOMAIN* y un 1.7 % (230 servidores) *NOTIMP*.

Posterior al DNS Flag day, un 74 % (14105 servidores) responde a la prueba y 26 % (4956 servidores) genera respuestas con tiempo de espera agotado. Basado en el 74 % de los servidores que responde, un 14.6 % (2059 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 11 % (1552 servidores) se clasifica en *WARNINGS* debido al código OPT 13 en la sección adicional con código de respuesta diferente a *NOERROR* y *FORMERR*, y un 74.4 % (10494 servidores) se clasifica en *NO CHAIN*, basado en códigos de respuesta erróneos con un 69 % (9732 servidores) *REFUSED*, un 3.1 % (437 servidores) *SERVFAIL*, un 1.4 % (198 servidores) *NXDOMAIN* y un 0.9 % (127 servidores) *NOTIMP*.

Los siguientes resultados son de la clasificación del estado de los servidores para la prueba EDNS subred de cliente y se observan en la Fig. 4.10. Los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, un 72.5 % (13819 servidores) responde a la prueba y un 27.5 % (5242 servidores) genera respuestas con tiempo de espera agotado. Basado en el 72.5 % de los

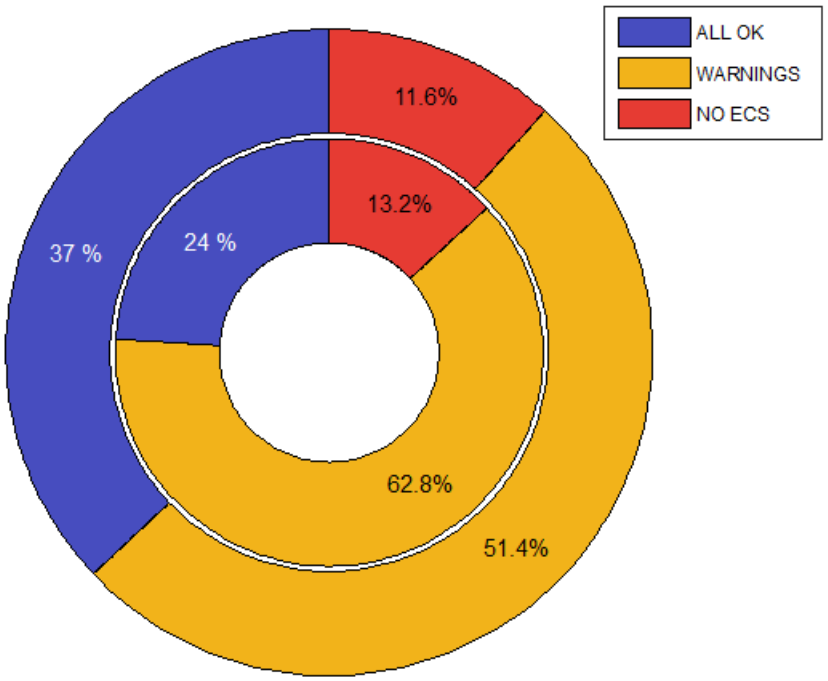

Figura 4.10: Clasificación del estado de los servidores para la prueba EDNS subred de cliente, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

servidores que responde, un 24 % (3317 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 62.8 % (8678 servidores) se clasifica en *WARNINGS* debido al código OPT 8 en la sección adicional con código de respuesta diferente a *NOERROR* y *FORMERR*, y un 13.2 % (1824 servidores) se clasifica en *NO ECS*, basado en códigos de respuesta erróneos con un 8 % (1105 servidores) *REFUSED*, un 3.1 % (428 servidores) *SERVFAIL*, un 1.7 % (235 servidores) *NOTIMP* y un 0.4 % (56 servidores) *NOXDOMAIN*.

Posterior al DNS Flag day, un 76 % (14482 servidores) responde a la prueba y un 24 % (4579 servidores) genera respuestas con tiempo de espera agotado. Basado en el 76 % de los servidores que responde, un 37 % (5358 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 51.4 % (7445 servidores) se clasifica en *WARNINGS* debido al código OPT 8 en la sección adicional con código de respuesta diferente a *NOERROR* y *FORMERR*, y un 11.6 % (1679 servidores) se clasifica en *NO ECS*, basado en códigos de respuesta erróneos con un 9.8 % (1421 servidores) *REFUSED*, un 1.2 % (174 servidores) *NOTIMP* y un 0.6 % (84 servidores) *SERVFAIL*.

La cuarta extensión en prueba es Cookies en DNS y los resultados de clasificación se observan en la Fig. 4.11, donde los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, un 64.7 % (12332 servidores) responde a la prueba y un 35.3 % (6729 servidores) genera respuestas con tiempo de espera agotado. Basado en el 64.7 % de los servidores que responde, un 23.9 % (2947 servidores) se clasifica en *ALL OK* de acuerdo

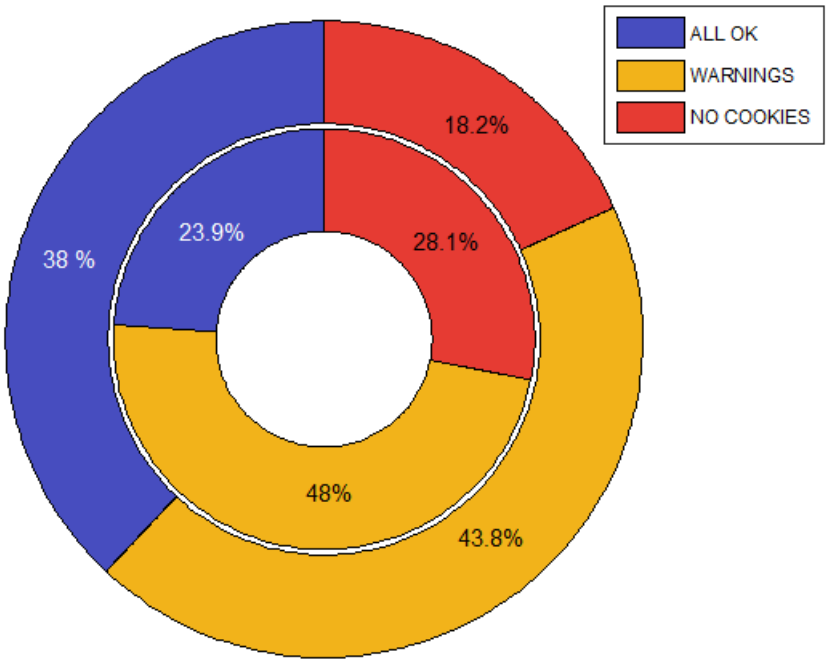

Figura 4.11: Clasificación del estado de los servidores para la prueba Cookies en DNS, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

con el cumplimiento de la respuesta esperada en la prueba, un 48 % (5920 servidores) se clasifica en *WARNINGS* debido a la presencia del código OPT 10 en la sección adicional, pero con un código de respuesta diferente a *NOERROR* y *FORMERR*. Un 28.1 % (3465 servidores) se clasifica en *NO Cookies*, basado en códigos de respuesta erróneos con un 22.1 % (2726 servidores) *REFUSED*, un 3.6 % (445 servidores) *SERVFAIL*, un 1.6 % (197 servidores) *NXDOMAIN* y un 0.8 % (97 servidores) *NOTIMP*.

Posterior al DNS Flag day, un 74 % (14112 servidores) responde a la prueba y un 26 % (4949 servidores) genera respuestas con tiempo de espera agotado. Basado en el 74 % de los servidores que responde, aproximadamente un 38 % (5360 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 43.8 % (6180 servidores) se clasifica en *WARNINGS* debido a la presencia del código OPT 10 en la sección adicional, pero con un código de respuesta diferente a *NOERROR* y *FORMERR*. Un 18.2 % (2572 servidores) se clasifica en *NO Cookies*, basado en códigos de respuesta erróneos con un 14.7 % (2075 servidores) *REFUSED*, un 2.4 % (339 servidores) *SERVFAIL*, un 0.9 % (127 servidores) *NXDOMAIN* y un 0.2 % (31 servidores) *NOTIMP*.

Finalmente se presenta los resultados de la clasificación del estado de los servidores para la prueba EDNS EXPIRE Option que se pueden observar en la Fig. 4.12. Los resultados posteriores al DNS Flag day son representados por el círculo externo y los resultados previos al DNS Flag day son representados por el círculo interno.

Antes del DNS Flag day, un 61 % (11627 servidores) responde a la prueba y un 39 % (7434 servidores) genera respuestas con tiempo de espera agotado. Basado en el 61 % de los servidores que responde, aproximadamente un 17 % (1980 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 8.7 % (1012

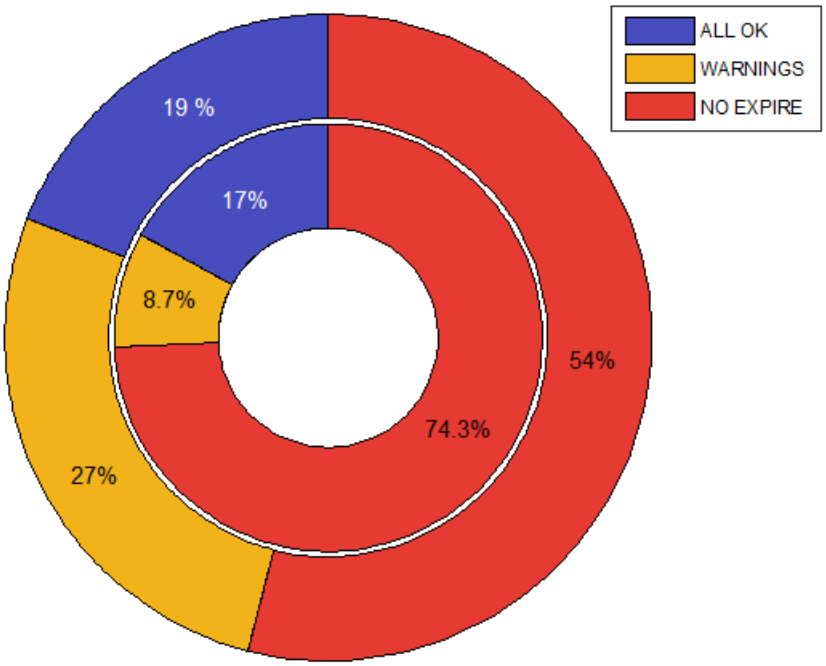

Figura 4.12: Clasificación del estado de los servidores para la prueba EDNS EXPIRE Option, antes (círculo interno) y después (círculo externo) del DNS Flag day 2019

servidores) se clasifica en *WARNINGS* debido al código OPT 9 en la sección adicional con código de respuesta diferente a *NOERROR*, y un 74.3 % (8635 servidores) se clasifica en *NO EXPIRE*, basado en códigos de respuesta erróneos con un 67 % (7791 servidores) *REFUSED*, un 3.1 % (359 servidores) *FORMERR*, un 1.7 % (197 servidores) *NXDOMAIN*, un 1.4 % (163 servidores) *SERVFAIL* y un 1.1 % (125 servidores) *NOTIMP*.

Posterior al DNS Flag day, un 66 % (12583 servidores) responde a la prueba y un 34 % (6478 servidores) genera respuestas con tiempo de espera agotado. Basado en el 66 % de los servidores que responde, aproximadamente un 19 % (2392 servidores) se clasifica en *ALL OK* de acuerdo con el cumplimiento de la respuesta esperada en la prueba, un 27 % (3398 servidores) se clasifica en *WARNINGS* debido a la presencia del código OPT 9 en la sección adicional con código de respuesta diferente a *NOERROR*, y un 54 % (6793 servidores) se clasifica en *NO EXPIRE*, basado en códigos de respuesta erróneos con un 49 % (6165 servidores) *REFUSED*, un 2.6 % (327 servidores) *FORMERR*, un 1.3 % (164 servidores) *NXDOMAIN*, un 0.7 % (88 servidores) *SERVFAIL* y un 0.4 % (49 servidores) *NOTIMP*.

Basado en los rCODE o versión se puede hacer predicción de tiempos de respuesta, ver si mejoran respecto una configuración correcta es decir que los que responde REFUSED o server no reached, esos puedan responder de forma rápida a esas consultas. Mejorar RTT aunque no lo soporten, debido a que no tienen que reintentar para lograr una respuesta de ese servidor.

4.4. Análisis de resultados del impacto de la *DNS Chain-Query* para validación DNSSEC en clientes

Para abordar las ventajas del uso de la extensión se analiza desde dos extremos de la red, el lado del cliente y el lado del servidor.

4.4.1. Análisis del lado del cliente (Servidor Stub para validación DNSSEC)

Para el análisis se realiza una comparación entre los protocolos de transporte UDP, TCP y *DNS ChainQuery* para realizar la validación DNSSEC al dominio ***nic.cl***. El dominio ***nic.cl*** contiene todos los registros de recursos DNSSEC como se puede verificar a través del siguiente link. La primera métrica de análisis son los bytes totales (bytes transmitidos y recibidos por el cliente) por la consulta de cada recurso DNSSEC como se observa en la Fig. 4.13.

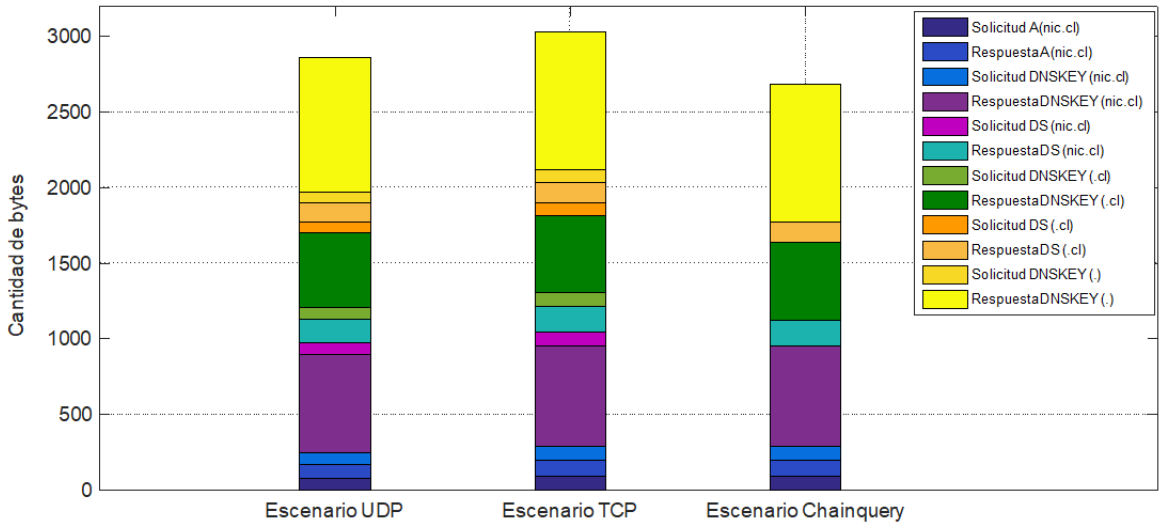

Figura 4.13: Cantidad de bytes transmitidos en la validación de la cadena de confianza DNSSEC en los escenarios de prueba UDP, TCP y *DNS ChainQuery*

Los resultados muestran que el protocolo TCP utiliza un 5.5 % más de bytes que el escenario UDP para completar la cadena de validación en el cliente, basado en el proceso *three-way handshake*. Por otro lado aunque el protocolo de transporte TCP sea utilizado en el escenario *DNS ChainQuery*, la cantidad de bytes para validar la cadena de confianza se reduce en un 11.5 % comparado con el escenario TCP y un 6.3 % con el escenario UDP en el lado del cliente.

La segunda métrica de evaluación son los tiempos de solicitud y respuesta a cada registro DNSSEC del dominio ***nic.cl***, esto se puede observar en la Fig. 4.14. La métrica es evaluada en los 3 escenarios propuestos con la caché en frío. En la Fig. 4.14 se observa que el escenario UDP tiene 5 apuntadores a lo que equivalen las consultas DNSKEY (nic.cl), DS (nic.cl), DNSKEY (.cl), DS (.cl), DNSKEY (.) y cuyo valor es mínimo para observarse en la gráfica.

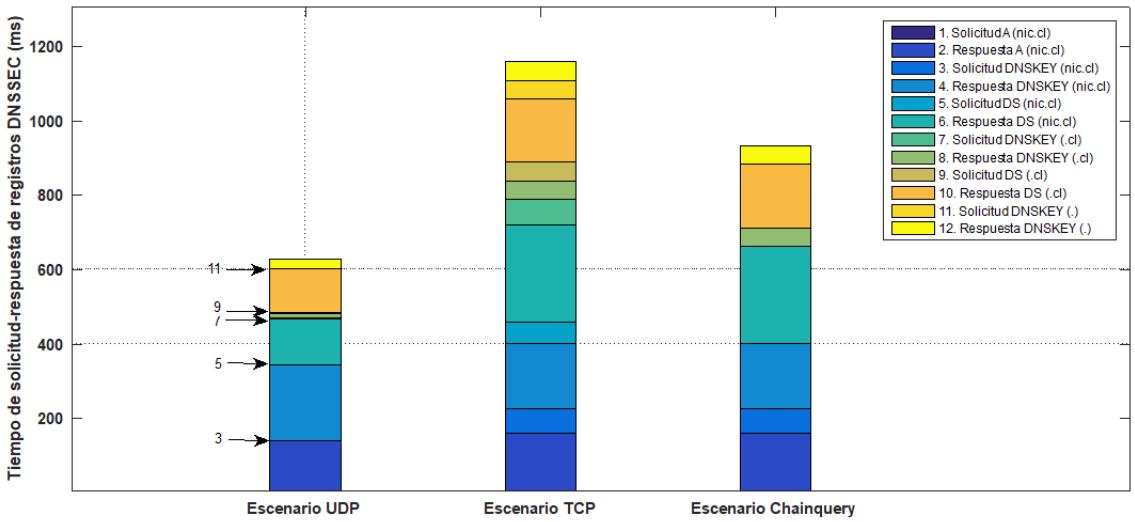

Figura 4.14: Tiempos de solicitud/respuesta en la validación de la cadena de confianza DNSSEC en los escenarios de prueba UDP, TCP y *DNS ChainQuery*

El escenario UDP completa la validación de la cadena de confianza en 628 ms, el escenario TCP en 1158 ms y el escenario *DNS ChainQuery* en 932 ms. Los resultados muestran que el escenario UDP tiene mejor rendimiento en tiempos de respuesta por un 45 % (530 ms aproximadamente) en comparación con el escenario TCP. Sin embargo, la diferencia entre el escenario UDP con el escenario *DNS ChainQuery* es de 32.5 % menor (304 ms aproximadamente).

La tercera métrica de análisis es la cantidad de paquetes transmitidos en cada escenario, como se puede observar en la Tabla 4.2. Basado en la cantidad de paquetes por cada solicitud o respuesta DNS, los escenarios UDP y TCP transmiten 12 paquetes de acuerdo a la resolución tipo A y la validación DNSSEC del dominio ***nic.cl***. El escenario *DNS ChainQuery*, requiere 1 paquete de solicitud y 1 paquete de respuesta de la resolución tipo A. Adicionalmente, 1 paquete de la solicitud hacia el servidor recursivo para la cadena DNSSEC y 2 paquetes con la respuesta del servidor recursivo. Los 2 paquetes de respuesta están basados en la cantidad de bytes de los registros DNSSEC (2484 bytes) sobre la capacidad *MSS* (1460 bytes).

	UDP	**TCP**	***DNS ChainQuery***
Número de paquetes	12	12	5

Tabla 4.2: Número de paquetes transmitidos para el escenario de pruebas UDP, TCP y *DNS ChainQuery*

Adicionalmente se realiza un análisis del uso de CPU para el servidor stub cuando se realiza la validación DNSSEC en los escenarios propuestos. Para esto se utiliza la herramienta *s-tui*[4] que permite realizar un monitoreo al uso de CPU mientras se realizan las consultas y se reciben los datos de los registros DNSSEC. La configuración de la frecuencia del muestreo es de 0.5 segundos, la comparación del uso de CPU en los escenarios UDP y TCP se puede observar en la Fig. 4.15.

El uso de CPU en el escenario TCP aumenta un 23.5 % en promedio de 30 pruebas

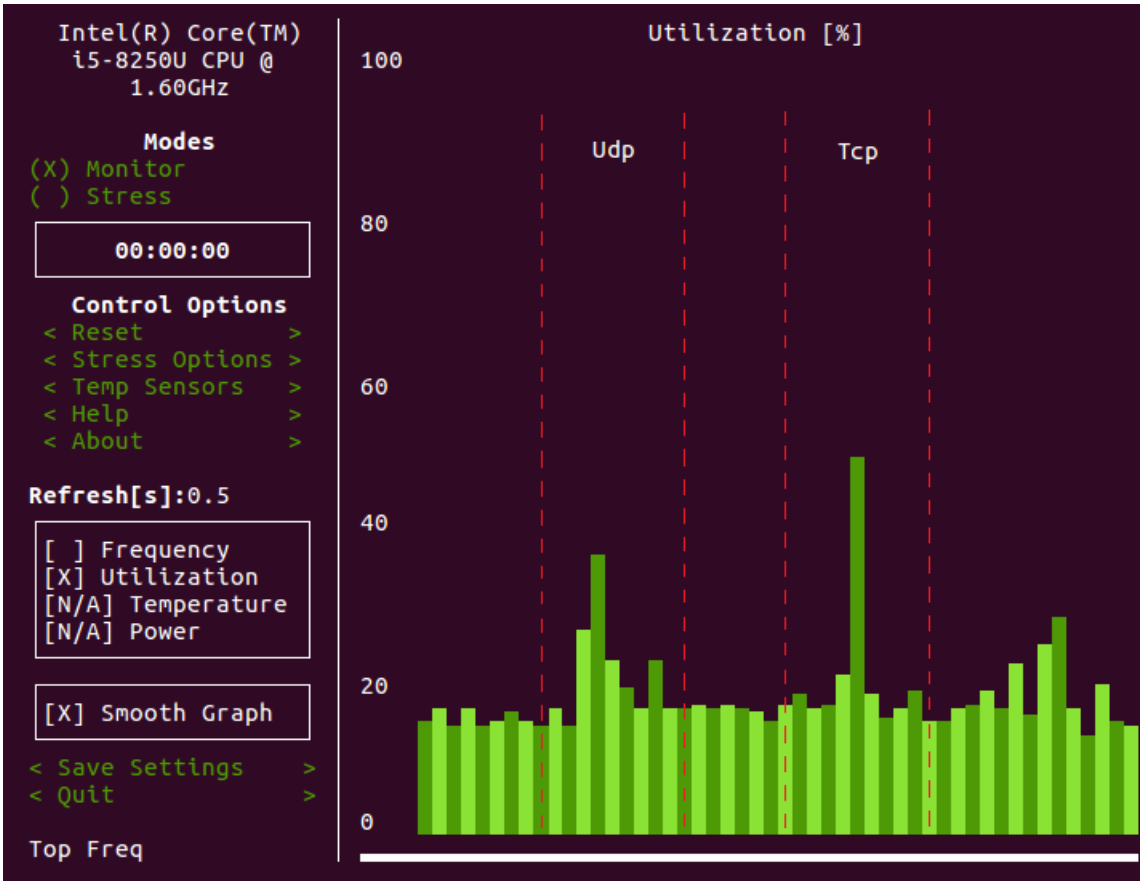

Figura 4.15: Comparación del uso de CPU en el servidor stub para realizar la validación DNSSEC en los escenarios UDP y TCP

solicitando la cadena de validación DNSSEC al dominio ***nic.cl*** respecto al escenario UDP. Sin embargo, con el escenario cadena de solicitudes se realiza un análisis de los registros DNSSEC de manera individual para determinar cuánto procesamiento de CPU consume cada uno y computar las respuestas DNS. El escenario *DNS ChainQuery* puede generar un aumento de 13 % el uso de CPU en comparación al escenario UDP.

Finalmente, la prueba se repite con almacenamiento en caché de los registros DNSSEC para analizar la diferencia en cada uno de los escenarios, como se puede observar en la Fig. 4.16. Los primeros registros DNSSEC almacenados por defecto son las llaves DNSKEY del servidor raíz (.) y DNSKEY del "Top level domain"(.cl), para realizar la consulta al dominio ***nic.cl***. La métrica de análisis es el tiempo de respuesta.

La reducción de los tiempos en la validación DNSSEC en el escenario UDP es de 24 ms, en el escenario TCP es de 142 ms y en el escenario *DNS ChainQuery* es de 94 ms. sin embargo, los tiempos de respuesta a las solicitudes DNS en el escenario UDP siguen siendo superiores por un 40 % respecto al escenario TCP y un 27 % en comparación al escenario *DNS ChainQuery*.

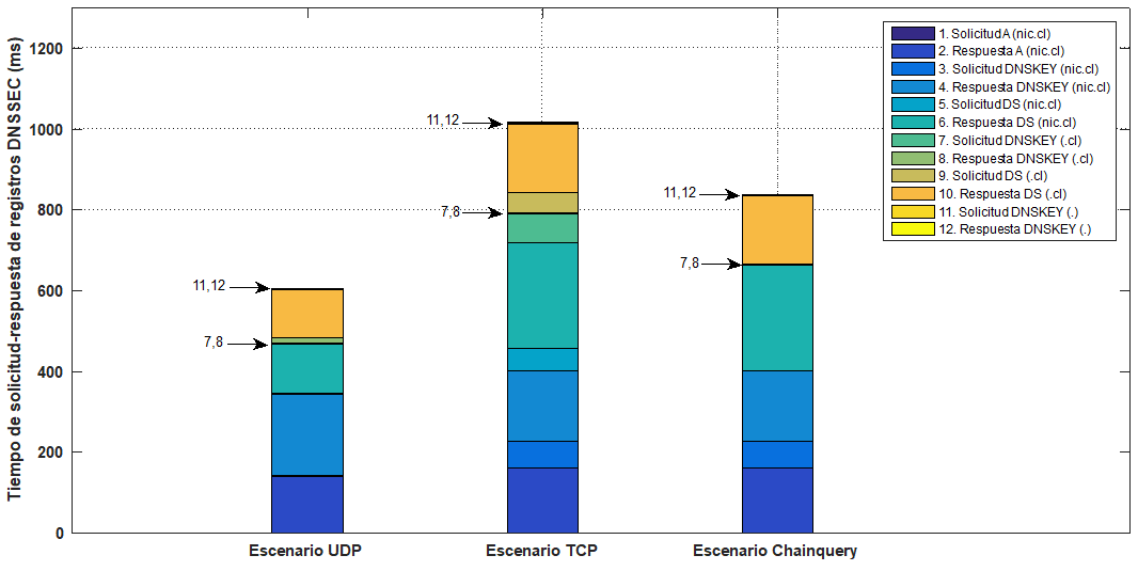

Figura 4.16: Comparación de tiempos de solicitud-respuesta para la validación DNSSEC con almacenamiento en caché en los escenarios UDP,TCP y *DNS ChainQuery*

4.4.2. Análisis del lado del servidor de validación DNSSEC

El análisis de la validación DNSSEC en el lado del servidor recursivo se realiza sobre 10 dominios. Los dominios que cumplen los requerimientos de los registros DNSSEC son ***nic.cl***, ***niclabs.cl***, ***despegar.cl***,***fepa.cl***, ***conicyt.cl***, ***wom.cl***, ***scielo.cl***, ***prosegur.cl***, ***consorcio.cl*** y ***lider.cl***. La primera métrica de análisis son los bytes totales por los 10 dominios en cada consulta de los recursos DNSSEC, como se observa en la Fig. 4.17, se presentan los resultados acumulados para analizar la funcionalidad que cumple el servidor recursivo.

Los resultados muestran que el escenario *DNS ChainQuery* tiene mejor rendimiento en 15 % (3430 bytes) en la cantidad de bytes en las transferencia DNS para la validación DNSSEC respecto al escenario TCP y un 10 % (2000 bytes) respecto al escenario UDP. El análisis permite evaluar de manera positiva el impacto de la implementación de la extensión *DNS ChainQuery* en un servidor cuya función sea de reenvío de solicitudes o de validación DNSSEC, aún no siendo un servidor stub.

Adicionalmente se analiza la métrica de tiempos de solicitud-respuesta en la validación DNSSEC de los 10 dominios. En la Fig. 4.18 se presenta los resultados acumulados para analizar el soporte del servidor recursivo.

Los resultados muestran que el escenario UDP mantiene mejor rendimiento en un 21 % (2750 ms) en los tiempos de solicitud-respuesta de cada recurso DNSSEC respecto al escenario TCP y un 10.5 % (1190 ms) respecto al escenario *DNS ChainQuery*. En este caso la evaluación de la implementación de la *DNS ChainQuery* presenta mejores resultados a nivel de validación de múltiples dominios que para un solo dominio. Mientras que el escenario UDP obtiene un 32.5 % de optimización de tiempos validando el dominio ***nic.cl***, el escenario *DNS ChainQuery* en la validación de los 10 dominios mejora consecutivamente un 10.5 %.

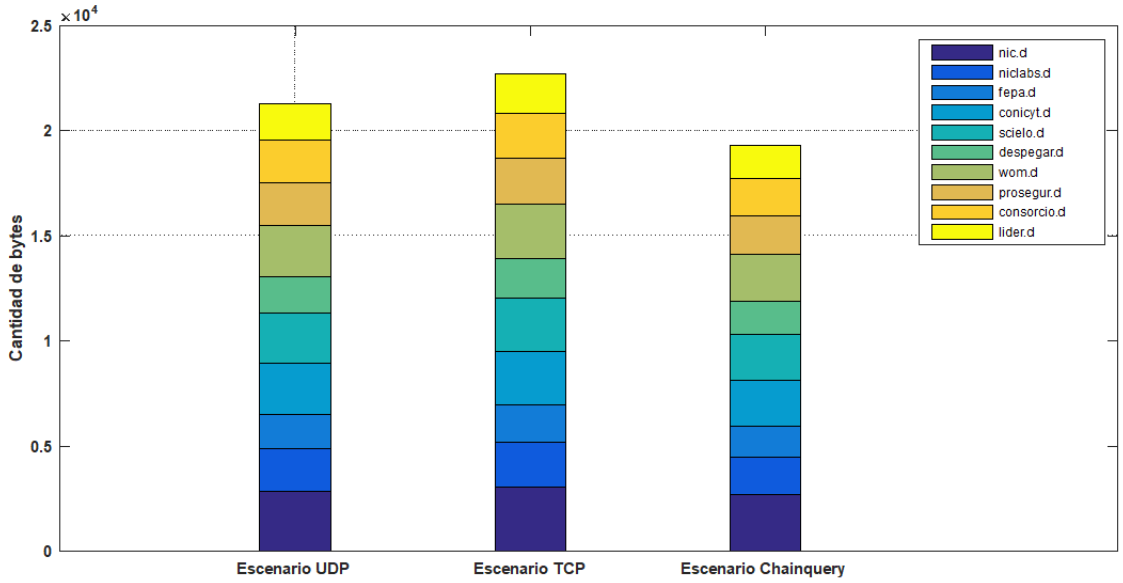

Figura 4.17: Cantidad de bytes transmitidos en la validación de la cadena de confianza DNSSEC en los escenarios de prueba UDP, TCP y *DNS ChainQuery* para 10 dominios consecutivamente

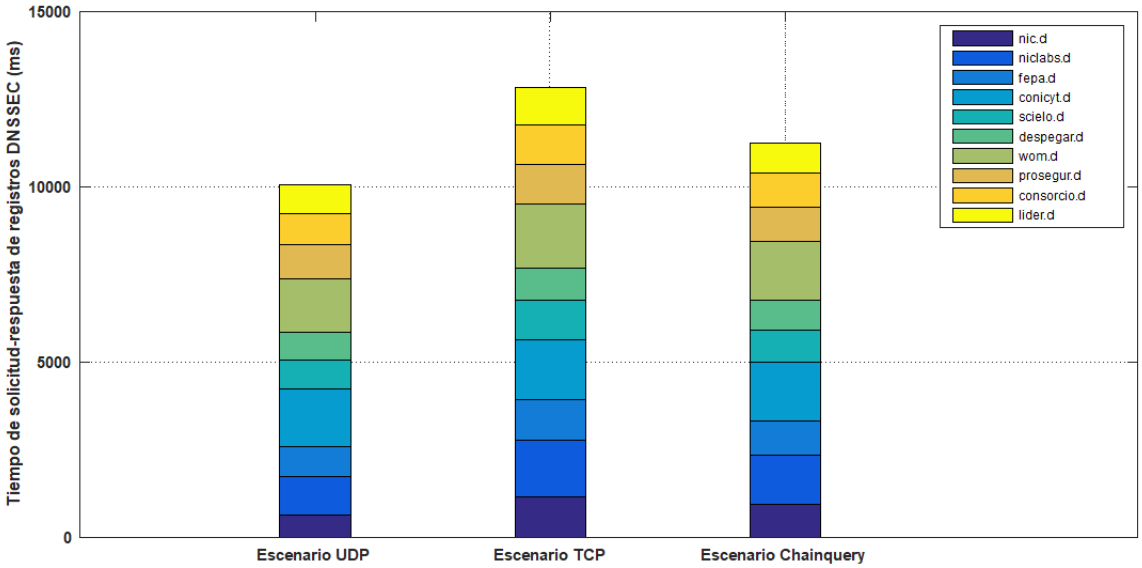

Figura 4.18: Tiempos de solicitud/respuesta en la validación de la cadena de confianza DNSSEC en los escenarios de prueba UDP, TCP y *DNS ChainQuery* para 10 dominios consecutivamente

Capítulo 5

Conclusiones y trabajo futuro

5.1. Conclusiones

Esta tesis presenta una evaluación de la implementación de la extensión *DNS ChainQuery* con distintos parámetros de red para un contexto de validación DNSSEC en un cliente. Para ello se realiza un estudio del estado de adopción y configuración de los mecanismos EDNS0 que influyen en el análisis de *DNS ChainQuery* en cerca de 20000 servidores recursivos. Este estudio presenta un sistema de clasificación del estado de cada servidor evaluado respecto al diagrama presentado en la sección 3.1 y generando como resultado un algoritmo replicable en otras zonas DNS.

Los resultados obtenidos de la sección 4.1 confirman una correcta configuración de los servidores recursivos para responder a una consulta EDNS0. Además se puede concluir que existe un alta congruencia de los resultados de las pruebas a cada extensión DNS estudiada en este trabajo con una tasa baja de adopción y la clasificación por versión del software DNS que permite analizar que servidores han sido configurados para soportar en teoría cada característica EDNS0.

Por otro lado, en la sección 4.2 se ilustra un alto índice de adopción de la extensión de seguridad DNSSEC en la muestra utilizada, más no de una correcta configuración por parte de los servidores recursivos, presentado como advertencias. Esta evaluación permite determinar que la consulta DNSSEC generada hacia el servidor recursivo puede terminar en una resolución DNS fallida u otros problemas. Estas advertencias generadas por el algoritmo de clasificación podrían ser una base para corregir la baja tasa de validación DNSSEC, presentada como una de las hipótesis de esta tesis en la sección 1.3.

Posterior al análisis del bajo estado de adopción y configuración de los servidores recursivos para responder consultas *DNS ChainQuery*, se confirma que falta un interés de despliegue de esta y otras extensiones a nivel operacional. Por ese motivo, de acuerdo a los resultados de esta tesis se muestra que la extensión *DNS ChainQuery* podría mejorar dos factores en la red: la disminución de tráfico de red (bytes) y el número de paquetes transmitidos por resolución DNS.

Desde otra perspectiva, los resultados obtenidos en la sección muestran que los tiempos de respuesta en el escenario UDP son mejores que con el escenario *DNS ChainQuery*. Esto se debe a la transacción del proceso *three-way handshake*. No obstante, el escenario UDP no tiene la confiabilidad ni genera la seguridad para construir la cadena de confianza DNSSEC. Mientras que el escenario *DNS ChainQuery* sí supera al escenario TCP en un 12.5 % los tiempos de respuesta para la validación DNSSEC en un cliente mediante el uso de un mecanismo confiable, respondiendo de manera afirmativa a la hipótesis planteada en esta tesis.

Otro punto de análisis fue el costo de CPU en el cliente para la validación de un dominio, el cual aumenta con el escenario *DNS ChainQuery* sin afectar otros tareas para el host del cliente. Adicionalmente, se destaca que el uso correcto de caché en las pruebas mejoró el rendimiento de los tiempos de respuesta del escenario *DNS ChainQuery* en al menos un 33 %. Basado en que la validación de la respuesta contiene una carga útil mayor por las llaves DNSSEC a la validación de la solicitud. Por último se muestra que la resolución DNS de los registros tipo A, AAAA, MX, entre otras, no se ve afectada por la implementación de la extensión *DNS ChainQuery*.

Adicionalmente, se presentaron las ventajas del uso de la extensión *DNS ChainQuery* en la resolución DNS a nivel global, de acuerdo a la evaluación de rendimiento en un servidor recursivo en un contexto de validación DNSSEC. En el análisis de validación de múltiples dominios, *DNS ChainQuery* reduce los tiempos de respuestas acumulados, lo que genera reducción en latencia de la red.

Finalmente, los resultados revelan que un trabajo en conjunto permite reducir latencia en red cuando la carga de un servidor recursivo en un contexto de validación de llaves de seguridad disminuye con la implementación de la extensión *DNS ChainQuery*. Esto además de aumentar un nivel de seguridad, permite en un ambiente de operación de los administradores o registradores DNS utilizar la cadena de validación en escenarios en los que se debe depurar la resolución DNS a través de otros protocolos como *DNS over HTTPs* (DoH) o *DNS over TLS* (DoT).

5.2. Trabajo futuro

Basado en la función y resultados del algoritmo de clasificación de los servidores recursivos en la zona DNS de Chile, uno de los futuros retos es analizar servidores de otras zonas DNS generando nuevos reportes, y así ampliar la evaluación del estado DNS respecto a las extensiones para corregir las fallas de configuración y cumplir con los lineamientos de los estándares publicados. Adicionalmente, en una nueva versión del algoritmo se puede realizar un análisis del impacto de la configuración EDNS0 en toda la arquitectura DNS, incluyendo servidores autoritativos.

De acuerdo a los resultados obtenidos del estudio de la extensión *DNS ChainQuery* se tienen las bases para iniciar el desarrollo de su implementación. Como trabajo futuro, este desarrollo tiene que ser implementado en un software DNS como característica adicional y así instalarla en múltiples servidores recursivos para crear un red en un contexto de seguridad

hasta la última milla. No obstante, el alcance del desarrollo no solo debe ser implementado en los servidores sino agregar su función como *plugin*, nueva API, extensión de un *Browser* o como característica adicional de un *Stub resolver* en el cliente.

Bibliografía

[1] Dnssec deployment statistics for tlds (rick lamb) about, https://www.internetsociety.org/resources/deploy360/2014/dnssec-deployment-statistics-for-tlds-rick-lamb/, author=Rick, Lamb, year=2014.

[2] The resolvers we use about, https://blog.apnic.net/2014/11/28/the-resolvers-we-use/, author=Huston, Geoff, year=2014.

[3] D. Eastlake 3rd and M. Andrews. RFC 7873: Domain name system (dns) cookies. Technical report, www.tools.ietf.org/html/rfc7873, 2016, DOI 10.17487/RFC7873, 2016.

[4] Alex Manuskin. Alternative (more granular) approach to a dns library about, https://github.com/amanusk/s-tui, 2019.

[5] M. Andrews. RFC 2308: Negative caching of dns queries (dns ncache). Technical report, www.tools.ietf.org/html/rfc2308, 1998, DOI 10.17487/RFC2308, 1998.

[6] M. Andrews. RFC 7314: Extension mechanisms for dns (edns) expire option. Technical report, www.tools.ietf.org/html/rfc7314, 2014, DOI 10.17487/RFC7314, 2014.

[7] M. Andrews and R. Bellis. Internet draft: A common operational problem in dns servers - failure to respond. draft-ietf-dnsop-no-response-issue-12. Technical report, https://tools.ietf.org/html/draft-ietf-dnsop-no-response-issue-12, 2018.

[8] APNIC, Geoff Huston. Dnssec validation rate by country about, https://stats.labs.apnic.net/dnssec.

[9] Austein R. Larson M. Massey D. Arends, R. and S. Rose. RFC 4033:dns security introduction and requirements. Technical report, https://tools.ietf.org/html/rfc4033, DOI: 10.17487/RFC4033, 2005.

[10] Austein R. Larson M. Massey D. Arends, R. and S. Rose. RFC 4035:protocol modifications for the dns security extensions. Technical report, https://tools.ietf.org/html/rfc4035, DOI: 10.17487/RFC4035, 2005.

[11] R. Bellis and A. Clegg. Internet draft: Dns edns tags. draft-bellis-dnsop-edns-tags-00. Technical report, https://tools.ietf.org/html/draft-bellis-dnsop-edns-tags-00, 2019.

[12] Ilker Nadi Bozkurt, Anthony Aguirre, Balakrishnan Chandrasekaran, P Brighten God-

frey, Gregory Laughlin, Bruce Maggs, and Ankit Singla. Why is the internet so slow?! In *International Conference on Passive and Active Network Measurement*, pages 173–187. Springer, 2017.

[13] D. Lawrence C. Contavalli, W. van der Gaast and W. Kumari. RFC 7871: Client subnet in dns queries. Technical report, www.tools.ietf.org/html/rfc7871, 2016, DOI 10.17487/RFC7871, 2016.

[14] Matt Calder, Xun Fan, Zi Hu, Ethan Katz-Bassett, John Heidemann, and Ramesh Govindan. Mapping the expansion of google's serving infrastructure. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 313–326. ACM, 2013.

[15] Matt Calder, Ashley Flavely, Ethan Katz-Bassett, Ratul Mahajany, and Jitendra Padhyey. Analyzing the performance of an anycast cdn. In *Proceedings of the 2015 Internet Measurement Conference*, pages 531–537. ACM, 2015.

[16] Sebastian Castro, Min Zhang, Wolfgang John, Duane Wessels, and Kimberly Claffy. Understanding and preparing for dns evolution. In *International Workshop on Traffic Monitoring and Analysis TMA 2010: Traffic Monitoring and Analysis*, pages 1–16. Springer, Berlin, Heidelberg, 2010.

[17] S. Cheshire and M. Krochmal. Internet draft: Apple's dns long-lived queries protocol. draft-sekar-dns-llq-06. Technical report, https://tools.ietf.org/html/draft-sekar-dns-llq-06, 2019.

[18] S. Cheshire and T. Lemon. Internet draft: Dynamic dns update leases. draft-sekar-dns-ul-02. Technical report, https://tools.ietf.org/html/draft-sekar-dns-ul-02, 2018.

[19] 'Etuate Cocker. *Active longitudinal measurement in global networks and goodput recovery with network coding over high latency satellite links*. PhD thesis, The University of Auckland, 2016.

[20] M. Crawford. RFC 2673: Binary labels in the domain name system. Technical report, www.tools.ietf.org/html/rfc2673, DOI 10.17487/RFC2673, 1999.

[21] S. Crocker and S. Rose. RFC 6975: Signaling cryptographic algorithm understanding in dns security extensions (dnssec). Technical report, https://tools.ietf.org/html/rfc6975, DOI: 10.17487/RFC6975, 2013.

[22] CZ.NIC, Petr Špaček. Edns-zone-scanner, `https://gitlab.labs.nic.cz/knot/edns-zone-scanner/`, 2018.

[23] Conrad D. RFC 3225:indicating resolver support of dnssec. Technical report, http://www.rfc-editor.org/info/rfc3225, STD 75, DOI 10.17487/RFC3225, 2001.

[24] J. Damas, M. Graff, and P. Vixie. RFC 6891:extension mechanisms for dns (edns(0)). Technical report, http://www.rfc-editor.org/info/rfc6891, STD 75, DOI 10.17487/RFC6891, 2013.

[25] Marcel Flores, Alexander Wenzel, Kevin Chen, and Aleksandar Kuzmanovic. Fury route: Leveraging cdns to remotely measure network distance. In *International Conference on Passive and Active Network Measurement-PAM*, pages 87–99. Springer, Cham, 2018.

[26] Fred Baker,Internet Systems Consortium. Dns compliance about, `https://www.isc.org/wp-content/uploads/2017/07/ICANN-EDNS-Preso.pdf`, 2017.

[27] Xavier Torrent Gorjon. Discovery method for a dnssec validating stub resolver. Master's thesis, Universiteit Van Amsterdam, 2015.

[28] Arnir Herzberg and Haya Shulrnan. Fragmentation considered poisonous, or: one-domain-to-rule-them-all.org. In *IEEE Conference on Communications and Network Security (CNS)*, pages 224–232. The Institute of Electronics, Information and Communication Engineers, 2013.

[29] Filip Hock and Peter Kortiš. Design, implementation and monitoring of the firewall system for a dns server protection. In *Emerging eLearning Technologies and Applications (ICETA), 2016 International Conference on*, pages 91–96. The Institute of Electronics, Information and Communication Engineers, 2016.

[30] Jian Jiang Yan Chen Phillip Porras Shalini Ghosh Hongyu Gao, Vinod Yegneswaran and Haixin Duan. Reexamining dns from a global recursive resolver perspective. *IEEE/ACM TRANSACTIONS ON NETWORKING*, 24(1):43–57, 2016.

[31] C Hornig. RFC 894:a standard for the transmission of ip datagrams over ethernet networks. Technical report, http://www.rfc-editor.org/info/rfc894, STD 13, DOI 10.17487/RFC894, 1984.

[32] IBM. Extension mechanisms for dns standards and the resolver, $\texttt{https://www.ibm.com/support/knowledgecenter/en/SSLTBW}_2$,3,0/$com.ibm.zos.v2r3.halz002/resolver_{\mathrm{e}}dns0.htm$, 2018.

[33] IETF. Domain name system operations (dnsop) , `https://datatracker.ietf.org/group/dnsop/about/`, 2018.

[34] Internet Assigned Numbers Authority. Address family numbers, `https://www.iana.org/assignments/address-family-numbers/address-family-numbers.xhtml`, 2018.

[35] Internet Assigned Numbers Authority. Domain name system (dns) parameters, `https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml-dns-parameters-11`, 2019.

[36] Internet Systems Consortium. 5 stages of dnssec deployment about, `https://www.internetsociety.org/deploy360/dnssec/maps/5-stages/`.

[37] Internet Systems Consortium. Dig, `https://ftp.isc.org/isc/bind/9.11.0a1/doc/arm/man.dig.html`, 2014.

[38] Internet Systems Consortium. The two sides of dnssec – signing and validation about, https://www.internetsociety.org/resources/deploy360/2014/the-two-sides-of-dnssec-signing-and-validation/, 2014.

[39] Internet Systems Consortium. Edns compliance, https://ednscomp.isc.org/, 2018.

[40] Internet Systems Consortium. End to bandaids for broken edns about, https://www.isc.org/blogs/end-to-bandaids/, 2018.

[41] Internet Systems Consortium. Bind, https://www.isc.org/bind/, 2019.

[42] ISC-UBUNTU. Delv, http://manpages.ubuntu.com/manpages/xenial/man1/delv.1.html, 2014.

[43] Kakoi K. Tomoishi M. Yamai N Jin, Y. Efficient detection of suspicious dns traffic by resolver separation per application program. In *Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC)*, pages 87–92. The Institute of Electronics, Information and Communication Engineers, 2017.

[44] Yong Jin, Kunitaka Kakoi, Nariyoshi Yamai, Naoya Kitagawa, and Masahiko Tomoishi. A client based dnssec validation system with adaptive alert mechanism considering minimal client timeout. *IEICE TRANSACTIONS on Information and Systems*, 100(8):1751–1761, 2017.

[45] Soyoung Kim, Sora Lee, Geumhwan Cho, Muhammad Ejaz Ahmed, Jaehoon Paul Jeong, and Hyoungshick Kim. Preventing dns amplification attacks using the history of dns queries with sdn. In *European Symposium on Research in Computer Security*, pages 135–152. Springer, 2017.

[46] Panagiotis Kintis, Yacin Nadji, David Dagon, Michael Farrell, and Manos Antonakakis. Understanding the privacy implications of ecs. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 343–353. Springer, 2016.

[47] John Heidemann Duane Wessels Allison Mankin Liang Zhu, Zi Hu and Nikita Somaiya. Connection-oriented dns to improve privacy and security (extended). Technical report, https://isi.edu/ johnh/PAPERS/Zhu15c.pdf, USC/ISI Technical Report ISI-TR-695, 2015.

[48] Linux man page, die.net. Name service cache daemon, https://linux.die.net/man/8/nscd, 2018.

[49] Mark Andrews, Internet Systems Consortium. Ietf-91 edns compliance about, https://www.ietf.org/proceedings/92/slides/slides-92-dnsop-7.pdf, 2015.

[50] A. Mayrhofer. RFC 7830: The edns(0) padding option. Technical report, https://tools.ietf.org/html/rfc7830, DOI: 10.17487/RFC7830, 2016.

[51] Wei Meng, Ruian Duan, and Wenke Lee. Dns changer remediation study. *Talk at M3AAWG 27th*, 2013.

[52] P. Mockapetris. RFC 882: Domain names - concepts and facilities. Technical report, https://tools.ietf.org/html/rfc882, DOI: 10.17487/RFC882, 1983.

[53] P. Mockapetris. RFC 883: Domain names - implementation and specification. Technical report, https://tools.ietf.org/html/rfc883, DOI: 10.17487/RFC883, 1983.

[54] P. Mockapetris. RFC 973: Domain system changes and observations. Technical report, https://tools.ietf.org/html/rfc973, DOI: 10.17487/RFC973, 1986.

[55] P Mockapetris. RFC 1034: Domain names - concepts and facilities. Technical report, http://www.rfc-editor.org/info/rfc1034, STD 13, DOI 10.17487/RFC1034, 1987.

[56] P Mockapetris. RFC 1035: Domain names - implementation and specification. Technical report, http://www.rfc-editor.org/info/rfc1035, STD 13, DOI 10.17487/RFC1035, 1987.

[57] David A. Moon. Chaosnet. 1981.

[58] Giovane C. M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Müller, Lan Wei, and Cristian Hesselman. Anycast vs. ddos: Evaluating the november 2015 root dns event. In *Proceedings of the 2016 Internet Measurement Conference*, pages 255–270. ACM, 2016.

[59] Tomokazu Otsuka, Gada, Nariyoshi Yamai, Kiyohiko Okayama, and Yong Jin. Design and implementation of client ip notification feature on dns for proactive firewall system. In *IEEE 39th Annual Computer Software and Applications Conference*, pages 127–132. The Institute of Electronics, Information and Communication Engineers, 2015.

[60] Petr Špaček. Dns flag day `https://dnsflagday.net/es/`, 2018.

[61] Petr Špaček. Together for better stability, speed and further extensibility of the dns ecosystem about, `http://en.blog.nic.cz/2018/03/14/together-for-better-stability-speed-and-further-extensibility-of-the-dns-ecosystem/`, 2018.

[62] S. Dickinson P.Wouters, J. Abley and R. Bellis. RFC 7828: The edns-tcp-keepalive edns0 option. Technical report, http://www.rfc-editor.org/info/rfc7828, 2016, DOI 10.17487/RFC7828, 2016.

[63] Austein R. RFC 5001:dns name server identifier (nsid) option. Technical report, https://tools.ietf.org/html/rfc5001, DOI: 10.17487/RFC5001, 2007.

[64] Sara Dickinson. Configuring stubby, `https://dnsprivacy.org/wiki/display/DP/Configuring+Stubby`, 2019.

[65] Sara Dickinson, DNS privacy project. Dns privacy daemon - stubby about, `https://github.com/getdnsapi/stubby`, 2018.

[66] Florian Streibelt, Jan Böttger, Nikolaos Chatzis, Georgios Smaragdakis, and Anja Feldmann. Exploring edns-client-subnet adopters in your free time. In *Proceedings of the*

2013 conference on Internet measurement conference, pages 305–312. ACM, 2013.

[67] J.H.C. van Heugten. Privacy analysis of dns resolver solutions. 2018.

[68] Vicky Risk, Internet Systems Consortium. Partial edns compliance hampers deployment of new dns features about, `https://www.isc.org/blogs/partial-edns-compliance-hampers-deployment-of-new-dns-features/`, 2015.

[69] Barron T. Van Goethem T. Joosen W. Nikiforakis N Vissers, T. The wolf of name street: Hijacking domains through their nameservers. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 957–970. ACM, 2017.

[70] P Vixie. RFC 2671: Extension mechanisms for dns (edns0). Technical report, www.tools.ietf.org/html/rfc2671, DOI 10.17487/RFC2671, 1999.

[71] Zheng Wang. Optimizing negative caching for dnssec-oblivious resolvers. In *14th International Symposium on Network Computing and Applications*, pages 267–274. The Institute of Electronics, Information and Communication Engineers, 2015.

[72] Nicholas Weaver, Christian Kreibich, Boris Nechaev, and Vern Paxson. Implications of netalyzr's dns measurements. In *Proceedings of the First Workshop on Securing and Trusting Internet Names (SATIN)*, pages 1–8. NPL, 2011.

[73] Kumari W. Wessels, D. and P. Hoffman. RFC 8145: Signaling trust anchor knowledge in dns security extensions (dnssec). Technical report, https://tools.ietf.org/html/rfc8145, DOI: 10.17487/RFC8145, 2017.

[74] Paul Wouters. Chain query requests in dns. Technical report, www.tools.ietf.org/html/rfc7901, DOI 10.17487/RFC7901, 2016.

[75] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin, and Nikita Somaiya. Connection-oriented dns to improve privacy and security. In *IEEE Symposium on Security and Privacy*, pages 171–186. The Institute of Electronics, Information and Communication Engineers, 2015.