



# Accès Internet pour visiteurs

---

Réseau dédié et cloisonné :  
contrôle par portail captif

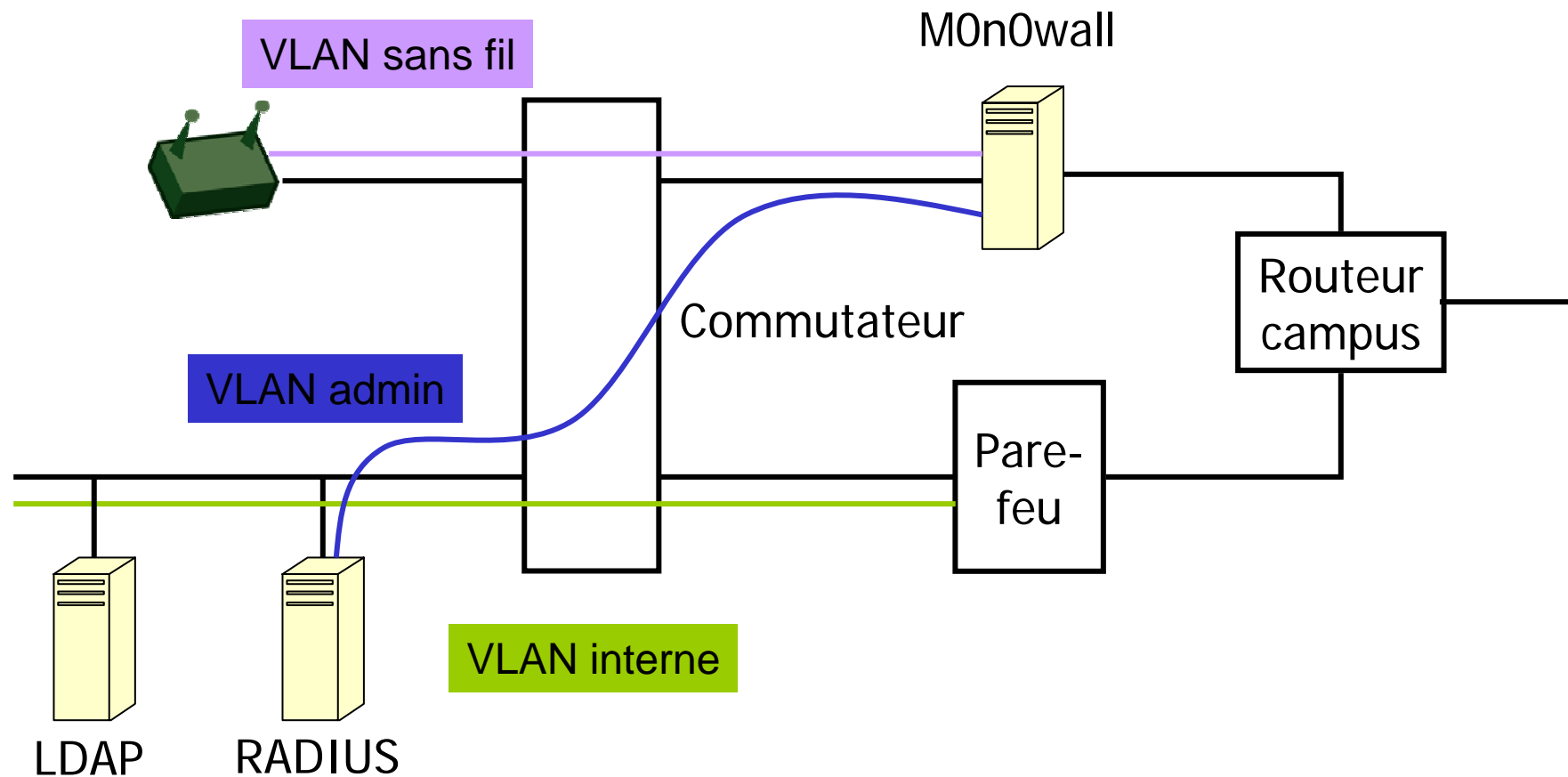


# WiFi pour les visiteurs

---

- Contraintes
  - Voisinage (détecte > 10 réseaux de particuliers)
  - Juridique : traces des connexions
  - Sécurité : isolé du réseau interne, connecté directement à extérieur  
⇒ c'est le problème des visiteurs, pas celui du labo
- WEP
  - Résistance < 10 mn
  - Pas si simple à paramétrer
- Adresse MAC
  - Usurpation facile
  - Difficile à gérer
- 802.11i (WPA, WPA2)
  - Sûr
  - Prématuré, peu de machines le gère

# Architecture réseau





# Portail captif

---

- M0n0wall
- WiFi : ouvert, aucun chiffrement
- Principe
  - Intercepte la 1ère requête web
  - Authentification -> formulaire https
  - Ouverture du firewall vers Internet pour le couple (IP, MAC) considéré
  - Redirection vers la requête web initiale

https://www1.impmc.jussieu.fr/intranet/informatique/wifi/login.html OK php mktime

Démarrage Dernières nouvelles (en)

# Bienvenue à l'IMPMC

Afin de répondre aux besoins de ses visiteurs l'IMPMC offre à titre gracieux un accès sans fil à Internet. Nous ne garantissons pas la qualité de service et nous faisons appel à la responsabilité de chacun pour ne pas abuser des possibilités offertes.

**L'accès est réservé aux personnes dûment autorisées.**

## Mise en garde

- Le réseau sans fil n'est absolument pas sécurisé. Les données échangées peuvent être écoutées, interceptées ou modifiées. Il est de votre responsabilité de vous protéger :
  - Antivirus
  - Pare-feu
  - Utilisation de protocoles sécurisés
  - Réseau privé virtuel (VPN)
- Les traces des connexions sont enregistrées dans des journaux et conservées un an.
- Un identificateur et son mot de passe associé ne peut être utilisé que sur une seule machine.
- De la traduction d'adresses (NAT) est effectuée ce qui peut poser des problèmes avec certains protocoles.

## Veillez vous identifier

Identifiant :

Mot de passe :

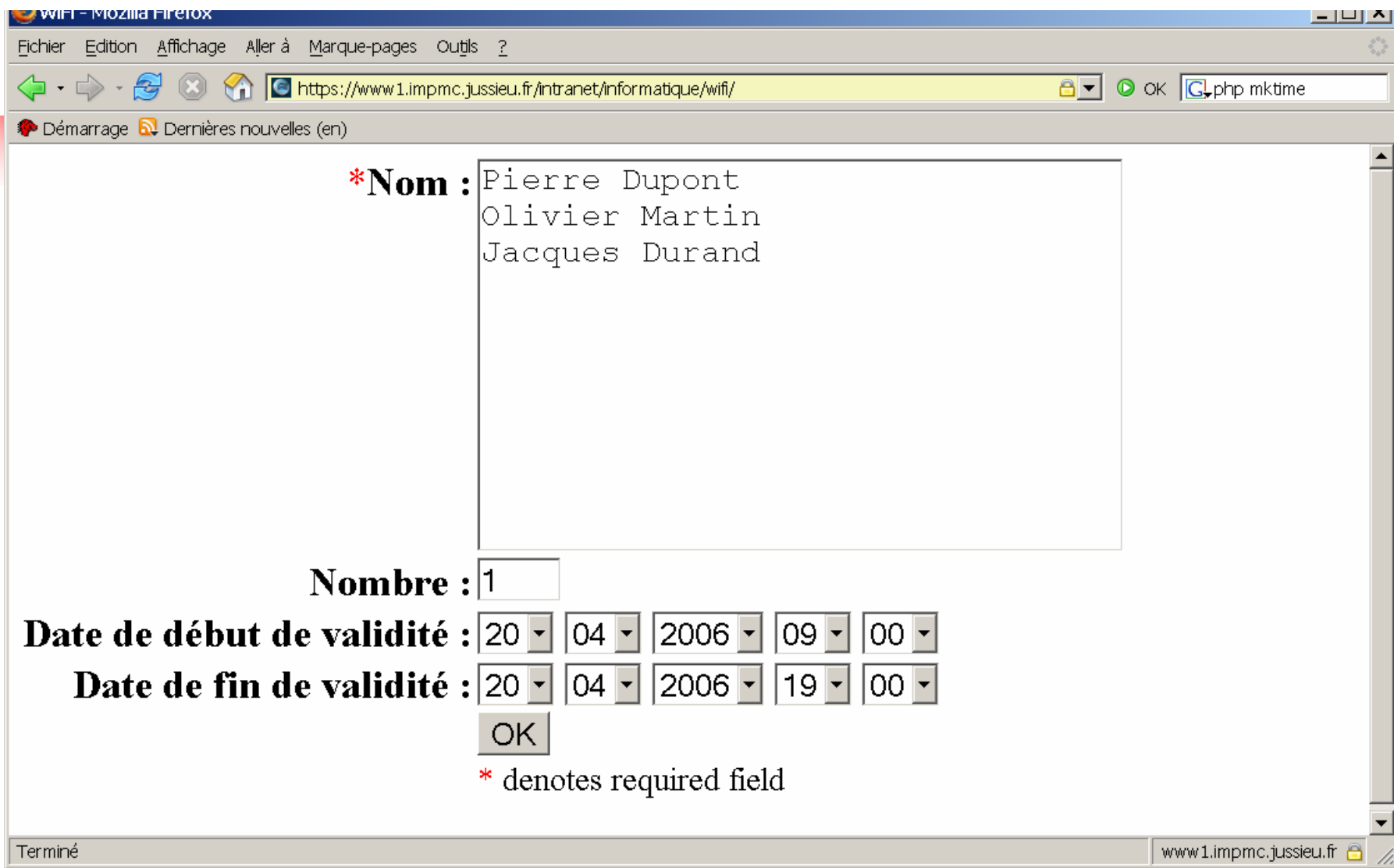
OK



# Authentification

---

- Mécanisme
  - Identifiant/mot de passe transmis par m0n0wall à un serveur RADIUS
  - RADIUS sous-traite l'authentification à LDAP
  - Choix lié à l'existant. Autres possibilités :
    - Base d'utilisateurs gérée par RADIUS
    - Base d'utilisateurs locale à m0n0wall
- Application PHP
  - Génère des identifiants éphémères
  - Les stockent dans l'annuaire LDAP



WiFi - Mozilla Firefox

Fichier Edition Affichage Aller à Marque-pages Outils ?

https://www1.impmc.jussieu.fr/intranet/informatique/wifi/index.php

Démarrage Dernières nouvelles (en)

# Bienvenue à l'IMPMC

## Pierre Dupont

Vous êtes invité par : Francois Morris (Francois.Morris@impmc.jussieu.fr)

Afin de répondre aux besoins de ses visiteurs l'IMPMC offre à titre gracieux un accès sans fil à Internet. Nous ne pouvons garantir la qualité du service et nous faisons appel à la responsabilité de chacun pour ne pas abuser des possibilités offertes.

### Mise en garde

- Le réseau sans fil n'est absolument pas sécurisé. Les données échangées peuvent être écoutées, interceptées ou modifiées. Il est de votre responsabilité de vous protéger :
  - ◊ Antivirus
  - ◊ Pare-feu
  - ◊ Utilisation de protocoles sécurisés
  - ◊ Réseau privé virtuel (VPN)
- Les traces des connexions sont enregistrées dans des journaux et conservées un an.
- Un identificateur et son mot de passe associé ne peut être utilisé que sur une seule machine.
- De la traduction d'adresses (NAT) est effectuée ce qui peut poser des problèmes avec certains protocoles.

### Pour vous connecter

Le nom du réseau (SSID) est **impmc**. L'accès est ouvert, sans aucun chiffrement (ni WEP, ni WPA). Les accès au réseau sans fil sont contrôlés par un portail captif. Tant que vous n'êtes pas authentifié aucune connexion à Internet n'est possible. Pour vous authentifier vous devez lancer votre butineur favori. Il vous sera alors demandé de fournir un identifiant et son mot de passe associé.

**Identifiant : ufzpd**

**Mot de passe : gqnag19d**



# Tunnel sur DNS

---

- Nécessité DNS avant authentification
- M0n0wall serveur DNS
  - Défini dans le DHCP
  - Relais les requêtes DNS
- Tunnel sur DNS
- Faiblesse de bien des « hot spots »
- Parades
  - Surveillance + liste noire adresses MAC
  - Limitation du trafic



# M0n0Wall

---

- Pare-feu + portail captif
- Site : <http://m0n0.ch/wall/>
- Présentation :  
<http://www.ossir.org/sur/supports/2006/20060314m0n0wall.pdf>
- FreeBSD 4-11



# Risques et perspectives

---

- Se méfier des faux point d'accès
  - Très simple à mettre en œuvre pour un pirate
  - Récupère identifiant/mot de passe
  - Contre mesure : identifiants éphémères
- Fonctionne aussi pour le réseau filaire
  - Toute machine non reconnue -> VLAN WiFi invité
    - Adresse MAC (VMPS Cisco)
    - 802.1x
- Ouverture aux permanents
  - Accès au réseau interne via openVPN
  - Authentification par certificat client
    - Eviter les multiples identifiants et mots de passe
    - Nécessite une modification de m0n0wall