



DNS Update

FRnOG 23



Agenda

- **Stealth DNS**
- **Life without 0-day**
- **DDoS – les serveurs DNS devraient être plus performants**
- **Qu'est ce que RPZ ?**

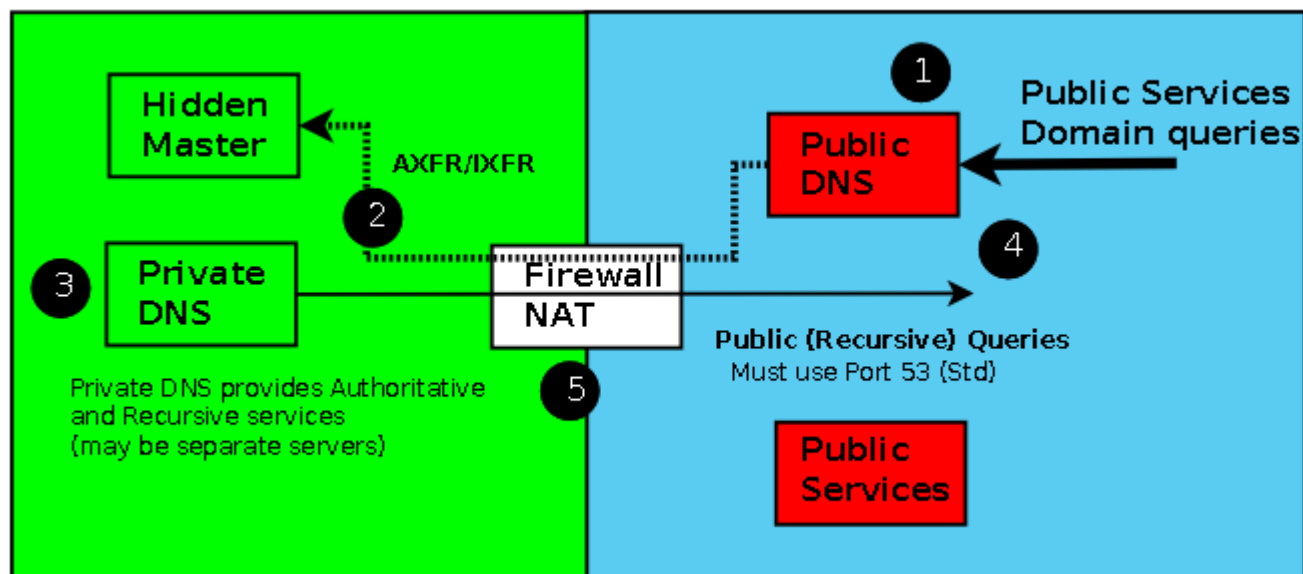


Stealth DNS

Deployer une architecture Stealth DNS

■ Qu'est-ce donc ?

- Un DNS master caché
- Un serveur Slave choisi comme Pseudo-Master
- Seuls le Pseudo-Master et les Slaves sont NS



Deployer une architecture Stealth DNS

■ Avantages

- Le serveur DNS maitre n'est pas visible : sécurité renforcée
- Conforme aux bonnes pratiques pour le DNS public

■ Challenges

- Architecture plus complexe à déployer et à maintenir
- Il ne faut pas faire d'erreur, sinon on perd tout l'intérêt du Stealth !

Vulnerabilités Zero-Day

Utiliseur un seul moteur DNS: forces et faiblesses

- **BIND est le moteur DNS le plus populaire et le plus déployé**
 - Très flexible, intègre (quasi) toutes les RFCs
 - C'est un “Standard”
- **Risques de sécurité**
 - Authoritative et Recursif pas séparés
 - Populaire = ciblé par les attaques
- **Que faites-vous quand une faille Zero-day BIND est publiée ?**
 - Vous monitorerez (encore plus?) vos serveurs DNS ?
 - Vous croisez les doigts jusqu'à ce qu'un patch soit disponible ?

Déployer plusieurs moteurs DNS

Par exemple :

ISC BIND pour le DNS Authoritative et Cache

NSD (NLnet Labs) ou KnotDNS pour le DNS Authoritative

Unbound (NLnet Labs) pour le DNS Cache

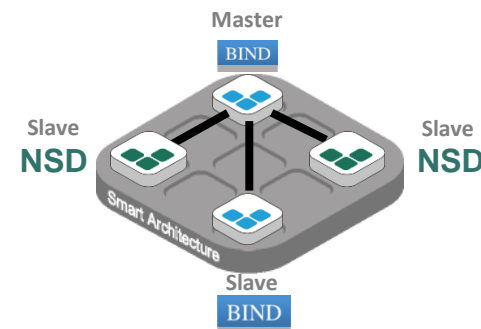


Avantages :

- Mitiger les vulnérabilités 0-day
- Eliminer le SpoF

Challenges:

- Plusieurs configurations différentes à maintenir
- Plusieurs logiciels à maintenir / patcher





Attaques DDoS: Les serveurs DNS devraient être plus performants

Que faire face à un DDoS ?

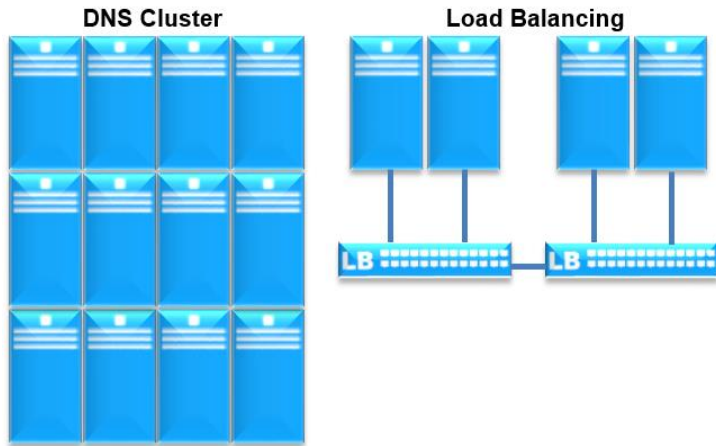
■ Tactique #1 : Filtrer

- Filtrer oui, mais comment ?
 - Manuellement ? Avec des seuils ? Des heuristiques ?
- Filtrer ne résoud pas le problème d'engorgement
 - Le trafic arrive quand même sur le reseau !

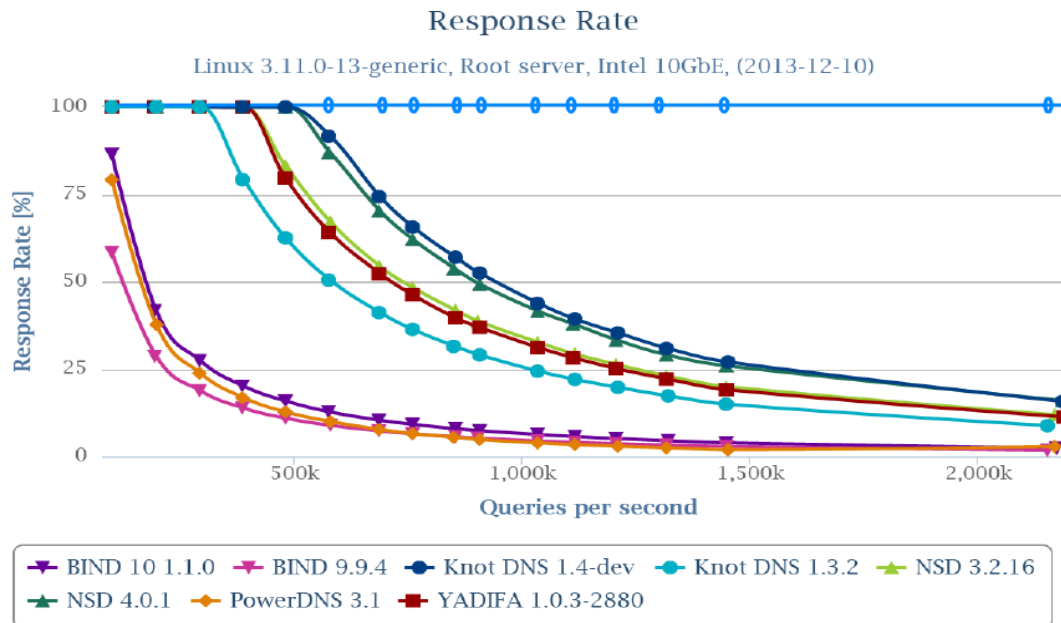
■ Tactique #2 : Absorber

- Nécessite une architecture adaptée
- RRL (Response Rate Limit) obligatoire pour ne pas être utilisé pour amplification

2 facons d'absorber



- 1) Empiler des serveur DNS et des Load Balancers
- Déploiement et gestion complexes
 - Evolutivité limitée

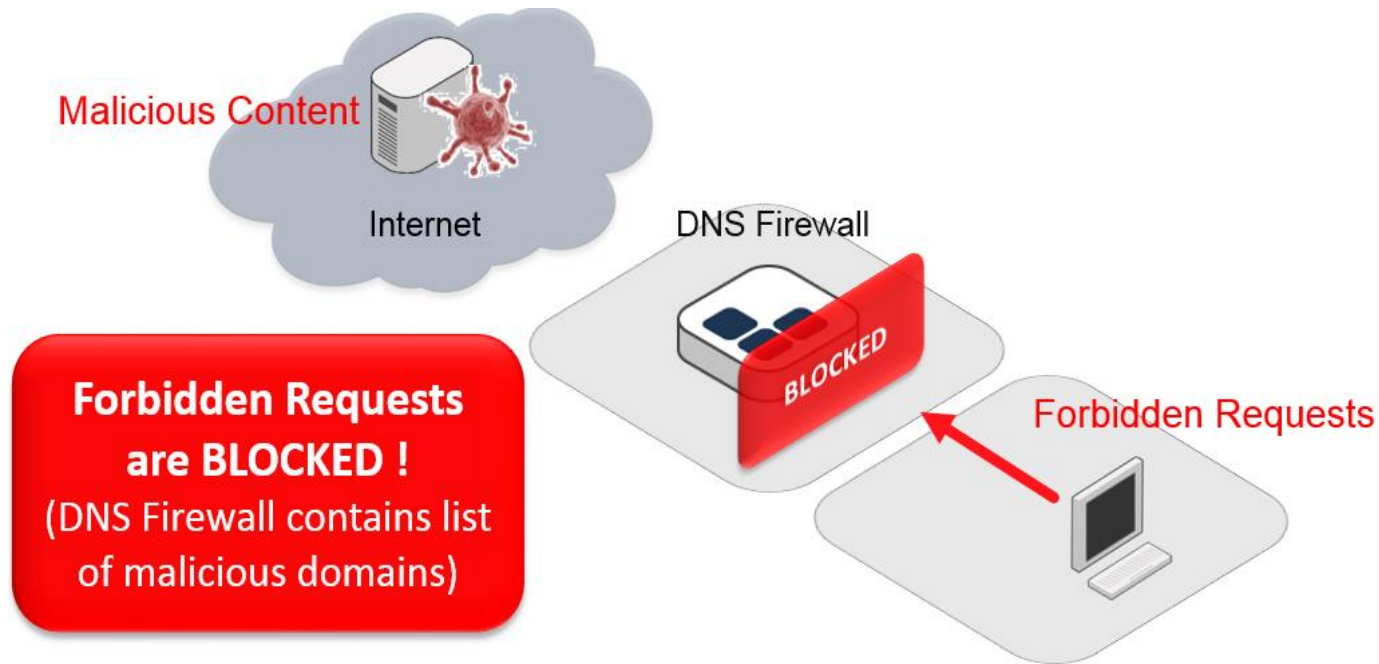


- 2) Déployer des serveur DNS plus performants

RPZ ?

Protection contre les malwares utilisant DNS

- DNS Firewall ou Response Policy Zone (RPZ)
 - Filtre les requetes DNS vers les sites malicieux
 - Bloque les communications avec les serveurs C&C (Command & Control)
 - Permet d'identifier les équipements infectés



DNS Firewall : politiques

- Les règles RPZ utilisent des “Policies”
 - REDIRECT: rediriger (vers un Honeypot par exemple)
 - NXDOMAIN: or Denial of Existence Response
 - NODATA: Response to DNS queries
 - PASSTHRU: laisser passer mais loggue

```
; 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.
```

- Il est possible d'utiliser des “Black List”
 - Filtrage par creation de RR (A, AAAA, CNAME) pour chaque domaine ou adresse IP
 - Abonnement à un flux externe: anti-spam, anti-phishing et anti-malware.

RPZ ?

■ Avantages

- Plus fin que la création de zone avec wildcard 127.0.0.1 !
- Plusieurs politiques disponibles (NXDOMAIN, redirection, ...)

■ Challenges

- DNS «Menteur»
- Augmente la charge sur le DNS (chaque requête doit être évaluée)

CONCLUSION

Les usages et les attaques vont solliciter de plus en plus le DNS.



Changez de modèle Linux/BIND/Master-Slave ! 😊

QUESTIONS ?



Contact:

Nicolas Cartron <nc@efficientip.com>

<http://www.efficientip.com>

Twitter: @efficientip