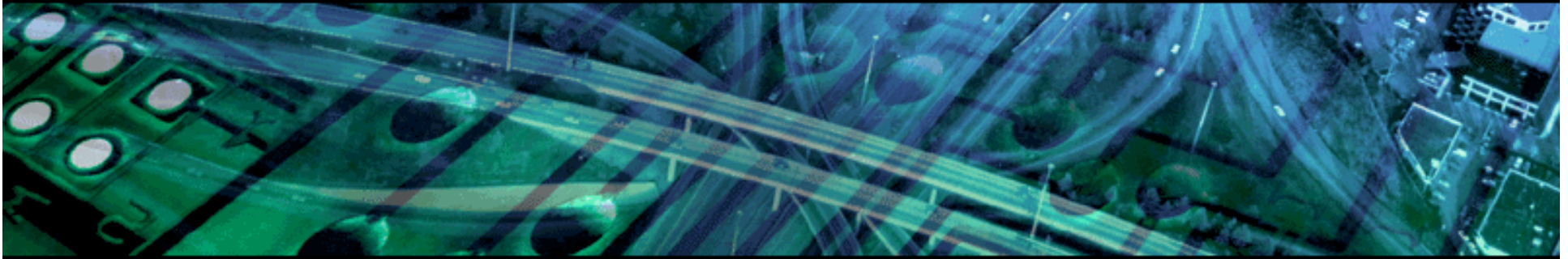


La sécurité des réseaux est-elle compromise  
avec l'arrivée du sans-fil et des réseaux  
virtuels privés (VPN) ?



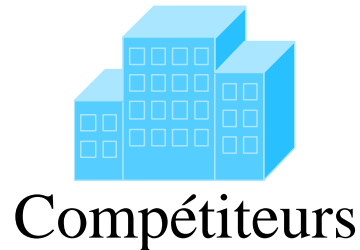
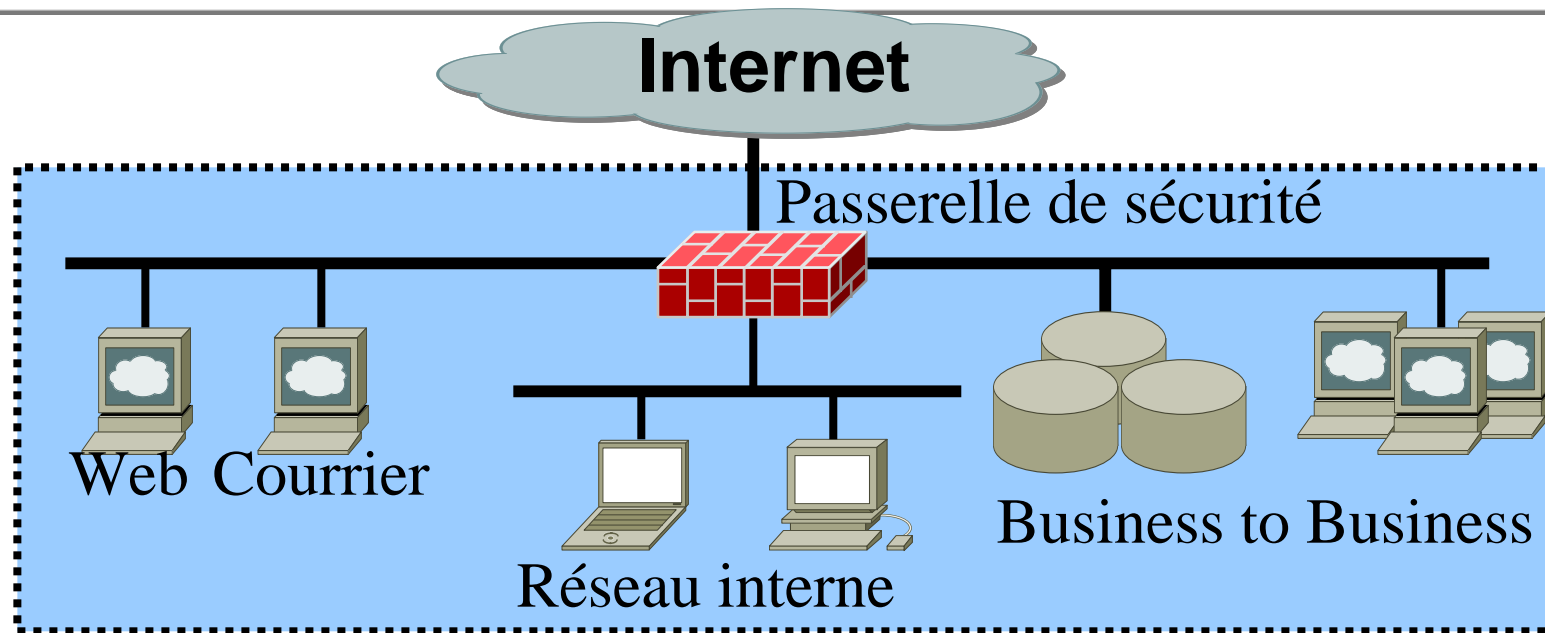
Régis Desmeules  
Viagénie inc  
6 mai 2002



[Regis.desmeules@viagenie.qc.ca](mailto:Regis.desmeules@viagenie.qc.ca)

- Effort important pour protéger les données, les systèmes et les transactions B2C et B2B
- Développement de politiques de sécurité
- Changement de certaines habitudes de travail
- Investissement important dans les infrastructures, les architectures réseaux, les produits de sécurité
- Embauche et formation du personnel en sécurité
- Veille technologique
- Effort permanent pour assurer le respect des politiques de sécurité

# Périmètre de sécurité avant le sans-fils



## **Économique**

- Fraction du coût en comparaison des réseaux câblés
- Interface à ~150\$ par ordinateur, AP pour ~200\$
- Interfaces de plus en plus incluses dans les portables et les palm

## **Flexibilité**

- Facile et rapide à déployer par comparaison aux réseaux câblés
- Connectivité réseau dans une salle de réunion, de conférence
- Mise en place temporaire d'un réseau pour des centaines/milliers d'utilisateurs

## **Mobilité**

- Outil idéal pour rester connecté même en voyage : aéroports, hôtels et centres de congrès offrent le service, liberté de mouvement

## Écoute passive

- Trames 802.11b circulent librement dans l'air
- Interception des trames 802.11
- Ouverture et analyse des paquets IP

## Conséquences

- Lecture des courriers reçus et envoyés par les usagers
  - Protocoles POP, SMTP, IMAP...
- Interception des codes d'accès et des mots de passe des applications corporatives
  - Protocoles Microsoft, Oracle DB, SQL-net, POP, Telnet, FTP, Web
- Accès à des données confidentielles
  - Contenu des sessions transactionnelles internes non chiffrées

## Matériel utilisé

- Portatif avec une carte 802.11b et logiciel d'écoute
- PDA (Palmtop) avec interface 802.11b

## Distance

- Proche ou loin, pas de différence
  - Proche :
    - Dans le corridor, près ascenseurs, dans les escaliers de secours, dans les toilettes publiques, etc.
    - Extérieur de l'édifice, dans le stationnement, de l'autre côté de la rue, d'une auto, dans un édifice voisin
  - Loin :
    - Avec une antenne avec un bon gain, c'est possible à des dizaines de kilomètres de distance

## **WEP : Wired Equivalent Privacy protocol**

- Protection communications 802.11 pour contrer écoute passive
- Clé WEP pour protéger les échanges entre ordinateurs et AP
- Problèmes de sécurité importants découverts dans WEP
- Démonstration que WEP est vulnérable

## **Conséquences**

- Avec un « sniffer » de paquets 802.11 de type Airopeek, AirSnort, NetStumbler il est possible :
  - Extraction automatique de la clé WEP et accès aux réseaux sans autorisation
  - Détection de la « MAC address » du AP, nom du réseau, SSID, manufacturier, canal en usage (WEP utilisé ou pas)

## ARP poisoning

- Access Point est un « pont » entre 802.11 et 802.3 (Ethernet)
- Ordinateurs 802.11 et 802.3 se voient comme étant sur le même réseau physique, le même VLAN
- Personne malveillante avec un ordinateur 802.11 peut subtiliser l'adresse IP d'un ordinateur câblé (802.3) en forçant tous les ordinateurs et routeurs du réseau à modifier leur table ARP
- Il envoie des paquets « ARP reply » avec sa MAC address

## Conséquences

- Paquets IP destinés à l'ordinateur 802.3 lui sont envoyés, ensuite il peut les faire parvenir réellement à l'ordinateur 802.3
- Attaque de type man-in-the-middle
- Permet d'écouter et de modifier les sessions et les transactions

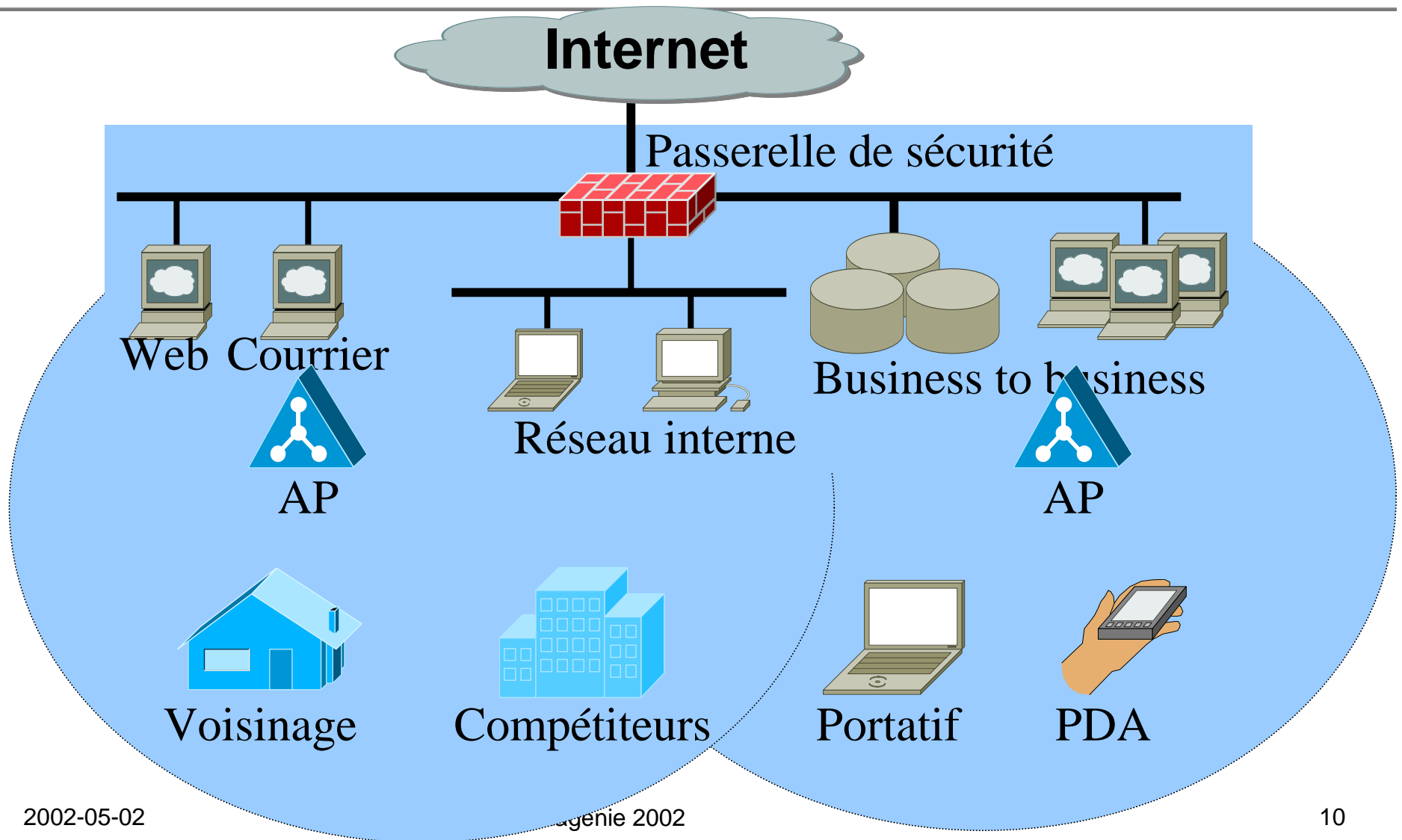
## **Mauvaises configurations**

- Utilisation de la configuration par défaut des AP
- Branchement du AP sur le backbone du réseau
- WEP n'est pas utilisé
- Si WEP est utilisé, utilisation de la clé de chiffrement par défaut
- Valeur SSID défaut du manufacturier
- Pas de restriction par MAC address

## **Conséquences**

- Intrusion sur le réseau interne de l'entreprise, sans aucun filtrage
- Écoute et attaque des communications internes
- Connectivité Internet gratuite pour tous !!

# Périmètre de sécurité avec le sans-fil



# Exagération du problème ?

<http://www.dis.org/wl/maps/>



## **Configurer adéquatement AP**

- WEP
- Désactiver le mode bridging dans AP
- Accès selon MAC address (freine seulement)

## **Modifier architecture**

- Réseau 802.11b sur une branche externe spécifique de la passerelle de sécurité
- Aucun accès vers le réseau interne sans authentification forte et chiffrement élevé

## **Évaluer le risque pour chaque application**

- Considérer le réseau sans-fil comme un réseau autant sinon plus dangereux qu'Internet
- Sécurité sur IP : ~ IPsec, couche SSL sur applications importantes

# Pourquoi les VPNs ?

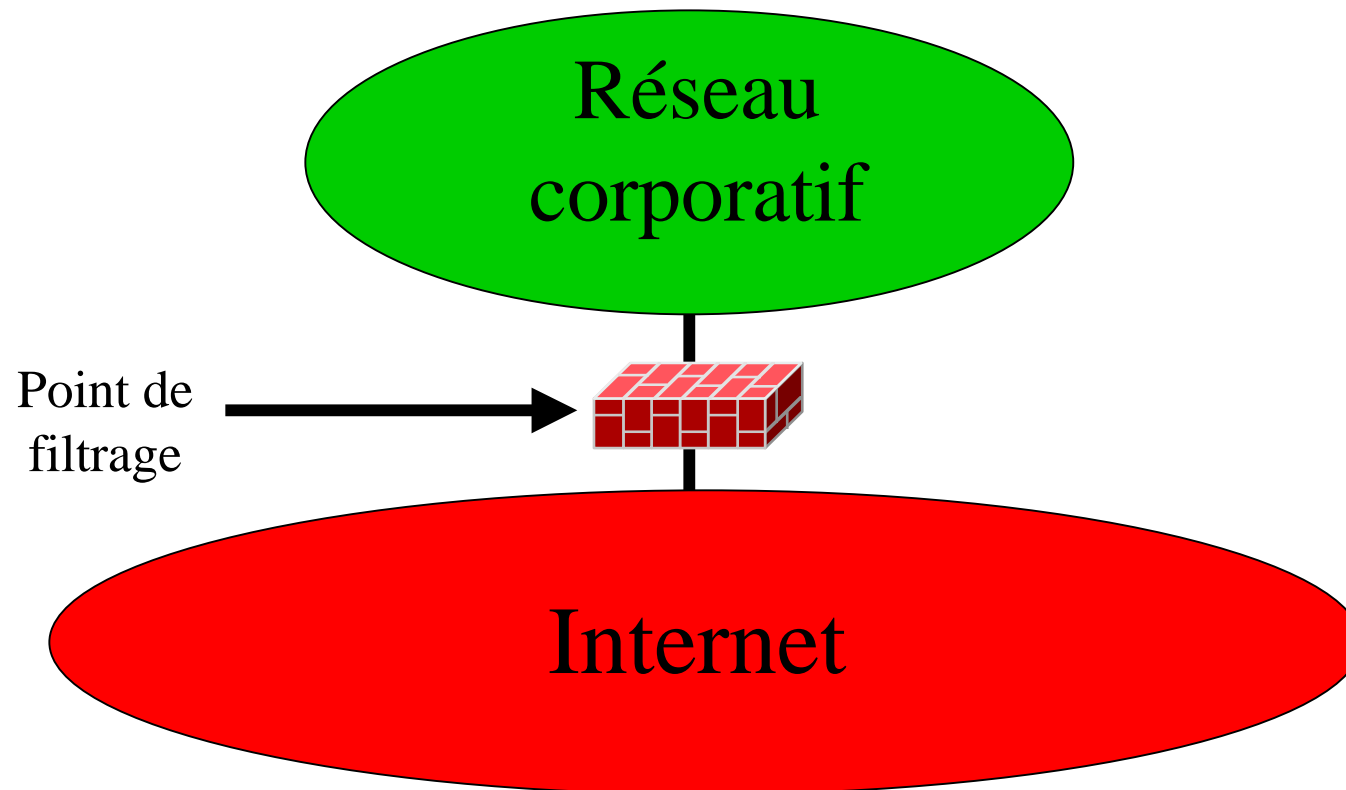


## **Accessibilité**

- Moyen facile de donner accès à un réseau à ses employés externes et aux partenaires d'affaires
- Facile à déployer par rapport à la mise en place de liens dédiés

## **Travail à distance**

- Moins d'infrastructure (espace de bureau) dans l'entreprise
- Permet la mobilité dans les affaires



## **Réseau corporatif est sécuritaire parce que**

- Derrière une passerelle de sécurité
- Employés accèdent par ligne téléphonique (modem) et VPN

### **FAUX**

- Comment être certain que l'ordinateur utilisé est seulement connecté à une ligne téléphonique ?
- Avons-nous le détail exact de tous les programmes et applications installés sur l'ordinateur distant (IRC, etc.)?

## **Réseau corporatif est sécuritaire parce que**

- Employés accèdent par des VPN à travers Internet avec chiffrement 128 bits et authentification forte

### **FAUX**

- Comment être absolument certain que l'ordinateur distant n'est pas compromis ?

## **Ordinateur employé :**

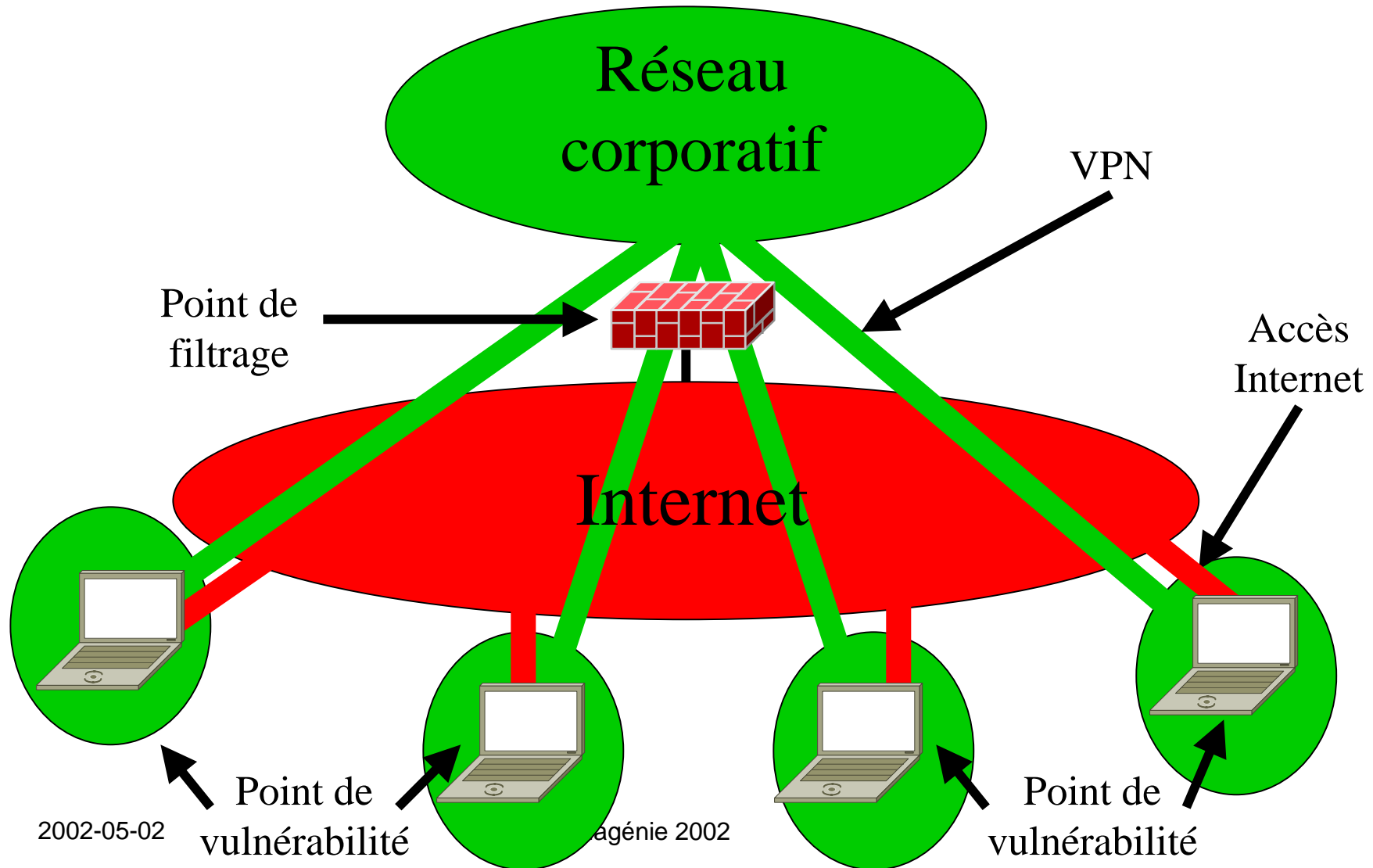
### **Utilisé par toute la famille pour accéder à Internet**

- Jeux et toutes sortes de programmes sont installés
- Connaissance de tous les programmes installés et de leur vulnérabilités ?

### **Connecté à Internet avec ou sans passerelle de sécurité personnelle**

- Système d'exploitation comme Microsoft, même lorsque bien installé, très vulnérable, services IP ouverts...
- Passerelles pour les consommateurs sont très simplistes

### **Comment assurer l'application des politiques de sécurité de l'organisation lorsque le poste est à distance ?**



# Exagération du problème ?



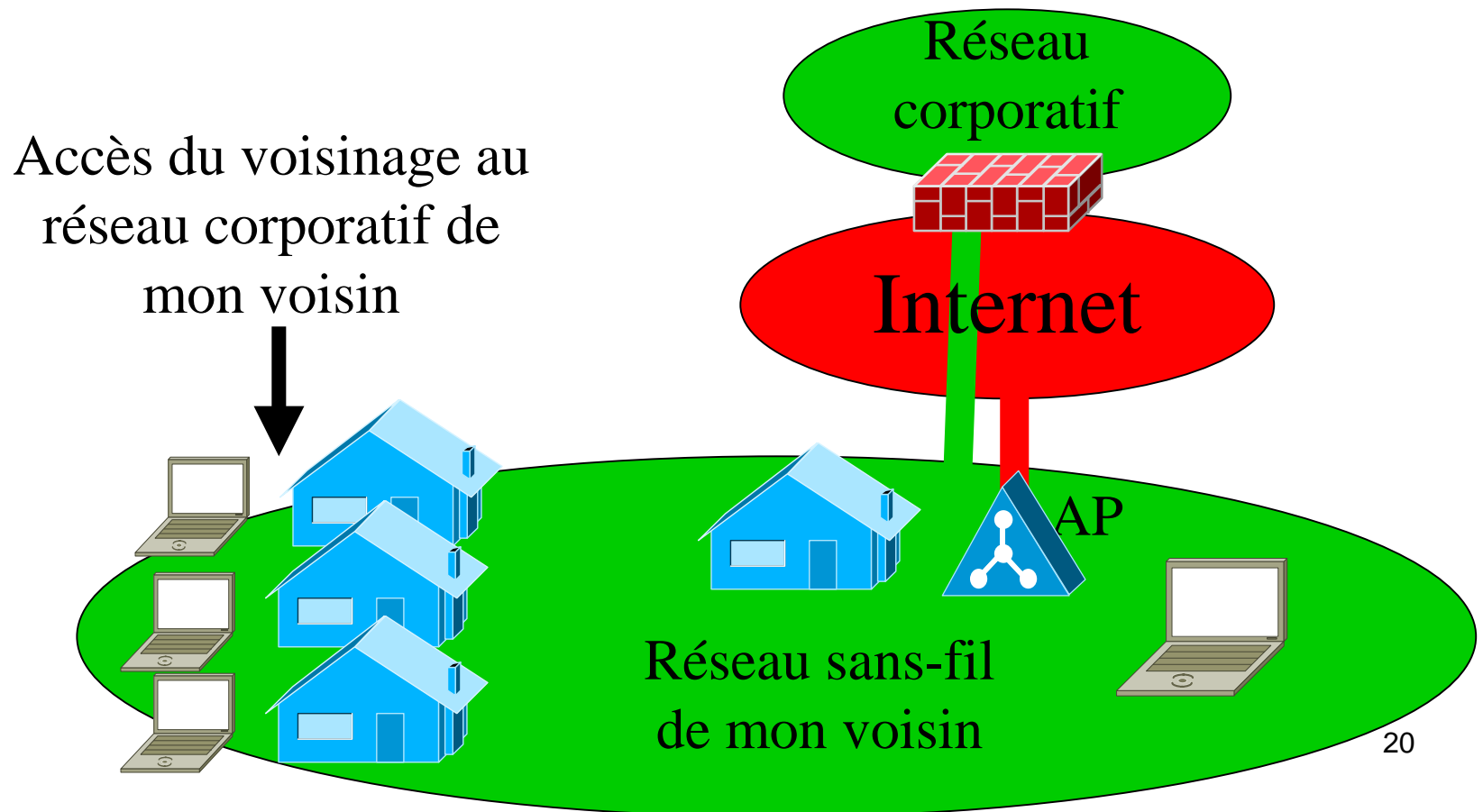
- À l'automne 2000, du code source, des schémas, des plans et des documents numériques ont été dérobés chez Microsoft Corporation par des pirates informatiques
- Pirates se seraient d'abord introduits par l'ordinateur d'un employé de Microsoft qui travaillait de son domicile
- Pirates se sont servis de cet ordinateur comme pivot pour pénétrer le réseau corporatif de Microsoft

## Référence :

<http://www.cnn.com/2000/TECH/computing/11/07/home.workers.idg/>

- Forcer l'utilisation d'une passerelle de sécurité personnelle, d'un système de détection d'intrusions et de chiffrement du disque dur sur l'ordinateur
- Corporation s'occupe de l'installation, de la configuration et du support de l'ordinateur
- Assurer l'application des politiques de sécurité corporatives pour les accès distants
- Surveillance et vérification régulière des logiciels installés dans les ordinateurs

- Imaginez maintenant un employé qui travaille de chez lui avec un VPN via son réseau local sans-fil !!!!



- Investissements importants ont été réalisés dans la sécurité des réseaux corporatifs
- Technologies sans-fil et des VPN offrent plus de flexibilité aux organisations
- Cependant, une méconnaissance de ces technologies et de la bonne façon de les utiliser/déployer :
  - Augmente risque
  - Infraction aux politiques de sécurité corporatives
- Plusieurs pistes et solutions sont possibles pour diminuer les risques de sécurité de ces technologies

- La sécurité des réseaux est-elle compromise avec l'arrivée du sans-fils et des VPN  
**<http://www.viagenie.qc.ca/fr/doc/cours/crim2002.pdf>**
- AEROPEEK <http://www.wildpackets.com/products/airopeek>
- AIRSNORT <http://airsnort.shmoo.com/>
- NETSTUMBLER <http://www.netstumbler.com/>