Challenges and Successes of DNSSEC Signing an F5 BIG-IP DNS Hosted Zone

Neda Kianpour - Lead Network Engineer - Salesforce

Tyler Shaw - Sr. Systems Engineer - F5

Abstract

- Due to compliance requirements from our customers, determined to sign the whole footprint and that involved signing the BIG-IP DNS hosted zones.
- The BIG-IP DNS devices in our infrastructure listen and respond to DNS queries to the zones hosted on them.
- Signing the BIG-IP DNS hosted zones had its own challenges.
- Only Two Engineering Hotfixes later and plenty of testing and now DNSSEC can be deployed on the BIG-IP DNS devices.

Challenges

1. Signature Inception Offset Issue
2. F5 BIG-IP DNSSEC vulnerability
3. Master Key changes on an F5 BIG-IP DNS (code upgrades, RMAs,etc)
4. ECDSA support (Algorithm 13) - (Feature Request Submitted)
5. Implementing DNSSEC on Active/Active standalone BIG-IP DNS

1. Signature Inception Offset

- After implementing DNSSEC on our F5 BIG-IP DNS, we noticed that every time we queried an F5 hosted zone, **the signature inception date returned was set to 0 seconds in the past.**

- Certain resolvers could treat the zones as invalid due to **clock skew**.
  - **Major impact to clients behind those resolvers (bogus responses).**

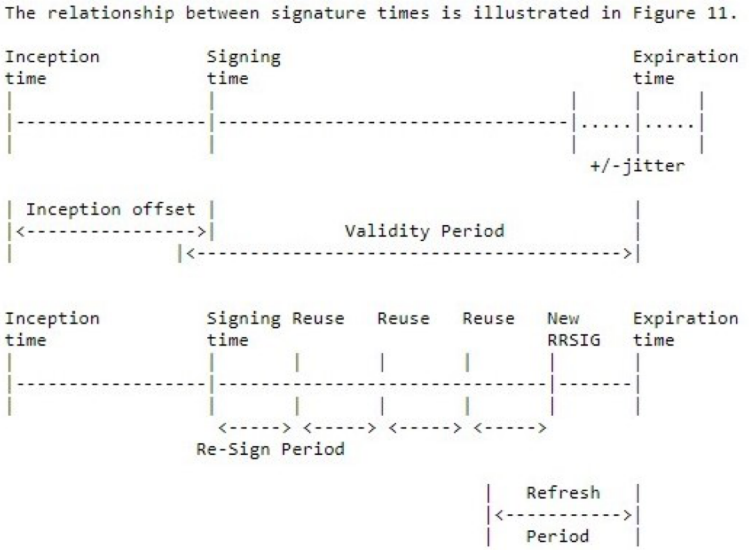
```
$ date && dig na107.inst.siteforce.com A +dnssec  | grep RRSIG
Sat 23 Mar 2019 19:37:42 GMT
na107-hio.hio.r.inst.siteforce.com. 30 IN RRSIG   A 8 6 30 20190330193742 20190323193742

$ date && dig na107.inst.siteforce.com A +dnssec  | grep RRSIG
Sat 23 Mar 2019 19:38:17 GMT
na107-hio.hio.r.inst.siteforce.com. 30 IN RRSIG       A 8 6 30 20190330193817 20190323193817 57048
```

1. Signature Inception Offset (continued)

RFC 6781 allows a parameter called the **inception offset:**

"The validity of the signature starts shortly before the signing time. That is done to deal with validators that might have some clock skew. This is called the inception offset, and it should be chosen so that false negatives are minimized to a reasonable level."



1. Signature Inception Offset (continued)

- A feature request was made with F5 to add inception offset.
- New code now sets the inception offset for the DNSSEC signatures to a configured time before the signature creation (default of 60 mins).
- This is available in Version 15.1 due approximately Q1 2020, but can be backported as far as version 12.1.X
  Bug ID 767989 should be referenced if needed in versions earlier than 15.1

2. F5 BIG-IP DNSSEC vulnerability

- July 2019: **CZ.NIC**(Petr Špaček and Jan Vcelak of **NS1**) published this article Error-in-dnssec-implementation-on-f5-big-ip-load-balancers about the issue. Can be exploited to **perform a denial-of-service (DoS)**.

- **ISSUE**: F5 returns an **incorrect NSEC3 record** for a DNS query for an RR type, which does not exist at given name.
  - This indicates that only one of TXT/HINFO/RP RR types exists at given name, even if A or AAAA types actually exist and are returned if a client queried for them.
- **IMPACT**: If resolver uses Aggressive Negative caching it can incorrectly infer non-existence of other record types at the NSEC3 record name

2. F5 BIG-IP DNSSEC vulnerability

- Aug 2019: F5 team acknowledged and published a KB advising of the following workaround: https://support.f5.com/csp/article/K00724442
- After discussions with the F5 team, they provided us with a permanent fix in a form of **Engineering Hotfix**.

3. Master Key changes on an F5 BIG-IP DNS

- BIG-IP DNS devices that are configured with DNSSEC use **their own master key** to decrypt the DNSSEC keys.

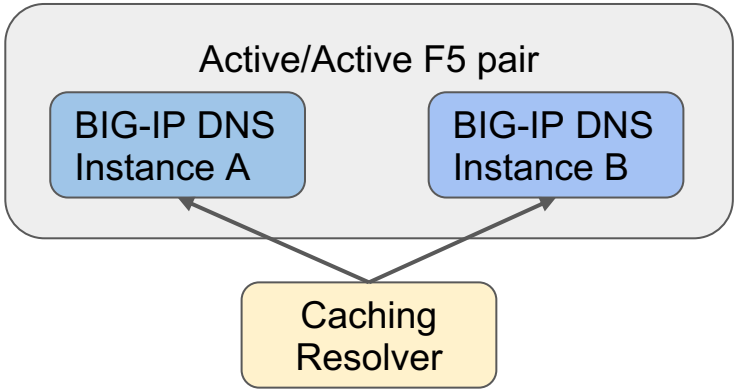
- **ISSUE**: We observed an issue where after a code upgrade, the BIG-IP DNS device **fails to load the configuration due to a master key change**.
  - That results in a DNSSEC Key set to also fail to decrypt!!

- **CURRENT WORKAROUND:** User has **to manually take a copy** of the master key prior to any code upgrade and **manually use this key** to restore the configuration file in case of a master key change.
  - https://support.f5.com/csp/article/K13542

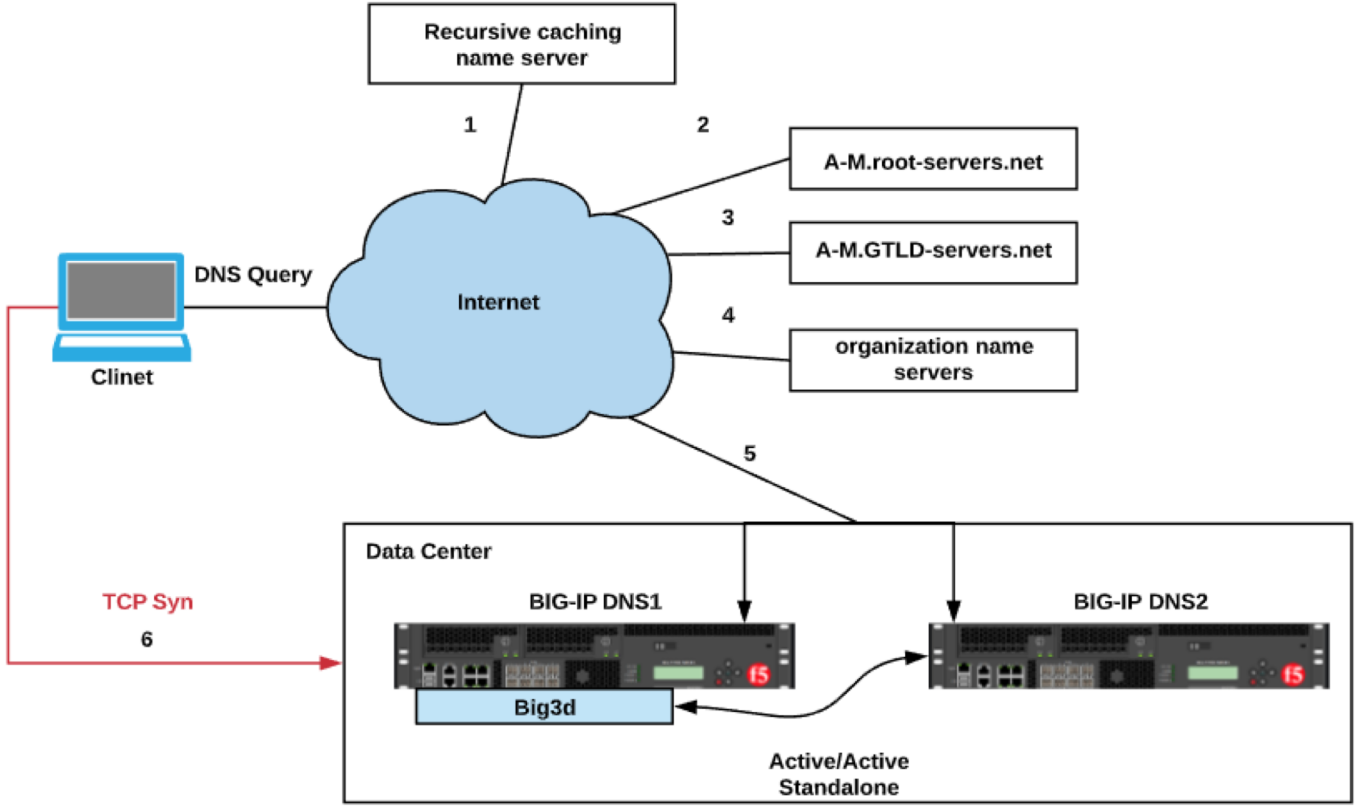
4. ECDSA support (Algorithm 13)

- We have officially requested code support for the Elliptic Curve Digital Signature Algorithm on the F5 BIG-IP DNS.
- F5 has indicated that this will be available in TMOS V15.1 with the current ETA being calendar Q1 of 2020.
- Backport to the previous version of TMOS ie V12.1.x and v13.1.x will not be possible.
- RFE ID 672374 was already filed by another F5 customer
- F5 has attached our request to RFE

5. Implementing DNSSEC on Active/Active standalone BIG-IP DNS



- This is analogous to a multi-signer DNSSEC model using **unique key sets**:
  - Two signing entities must **SHARE the ZSK** for a chain of trust to exist
- Without this, responses from different entities could be treated as bogus
- 'Normal' active/active config cannot support this key sharing, **but can be done using DNS sync group in active/active**


Recursive caching name server
1
2
A-M.root-servers.net
3
A-M.GTLD-servers.net
4
organization name servers
DNS Query
Internet
Clinet
5
Data Center
TCP Syn
6
BIG-IP DNS1
BIG-IP DNS2
Big3d
Active/Active
Standalone

questions?

Thank you!