DNSSEC para proveedores de Internet

Relator: Hugo Salgado H.

Agosto / 2017

Evento "PIT Chile", Osorno

Temario

1) ¿Por qué DNSSEC?
2) Cómo funciona
3) Beneficios (y costos) para ISP
4) Implantación
    1) Requisitos
    2) Planificación
    3) Operación

1. ¿Por qué DNSSEC?

¿Por qué DNSSEC? (1/3)

- Confianza en las respuestas DNS. Ataques de envenenamiento de cache:
  - Problemas económicos
    - Pérdida de recursos
    - Fraude
    - Daño a la reputación
  - Seguridad
    - Usuarios (robo de identidad, fraude)
    - Empresas (redirección de tráfico, intercepción)

¿Por qué DNSSEC? (2/3)

- Nuevos servicios
  - Certificados PKI (DANE)
  - Correo seguro (TLSA)
  - SSH fingerprints
  - Identidades PGP
  - etc...

¿Por qué DNSSEC? (3/3)

- Despliegue en firmado
  - CL desde 2011 (6 años)
  - Software que automatiza
    - Bind
    - OpenDNSSEC
    - “Cajas negras”
- Despliegue en validación
  - Software desde hace > 5 años
  - Google, grandes ISPs

¿Por qué DNSSEC? (3/3)

- LAC ccTLD DNSSEC Status on 2017-08-14

-

"DNSSEC deployment in ccTLDs / LAC region"
http://www.internetsociety.org/deploy360/dnssec/maps/

¿Por qué DNSSEC? (3/3)

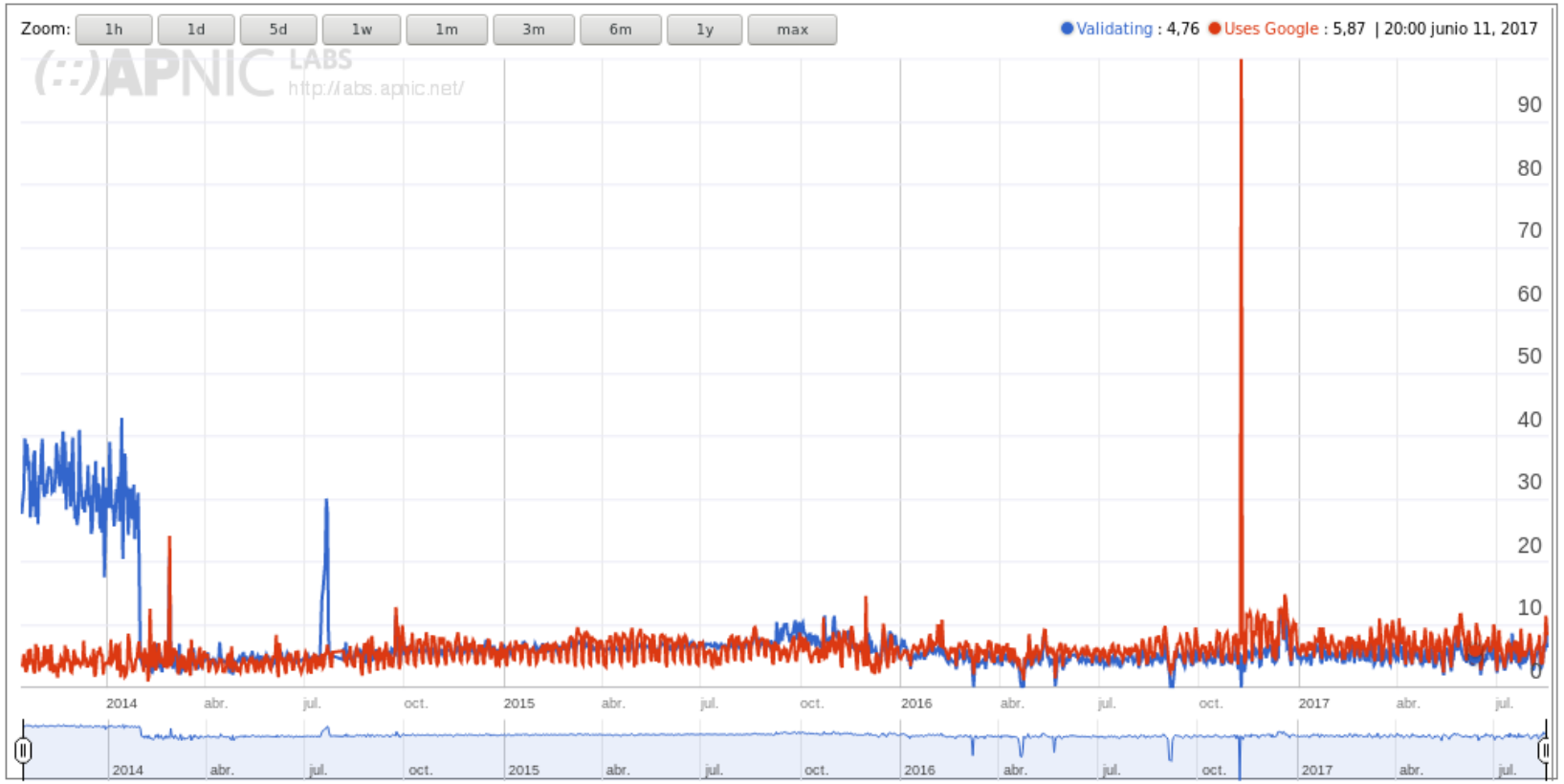
- Region Map for South America (005)

-

"DNSSEC validation status map / South America"
https://stats.labs.apnic.net/dnssec/CL

¿Por qué DNSSEC? (3/3)

Use of DNSSEC Validation for Chile (CL)



"DNSSEC validation graph for Chile"
https://stats.labs.apnic.net/dnssec/CL

¿Por qué DNSSEC? (3/3)

ASN	AS Name	DNSSEC Validates	Uses Google PDNS	Samples
AS27897	SEGIC USACH LTDA	99.74%	60.98%	387
AS10753	LVLT-10753 - Level 3 Communications, Inc.	99.17%	99.58%	240
AS262213	Comsat Limitada	98.76%	5.71%	1.051
AS264681	Sociedad de Telecomunicaciones Netsouth SPA	98.59%	93.58%	3.271
AS265672	ALCOM SPA	98.58%	100.00%	424
AS265678	W M Servicios y Gestiones Ltda.	98.42%	100.00%	253
AS264806	TNA Solutions SpA	97.14%	7.14%	70
AS61460	NETLAND CHILE S.A.	97.03%	98.02%	202
AS264838	INVERSIONES MYJ LTDA	96.38%	100.00%	221
AS264780	HomeNet LTDA	95.56%	97.78%	90
AS265675	ARTEC TELECOMUNICACIONES LIMITADA	94.65%	95.79%	1.046
AS7049	Silica Networks Argentina S.A.	94.33%	99.29%	141
AS61503	SERVICIOS DE TELECOMUNICACIONES INTERCABLE LTDA.	91.17%	99.71%	1.722
AS52280	INTERNEXA Chile S.A.	80.94%	57.06%	829
AS52368	ZAM LTDA.	80.83%	90.16%	193
AS52439	OPTIC	80.09%	99.77%	1.763
AS27746	LAN CHILE (Lineas Aereas de Chile)	77.97%	93.22%	59
AS26610	Universidad Tecnica Federico Santa Maria	60.50%	0.84%	119
AS3549	LVLT-3549 - Level 3 Communications, Inc.	53.95%	61.85%	1.342
AS18747	IFX18747 - IFX Corporation	51.33%	71.98%	1.695
AS28096	Sociedad de Telecomunicaciones Geonet Ltda.	48.28%	82.76%	58
AS15311	Telefonica Empresas	46.70%	59.34%	10.832
AS20015	FullCom S.A.	44.76%	48.57%	105
AS6471	ENTEL CHILE S.A.	41.66%	52.82%	33.156
AS22860	SERVICIOS INTERNET LTDA	40.59%	45.54%	101
AS61440	Digital Energy Technologies Chile SpA	32.84%	37.31%	67
AS27651	ENTEL CHILE S.A.	30.67%	39.87%	1.891
AS11340	Red Universitaria Nacional	27.59%	22.52%	1.834
AS16629	CTC. CORP S.A. (TELEFONICA EMPRESAS)	27.18%	55.86%	6.552
AS27659	Ingeniera e Informtica Asociada Ltda (IIA Ltda)	21.40%	47.60%	271
AS16874	SONDA S.A.	18.64%	30.08%	236
AS7004	CTC Transmisiones Regionales S.A.	17.37%	33.57%	3.178
AS264814	BITRED GROUP SPA	15.82%	98.31%	177
AS262237	Orbyta S.A.	14.63%	64.23%	123
AS6429	Telmex Chile Internet S.A.	13.57%	35.86%	4.275
AS14259	Gtd Internet S.A.	11.43%	36.06%	8.888
AS52226	CODELCO Chuquicamata	9.09%	100.00%	110
AS27901	Pacifico Cable S.A.	7.90%	8.14%	33.957
AS52435	Plug and play Net S.A.	7.63%	10.22%	773
AS23416	Telefonica Data Chile S.A.	7.49%	35.29%	187
AS52313	Luz Linares S.A.	7.47%	40.04%	562

"DNSSEC validation - ASN ranking / Chile"
https://stats.labs.apnic.net/dnssec/CL

2. ¿Cómo funciona DNSSEC?

¿Cómo funciona DNSSEC?

- DNS con autenticación interna de “datos”, sin importar transporte
  - Criptografía asimétrica
- Autenticidad e Integridad.
- Abre nuevas “preocupaciones”:
  - Agrega “timing” al DNS
  - Aumento de tamaños zonas y respuestas
  - Coordinación llave raíz

Cómo funciona: Zonas

```
ejemplo.cl.   IN  SOA  ….

              IN NS ns1.ejemplo.cl
              IN NS secundario.nic.cl

              IN MX 10 mail.ejemplo.cl

www           IN A 127.0.0.6

ns1           …
```

El DNS de 1987

Cómo funciona: Zonas

```
ejemplo.cl.   IN  SOA  ….
              RRSIG SOA ...
              IN NS ns1.ejemplo.cl
              IN NS secundario.nic.cl
              RRSIG NS ...
              IN MX 10 mail.ejemplo.cl
              RRSIG MX ...

www           IN A 127.0.0.6
              RRSIG A

ns1           …
              RRSIG ...
```

Cada registro tiene su firma
(en realidad RRset)

Cómo funciona: Zonas

```
ejemplo.cl.   IN  SOA  ….
              RRSIG SOA ...
              IN NS ns1.ejemplo.cl
              IN NS secundario.nic.cl
              RRSIG NS ...
              IN MX 10 mail.ejemplo.cl
              RRSIG MX ...

              DNSKEY 256 ...
              DNSKEY 257 ...
              RRSIG DNSKEY …



www           IN A 127.0.0.6
              RRSIG A

ns1           …
              RRSIG ...
```

Y las llaves públicas van en la misma zona (con su autofirma, obvio)

Cómo funciona: Zonas

ejemplo.cl.	IN SOA ….
	RRSIG SOA ...
	IN NS ns1.ejemplo.cl
	IN NS secundario.nic.cl
	RRSIG NS ...
	IN MX 10 mail.ejemplo.cl
	RRSIG MX ...
	DNSKEY 256 ...
	DNSKEY 257 ...
	RRSIG DNSKEY …
	NSEC
	RRSIG NSEC
www	IN A 127.0.0.6
	RRSIG A
	NSEC ...
	RRSIG NSEC ...
ns1	…
	RRSIG ...

También debemos pensar en las “negaciones de existencia”
(y sus firmas...)

Cómo funciona: Zonas

- Distribución de llaves dentro del DNS!
  - Usando la misma jerarquía
  - Cada hijo debe pasarle su llave al padre
  - Padre la publica (DS) y la entrega junto a la delegación (NS)

Cómo funciona: resolvers

root.hints:

.	NS	a.root-servers.net.
a.root-servers.net	A	198.41.0.4
a.root-servers.net	AAAA	2001:503:ba3e::2:30

. NS b.root-servers.net…
...

Cómo funciona: resolvers

root.hints:

```
.                       NS      a.root-servers.net.
a.root-servers.net      A       198.41.0.4
a.root-servers.net      AAAA    2001:503:ba3e::2:30

.                       NS      b.root-servers.net…
...
```

root.keys:

```
.       DNSKEY  257 3 8 AwEAAagAIKlVZrpC6I…
.       DNSKEY  257 3 8 AwEAAaz/tAm8yTn4M…
```

4. Implantación

Requisitos: Software

- Soporte de “validación DNSSEC”
  - Bind desde 2010 (9.7)
  - Unbound desde 1.4
  - Windows desde Server 2012
- Una línea de configuración (o 1 click)
  - dnssec-enable: yes

Requisitos: Hardware

- Operaciones criptográficas intensivas en CPU
- Uso de acelerador criptográfico HSM
- Servidores fabricados > 2005 tienen soporte suficiente de aceleración
  - Incluídos virtuales

Requisitos: Red

- Paquetes UDP más grandes
  - DNS original: 512 bytes
  - Actualizado en 1999 (EDNS0) hasta 64KB
- En la práctica ronda 1.500 bytes, se asume máximo 4K.
- DNS sobre TCP/53
- Revisar firewalls para
  - UDP grandes
  - UDP fragmentos (especialmente IPv6)

Requisitos: Red

¡No solo validando!

- Paquetes UD[illegible]P más gra[illegible]e[illegible]
  - DN[illegible] 51[illegible]2 b[illegible]
  - Ac[illegible]ua[illegible]z[illegible] e[illegible] 1[illegible]9[illegible] [illegible]KB
- [illegible] la pr[illegible]ic[illegible]nd[illegible]
  [illegible]s[illegible]r[illegible]e m[illegible] K.
- D[illegible] sob[illegible]e [illegible]CP/53
- Revisar firewalls para
  - UDP grandes
  - UDP fragmentos (especialmente IPv6)

"DNSSEC para ISPs"

Requisitos: checklist

Requisito	Check
Software soporta DNSSEC	
Bind versión 9.7 y superior	
Unbound versión 1.4 y superior	
Microsoft Windows Server 2012 y superior	
Servidores suficientemente modernos	
Redes pueden soportar DNSSEC	
DNS sobre TCP	
Permitir paquetes UDP grandes	

De “Deploying DNSSEC: Validation on recursive caching name servers” por SURFnet
https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_Deploying_DNSSEC_v20.pdf

Planificación

- Validar/obtener la llave de la raíz
  - https://www.iana.org/dnssec
  - Viene de paquete en software y/o OS
- Probar primero en 1 resolver
  - dig +dnssec @resolver www.nic.cl a
  - dig @resolver malo.vulcano.cl aaaa
- Informar a usuarios
  - “Extra protección en su navegación...”
  - “Cambio transparente...”

Operación

- Sincronización (NTP)
- Mantención de llave raíz
  - En rotación cada ~5 años (¡ahora!)
- Fallos de zonas importantes
  - “NTA”
  - Controversial y en desuso

Conclusiones

- Muy bajo costo
- Riesgos son mucho menores a los beneficios
  - al menos en el lado de la validación
- Empresas y organizaciones reportan menos de 2 semanas en desplegarlo
  - por supuesto depende de cada realidad

Enlaces útiles

- Estándar: RFC's 4033, 4034, 4035 y 5155
- Buena introducción:

  http://ispcolumn.isoc.org/2006-08/dnssec.html
- Portal ISOC - Deploy 360

  internetsociety.org/deploy360/dnssec/
- “Deploying DNSSEC: Validation on recursive caching name servers” - SURFnet
- Lista “DNS en español”
  - https://listas.nic.cl/mailman/listinfo/dns-esp
- ¿Estoy validando?

  https://en.internet.nl/
- ¿Acepto UDP grandes?

  https://www.dns-oarc.net/oarc/services/replysizetest

¡Gracias!

Hugo Salgado H.
Ingeniero de Proyectos NIC Chile
hsalgado@nic.cl
@huguei