Sécurité Réseaux Avancée

Enjeux, technologies et perspectives

Sommaire

- Présentation
- Introduction
- État des lieux
  - Tendances
  - Vers et virus
  - Spam
  - Phishing
  - Dénis de service
- Concepts
  - Défense en profondeur
  - Extension du périmètre
  - Architecture distribuée
- Technologies
- Perspectives

Présentation

- Sécurité des systèmes Unix et réseaux TCP/IP
  - Solutions de sauvegarde
  - Solutions de filtrage
  - Détection d'intrusions
  - Solutions antivirus
- Objectifs du cours
  - Présenter les enjeux et les outils de sécurité des réseaux sous un angle pragmatique et pratique

Introduction

- Limites des solutions de sécurité traditionnelles
  - Le filtrage simple ne suffit plus.
  - Les applications deviennent la cible des attaques.
  - Les contours du SI deviennent flous.
- Les évolutions actuelles de la menace ont des impacts :
  - Technologiques
    - Pare feux « intelligents »
  - Architecture du SI

État des lieux (1)

- Tendances
  - Permanence de la menace virale
  - Montée en puissance des malwares
  - Mobilité croissante
- Changement dans la topologie des cibles
  - Entreprises de mieux en mieux protégées
    - Techniquement
    - Juridiquement
  - Particuliers de plus en plus exposés
    - Offres de connexion haut débit
    - Pas ou peu d'expertise technique

État des lieux (2)

- Menace virale
  - Mobiles des attaquants
    - Nature des attaques
      - Nuisance, vandalisme
    - Motivations
      - Publicité
    - Vecteurs
      - Courrier électronique
    - Évolutions actuelles
      - Professionnalisation de l'activité
      - Appât du gain
      - Nouveaux vecteurs (messagerie instantanée, outils P2P)

État des lieux (3)

- SPAM
  - Ne constituent pas une attaque en soi mais portent atteinte à la disponibilité des ressources : bande passante, temps de traitement, stockage, temps de lecture.
  - Motivent la recherche de relais et donc encouragent la création et le diffusion de vers et de virus
- Phishing
  - Attaque « ultime » : la cible est l'utilisateur lui-même, que l'on cherche à tromper.
  - La réponse n'est pas seulement technologique.

Phishing (1)

- Faux messages d'alertes envoyés par courrier électronique.
- Renvoient le destinataire vers la copie d'un site réel.
- Objectifs
  - Vol de coordonnées bancaires
  - Vol de paramètres de connexion à des sites marchands
- S'appuient sur la crédulité des utilisateurs
- Associent parfois des attaques en déni de service contre les vrais sites.

Phishing (2)

- Plusieurs techniques de camouflage dans le code HTML
  - Valeur de la balise HREF différente du texte associé
    - www.bank.com
  - Ne résiste pas à la lecture de l'URL dans la barre de navigation.
  - Techniques plus sophistiquées
    - Utilisation d'un mot de passe dans l'URL
      - http://www.bank.com:1234FR7YY/ **219.110.2.3**
    - Utilisation de l'encodage Unicode dans l'URL
    - Remplacement de la barre d'URL par une image.
    - Utilisation de site de redirection (volontaire… ou non !)
      - Google, MSN, Yahoo!
    - Un « mix » de toutes ces techniques

Phishing (3)

Sujet : **SouthTrust Bank - urgent security notice [Mon, 27 Jun 2005 07:31:04 +0400]**
De : SOUTHTRUST BANK <support_id_42694086854802@southtrust.com>
Date : 5:39
Pour : guillaume.alet@free.fr

SouthTrust

Dear SouthTrust bank customer,

Technical services of the SouthTrust bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

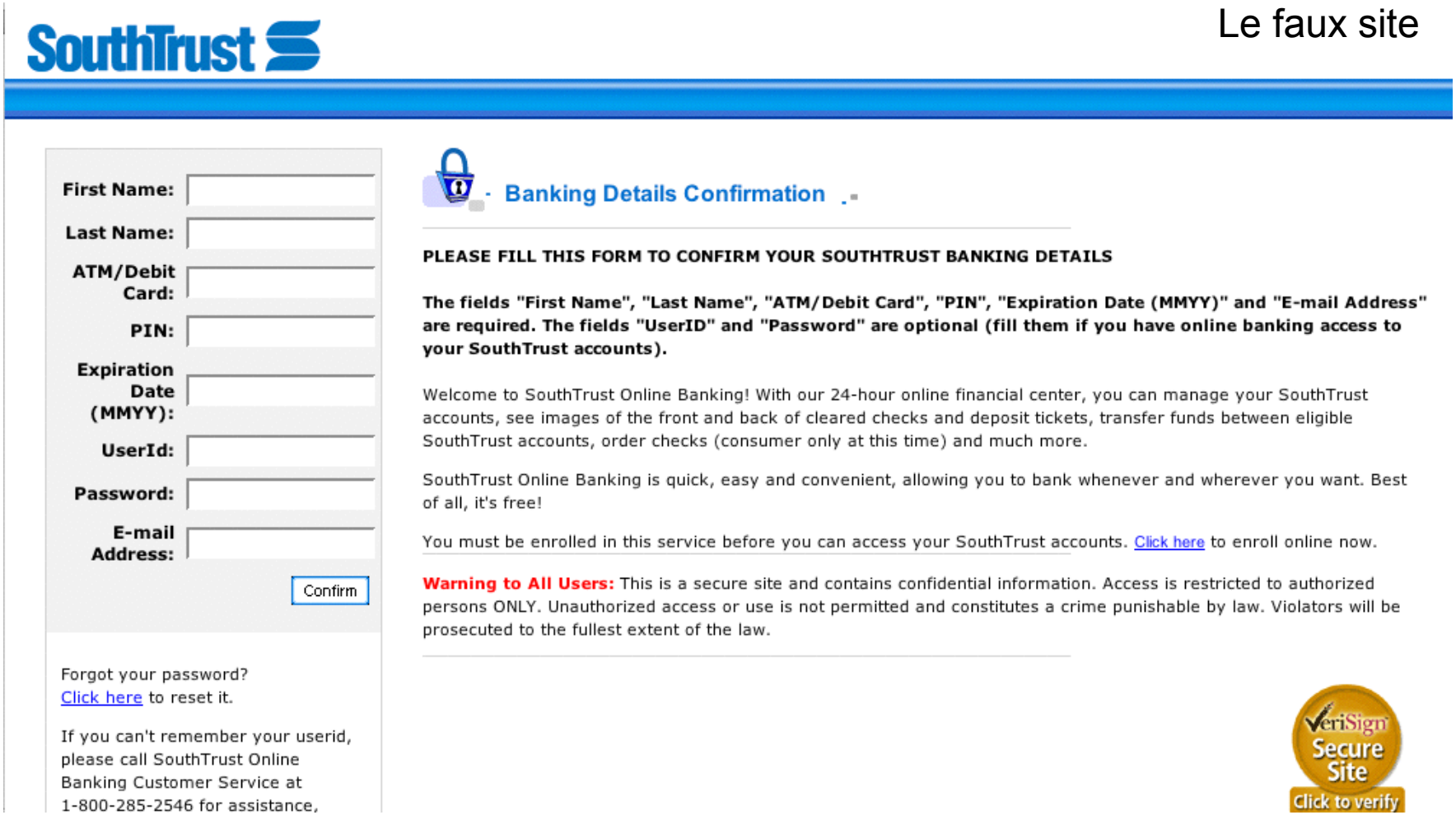
https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation

Please do not answer to this email – follow the instructions given above.

We present our apologies and thank you for co-operating.

Phishing (4)

Le faux site



Phishing (5)

SouthTrust

Le vrai site

UserId:

Password:

Log In Exit

Note: SouthTrust and Wachovia are joining together under the Wachovia name. If you have completed the process to set-up a Wachovia User ID and Password, please log in to Wachovia Online Services.

Forgot your password?
Click here to reset it.

New Log In Instructions:

- If you access accounts in Florida, Georgia, South Carolina, North Carolina or Virginia, you will need to log in as usual and follow the steps to switch over to Wachovia.

Online Banking Log In

No Merger Communications via Email

SouthTrust and Wachovia have become aware of fraudulent emails designed to capitalize on our merger activities. Please note all communications about the conversion of your Online Services will be sent to you by U.S. Mail or SouthTrust's internal Bank Messages. We will not send any conversion communications by email during the merger.

If you do receive email about the Online Services conversion that appears to be from Wachovia or SouthTrust, do not reply or click on any links. Email, sent to your personal or business address, regarding the merger is not authorized by Wachovia or SouthTrust. If you receive a suspicious email regarding the merger, please forward the email to abuse@southtrust.com or call us at 800-285-2546.

Effective, June 13, 2005, SouthTrust and Wachovia have combined banking networks in Florida, Georgia, South Carolina, North Carolina and Virginia. If you have SouthTrust accounts in those states, online access to your accounts has been transferred to Wachovia Online Services. To access your accounts, you must switch your log in information to Wachovia. Follow the **New Log In Instructions** at left.

Later in 2005, SouthTrust and Wachovia will combine banking networks in Tennessee, Mississippi, Alabama, and Texas. If you have accounts in those states, continue to log in to SouthTrust Online Banking until further notice.

Warning to All Users: This is a secure site and contains confidential information. Access is restricted to authorized persons ONLY. Unauthorized access or use is not permitted and constitutes a crime punishable by law. Violators will be prosecuted to the fullest extent of the law.

Phishing (6)

Bank of America Higher Standards

Le message d'alerte

Dear Bank of America Member,

This information is collected to provide a record of communications between Bank of America and members and to comply with any applicable legal and/or regulatory requirements. For example, the information we collect is used for purposes such as:

* To identify you in order to protect against fraud and guard against unauthorized access to your accounts.
* To enable us to complete your transactions quickly and efficiently, and to provide you with quality customer service.
* To better serve your relationship by understanding which services may be the right match for your needs, and telling you about new offers that may be of interest to you.
* To help ensure that our information about you is current and accurate.

We suspect that your Bank of America account has been accessed by an unouthorised third party. Numerous login attempts were made from:
IP address: 24.123.125.75
ISP host: rrcs-24-123-125-75.central.biz.rr.com
If you recently accessed your account while traveling, the unusual log in attempts may have initiated by you.

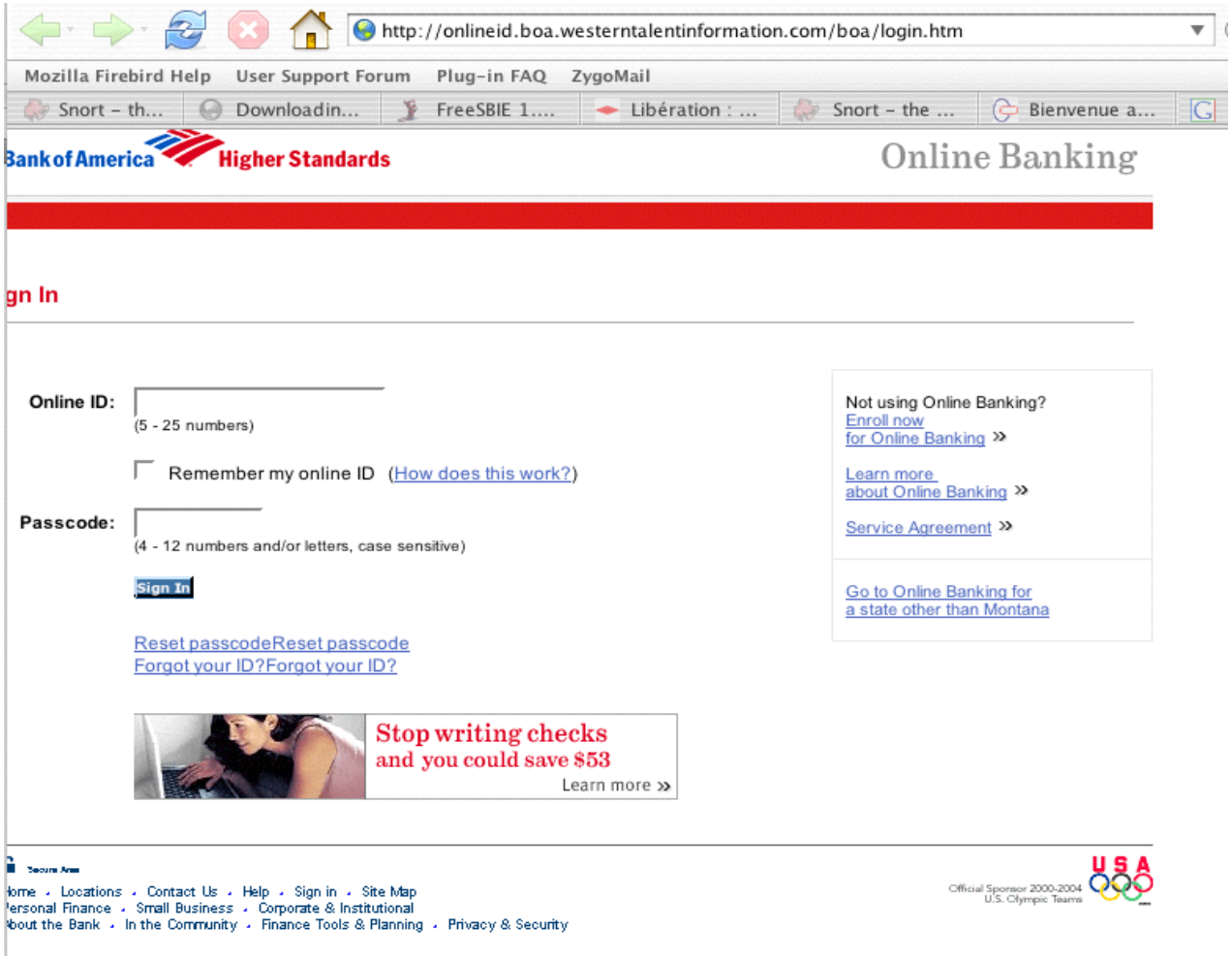
Therefore, as a precautionary measure and to ensure yourself that everything is normal with your ballance and personal information, please confirm your identity by completing the account verification process.

To get started click on the link below:

https://onlineid.bankofamerica.com/cgi-bin/sso.login.controller?state=all

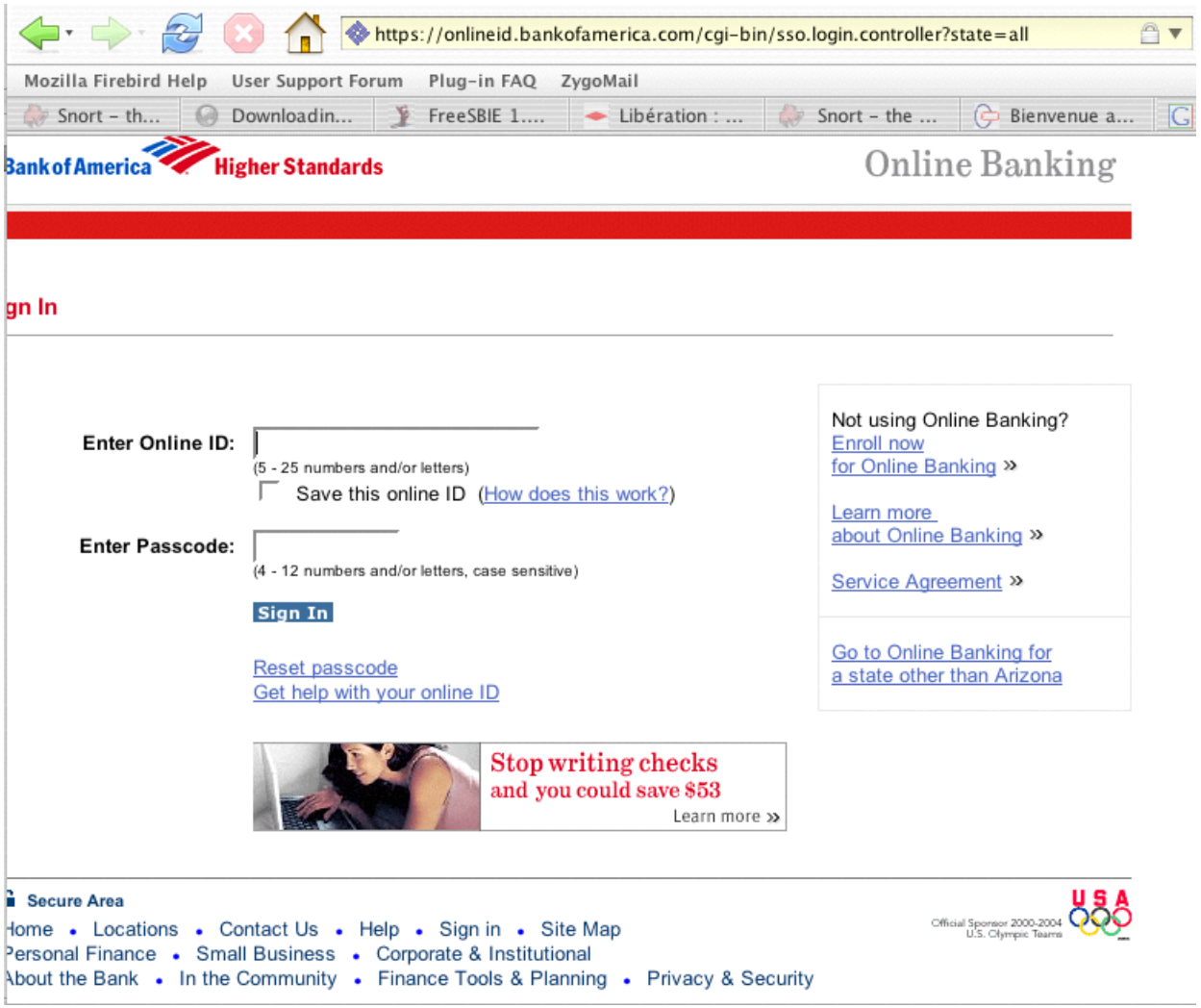
Phishing (7)

Le faux site :

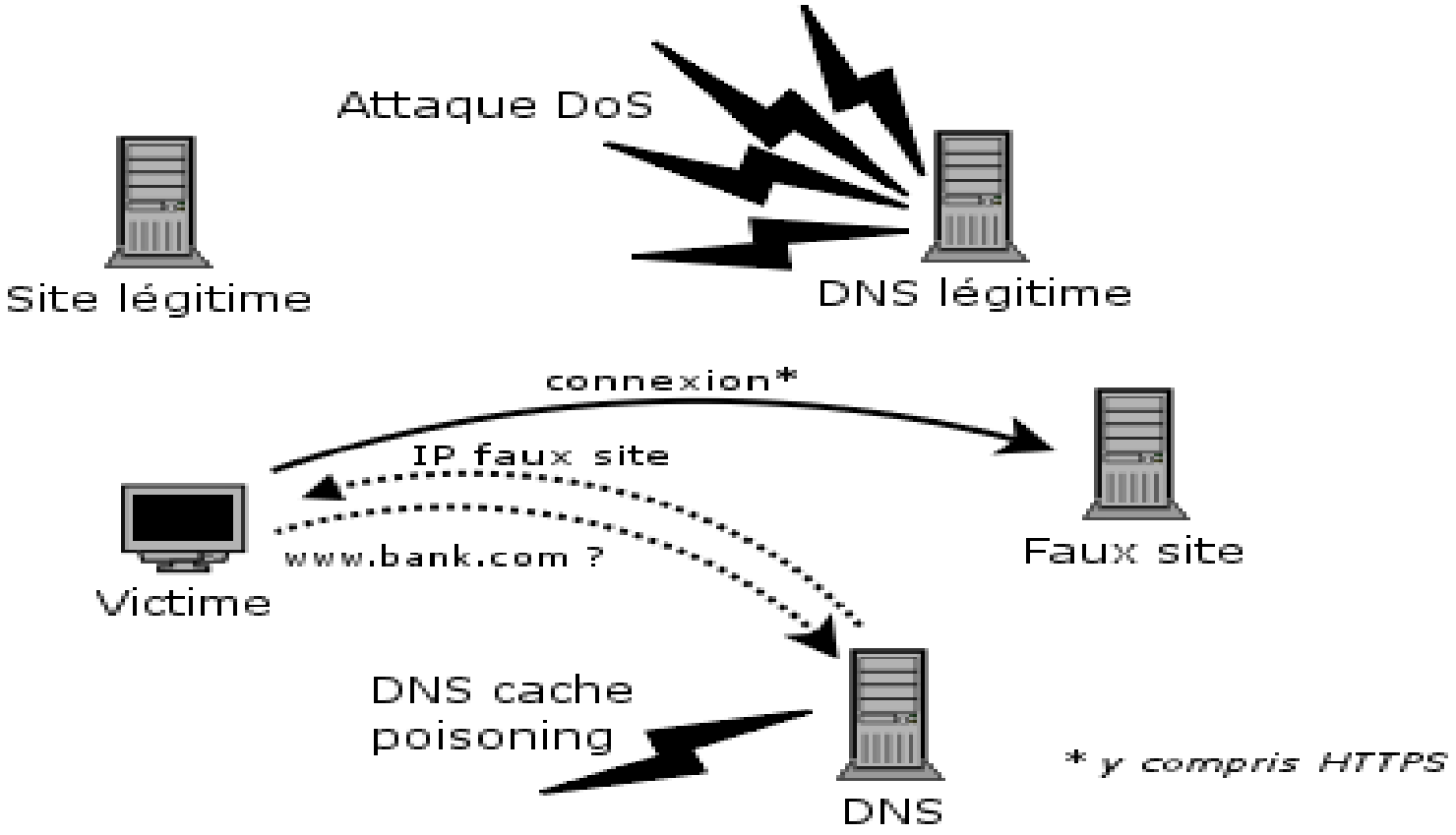


Phishing (8)

Le vrai site :



Phishing + Pharming



État des lieux (4)

- Entreprises
  - Globalement mieux protégées que par le passé
    - Prise de conscience de la nécessité de se protéger
    - La riposte s'organise aussi sur le plan juridique
  - Espionnage et vol de données restent d'actualité
    - Revente d'informations à la concurrence
    - Vol de code source (éditeurs de logiciels)
    - Extorsion de fonds, chantage au déni de service
      - Touchent les entreprises dont l'activité est intimement liée à Internet : sites de commerce électronique, sites de jeux en ligne
    - Attaques plus furtives

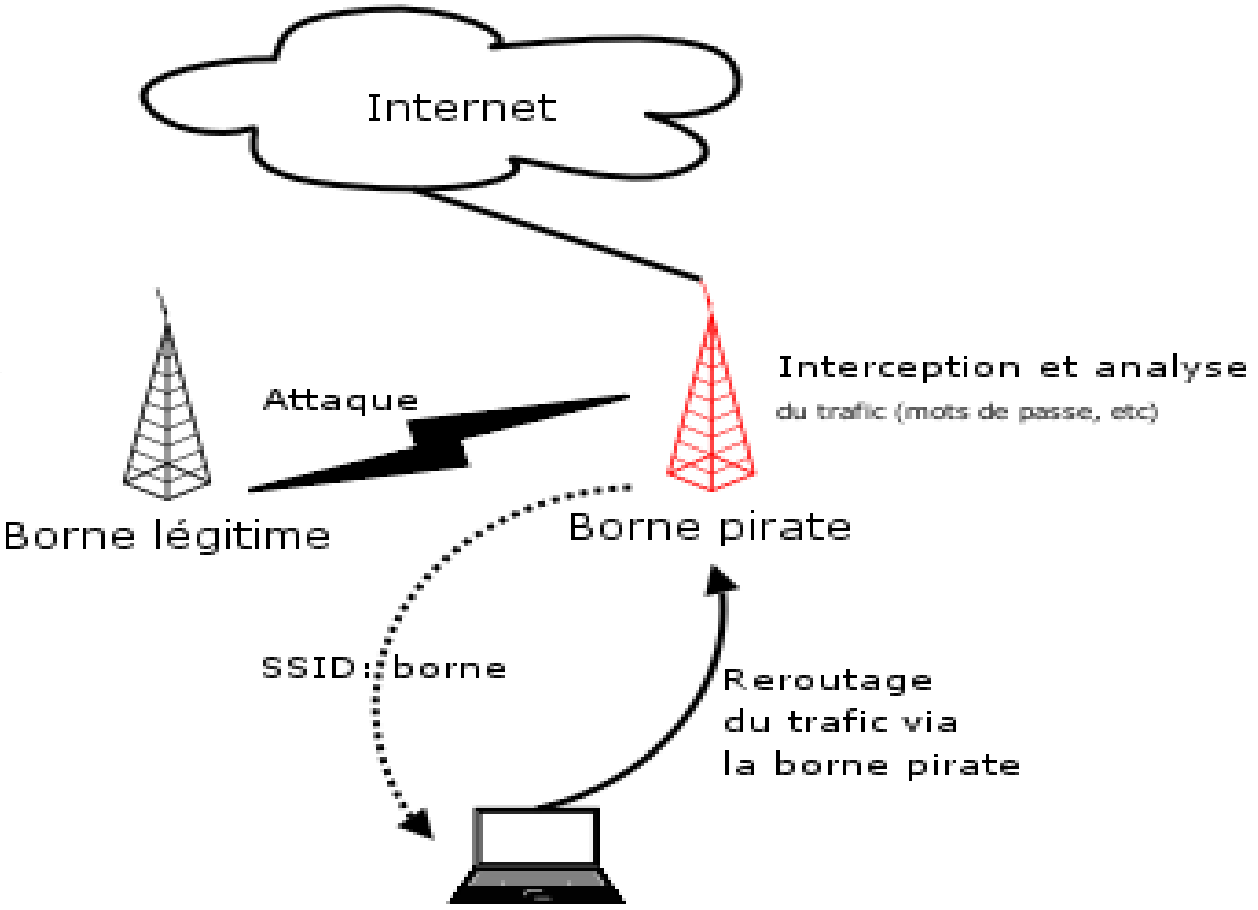
État des lieux (5)

- Particuliers
  - Forte concurrence sur les offres de connexion Haut Débit
  - Couplage Internet / Téléphonie sur IP
  - Peu d'expertise technique
  - Cibles à plusieurs titres
    - Directes
      - Vol de données bancaires, détournement de fonds
    - Indirectes
      - Vol de ressources, création de « botnets »
        - Utilisées pour des attaques en déni de service ou comme relais d'envoi de spams

État des lieux (6)

- Mobilité
  - WiFi
    - Équipements livrés « prêts à l'emploi »
    - Déploiement parfois anarchique en entreprises
    - Connexions « pirates » (points d'accès mal configurées)
  - Téléphones mobiles
    - Apparition de virus pour GSM
    - Virus BlueTooth

Attaque WiFi



État des lieux (7)

- Nomadisme
  - Ordinateurs portables qui sortent du SI de l'entreprise, sont connectés à Internet en dehors de ce cadre, puis sont réintroduits dans le SI.
  - Durant ce laps de temps, l'ordinateur ne bénéficie plus des mesures de protection : pare feux, antivirus, etc.
  - Il y a donc risque, et souvent réalité, d'infection ou de compromission du portable.
  - Contournement des protections lors de la réintroduction dans le SI.

État des lieux (8)

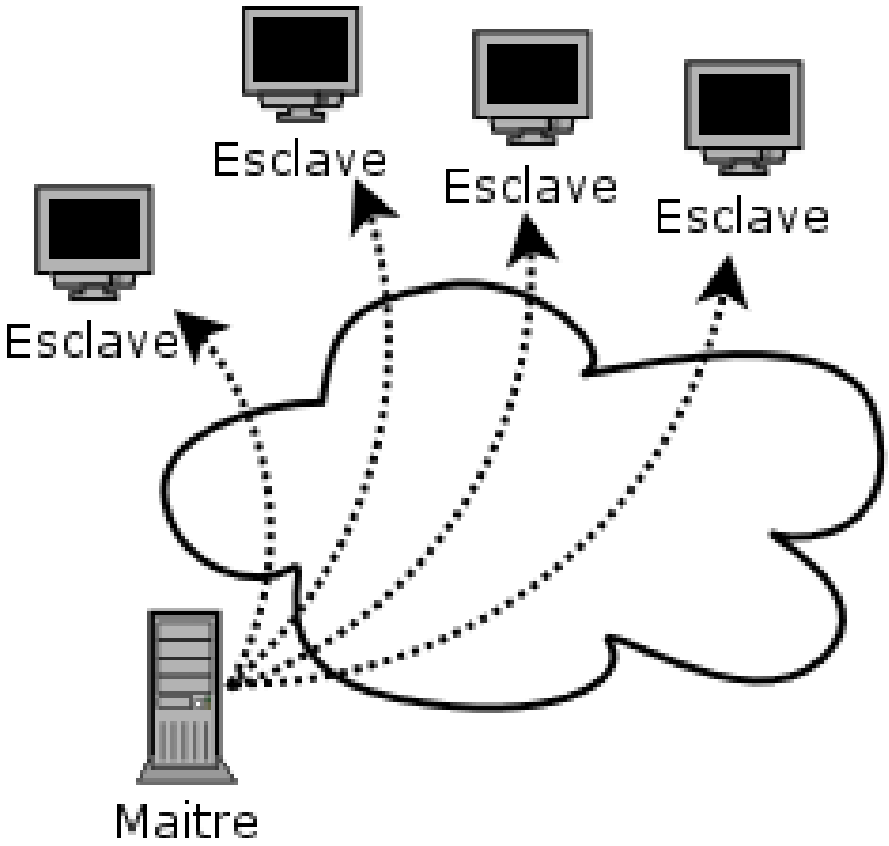
- Spyware / Adware
  - Adware : pollution publicitaire
    - Installation parfois volontaire mais pas toujours consentie
    - Peuvent rendre des services à l'utilisateur
    - Activité pas forcément illégal
  - Spyware : espionnage
  - Phénomène récent en constante progression
  - Souvent - mais pas exclusivement - lié à MS Windows et Internet Explorer
  - Point commun : appât du gain
    - Adware : revente aux annonceurs de l'espace publicitaire que constitue l'ensemble des « clients »
    - Spyware : vol de données, installation de portes dérobées, de « keyloggers »

État des lieux (9)

- Déni de service
  - « Vieille menace » redevenue d'actualité
  - Outil de chantage
    - Certains groupes de pirates n'hésitent pas à afficher les tarifs.
  - Outil de contre-propagande
    - Permet de réduire des sites « ennemis » au silence
  - Attaques encore très efficaces et redoutables
    - Leur résolution peut prendre plusieurs jours ou même semaines, et implique souvent plusieurs acteurs.

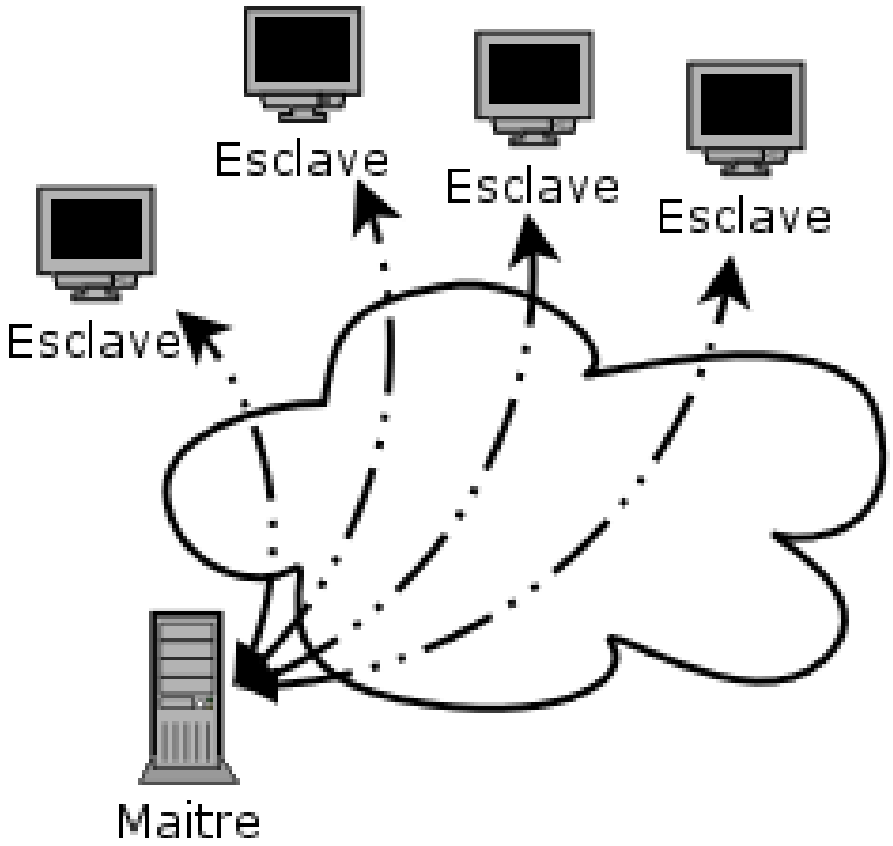
Déni de service (1)

Phase 1
Constitution du botnet :
- compromission directe
- infection informatique



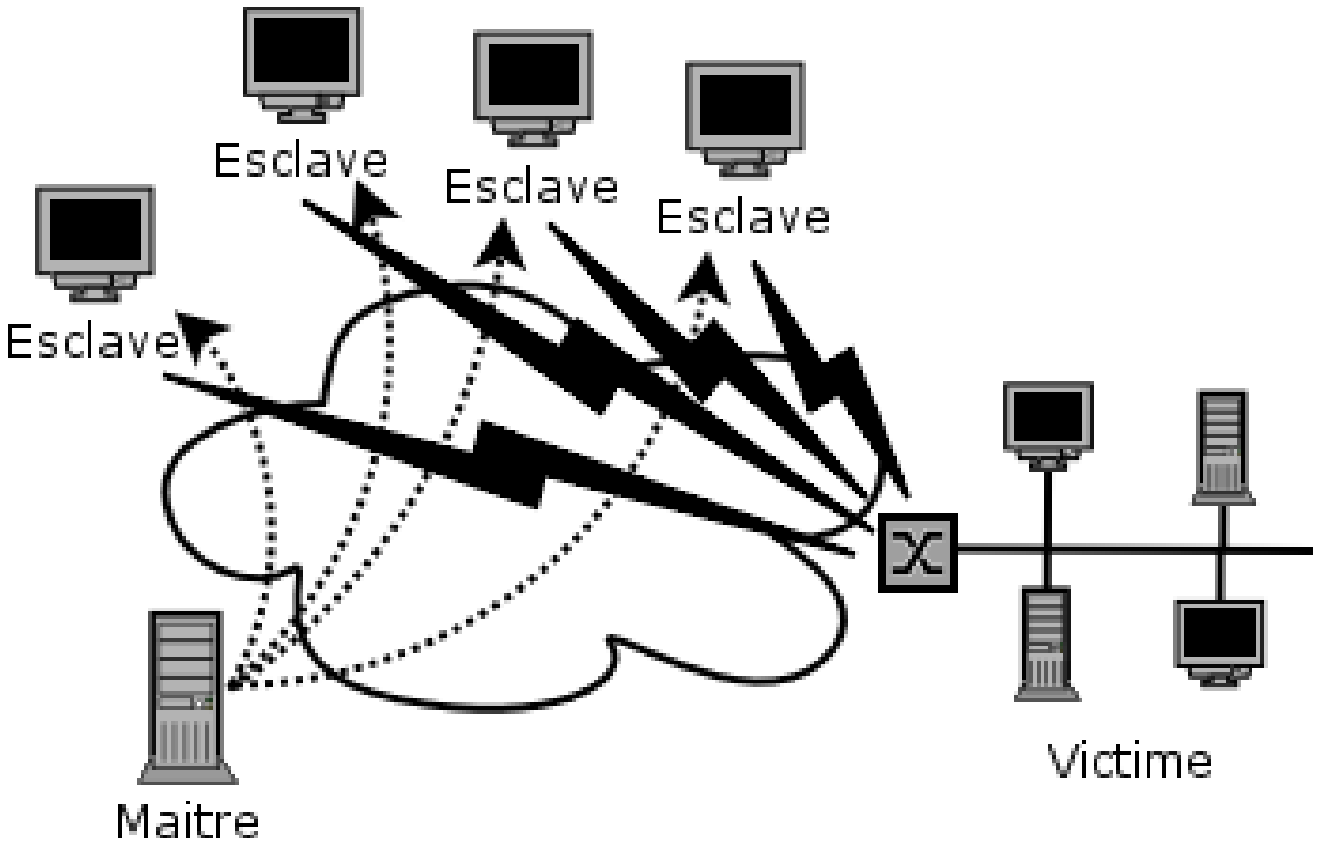
Déni de service (2)

Phase 2
Controle du botnet :
- Canaux IRC
- Peer to peer
- administration distante



Déni de service (3)

Phase 3 - Attaque



État des lieux (10)

- Cyberterrorisme
  - Notion vague
    - Les différentes définitions incluent les piratage de sites web jusqu'aux attaques contre des systèmes vitaux (énergie, transport, santé)
  - Aucun cas avéré à ce jour
    - Le ver Blaster aurait engendré ou aggravé des dysfonctionnements d'un système de supervision d'une centrale nucléaire américaine (panne de l'été 2003) mais aucun lien n'a pu être établi avec une quelconque organisation terroriste ni même criminelle.
  - Internet comme moyen de communication ou de financement (lien avec la cybercriminalité)

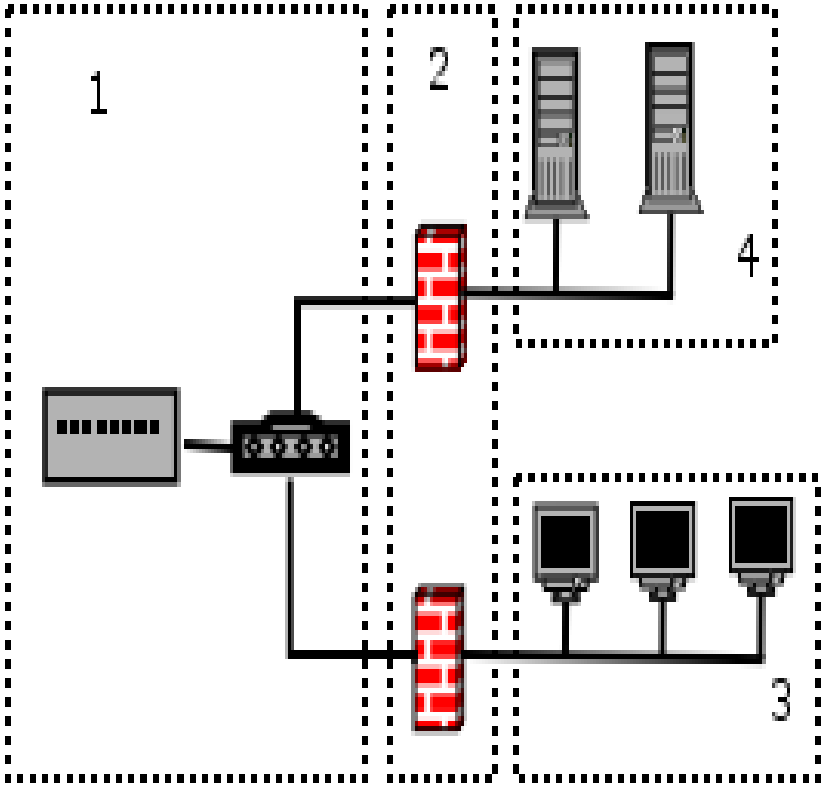
Concepts

- Défense en profondeur
  - Une barrière ou un seul type de barrières ne suffisent plus. La protection du SI s'organise en lignes de défense successives.
  - Ce concept permet de prendre en compte la complexité croissante des attaques.
- Extension du périmètre
  - Répondre aux défis du nomadisme et de la mobilité qui engendrent une certaine porosité du SI.
  - Le SI n'est plus localisé géographiquement, il tend à se « virtualiser ».
- Architecture distribuée

Défense en profondeur (1)

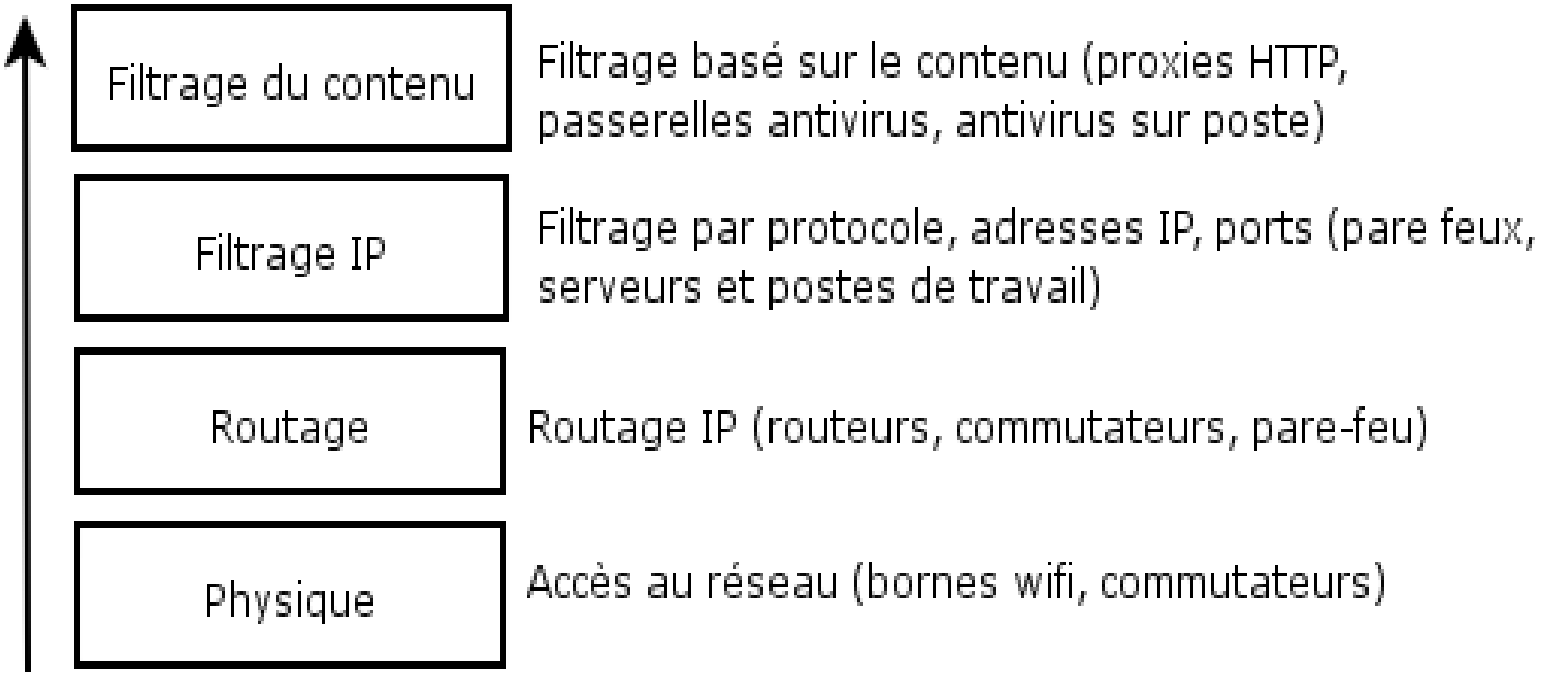
- Principes
  - Le SI est protégé par plusieurs lignes de défense.
  - Chaque ligne remplit trois fonctions :
    - Arrêter l'attaque
    - L'affaiblir ou la gêner
    - La retarder.
  - Chaque ligne de défense est autonome : la chute d'une ligne n'engendre pas celle d'une autre.
  - Certains éléments sont protégés plusieurs fois de façons différentes.
  - La gravité d'un événement dépend du nombre de barrières passées.

Défense en profondeur (2)



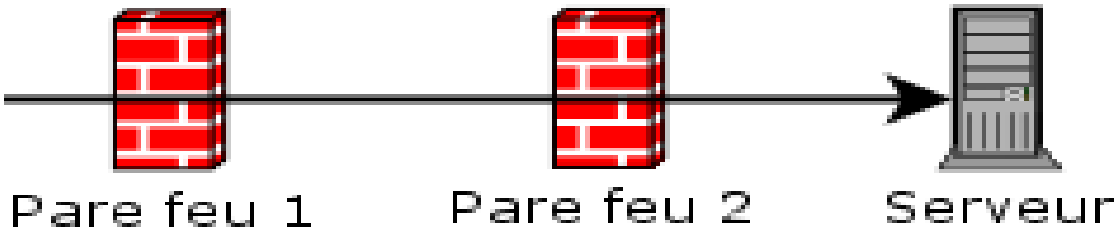
- Ligne 1
  - ACLs (routeurs)
  - Cloisonnement (VLANs)
- Ligne 2
  - Pare-feux
    - Reprennent les ACLs
    - Reproduisent le cloisonnement
- Lignes 3 et 4
  - Antivirus et passerelles applicatives.

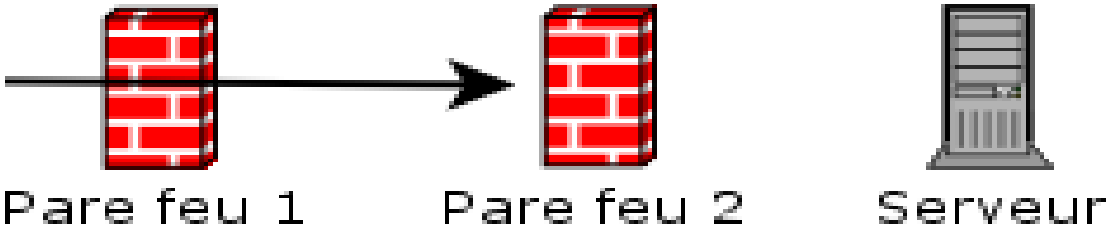
Défense en profondeur (3)



Défense en profondeur (4)

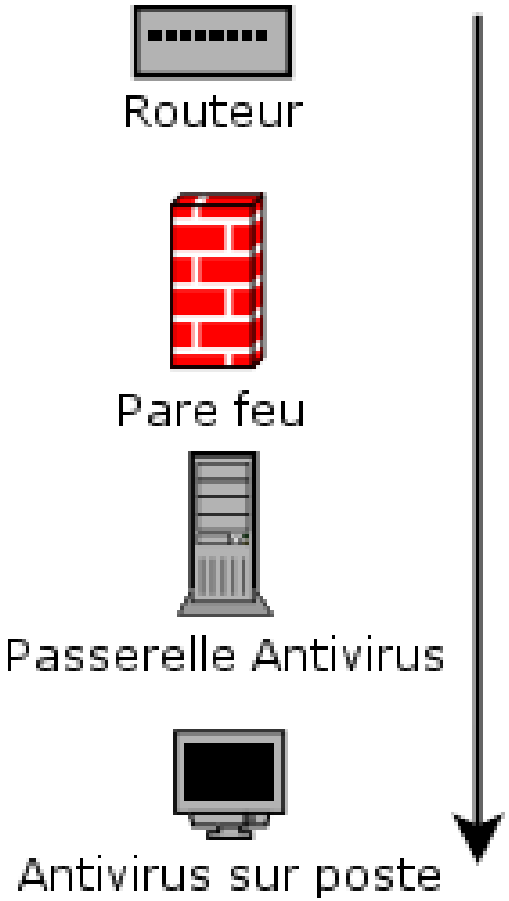
1. Les pare feux sont identiques (matériel et logiciel)
La meme vulnérabilité permet de les contourner.





2. Les pare feux sont différents.

Défense en profondeur (5)



1. Flux légitime
(adresse IP du serveur SMTP)

2. Flux autorisé
(adresse, protocole TCP, port 25)

3. Virus intercepté
(filtrage de contenu)

4. Si échec de la passerelle,
interception du virus

Extension du périmètre (1)

- Géographique
  - Nomadisme et mobilité
  - Systèmes étendus à l'échelle mondiale
    - Comment assurer la continuité du SI au-dessus de liens non dédiés ?
- Fonctionnelle
  - Sécurité sur plusieurs niveaux
  - Prise en compte des nouveaux moyens de connexion
    - PDA, GSM 3G/UMTS

Extension du périmètre (2)

- Impacts sur la politique de sécurité
  - Utilisation de nouveaux outils
  - Prise en compte de l'attaque de l'intérieur
    - Une attaque menée de l'intérieur peut être le fait d'un ordinateur infecté
  - Prise en compte de la diversité des composants du SI

SI distribués (1)

- Définition d'un SI distribué
  - Géographiquement, il s'agit d'un SI dont les fonctions sont remplies par des réseaux ou des serveurs répartis sur plusieurs sites mais gérés/administrés de manière centralisée.
  - Fonctionnellement, il s'agit d'un SI au sein duquel les fonctions sont réparties sur des segments distincts (serveurs dédiés).
- Objectifs
  - Accroître la disponibilité des services
  - Souplesse d'extension
  - Meilleure résistance aux attaques et aux défaillances
    - Notion de site de secours actif.

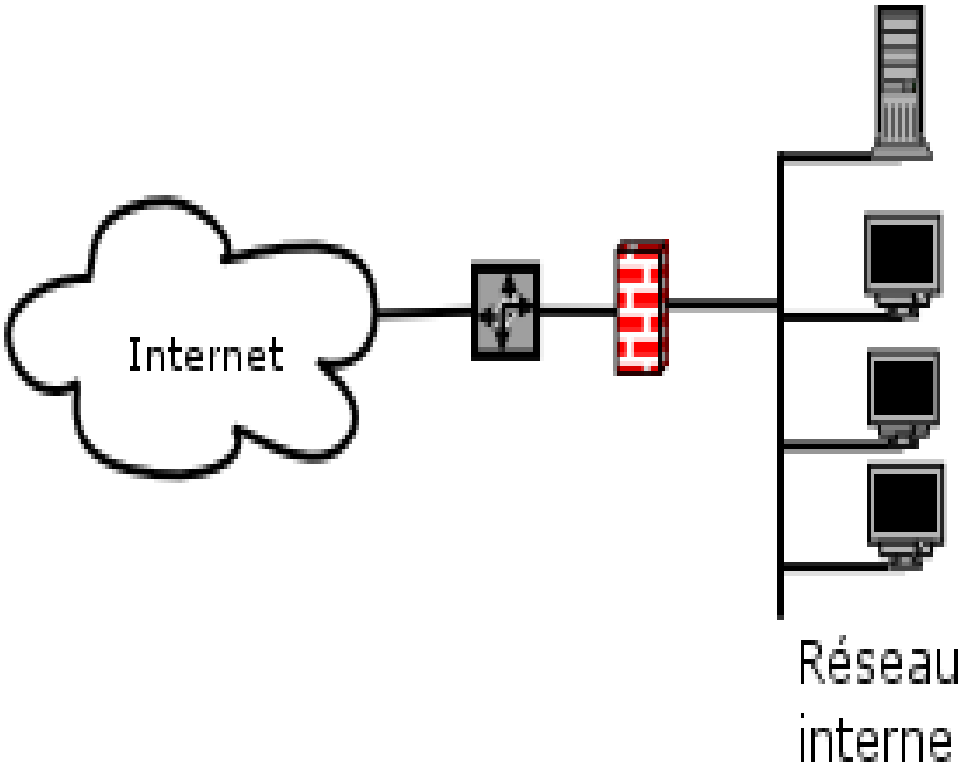
SI distribués (2)

- Concepts sous-jacents
  - Haute disponibilité
    - Gestion automatique des défaillances
  - Répartition de charge
  - Réplication des données
  - Infrastructure de gestion de la confiance
    - Identification des utilisateurs et matériels
  - Virtualisation des ressources
    - A commencer par le réseau
  - Administration sécurisée

Réponses

- Comment répondre à ces types de menaces ?
- Les technologies existent, parfois depuis longtemps, mais leur utilisation n'est pas encore généralisée.
- La réponse passe également par une réflexion sur l'architecture du SI.
  - Il ne s'agit pas – seulement – d' « empiler » des produits.
- Les utilisateurs seront de plus en plus impliqués :
  - Certaines solutions ne sont pas transparentes à 100%
  - La formation des utilisateurs aux réflexes de bonne conduite devient une nécessité (phishing).

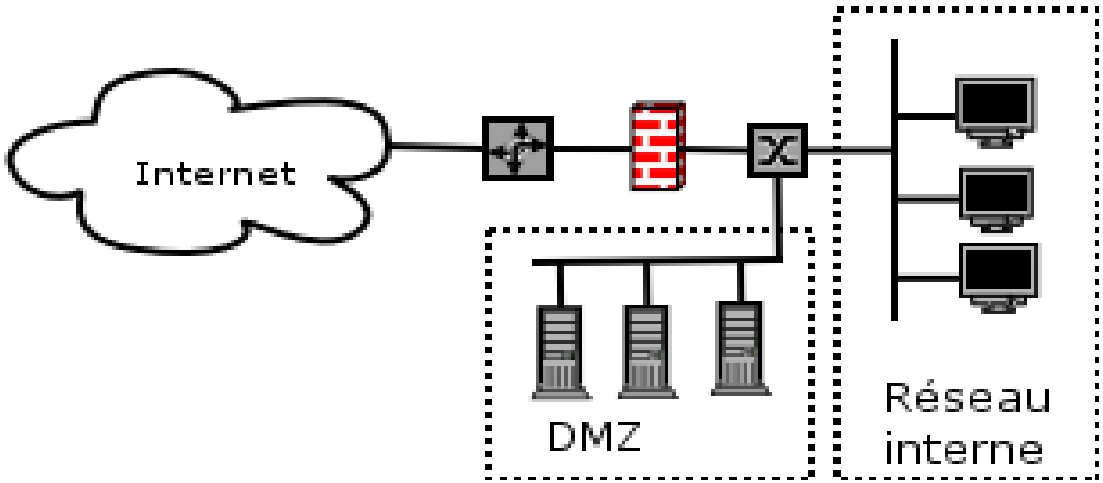
Évolutions de l’architecture (1)



- Il y a encore peu, le réseau de l’entreprise n’était séparé de l’extérieur que par un pare feu. Serveurs et postes de travail partageaient les ressources réseau.

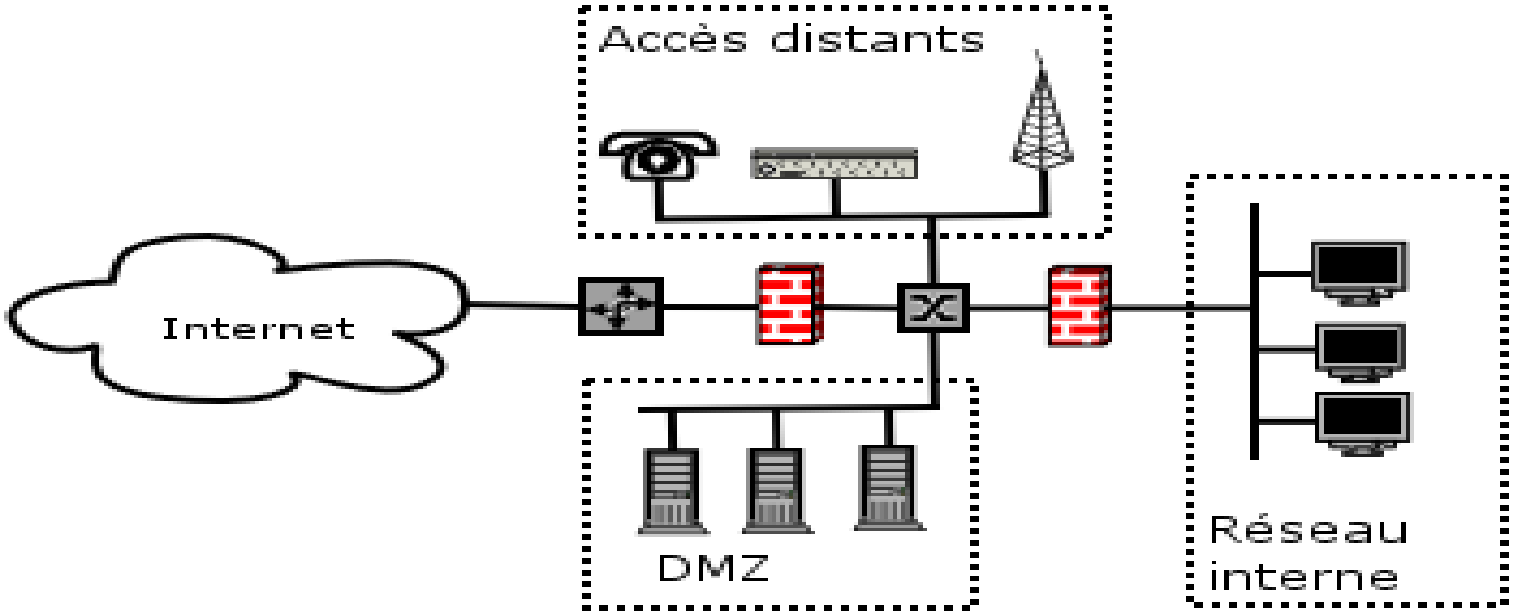
Évolutions de l’architecture (2)

- Puis sont apparues les DMZ, dont l’usage s’est généralisé.



Évolutions de l’architecture (3)

- Le concept de défense en profondeur appliqué à l’architecture du SI mène à ceci :



Technologies (1)

- Filtrage réseau
  - Toujours nécessaire mais plus suffisante seule.
  - Objectifs
    - Assurer la continuité d'une fonction qui reste essentielle.
    - Résister aux attaques par déni de service.
- Filtrage applicatif
  - Prend en compte l'évolution des attaques.
  - S'appuie sur des serveurs mandataires, capables de décoder et d'interpréter le contenu des flux.
    - Essentiel dans la lutte antivirale.

Technologies (2)

- Détection d'intrusions
  - Remplit une fonction de supervision de la sécurité.
  - Agit en complément des composants actifs de sécurité.
  - Agit comme système d'alarme avancée (« AWACS réseau ») et permet d'ajuster et d'adapter les mesures de sécurité.
- Cryptographie
  - Permet d'assurer la confiance dans un cadre de plus en plus « ouvert ».
  - Réponse à l'extension du périmètre du SI.

En guise de conclusion

- Nous aborderons les technologies citées à partir de logiciels Libre / Open Source dans un environnement Unix.
- Attention qu'elles ne répondent pas forcément à tous les défis de la sécurité réseaux telle qu'elle évolue.
- Mais elles constituent cependant une bonne base de départ.
- Elles ne doivent pas faire oublier l'étape suivante : la sensibilisation puis la formation des utilisateurs.

Références

- Tendances
  - Panorama 2004 sur la cybercriminalité
    - CLUSIF – http://www.clusif.fr
- Phishing
  - Cross Scripting et Phishing
    - HSC - http://www.hsc.fr/ressources/presentations/
  - Phishing: social engineering et subterfuges
    - HSC - http://www.hsc.fr/ressources/presentations/
- Défense
  - La défense en profondeur, Mr Valancogne
  - Mémento sur le concept de défense en profondeur, DCSSI