Capitoul – Mobilité

Le WiFi dans tous ses états

21/02/2013 – OMP

Xavier Jay – Denis Mirassou – Xavier Marty

Plan

- Les réseaux wifi pour la mobilité
- Nos solutions d'authentification
- Quelques difficultés
- Les chiffres

Plan

- **Les réseaux wifi pour la mobilité**
- Nos solutions d'authentification
- Quelques difficultés
- Les chiffres

Les réseaux wifi

- Mip-WiFi
- Eduroam
- eduspot

Les réseaux wifi - Mip-WiFi

- Lien : http://mipwifi.univ-tlse3.fr
- Principe
  - Portail Captif avec authentification radius
  - Interconnexion des radius des établissements membres au radius MiP-Wifi UT3
  - SSID propre à chaque établissement
  - Raccordement au service après avoir signé une convention avec l'UPS

Mip-WiFi

- Qui y est ?
  - Auch
  - Castres
  - Tarbes – IUT
  - Toulouse
    - CROUS
    - INP
    - INSA
    - ISAE
    - UT 1, 2 et 3

Mip-WiFi

- Qui n'y est pas ?
  - Albi – Champollion
  - Rodez
  - Tarbes - ENIT

eduroam

- Liens :
  - http://www.eduroam.fr / http://www.eduroam.org
- Principe
  - Interconnexion radius à l'échelle internationale
  - Pour la France, liaison avec les radius Renater
  - Connexion sécurisée basée sur 802.1X
  - SSID diffusé « eduroam »
  - Raccordement au service après validation de l'agrément Renater

eduroam

- Qui y est ?
  - CNRS – DSI
  - ENI - Tarbes
  - INP
  - INRA
  - INSA
  - ISAE
  - LAAS
  - UT 1, 2 et 3
  - CROUS – prochainement ...

eduspot

- Lien
  - https://services.renater.fr/mobilite/eduspot/index
- Principe
  - Authentification via le portail captif basée sur la fédération d'identité
    - Redirection sur le SSO de son établissement
  - SSID diffusé « eduspot »
  - Raccordement au service après validation de l'agrément Renater + déclaration du SP
- Solutions
  - Diverses solutions compatibles shibboleth

eduspot

- Logiciel utilisé à UT1 et CROUS y compris durant les JRES 2011 ;-) :

  - Lien : http://unpidf.univ-paris1.fr/univnautes
  - Solution : pfsense
    - Développé sous la tutelle de l'UNR Paris
    - Installation « Bare Metal »
      - Customisé pour l'éducation / recherche
    - Documentations d'installation / paramétrage
    - Liste de diffusion communautaire
    - Mise à jour et évolution régulières
    - Mais pas d'IPV6 ...

eduspot - UnivNautes

- Interface simple et adaptée pour mobile

eduspot

- Qui y est ?
  - UT1
  - CROUS bientôt

Plan

- Les réseaux wifi pour la mobilité
- **Nos solutions d'authentification**
- Quelques difficultés
- Les chiffres

Nos solutions d'authentification

- **Portail captif**
- Radius

Portail captif - Pfsense

- Présentation générale
- Quelques fonctionnalités
- Nfsens - Pfflowd

http://fr.wikipedia.org/wiki/Pfsense

Portail captif - Pfsense

Historique

Le projet pfsense, est basé sur un fork de m0n0wall réalisé en 2004 par Chris Buechler et Scott Ullrich.

La version 1.0 a été lancée le 4 octobre 2006.

La version 2.0 finale est arrivée fin décembre 2011.

A partir de pfSense 2.0, il existe des versions pour les architectures i386 (32 bits) et amd64 (64 bits).

Dernière mise à jour : V2.0.2 le 21/12/2012

http://blog.pfsense.org/

Portail captif - Pfsense

Présentation générale

pfSense est un routeur / pare-feu opensource basé sur FreeBSD.

pfSense peut être installé sur un simple ordinateur personnel comme sur un serveur.

Après une installation en mode console, il s'administre ensuite simplement depuis une interface web

Il existe également sous forme d’appliance :

http://www.pfsense.org/index.php?option=com_content&task=view&id=44&Itemid=50

Portail captif - Pfsense
Quelques Fonctionnalités

- Stateful firewall
- Network Address Translation
- Portail captif
- Failover basé sur CARP et pfsync
- Load balancer entrant / sortant
- Proxy et proxy inverse
- Réseau privé virtuel sur IPsec, L2TP, OpenVPN, or PPTP
- Monitoring basé sur RRDTool
- DNS dynamique
- DNS Forwarder
- Serveur et relay DHCP
- Et beaucoup d’autres…

S’ajoute à ces fonctions, une gestion de plugins venant parfaire l'installation de base, avec notamment, freeradius, squid, squidguard, iperf, nmap, short, nrpe, zabbix, avahi, pflowd.

Portail captif - Pfsense

Quelques Fonctionnalités :

Squid et Squidguard

Proxy server: General settings

General | Remote Cache | Local Cache | ACLs | Traffic Mgmt | Authentication | Users | Real time | Sync

Squid General Settings

Proxy interface

WAN
LAN
LAN2
loopback

The interface(s) the proxy server will bind to.

Proxy port

8080

This is the port the proxy server will listen on.

Portail captif - Pfsense

Quelques Fonctionnalités :

Squid et Squidguard

Status: Proxy Monitor

General | Remote Cache | Local Cache | ACLs | Traffic Mgmt | Authentication | Users | **Real time** | Sync

Max lines: 10 lines
Max. lines to be displayed.

String filter:
Enter a grep like string/pattern to filterlog.
eg. username, ip addr, url.
Use **!** to invert the sense of matching, to select non-matching lines.

Squid Logs

Date	IP	Status	Address	User	Destination
19.02.2013 11:29:43	172.17.177.25	TCP_MISS/200	http://adserver.playtv.fr/delivery/afr.php?	-	89.202.139.130
19.02.2013 11:29:43	172.17.176.17	TCP_REFRESH_UNMODIFIED/304	http://st.f1.thethao.vnexpress.net/i/v6/graphics/img_fpt.gif	-	63.220.1.57
19.02.2013 11:29:43	172.17.176.17	TCP_REFRESH_UNMODIFIED/304	http://st.f1.thethao.vnexpress.net/i/v6/graphics/img_noname_34x34.gif	-	63.220.1.57
19.02.2013 11:29:43	172.17.176.17	TCP_REFRESH_UNMODIFIED/304	http://st.f1.thethao.vnexpress.net/c/v8/images/icons/mail.gif	-	63.220.1.57
19.02.2013 11:29:43	172.17.176.17	TCP_REFRESH_UNMODIFIED/304	http://st.f1.thethao.vnexpress.net/i/v6/graphics/img_vnexpress_tet.jpg	-	63.220.1.57
19.02.2013 11:29:43	172.19.18.115	TCP_REFRESH_UNMODIFIED/200	http://www.gstatic.com/android/keyboard/dictionarypack/metadata.json	-	74.125.230.207
19.02.2013 11:29:43	172.17.176.17	TCP_REFRESH_UNMODIFIED/304	http://st.f1.thethao.vnexpress.net/c/v8/images/icons/hotline.gif	-	63.220.1.57
19.02.2013 11:29:43	172.17.176.17	TCP_REFRESH_UNMODIFIED/304	http://st.f1.thethao.vnexpress.net/i/v6/graphics/vne_slogan_3.gif	-	63.220.1.57
19.02.2013 11:29:43	172.17.177.248	TCP_MISS/200	http://ftvodhdsecz-f.akamaihd.net//z/streaming-adaptatif_france-dom-tom/2013/S08/J1/77488326-20130218-,398,632,934,k.mp4.csmil/2_ff872347d3c4987d_Seg1-Frag196?	-	88.221.14.137
19.02.2013 11:29:43	172.19.18.249	TCP_HIT/200	http://static.ak.fbcdn.net/rsrc.php/v2/yG/r/lRTMK---jRJ.png	-	-

SquidGuard Logs

Date-Time	ACL	Address	Host	User
19.02.2013 11:29:13	Request(etudiant/blk_blacklists_adult/-)	http://s.free-porn-vidz.com/xxx/vador/dating/2000005_300.jpg	172.19.17.242/-	-
19.02.2013 11:29:13	Request(etudiant/blk_blacklists_adult/-)	http://s.free-porn-vidz.com/xxx/vador/dating/2000004_300.jpg	172.19.17.242/-	-
19.02.2013 11:29:13	Request(etudiant/blk_blacklists_adult/-)	http://s.free-porn-vidz.com/xxx/vador/dating/2000003_300.jpg	172.19.17.242/-	-
19.02.2013 11:29:10	Request(etudiant/blk_blacklists_adult/-)	http://files.tvsexe.com/thumbs/4b5051ac58715110_Natural_10_Scene_1_lh.mp4/4b5051ac58715110_Natural_10_Scene_1_lh.mp4-10.jpg	172.19.17.242/-	-

Portail captif - Pfsense

Quelques Fonctionnalités :

Squid et Squidguard

Proxy filter SquidGuard: General settings

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log | XMLRPC Sync

Enable ☑

Check this option to enable squidGuard

For saving configuration YOU need click button 'Save' on bottom of page

After changing configuration squidGuard you must **apply all changes**

Apply

SquidGuard service state: **STARTED**

Target Rules

^whitelistecrous !norenater !blk_blacklists_adult !blk_blacklists_agressif blk_blacklists_arjel blk_blacklists_ast

Target Rules List (click here)

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

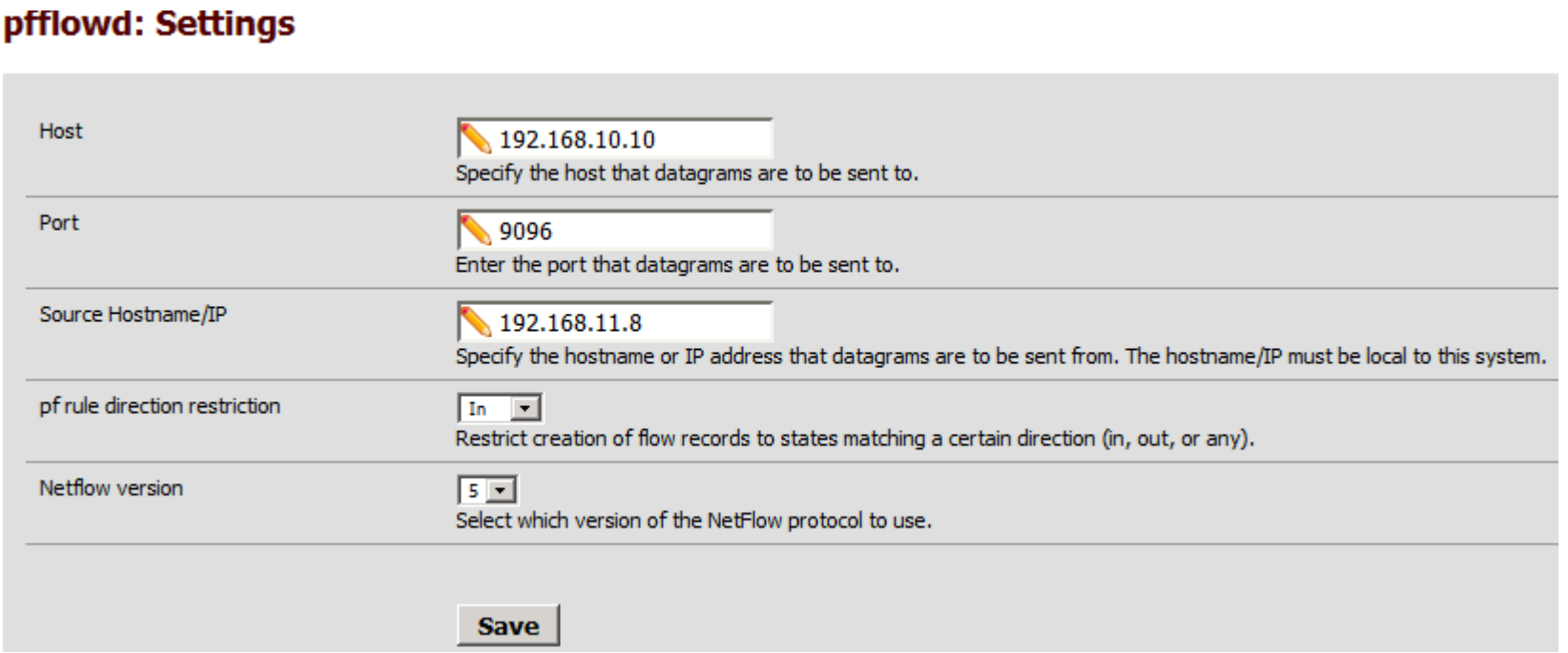
Target Categories			Target Categories for off-time (If 'Time' not defined, this is column will be ignored.)		
[whitelistecrous]	access	whitelist	[whitelistecrous]	access	whitelist
norenater [norenater]	access	deny	norenater [norenater]	access	deny
[blk_blacklists_adult]	access	deny	[blk_blacklists_adult]	access	deny
[blk_blacklists_agressif]	access	deny	[blk_blacklists_agressif]	access	deny
[blk_blacklists_arjel]	access	allow	[blk_blacklists_arjel]	access	allow
[blk_blacklists_astrology]	access	allow	[blk_blacklists_astrology]	access	allow
[blk_blacklists_audio-video]	access	allow	[blk_blacklists_audio-video]	access	allow

Blacklist URL :
ftp://ftp.univ-tlse1.fr/hidden/blacklists_crous.tar.gz

Portail captif - Pfsense

Quelques Fonctionnalités :

Pfflowd

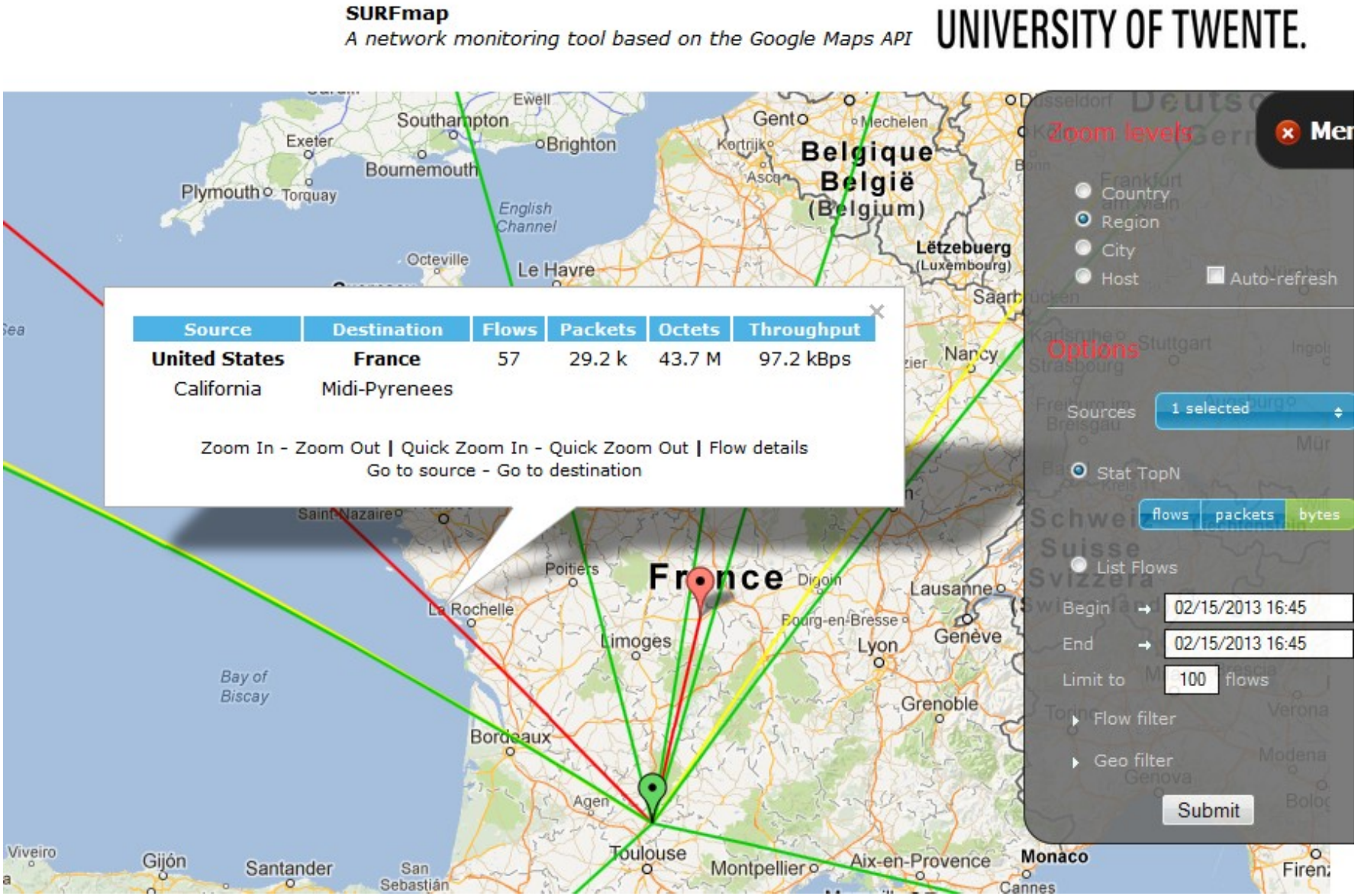


Portail captif - Pfsense

Quelques Fonctionnalités : NFSEN Plugins SURFmap (1/5)

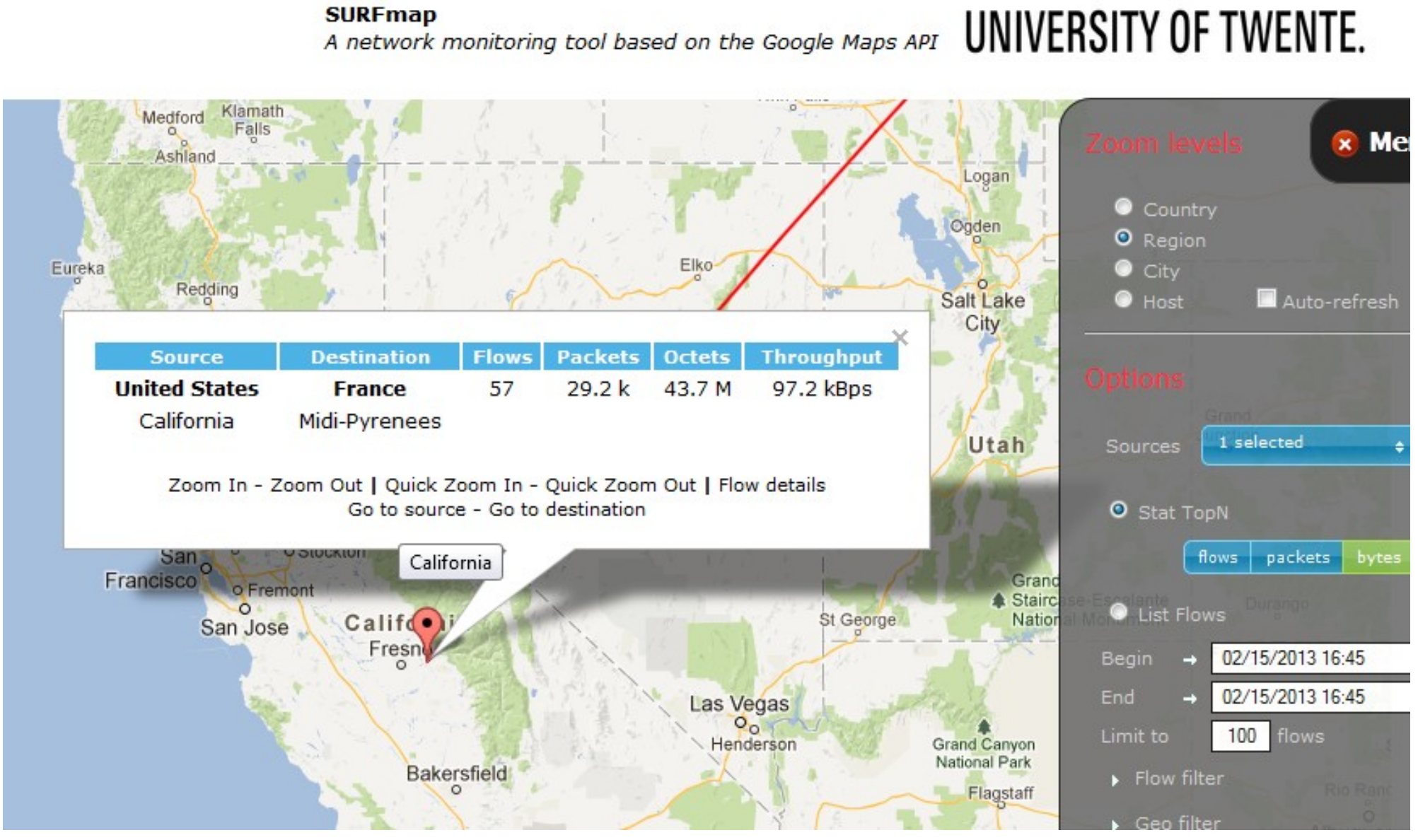
Portail captif - Pfsense

Quelques Fonctionnalités : NFSEN Plugins SURFmap (2/5)



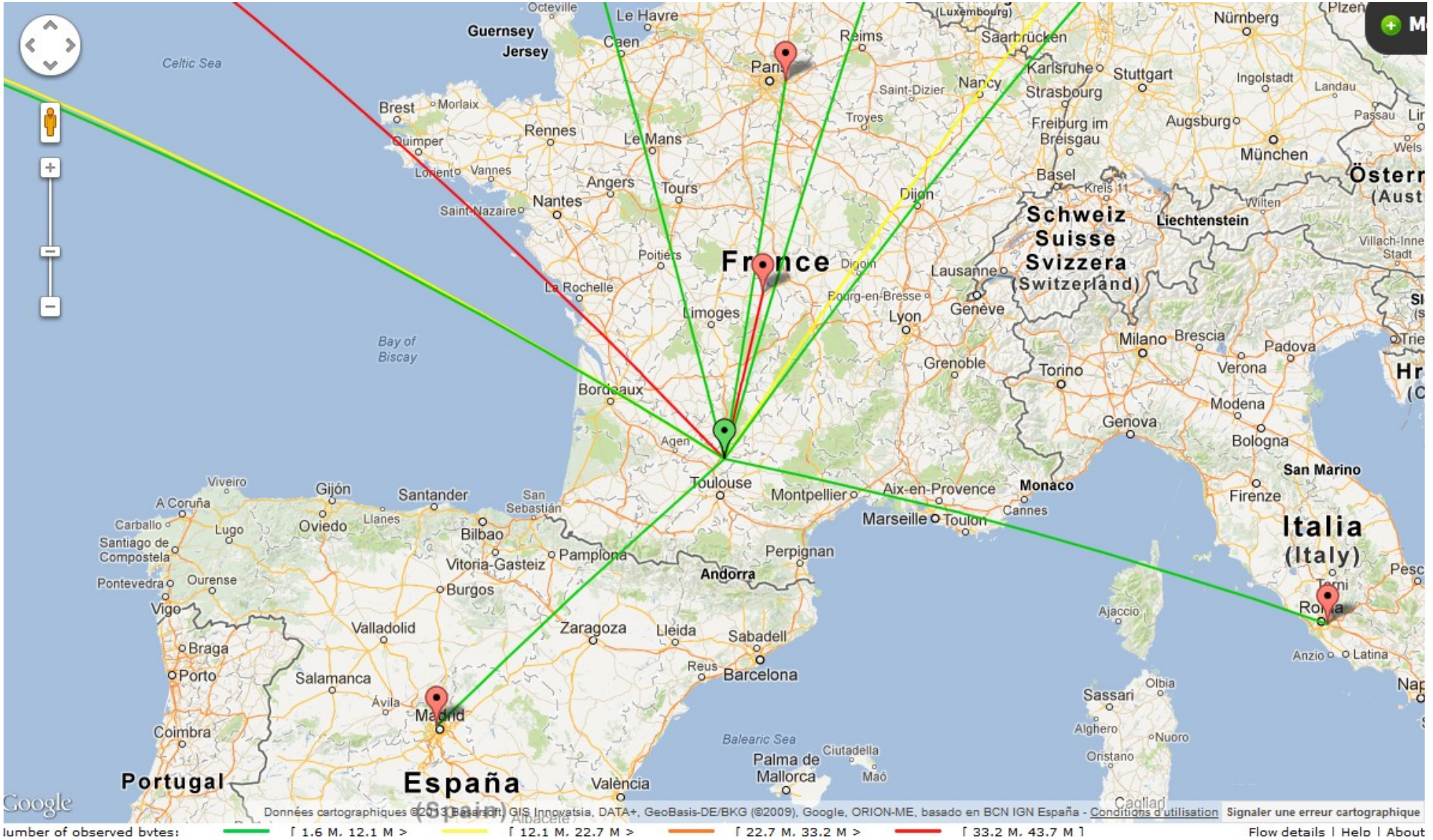
Portail captif - Pfsense

Quelques Fonctionnalités : NFSEN Plugins SURFmap (3/5)



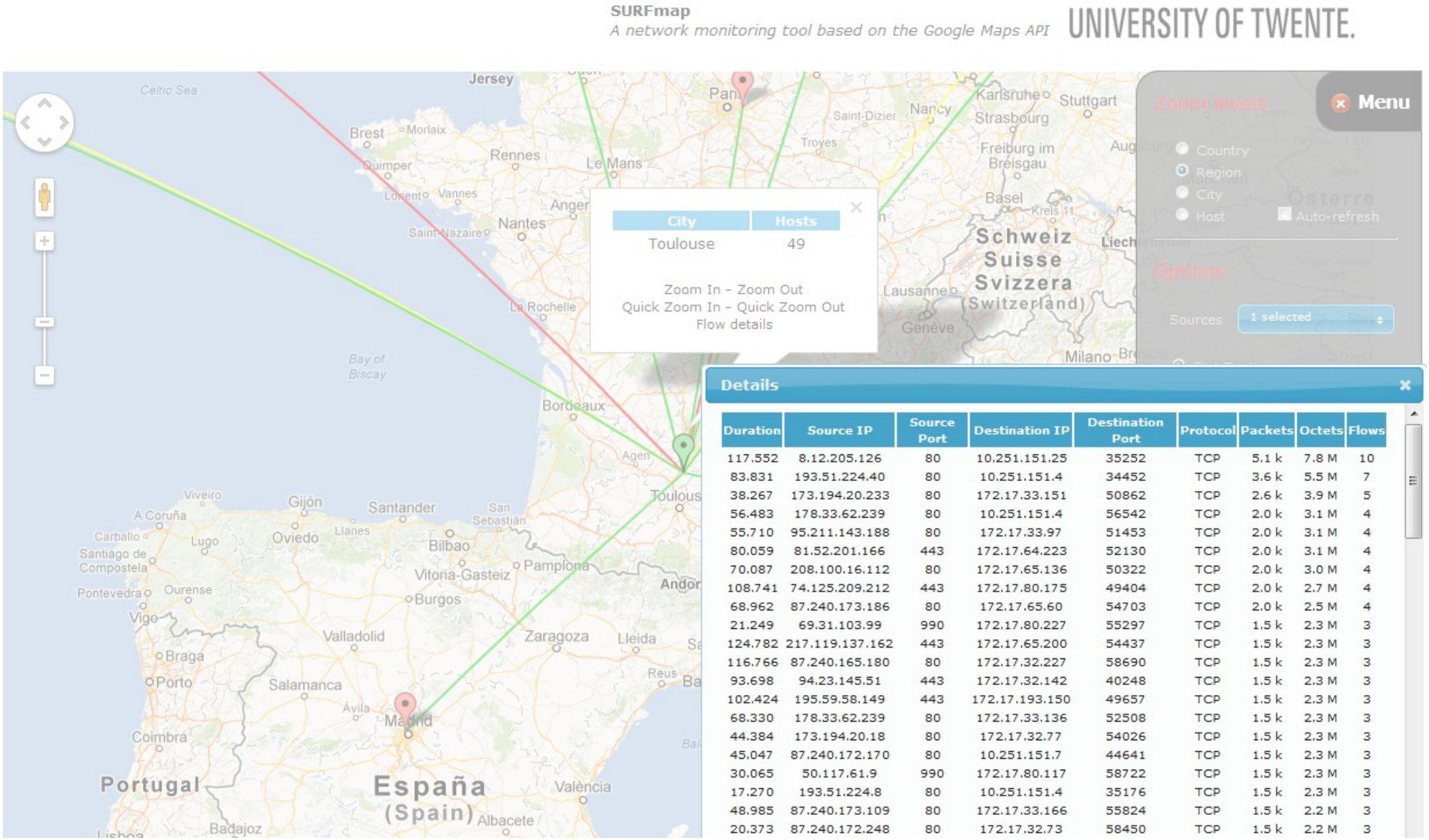
Portail captif - Pfsense

Quelques Fonctionnalités : NFSEN Plugins SURFmap (4/5)



Portail captif - Pfsense

Quelques Fonctionnalités : NFSEN Plugins SURFmap (5/5)



Nos solutions d'authentification

- Portail captif
- **Radius**

Radius

- RADIUS : Remote Authentication Dial In User Service
- Protocole réseau d'authentification, d'autorisation et de comptabilisation centralisées
- IETF RFC 2865 (Authentication + Authorization)
- IETF RFC 2866 (Accounting)
- Implémentation Free Radius très répandue dans notre communauté (http://freeradius.org)
  - Interface avec une(des) base(s) d'authentification variées (LDAP, Active Directory, Kerberos, SQL, Unix, fichier plat...)
  - Chaînage de services radius en mode proxy (eduroam, MiP-Wifi)
  - Service peu gourmand en ressources systèmes
  - Fiable (stable)
  - Support de larges configurations (dizaines de milliers d'utilisateurs)
  - Configuration hautement personnalisable mais d'un abord peu facile

Plan

- Les réseaux wifi pour la mobilité
- Nos solutions d'authentification
- **Quelques difficultés**
- Les chiffres

Quelques difficultés

- Périphériques bavards
  - Quand les trames ARP représentent plus de 60% du trafic
  - Qui sont renvoyées sur toute l'infra
  - → PROBLEME
- Nécessité de filtrage
  - Rate limiting
    - Au niveau des radio profiles
    - Moyenne de 10 pps / Max à 50 pps
    - Limitation de la bande passante multicast (6mpbs)

Quelques difficultés

- Protocole Zeroconf
  - Protocole Bonjour d'Apple
    - Port 5353 en UDP
  - Trafic multicast mDNS
    - Adresse 224.0.0.251
- Prise en compte du problème par plusieurs constructeurs
  - Cisco, Aruba
    - http://community.arubanetworks.com/t5/Technology-Blog/Aruba-BCPS-Webinar-Q-amp-A-Large-Scale-WLAN-Design-and/ba-p/34305

Quelques difficultés

- Problèmes proxy
  - Liés à la mise en place d'un proxy transparent
  - Nécessité de renseigner le proxy
    - Méthode dure
      - Forcer le proxy dans le navigateur client
    - Méthode simple
      - Détection automatique dans le navigateur client
      - Push du proxy via dhcp
      - Mise en place du nom wpad (serveur web) avec un fichier wpad.dat

Quelques difficultés

- Configuration bornes
  - Éviter les modes tout automatique
  - Préférer des canaux et des puissances fixes
  - Effectuer une étude
- Couverture wifi
  - A chaque borne / constructeur un niveau de puissance de couverture différent
    - Omni / Directionnelle

Quelques difficultés

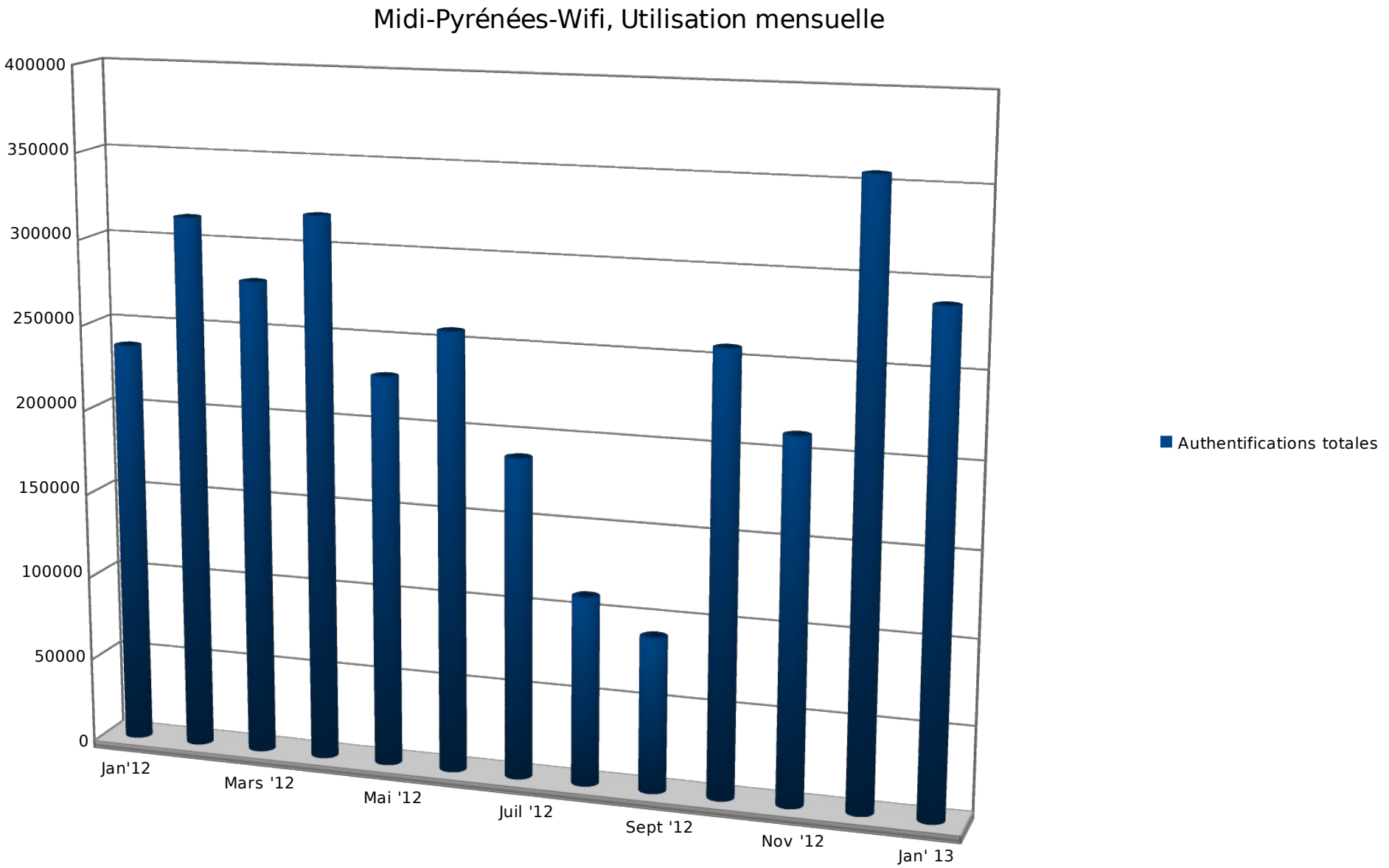
- Réticence utilisateurs
  - Exemple BNF
    - http://www.tomshardware.fr/articles/wi-fi-bibilotheque,1-15141.html
- Information
  - CHSCT (Comité d'Hygiène, de Sécurité et des Conditions de Travail)
  - Explication sur les rapports de puissance entre le WiFi et le GSM
    - http://www.afsset.fr/upload/bibliotheque/166004335031200624296094988253/09_10_ED_Note_Synthese_RF.pdf

Plan

- Les réseaux wifi pour la mobilité
- Nos solutions d'authentification
- Quelques difficultés
- **Les chiffres**

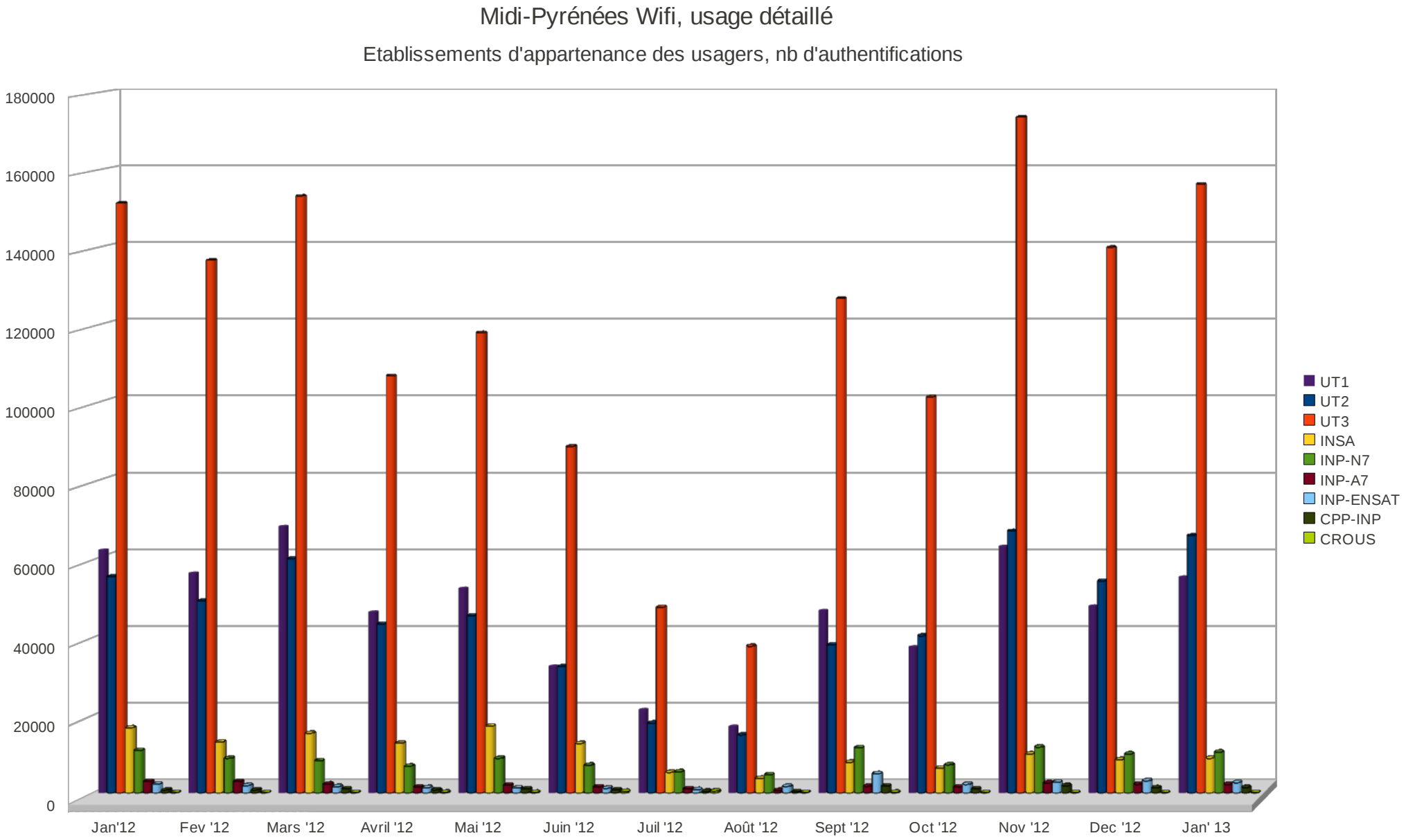
Les chiffres

Midi-Pyrénées Wifi (mobilité d'authentifications) 1/3



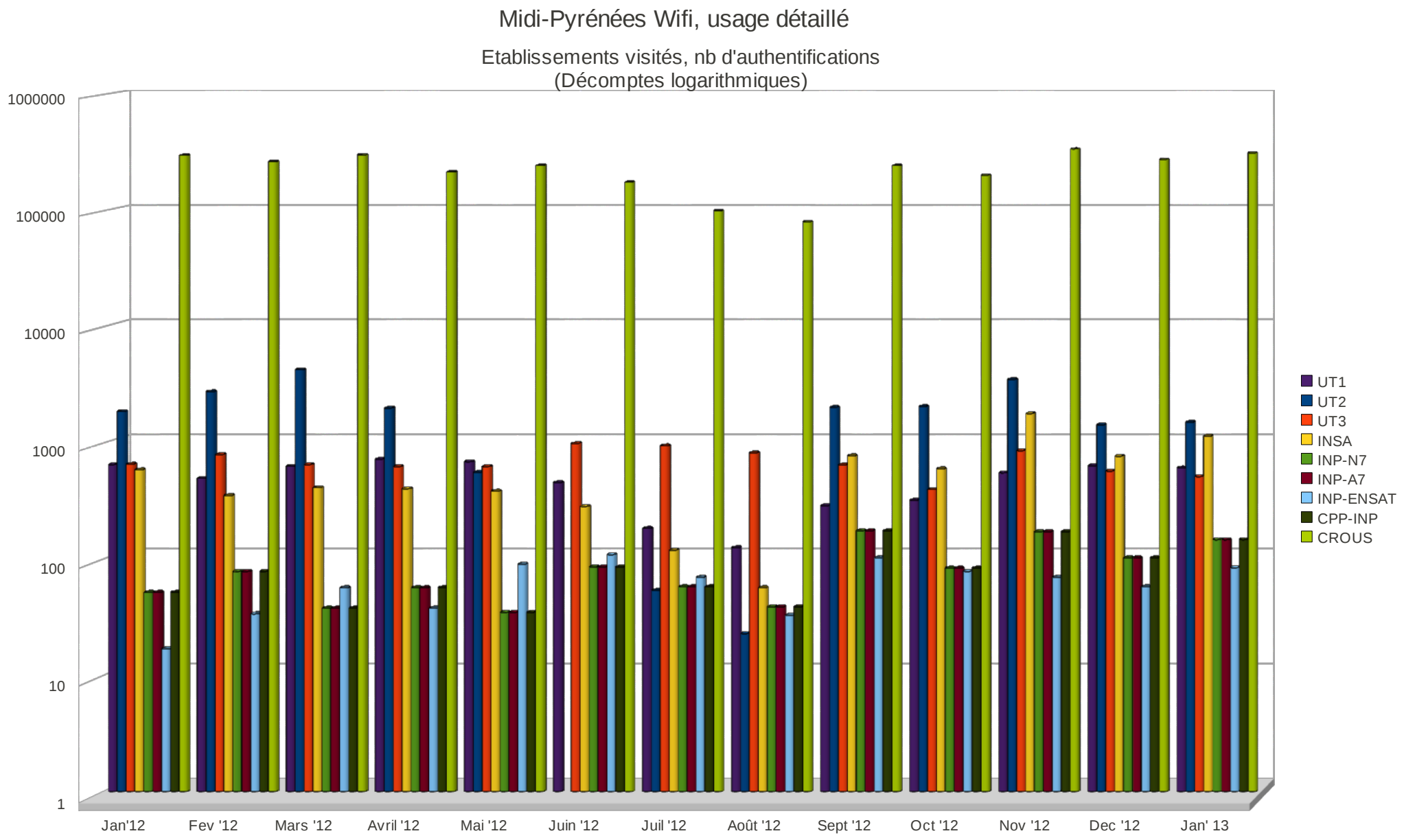
Les chiffres

Midi-Pyrénées Wifi (mobilité d'authentifications) 2/3



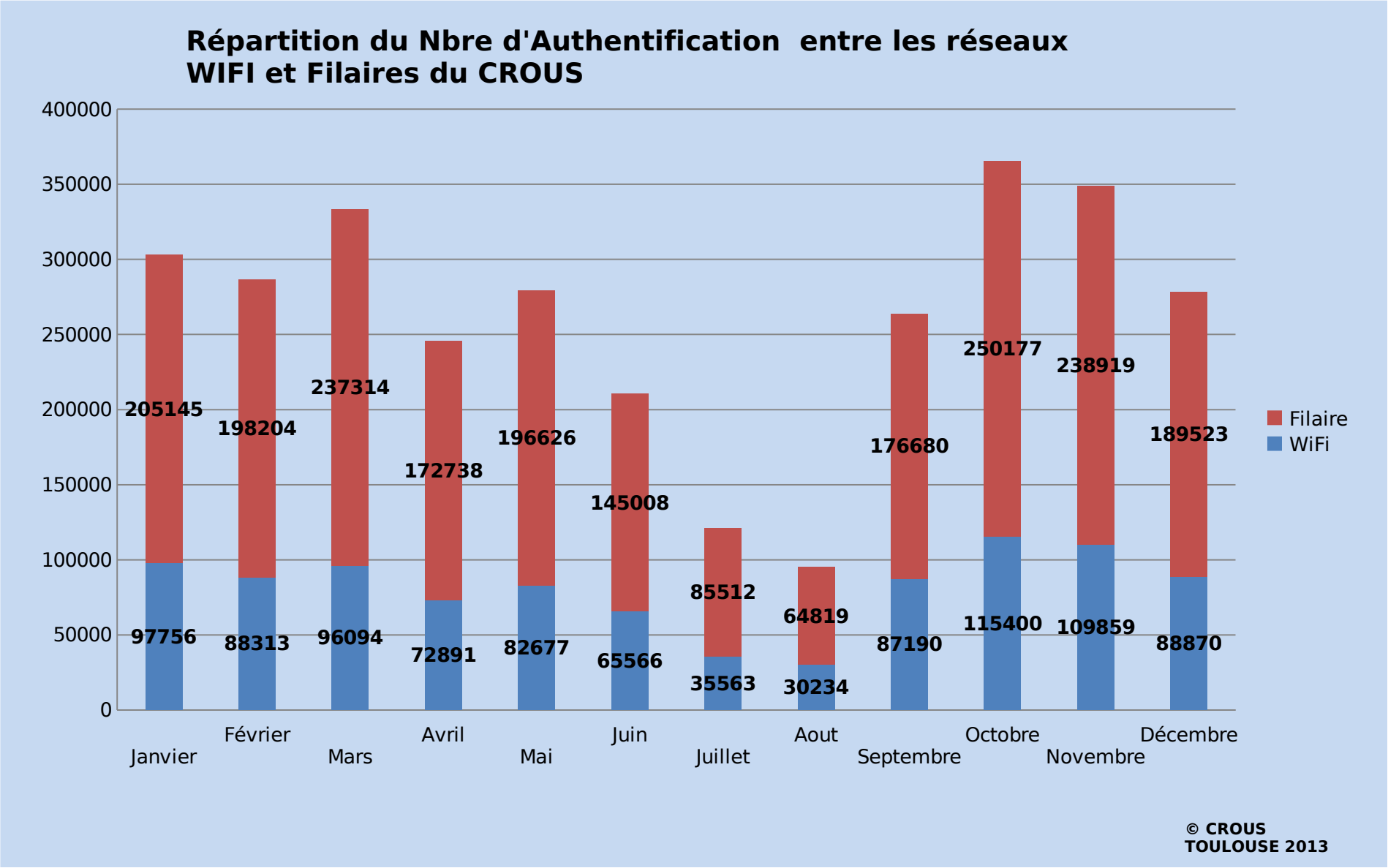
Les chiffres

Midi-Pyrénées Wifi (mobilité d'authentifications) 3/3



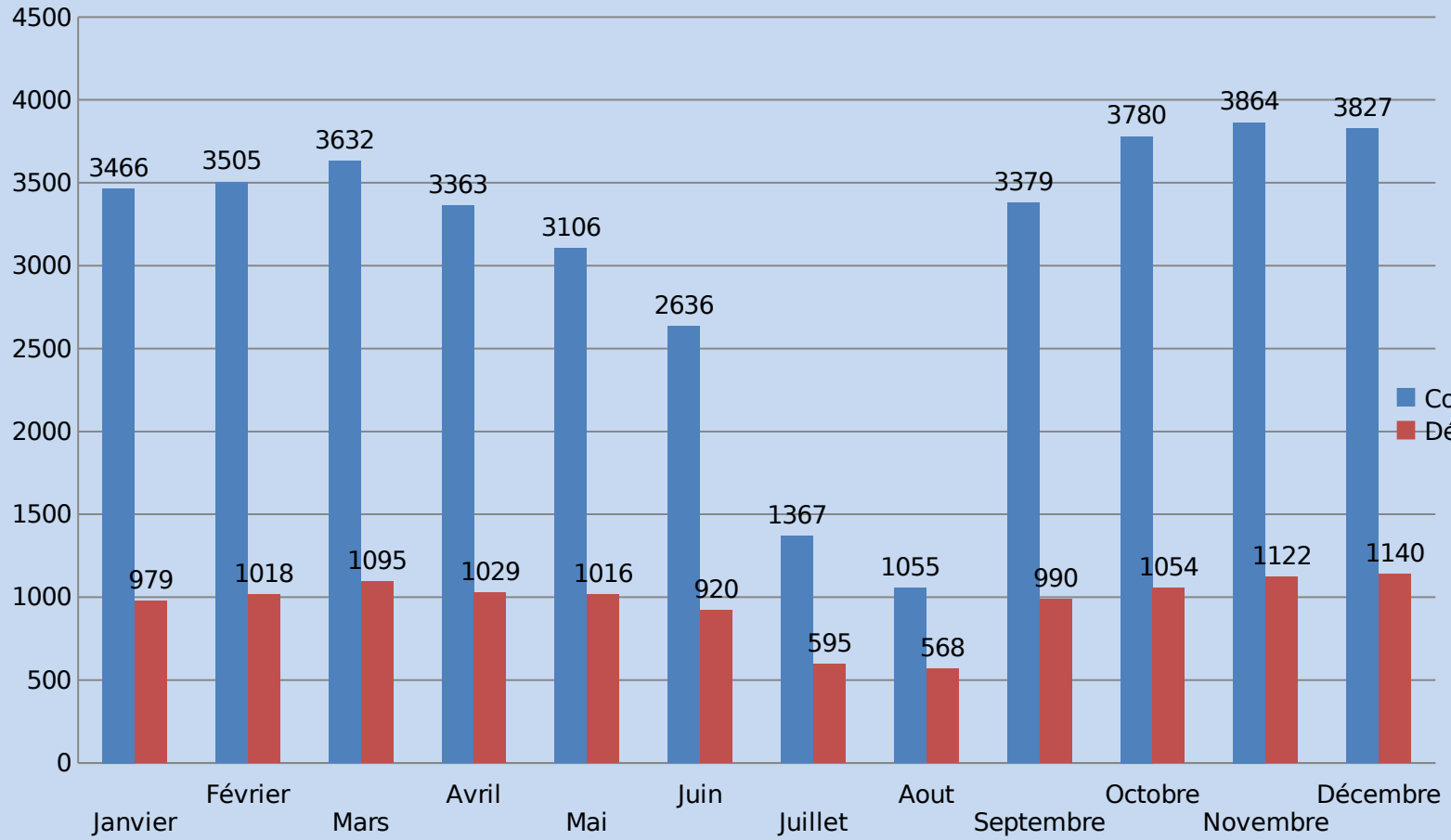
Les chiffres

Mobilité MipWifi au CROUS de TOULOUSE (1/2)



Les chiffres

Mobilité MipWifi au CROUS de TOULOUSE (2/2)



Points d'Accès Filaire : **9400**
Bornes WiFi : **174** Bornes légères
13 bornes lourdes

Portail Captif Filaire et WiFi :
8 PfSense pour Toulouse
7 PfSense sur Midi Pyrénées

Nombre d'étudiants différents qui se sont connectés durant l'année 2012: **11568**

Les chiffres

Université Toulouse 3 Paul Sabatier 1/4

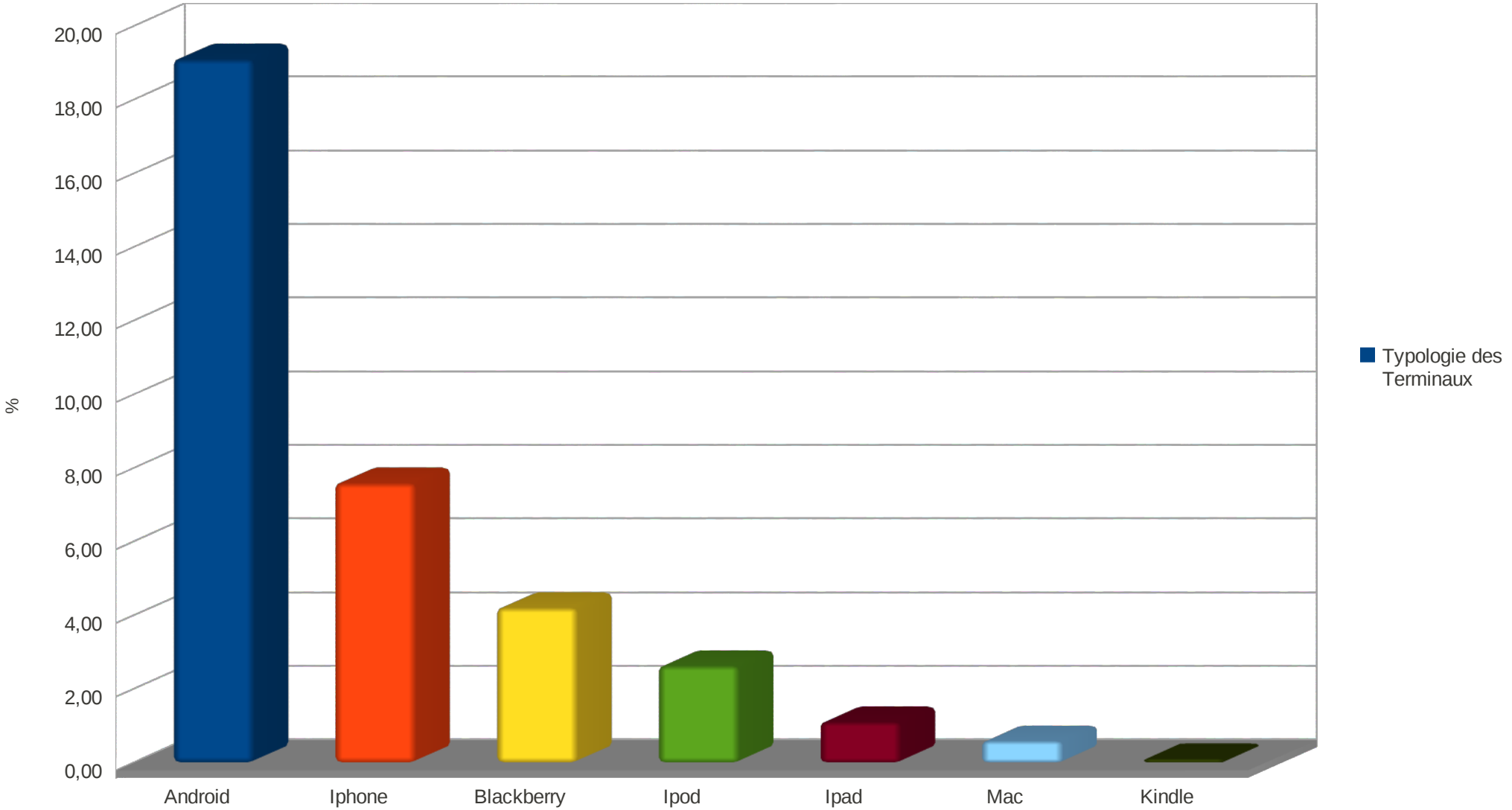
- 32000 étudiants, 4600 personnels, ~330 bornes wifi
- Authentifications utilisateurs wifi en 2012
  - 1 533 206 « indoor » (~ 4200/jour)
    - 98% d'usagers « locaux » (le reste des « invités »)
  - 3 018 400 « indoor + outdoor (en déplacement)»
    - 50% d'authentifications d'usagers en déplacement :
      - Notamment : Les étudiants UT3 en résidences universitaires (CROUS Toulouse)

Les chiffres

Université Toulouse 3 Paul Sabatier 2/4

UT3, wi-fi 2012, répartition par type de terminaux

(Source UT3/DTSI/dSRT/DM)



Les chiffres

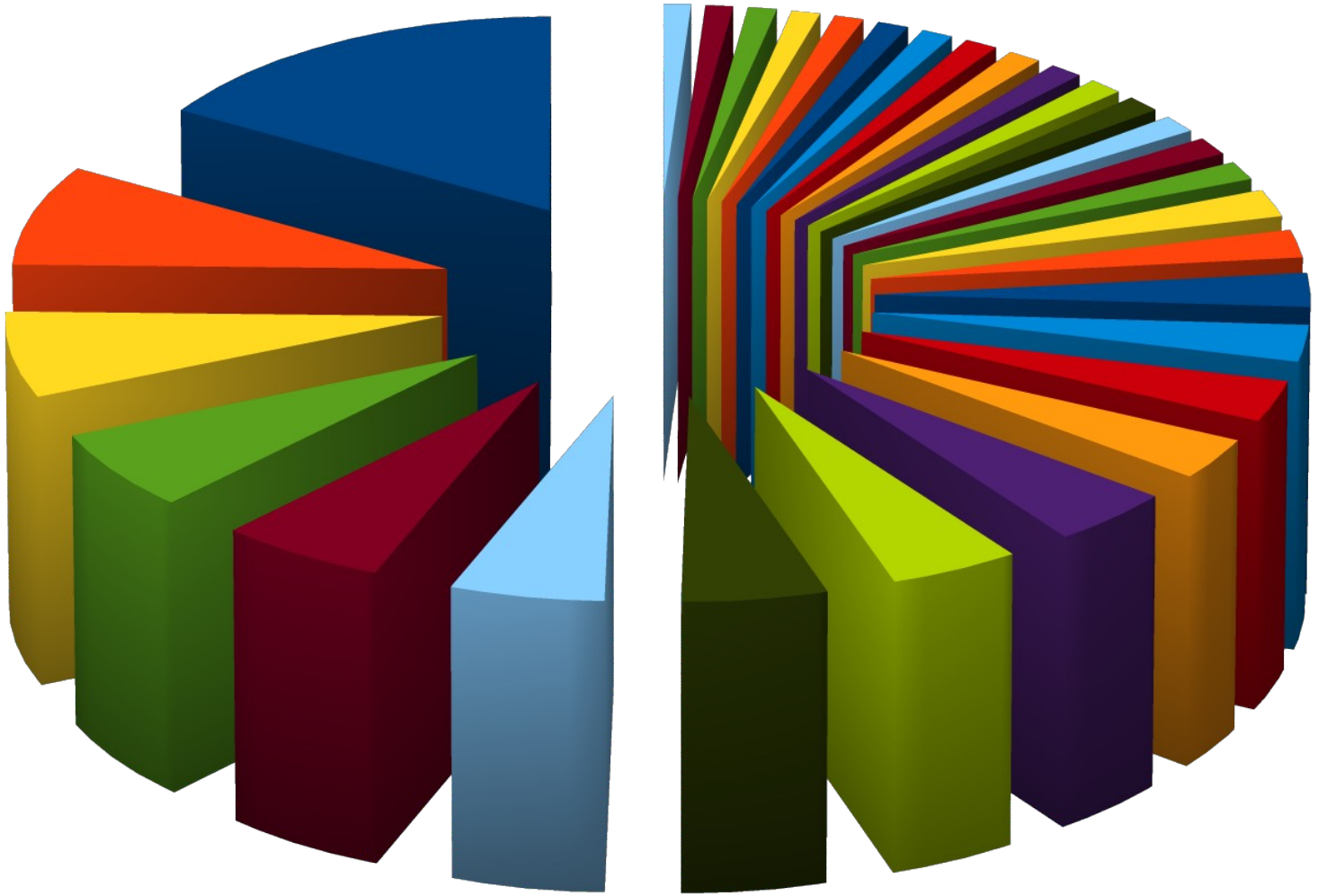
Université Toulouse 3 Paul Sabatier 3/4

- Nombre d'IP délivrées
  - Wifi portail captif : 8 classes C publiques (traçabilité)
    - ~ 2000 IP dispo
    - Bail DHCP 30 min.
  - Wifi eduroam : 4 classes C publiques
    - Sert également de wifi 802.1x interne établissement
    - ~ 1000 IP dispo
    - Bail DHCP 30 min.
  - ~ 1500 IP utilisées le 04/02/2013, 14h41
  - ~ 1 247 789 IP distribuées (DHCP) en janvier 2012, soit ~ 3021 IP différentes

Les chiffres

Université Toulouse 3 Paul Sabatier 4/4

Provenance des visiteurs wi-fi UT3 2012 (30 premiers)



- insa-toulouse.fr
- uhp-nancy.fr
- univ-tlse1.fr
- crous-toulouse.fr
- enseeiht.fr
- estumail.ucm.es
- etu.univ-tlse2.fr
- unilim.fr
- u-bordeaux1.fr
- LTU.SE
- unimib.it
- unizar.es
- uvsq.fr
- alumnos.upm.es
- unistra.fr
- bris.ac.uk
- utwente.nl
- laas.fr
- ensgsi.inpl-nancy.fr
- ipca.pt
- ucm.es
- isae.fr
- univ-tlse2.fr
- correo.ugr.es
- ucl.ac.uk
- unice.fr
- cnrs-dir.fr
- eduroam.mwn.de
- ensat.fr
- uwaterloo.ca

Bilan

- Les services sans-fil sont en forte expansion depuis 2-3 ans → multiplication des terminaux
- La demande de couverture wifi augmente.
- La baisse des prix de la data mobile => concurrence au wifi ?
  - Mais probablement avec la 4G, la 3G étant encore « lente »