



DNSSEC Signing at Scale on the Edge

Ólafur Guðmundsson

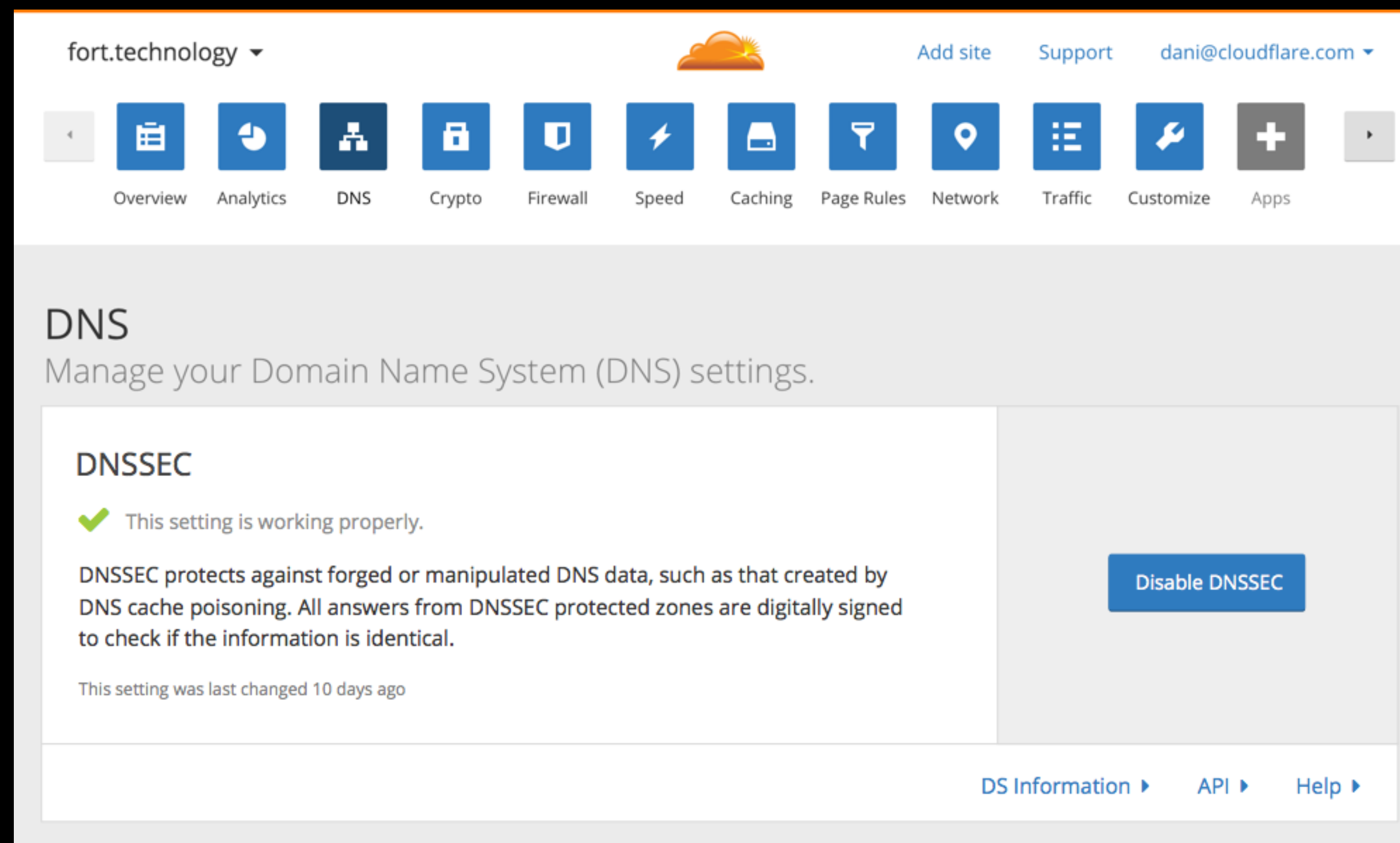
What we do: DNS

- Third party DNS operator for 2M+
- One of largest responders of DNS query traffic
- Largest dropper of DNS traffic in the world
- Operate large number of DNS servers at over 60 locations
- Custom DNS server developed in-house



DNSSEC launch

- Paid customers can enable it from user interface as of today
 - Soon Default on for all paid customers
- Use ECDSA P256 algorithm
 - speed and size
- Sign DNSKEY in central location
 - publish CDS/CDNSKEY as well
- All other RR's signed at the edge



fort.technology

Add site Support dani@cloudflare.com

Overview Analytics DNS Crypto Firewall Speed Caching Page Rules Network Traffic Customize Apps

DNS

Manage your Domain Name System (DNS) settings.

DNSSEC

✔ This setting is working properly.

DNSSEC protects against forged or manipulated DNS data, such as that created by DNS cache poisoning. All answers from DNSSEC protected zones are digitally signed to check if the information is identical.

This setting was last changed 10 days ago

Disable DNSSEC

[DS Information](#) [API](#) [Help](#)

Signing speed (and size): ECDSA P256

```
ietf.org. 1800 IN DNSKEY 256 3 5 AwEAAdDECajHaTjfSoNTY58WcBah1BxPKVIHBz4IfLjfqMvium4lgKtK ZLe97DgJ5/NQrNEGGQmr6fKv  
Uj67cfrZUojZ2cGRizVhgk0qZ9scaTVX NuXLM5Tw7VW0VIceeXAuuH2mPIiEV6MhJYUsW6dvmNsJ4XwCgNgroAmX hoMEiWEjBB+wjYZQ5GtZHBFKVXACSWTiCtddHcue0eSVPi5  
WH94Vlubh HfiytNPZLr0bhUCHT6k0tNE6phLoHnXWU+6vpsYpZ6GhMw/R9BFxW5Pd PFtWRgoWk2/XFVRSKG9Lr 61b2z1R126xeUwww46RVy3hanV3vN07LM5H niqaYc1Bbhk=  
ietf.org. 1800 IN DNSKEY 257 3 5 AwEAAaAjGkH8FE8A8E8GP0wQBFVLOEM9 BRfqxz9p/sZ+8AByyqFHLdZc Ho0GF7CgB50KYMvG0gysuYQ1  
oPlwbq7Ws5WywbutbXyG24lMwy4jij1J UsaFrS5EvUu4ydmuRc/TGnEXnN1XQK0+wa174CLtflcWjoY80qud6lD a Jdj1cKr2nX1NrmMRoWiu3DIVtGbQJmzpukpDVZaYMMAm8M5  
vz4U2vRCV ETLgDoQ7rhsiD127J8gVExj08B0113jCajbFRcMtUtFTjH4z7iXP2ZzD cXsgpe4LYEuenF0AcRBR1 E6oaykHR7r1Pqqmw58nIELJUFoMcb/BdRLg byTeurFlnxs=  
ietf.org. 1800 IN RRSIG DNSKEY 5128 00 20150422162528 42 ietf.org. 43650 45586 ietf.org. dp001u/mE0ZmcergtT4RA5DdV8E  
i3nTYvsuTFKqEou4Smku5Up01giVp sOpdDRwvei5g2HC8VK/nKHDhcoLNKzunawRvA5ynNgNrGAGSpXn5K0h2 I o/7yDr2TK529YHee0MTVeHqk6YeyyiFvCL1XMLt3jj4/G3pjo  
z7mS8M NLgysKQMEZqJHfZhARZeSNIuK/QpRJhBX9UQYrv6IJ/215WqdL6C6aeB fYe+bhn3G2s9apnUQFiq0xo3ybyQJm06UEPjuEnn8uLXnXT1RdthZbnY g5yZReSWb4jVYQKC  
yX4Pnm09TtrpduZQqz120v+8nMITf4HJnSj7EvPN AxmCXg==
```

**RSA:
1181 BYTES**

```
filippo.io. 3600 IN DNSKEY 257 3 13 DGpDkudNu/XQT1Km  
QkXFtKcfZPxFHGV07qSTIcDXS33/WtRSFEhiQVR53E69/E57IFm8b6Zw==  
filippo.io. 3600 IN DNSKEY 256 3 13 koPbw9wmYZ7ggcjn  
Q6ayHyhHaDNMYELKTqT+qRGrZp1C05LBhMmJZ115G1B3Azhii+sb0PYFkH1ruxLhe5g==  
filippo.io. 3600 IN RRSIG DNSKEY 13 2 3600 20150523  
162528 20150422162528 42 filippo.io. 1774 1774 1774 1774 +grfGMuA2a1/vQ9S5tBX0Jq  
ZbeTOYB0hfHG7S16hqR1 xfo1bSJA1B1X5r9Ujo5YVU/NE1H0TQ==
```

**ECDSA:
305 BYTES
and faster**

Minimal non-existent answers: “Black Lies”

- Our solution: true lies. sign a NOERROR.
- Generate a NSEC for the query name, cover minimal span, only set the NSEC and RRSIG bits ==> NXDOMAIN

```
missing.filippo.io.      3587      IN        NSEC      \003.missing.filippo.io. RRSIG NSEC
missing.filippo.io.      3587      IN        RRSIG     NSEC 13 3 3600 20150507190048 201505
05170048 35273 filippo.io. Fb/xInfArVCMJWBDBqsbBPxiKsC1ueUyBFGi5lAHbjRBGAGm8sKDJx/l
YA01bKYzJep3dRgQw5hS89JukD+m8w==
```

Quick negative's: the "NSEC shotgun"

- DNS Server optimized for answering exact query
- Query for TXT and there's no TXT?
 - Set all the other bits that might exist.
- The NSEC is a valid denial for TXT, and is useless for an attacker that wants to replay it for other queries.

```
filippo.io. 3600 IN NSEC \003.filippo.io. A NS SOA WKS  
HINFO MX TXT AAAA LOC SRV CERT SSHFP IPSECKEY RRSIG  
NSEC DNSKEY TLSA HIP OPENPGPKEY SPF
```

How expensive is online signing ?

- Minimal impact
 - We have highly optimized code
 - Cutting down on number of NSEC records helps
 - Reuse signed SOA
- Key Distribution
 - You must trust your servers and have secure software distribution and boot

Our Challenge

- Required new systems
 - Central signer
 - DNSSEC health check ==> if DS is configured correctly
- Changes affected many systems we have deployed
 - DNS servers, DB, UI, secure boot,
- Supporting TLSA
 - Coming soon
- Uploading and maintaining DS records for customers

DNSSEC's MAIN ROADBLOCK

- Registration System is out of touch with reality!!
- Need an easy way to update Parent
 - CDS/CDNSKEY publication is sufficient statement of intent!
 - Working with registrars and registers to enable DNSSEC at scale
 - will offer DNSSEC to free customers were we can update DS at parent
- CDS/CDNSKEY needs delete mode