RPZ : Gérer la BYOD

Fabrice Prigent

Université Toulouse 1 Capitole

Mardi 16 Décembre 2014

L'UT1 : contexte général

- L'UT1 est un établissement très fortement centralisé,
- Droit, gestion, économie,
- 20000 étudiants,
- Forte consommation de Iphone, Imac, Ipad, Ipod

*Et de **I**-neken*

L'UT1 : contexte technique

- Les éléments de sécurité "standard" sont installés
  - Firewall (Iptables),
  - Régulation de bande passante (tc),
  - IDS (Snort),
  - Proxy filtrant,transparent ou non (Squid + Squidguard),
  - Journalisation des communications (Argus),
  - Portail captif (univ-nautes),
  - Eduroam.
- 25 To de données échangées par mois.

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Une situation qui se dégrade

- 70% de nos utilisateurs ne passent pas par les proxies, malgré
  - le DHCP (wpad-url, code 252),
  - le DNS (wpad, et wpad.ut-capitole.fr),
  - la page d'accueil du portail captif,
  - les affiches,
  - les vacataires WiFi.

Et comment fais-tu pour qu'ils comprennent ?
Des explications, des schémas, une écoute.

Et s'ils ne comprennent toujours pas ?
Des baffes !

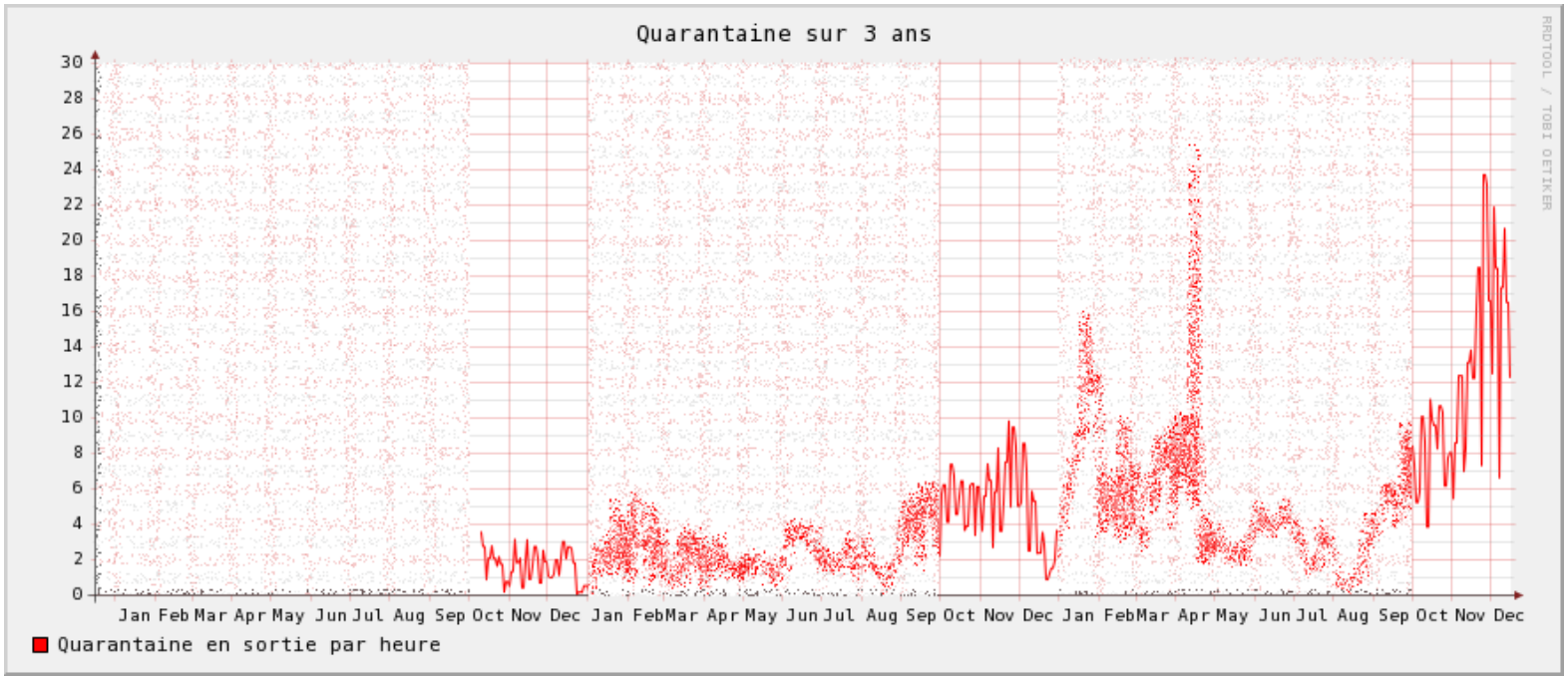
Une situation qui se dégrade

- 35% de requêtes en SSL,
- Un proxy-cache qui peine à justifier son intérêt,
- Les 20 colloques annuels, avec leurs 200-1200 chercheurs étrangers, deviennent une priorité.
- Des machines sur lesquelles on ne peut rien contrôler,
- Des malware à ne plus savoir qu'en faire,
- Bref du BYOD, du vrai, du pur, du tatoué.

Je croyais que les baffes te suffisaient pour expliquer la configuration des proxies ?

Ouais, mais j'ai pas le droit de toucher aux chercheurs étrangers

Les mises en quarantaine internes



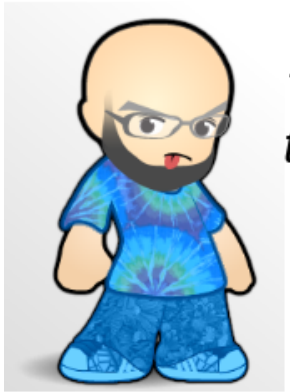
Les objectifs

Plusieurs objectifs

- Faciliter l'utilisation de notre réseau.
- Rester agnostique sur les clients.
- Conserver un peu la sécurité.
- Continuer à loguer plus que l'IP.

Les moyens

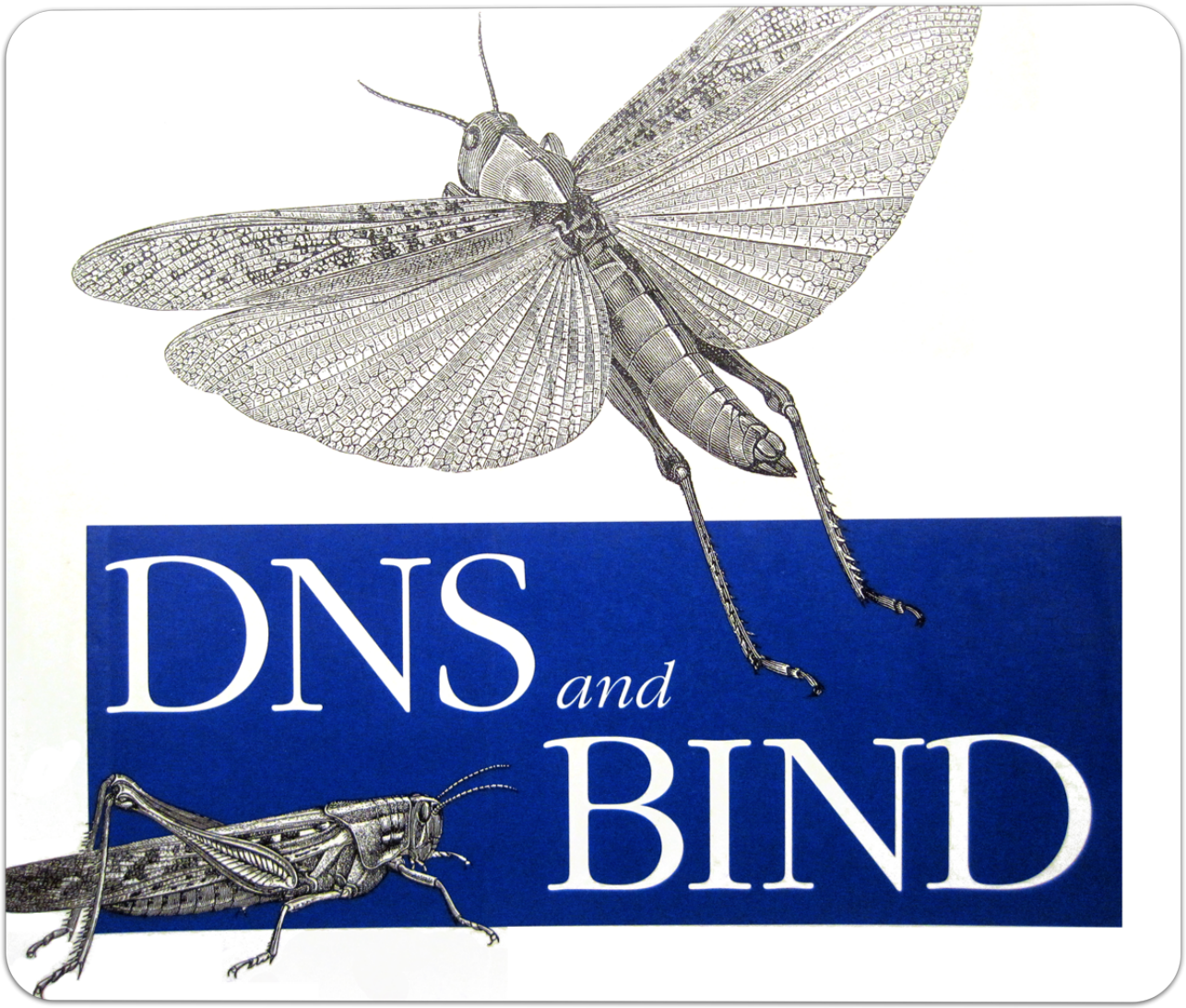
- Quelle information est
  - indispensable à l'usage d'internet ?
  - fournie par DHCP ?
  - respectée, par défaut, par TOUS les clients ?
  - manipulable à loisir ?



Toi, tu veux encore jouer au chat et à la souris avec tes utilisateurs

Uniquement quand je suis sûr de gagner

Le DNS



Le DNS RPZ : le principe

- Response Policy Zone.
- En bon français : DNS menteur.
- Ment à une question DNS : "Qui est www.playboy.com ?"
  - www.playboy.com n'existe pas.
  - www.playboy.com est un CNAME de piege.ut-capitole.fr.
  - www.playboy.com a pour IP 185.31.17.185
    - mais cette IP ne me convient pas,
    - donc c'est en fait un CNAME de piege.ut-capitole.fr.

Le RPZ pour les tout petits :
`http://www.bortzmeyer.org/rpz-faire-mentir-resolveur-dns.html`

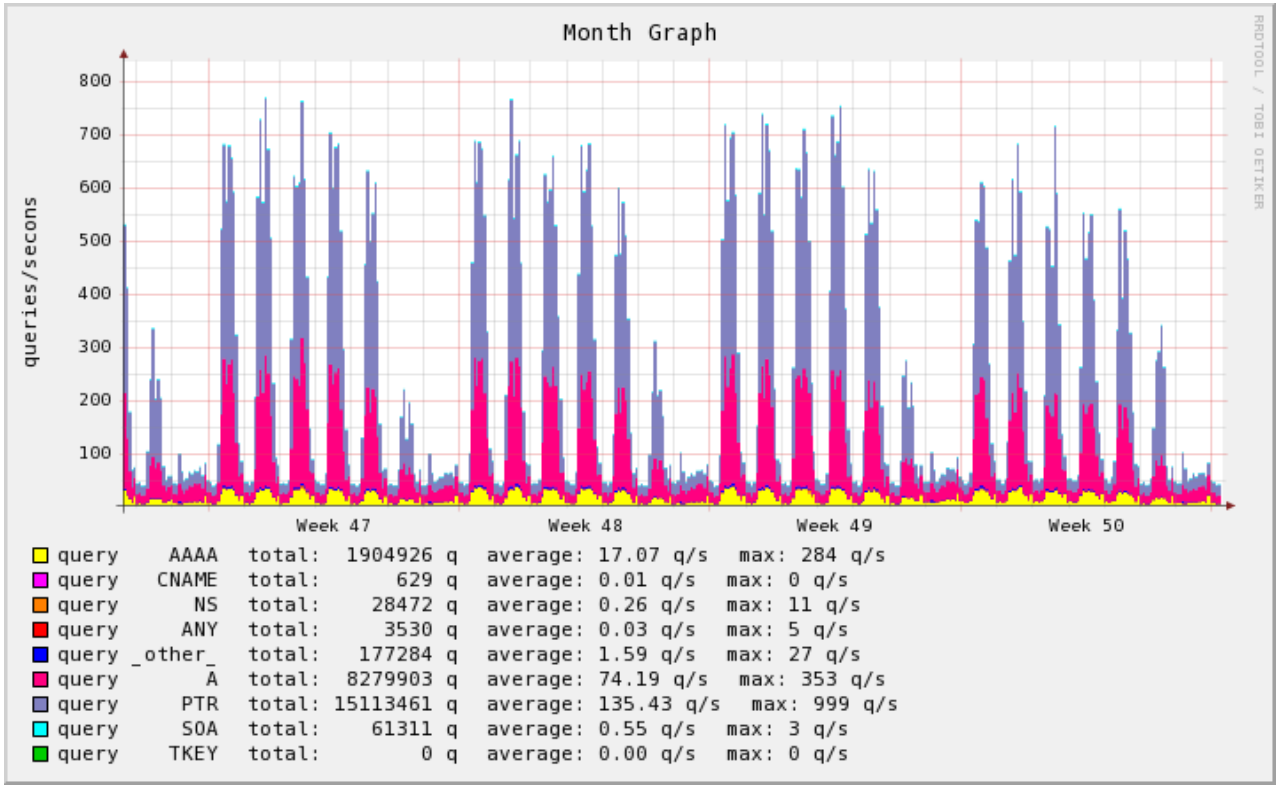
UNIVERSITÉ TOULOUSE 1 CAPITOLE

Le DNS RPZ : les besoins techniques

- Bind 9.8 minimum, mais 9.10 VRAIMENT préférable (9.9 en RHEL 7).
  - Possibilité d'exclure du RPZ des machines.
  - Accélération des recherches (Log(n) au lieu de (n)).
  - Fichier de zone en mode raw (attention au format map !).
- Des listes de domaines
  - Blacklists habituelles transformées en zone DNS (malware,adult,proxies)
  - RPZ externes (internalisées !), par exemple Spamhaus.
    - 500 000 domaines.
    - 150 domaines ajoutés/enlevés chaque 5 minutes.
- Plus de mémoire (2 Go).
- Plus de disque (Logs => 500 Ko compressés par minute).

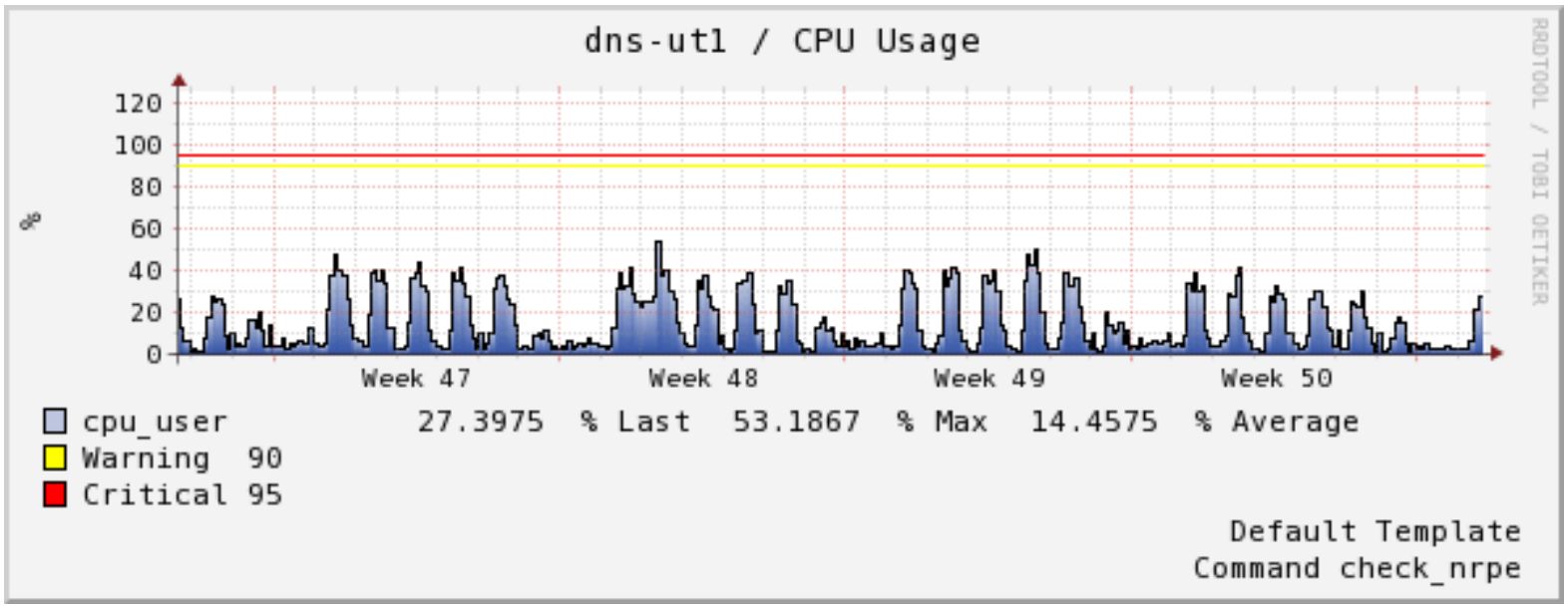
UNIVERSITÉ TOULOUSE 1 CAPITOLE

Le DNS RPZ : les requêtes

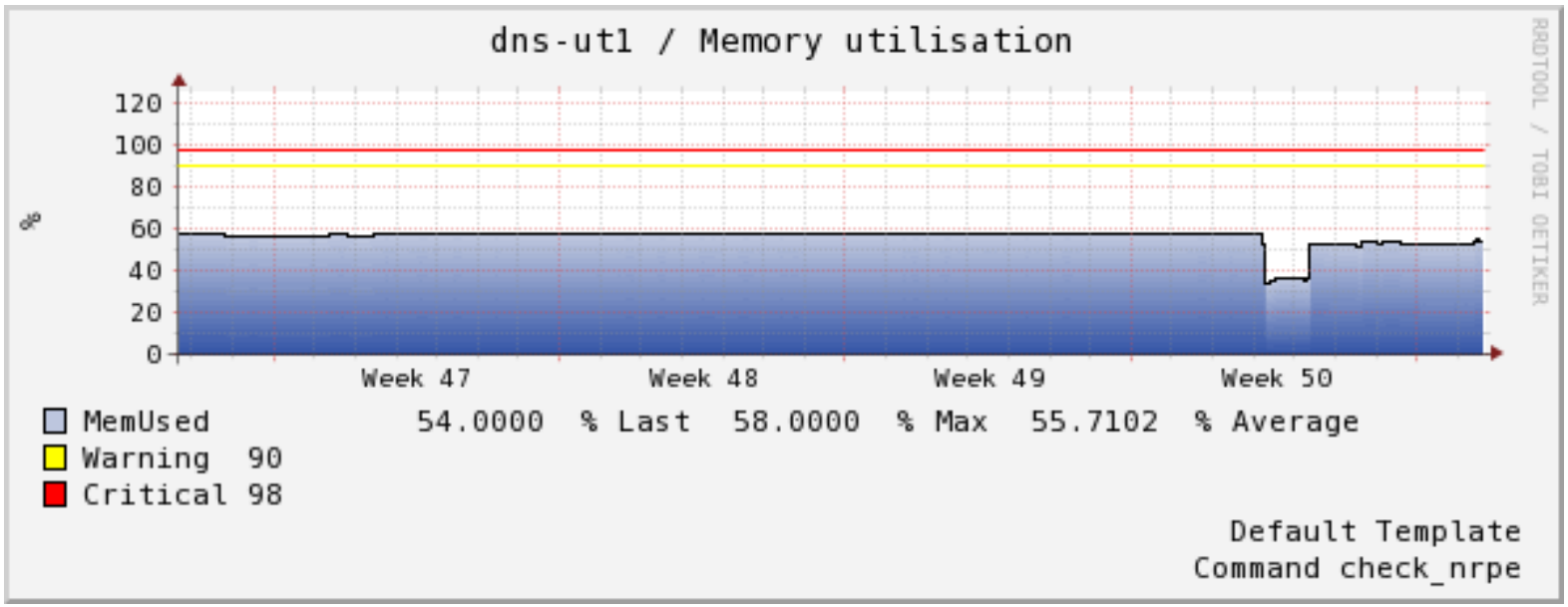


UNIVERSITÉ TOULOUSE 1 CAPITOLE

Le DNS RPZ : la charge cpu



Le DNS RPZ : la charge mémoire



Le DNS RPZ : Configuration

```
zone "rpz.warez.ut1" {
        type master;
        masterfile-format raw;
        file "rpz.warez.raw";
        allow-query { none; };
};

zone "rpz.spamhaus.org" {
        type slave;
        file "rpz.spamhaus.org.db";
        masterfile-format raw;
        masters { 199.168.90.51; 199.168.90.52; 199.168.90.53; };
};

response-policy {
        zone "rpz-whitelist-spamhaus" policy passthru;
        zone "rpz.spamhaus.org" policy cname narfi.ut-capitole.fr;
        zone "rpz.malware.ut1" policy cname narfi.ut-capitole.fr;
        zone "rpz.warez.ut1" policy cname narfi.ut-capitole.fr;
};
```

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Le DNS RPZ : Configuration d'une zone

```
$TTL 5M
@ 1H  IN SOA nonexistent.nodomain.none. hostmaster 1412036025 8H 2H 1W 2H
@                    IN  NS      nonexistent.nodomain.none.
*.777port.li     IN      CNAME   .
777prime.com     IN      CNAME   .
*.777prime.com   IN      CNAME   .
777primegames.com        IN      CNAME   .
*.777primegames.com      IN      CNAME   .
777promo.com     IN      CNAME   .
*.777promo.com   IN      CNAME   .
```

Le DNS RPZ : les problèmes

- Blocage des DNS extérieurs obligatoires.
- Contournable par fichier host local (mais pas pratique).
- Contournable par VPN fonctionnant en pure IP (10-20 contrevenants par jour).
  - Tor,
  - Frozenway.
- Beaucoup de tests avant que cela ne tombe en marche,
- Le DNS travaille beaucoup plus.
- Une même requête DNS a quelle durée de vie ? combien de connexions gère-t-elle ?

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Le DNS RPZ : les avantages

- Ultraportable (tout OS, tout matériel),
- Touche tous les protocoles,
- Permet l'utilisation de bases extérieures,
- La RPZ SPAMHAUS repère plus facilement des postes infectés (2-3 par jour).

Le DNS RPZ : les chiffres

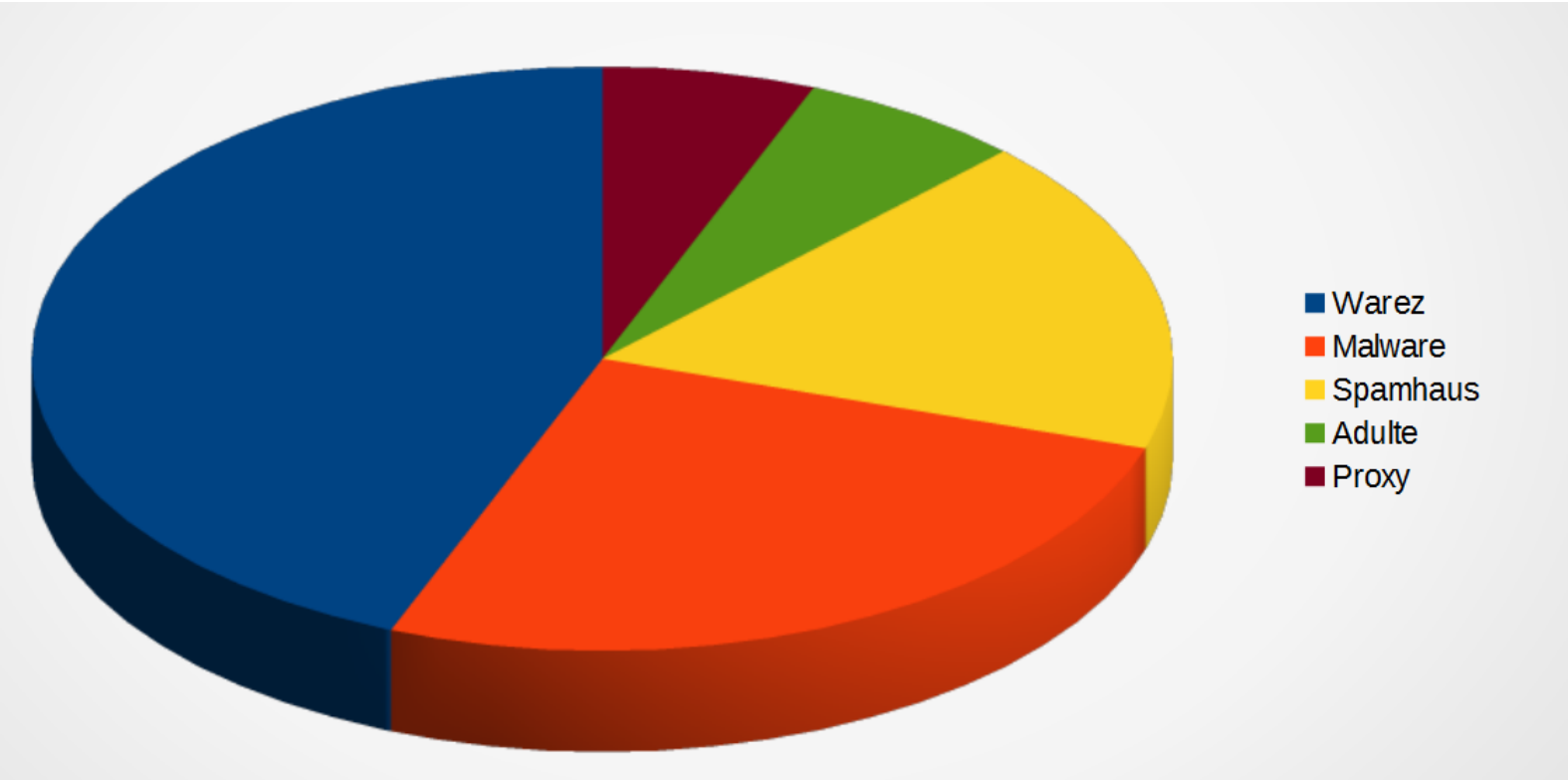
Sur les hors proxy

- 10 000 blocages DNS par jour
- 7 200 clients
- 900 clients bloqués

Par contraste sur les "proxifiés"

- 4 200 clients
- 179 clients bloqués

Le DNS RPZ : les catégories de blocage



Est-ce suffisant ?

- Gestion de la bande passante par utilisateur
  - Pour contrebalancer l'ouverture de la bande passante au HTTPS.
- Blocage IP des proxies de contournement
  - Pour éviter les VPN purs IP.
- Le CNAME (piege.ut-capitole.fr) doit être convenablement installé
  - Avertir correctement les utilisateurs.
  - Avertir éventuellement les administrateurs (malware, virus, etc.).
  - Détecter les ports utilisés.
  - Eventuellement capturer le trafic.

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Conclusion

Ca marche

- Les utilisateurs sont contents : le wifi "juste marche".
- Le filtrage est plus large.
  - Malware avec un C&C non web.
  - Clients "hors web" (IRC, mail, etc.).
- Notre proxy (transparent et standard) est conservé.
- Nous sommmes prêts pour le HTTP/2.0.

Mais

- Le DNSSEC risque de nous poser problème.
- On est passé du traitement de l'URL à celui du domaine.
- Le contenu SSL n'est plus analysé (analysable ?)
- Le HTTPS deviendrait-il "inspectable" ? (Note ANSSI)

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Merci de votre attention

Des questions ?

UNIVERSITÉ TOULOUSE 1 CAPITOLE