efficient iP™
DEFINING SMART DDI

DNS Attacks:
Can we still afford using
Old, ineffective solutions?

Nicolas CARTRON <nc@efficientip.com>

RIPE69 – London

November 6th, 2014

Goal of this presentation

- **What is it about ?**
  - More and more attacks targeting DNS
  - Still very few done / invested
- **But there are existing and solid technics !**
  - To secure DNS
  - Simplify the DNS administration
  - Not necessarily complex to implement

Agenda

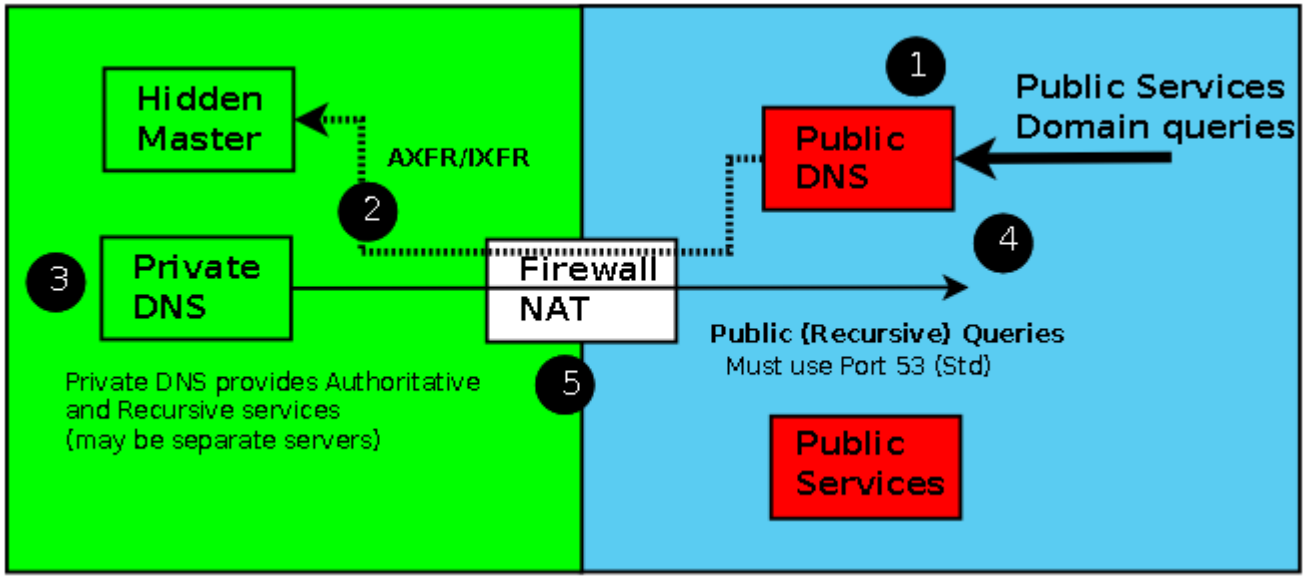
- **Stealth DNS**
- **Life without 0-Day**
- **DDoS Attacks**
- **RPZ**

Stealth DNS

Deploy a Stealth DNS Architecture

What is it ?

- Hidden Master server
- One Slave server is chosen to be the Pseudo-Master, and will be the NS configured as MNAME of the SOA
- Only the Pseudo-Master and Slaves are NS



Deploy a Stealth DNS Architecture

- **Challenges**
  - More complex to deploy and maintain
  - No mistake can be done, otherwise the interest of using Stealth is lost!
- **Pros**
  - Master DNS server is not visible : improved security
  - Conform to public-facing DNS best practices

Zero-Day vulnerabilities

Single DNS Engine: Strengths & Weaknesses

Disclaimer: this part is NOT about bashing BIND! :)

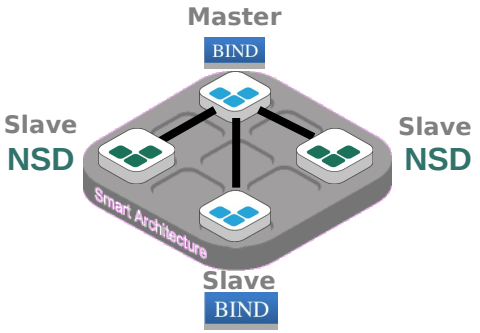
- **BIND is the Most Popular & Widely Deployed DNS Engine**
  - Very flexible, implements (almost) any RFC
  - De facto a “standard”
- **Security Risks**
  - Authoritative and recursive are not separated
  - Popular = targeted by attacks
- **What are you doing when a 0-day vuln is disclosed?**
  - Monitoring (even more) your DNS servers?
  - Cross you fingers until a patch is available?

Deploy several DNS engines

For instance :

ISC BIND for Authoritative DNS and Cache,
NSD (NLnet Labs) or KnotDNS (nic.cz) for Authoritative DNS,
Unbound (NLnet Labs) for Cache.

- **Challenges:**
  - Several different configurations to maintain
  - Several softwares to maintain / patch



- **Pros :**
  - Mitigate Zero-Day vulnerabilities
  - Eliminate SPoF

DDoS Attacks:
DNS servers should be more efficient

What can be done to face a DDoS ?

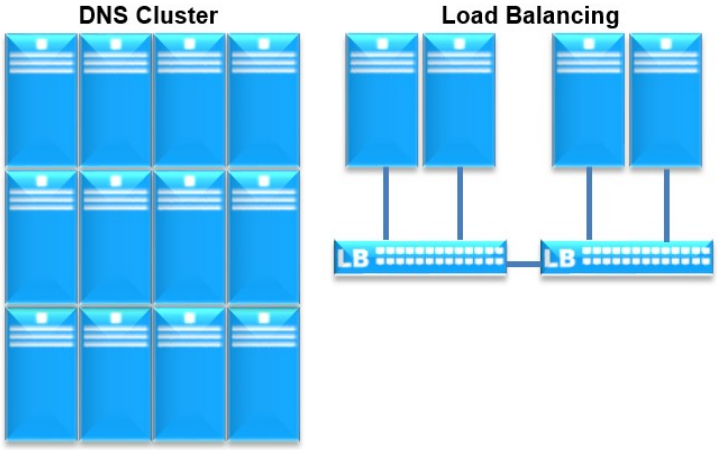
Tactic #1 : filter

- Filter : yes, but how?
  - Manually ? By using thresholds ? Heuristics ?
- Filter does not solve the problem of congestion
  - Traffic still enters the network !

Tactic #2 : Absorb

- Requires a specific architecture
- RRL (Response Rate Limit) mandatory to not be used for DDoS

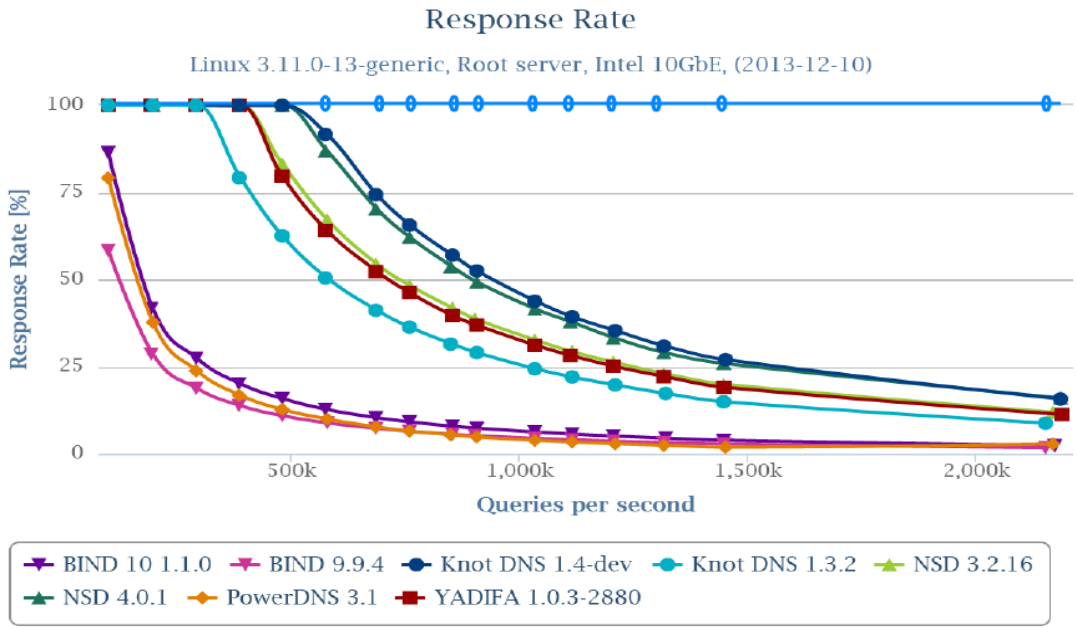
2 ways to absorb



1) Pile up DNS servers and Load Balancers to absorb the load increase

- **=> Not scalable: Individual Server Crash**
  => Deployment and management complex

How many servers/load balancers do you have to pile up to absorb 40 Gb/sec?

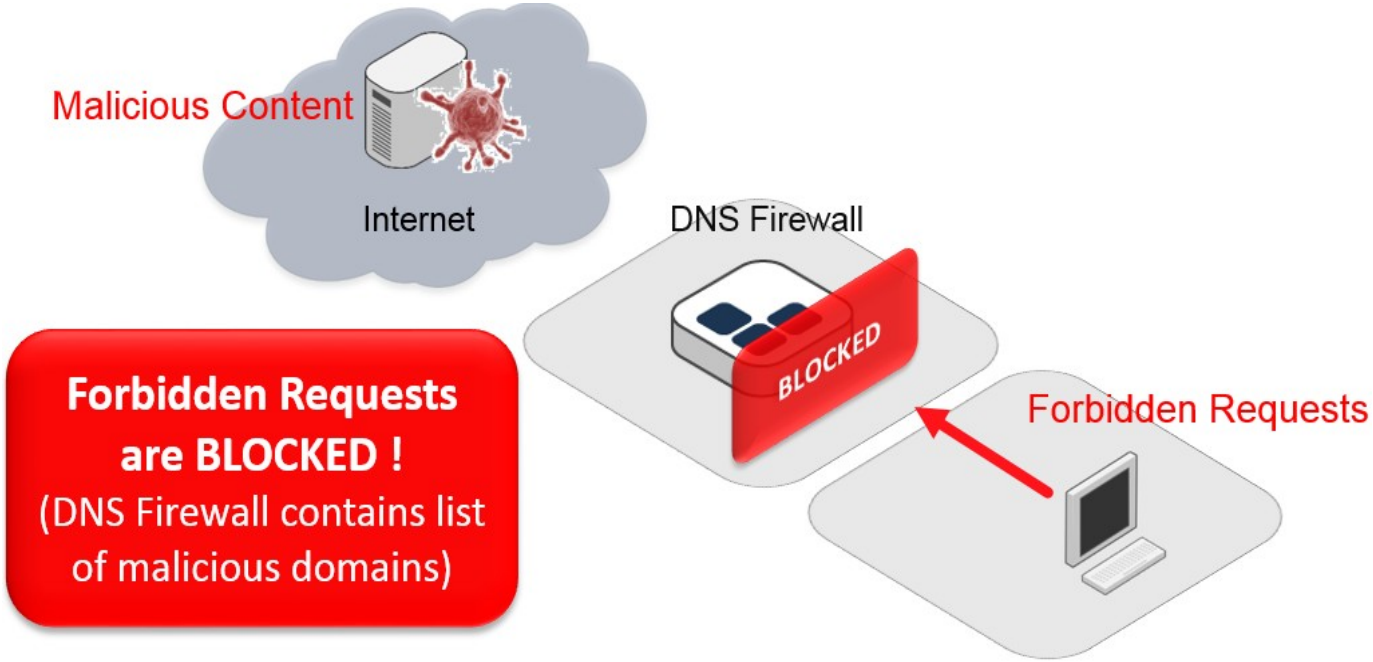


2) Deploy more efficient DNS engines/servers

RPZ

Protect Against DNS Based Malware

- DNS Firewall - or Response Policy Zone (RPZ)
  - Filters for DNS queries to malicious sites
  - Block communications with Command & Control Servers
  - Help identify infected client workstations



Policies of DNS Firewall

- Policy Driven RPZ Rules
  - REDIRECT to Walled Garden or Honeypot
  - NODATA Response to DNS queries
  - NXDOMAIN or Denial of Existence Response
  - PASSTHRU that allows response but tracks

```
; Language-enforcement policy: no access to Wikipedia except the
; French-speaking one
wikipedia.org           CNAME .
*.wikipedia.org           CNAME .
; and the exception:
fr.wikipedia.org         CNAME fr.wikipedia.org.
```

- Updating Malicious Black List
  - Filter by creating RRs (A, AAAA, CNAME) for each domain or IP address
  - Subscription to an external feed: anti-spam, anti-phishing and anti-malware

RPZ?

- **Challenges**
  - « Lying » DNS
  - Breaks DNSSEC
  - Increases the load on the DNS (each request must be evaluated)
- **Pros**
  - More granular than using a zone with a wildcard 127.0.0.1 !
  - Several policies available (NXDOMAIN, redirection, ...)

CONCLUSION

Usages and attacks will stress DNS more and more

Change your approach
“Linux/BIND/Master-Slave!!!” :-)

QUESTIONS?

Contact:

Nicolas Cartron <nc@efficientip.com>
http://www.efficientip.com
Twitter: @efficientip