DNSwitness: A Generic Platform For DNS-based Measurements

Journée « Mesures Internet », Paris, 24 April 2012

{Samia.Mtimet, Stephane.Bortzmeyer, Mohsen.Souissi} (at) afnic.fr

Overview

- **Motivation**
- **Principles & Requirements**
- **Architecture**
- **Past & Current Uses**
- **Some results**
- **Conclusion & Prospective work**

afnic

Motivation

- ✓ DNS registry is seated on a “gold mine” of DNS data
- ✓ What does DNS tell us?
  - ✓ There is precious information to extract and use
  - ✓ Our marketing team, technical team, management ask various questions we may have the answer for:
    - ✓ “How many of our domains are used for e-mail only?
    - ✓ What has the penetration rate of IPv6, DNSSEC or *phenomenon X* evolved over the last N years?
    - ✓ Could you assess the technical quality of a given portfolio of DNS zones?
- ✓ We focus on things that we can obtain by starting with the DNS
  - ✓ Either from the DNS itself
  - ✓ Or by further exploring

afnic

Principles & Requirements

- ✓ Generic
  - ✓ Can do many different surveys
  - ✓ Most known tools deal only with one survey
- ✓ Automatic
  - ✓ Works unattended (from cron, for instance), for periodic runs,
- ✓ Store raw results
  - ✓ Not just aggregates
  - ✓ For long-term analysis
- ✓ Free Software
- ✓ Usable by small and medium actors
  - ✓ ***Run it yourself***, and keep your own data, share aggregated & anonymized results
  - ✓ No data to be sent to a centralized analysis fabric

afnic

Global Architecture

- ✓ DNSwitness Platform: **2 main** (free) software **components**
  - ✓ **DNSdelve, for active measurement**
    - ✓ What we send out : active DNS queries sent to domains
    - ✓ *“Go on a fishing trip!”*
    - ✓ Typically: **sampling** in a zone TLD file vs **comprehensive walk**
  - ✓ **DNSmezzo, for passive measurement**
    - ✓ What comes in: DNS queries sent name servers, passively monitored
    - ✓ *“Who’s knocking at our door?”*
    - ✓ Sampling by default (might take all the traffic for a given window of time)

- ✓ **A database** to store results
  - ✓ To allow **long-term** surveys and study the **evolution**
  - ✓ To do **benchmark** with other partners based on **uniform indicators/metrics**

afnic

Architecture: Active Measurements Component (DNSdelve)

- ✓ A framework
  - ✓ To gather information from the DNS zones delegated by a registry
  - ✓ To get start points to explore the Internet for further information

- ✓ Composed of
  - ✓ A generic basis:
    - ✓ Handles zone file parsing and parallel querying of the zones
  - ✓ Modules dedicated for targeted surveys:
    - ✓ Perform the actual queries: ask explicit questions to the DNS
    - ✓ Examples: IPv6, DNSSEC, SPF modules already available

afnic

Architecture: Passive Measurements Component (DNSmezzo)

- ✓ Capture DNS traffic, analyze content and store in a Database
  - ✓ By sniffing the DNS traffic on a server (port mirroring, tcpdump…)
  - ✓ Storing structured info (what we have learnt) in a rDBMS

- ✓ Do measurements/statistics by querying the DB
  - ✓ Periodically, unattended or on-demand runs
  - ✓ Examples:
    - ✓ Top N domains queried for (and more specifically those which yield a NXDOMAIN answer)
    - ✓ Percentage of queries targeting AAAA (wrt A) records
    - ✓ Percentage of traffic transported on IPv6 (wrt IPv4)
    - ✓ How many queries use EDNS0 and for which sizes?
    - ✓ Percentage of recursive name servers patched against Kaminsky attack (SPR)

afnic

Similar Work (DNS-based)

- ✓ Active measurements
  - ✓ “The Health of the Internet in Sweden” (annual reports): https://www.iis.se/en/internet-for-alla/halsolaget

- ✓ Passive Measurements:
  - ✓ IIS.se dns2db http://opensource.iis.se/trac/dns2db
  - ✓ ISC SIE https://sie.isc.org/
  - ✓ DSC http://dns.measurement-factory.com/tools/dsc/

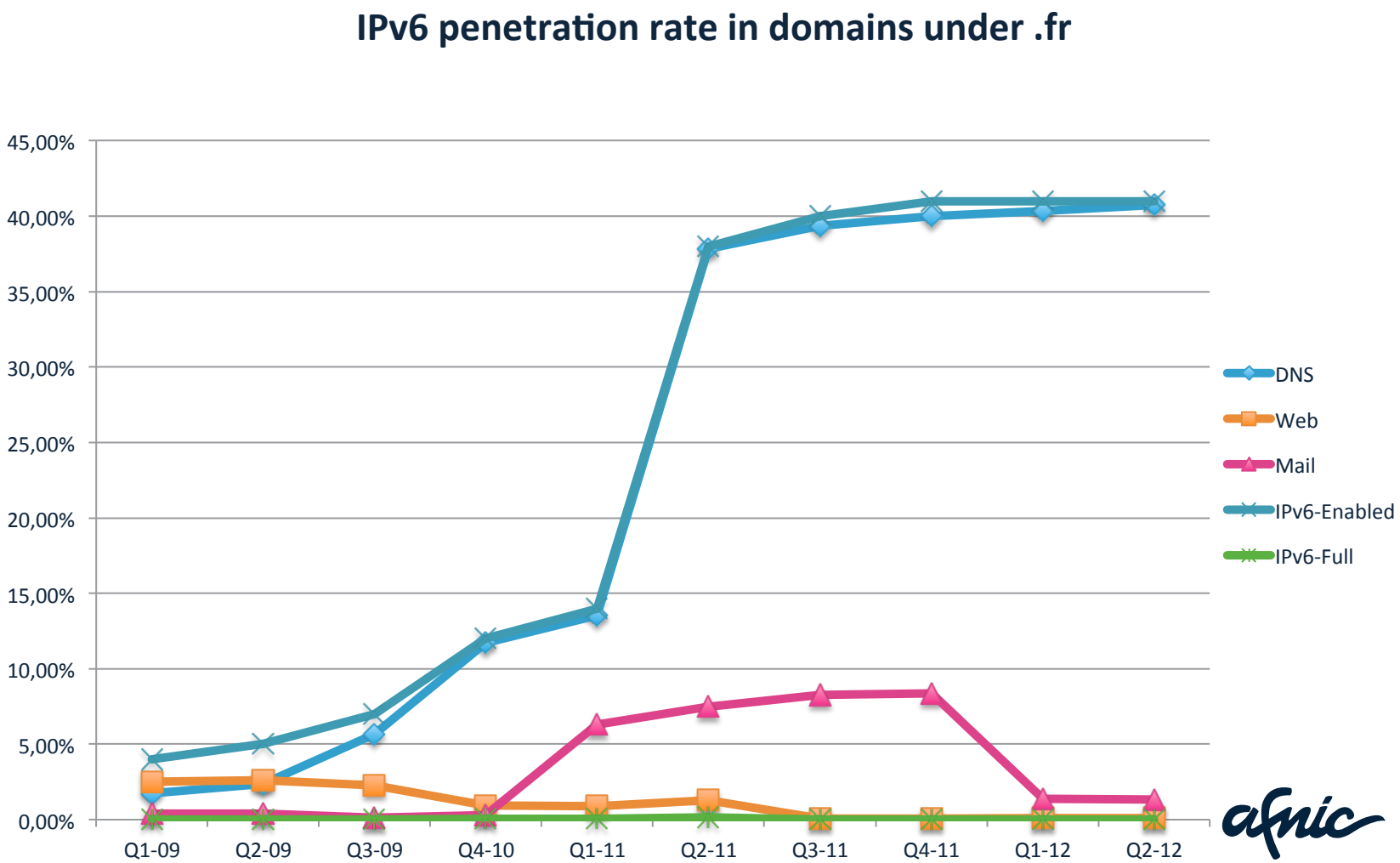
afnic

Past & Current DNSwitness Uses

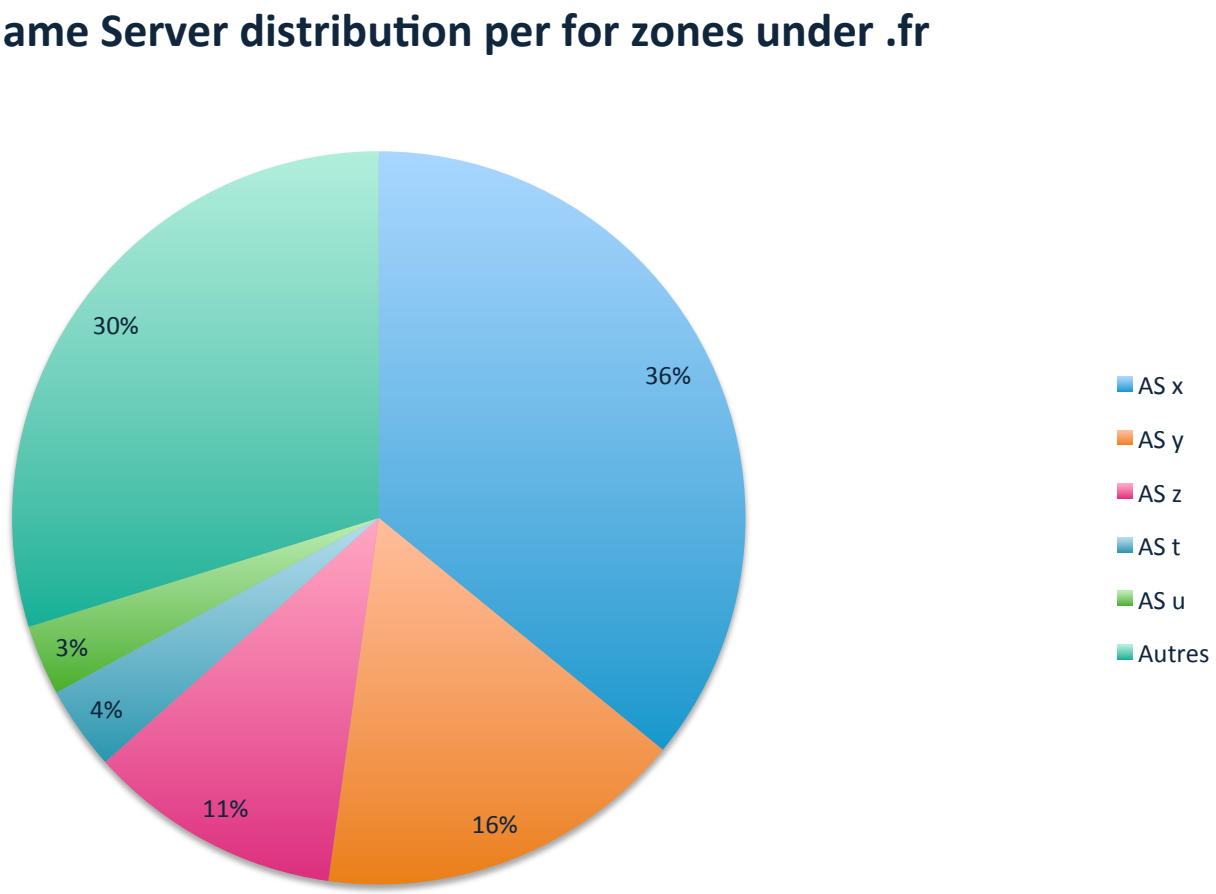
- ✓ Feeding the French Annual DNS Industry Report with IPv6 figures
  - ✓ http://www.afnic.fr/fr/ressources/publications/observatoire-du-marche-des-noms-de-domaine-en-france-3.html
- ✓ Contribution to the OECD Report on IPv6 Deployment Measurements in the world
  - ✓ http://www.oecd.org/dataoecd/48/51/44953210.pdf
- ✓ As a platform for Internet Resilience measurements in France
  - ✓ "Observatoire de la Résilience de l'Internet en France"
  - ✓ Jointly with ANSSI (the French Network and Information Security Agency)
  - ✓ AFNIC's contribution: from the DNS perspective
  - ✓ Results unveiled at the DNS-OARC meeting (while waiting for the 1st edition of the report to be published): https://www.dns-oarc.net/files/workshop-201203/OARC-London-2012.pdf
- ✓ Surveys on demand (AFNIC or third parties)

afnic

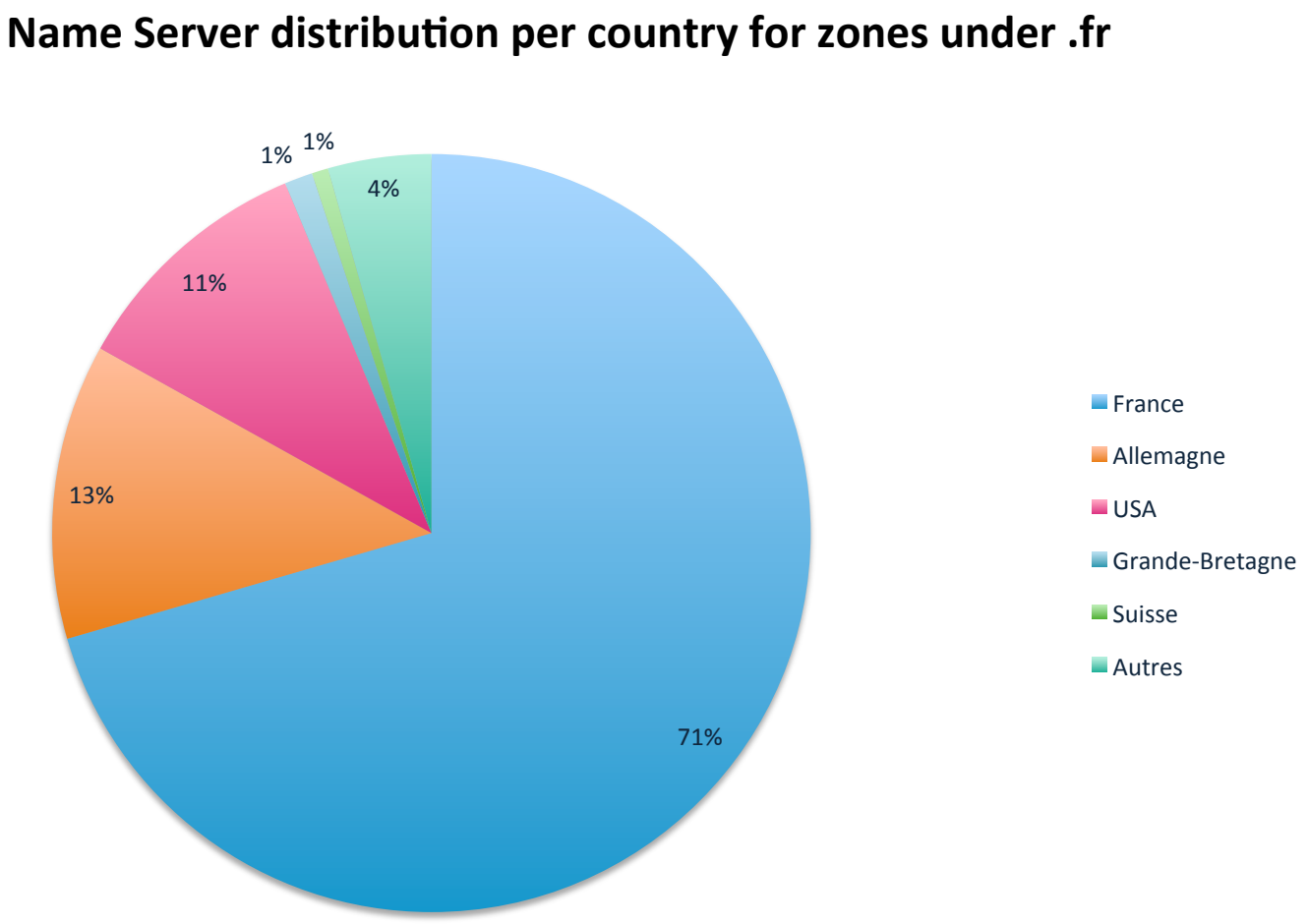
Active measurements results



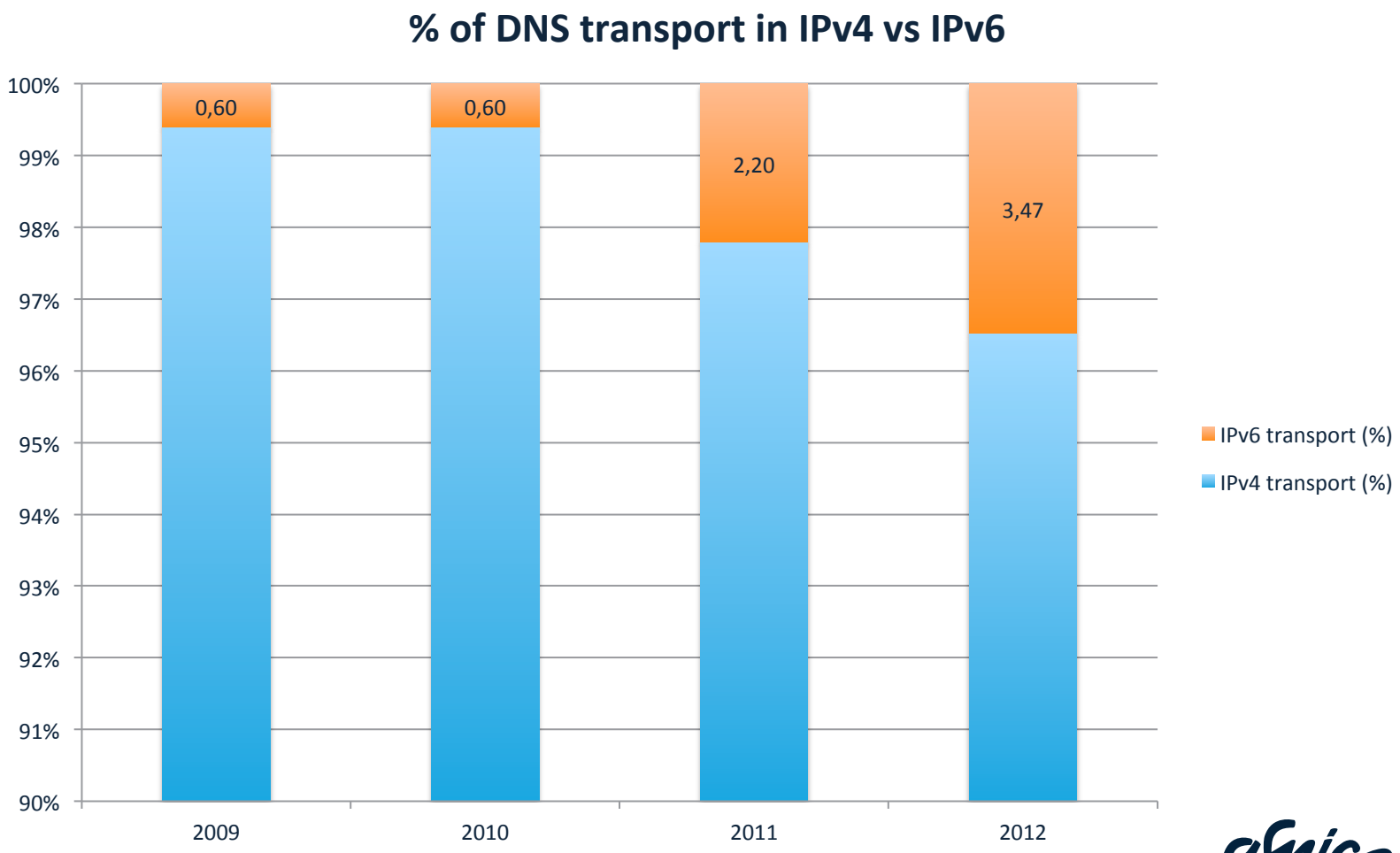
Active measurements results (2)



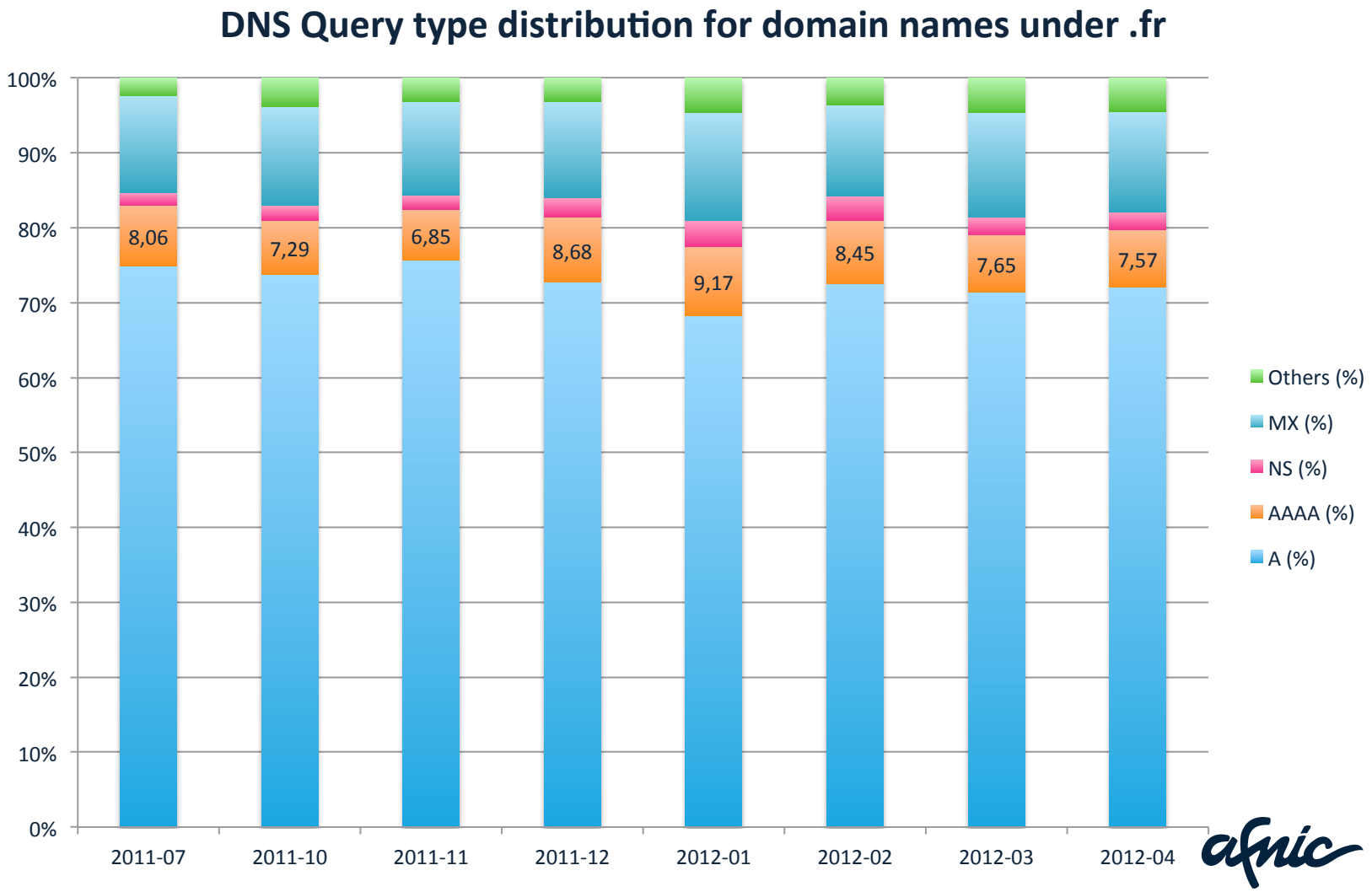
Active measurements results (3)



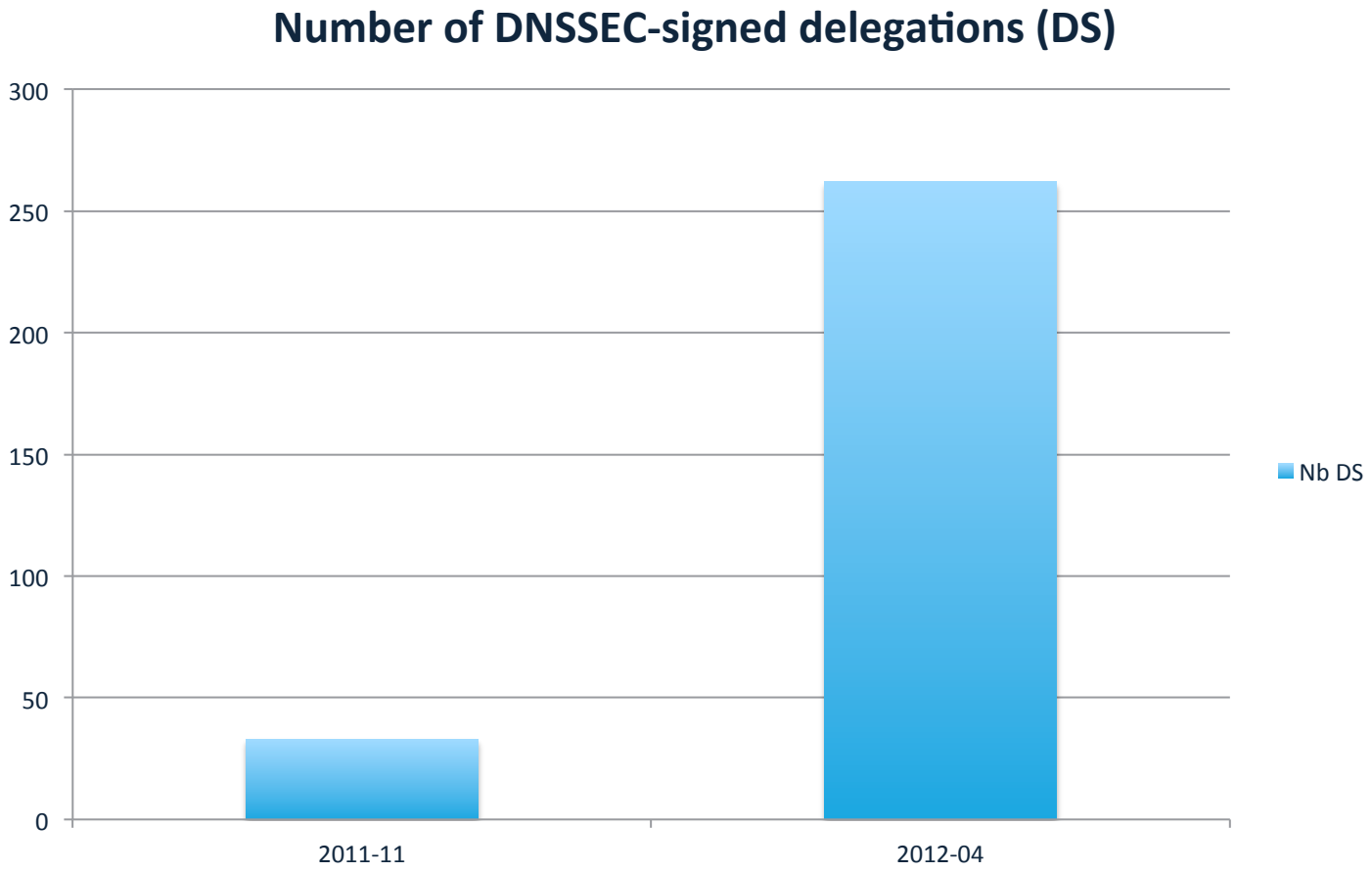
Passive measurements results



Passive measurements results (2)



Passive measurements results (3)



Conclusion & Prospective Work

- ✓ DNSwitness is a generic measurements platform used in different contexts for different needs
  - ✓ It has served multiple purposes so far
  - ✓ The platform is running in production at AFNIC premises

- ✓ Will evolve continuously in order to answer new needs
  - ✓ Collaboration with researchers
    - ✓ Define metrics and get periodic measurements
    - ✓ Put together results and get a joint analysis activity for a complete and long-term view
  - ✓ New developments for:
    - ✓ Additional resilience indicators measurements
    - ✓ Additional services penetration rate measurements
    - ✓ Added-value services for AFNIC and third parties

afnic

Merci !

www.afnic.fr
contact@afnic.fr
Twitter : @AFNIC
Facebook : afnic.fr