Sécurité des Systèmes d'Information

Nadia BENNANI*- Didier DONSEZ**

Université de Valenciennes

**Institut des Sciences et Techniques de Valenciennes

*IUT de Valenciennes

e-mail : {donsez,nbennani}@univ-valenciennes.fr

"CE NE SONT PAS LES MURS QUI PROTÈGENT LA CITADELLE, MAIS L'ESPRIT DE SES HABITANTS"

THUCYDITE

Introduction:
l'environnement « Réseau » de l'Entreprise

- Avant
  - Centralisé
  - Échange Papier
  - Pas d'Accès Distants
- Maintenant
  - Distribué sur plusieurs sites
    - » siège, filiale, commerciaux, télé travailleurs

    Extra entreprise ⇨ EDI - "Zéro Papier"

    Intra entreprise ⇨ le Client-Serveur
  - Accès Distants
  - Multiplication des partenaires commerciaux
  - Mondialisation des échanges
- Demain

Introduction:
l'environnement « Réseau » de l'Entreprise

- Futur
  - Clientèle : les « particuliers » informatisés

    Minitel, Set Top Box, Assistant Personnel, PC, …

    3 000 000 000 d 'individus
  - Agents Commerciaux (Intelligents)
  - Réseaux sans Fil (GSM, …) , Internet

Les Risques liés aux Réseaux

- interception des messages
  - prise de connaissance des mots de passe
  - vol d'information
  - Perte d'intégrité du système et du réseau.
- intrusion des Systèmes
  - Vol ou compromission des informations
  - Destruction des informations
    => pertes commerciales, tps de restitution
    => perte d'intégrité des données
  - Virus
  - Détournement de biens
- Perte d'accessiblité au système ou au réseau
- Faux client, Marchand escroc

Les différentes facettes de la Sécurité

- l'Identification
  Qui est-ce ?
- l'Authentification
  Est-ce bien lui ?
- la Confidentialité
  Est-ce qu'un autre nous écoute ?
- l'Intégrité
  Le contenu est-il intact ?
  » altération, malveillance
- la Non Répudiation
  Correspondant de Mauvaise Foi
  » nier ultérieurement une opération effectuée

Qui écoute ou falsifie ?

- Les Gouvernements
  - NSA (National Security Agency)

    Echelon
  - CIA (Central Inteligence Agency), DGSE ...
- Le Crime Organisé
- Les Concurrents de votre Entreprise

Big Brother is watching you

- Echelon de la NSA (National Security Agency)
  - réseau de 120 satellites avec l'aide du Canada, de l'Australie, de la Nouvelle-Zélande et du Royaumes-Unis (basé à Fort Meade)
  - But :
    - écouter de tout ce qui se dit ou s'écrit par téléphone, fax, email, etc

      Chaque message utilisant un mot-clé listé est aussitôt intercepté par les machines, puis lu ou écouté.

      Les machines (Super-Cray) digèrent l'équivalent de la bibliothèque du Congrès américain.
    - Cibles principalement économiques et technologiques depuis la fin de la Guerre Froide

Les mot-clés d 'Echelon
(non exhaustifs)

- Explosives, guns, assassination, conspiracy, primers, detonators, initiators, main charge, nuclear charges, ambush, sniping, motorcade, IRS, BATF, jtf-6, mjtf, hrt, srt, hostages, munitions, weapons, TNT, rdx, amfo, hmtd, picric acid, silver nitrite, mercury fulminate, presidential motorcade, salt peter, charcoal, sulfur, c4, composition b, amatol, petn, lead azide, lead styphante, ddnp, tetryl, nitrocellulose, nitrostarch, mines, grenades, rockets, fuses, delay mechanism, mortars, rpg7, propellants, incendiaries, incendiary device, thermite, security forces, intelligence, agencies, hrt, resistance, psyops, infiltration, assault team, defensive elements, evasion, detection, mission, communications, the football, platter charge, shaped charges, m118, claymore, body armor, charges, shrapnel, timers, timing devices, boobytraps, detcord, pmk 40, silencers, Uzi, HK-MP5, AK-47, FAL, Jatti, Skorpion MP, teflon bullets, cordite, napalm, law, Stingers, RPK, SOCIMI 821 SMG, STEN, BAR, MP40, HK-G3,FN-MAG, RPD,PzB39, Air Force One, M60, RPK74, SG530, SG540, Galil arm, Walther WA2000, HK33KE, Parker-Hale MOD. 82, AKR, Ingram MAC10, M3, L34A1, Walther MPL, AKS-74, HK-GR6, subsonic rounds, ballistic media, special forces, JFKSWC, SFOD-D, SRT, Rewson, SAFE, Waihopai, INFOSEC, ASPIC, Information Security, SAI, Information Warfare, IW, IS, Privacy, Information Terrorism, Kenya, Terrorism Defensive Information, Defense Information Warfare, Offensive Information, Offensive Information Warfare, NAIA, SAPM, ASU, ECHELON ASTS, National Information Infrastructure, InfoSec, SAO, Reno, Compsec, JICS, Computer Terrorism, Firewalls, Secure Internet Connections, RSP, ISS, JDF, Passwords, NAAP, DefCon V, RSO, Hackers, Encryption, ASWS, Espionage, USDOJ, NSA, CIA, S/Key, SSL, FBI, Secret Service, USSS, Defcon, Military, White House, Undercover, NCCS, Mayfly, PGP, SALDV, PEM, resta, RSA, Perl-RSA, MSNBC, bet, AOL, AOL TOS, CIS, CBOT, AIMSX, STARLAN, 3B2, BITNET, Tanzania, SAMU, COSMOS, DATTA, E911, FCIC, HTCIA, IACIS, UT/RUS, JANET, ram, JICC, VNET, BRLO, SADCC, NSLEP, SACLANTCEN, FALN, 877,
- NAVELEXSYSSECENGCEN, BZ, CANSLO, CBNRC, CIDA, JAVA, rsta, Active X, Compsec 97, RENS, LLC, DERA, JIC, rip, rb, Wu, RDI, Mavricks, BIOL, Meta-hackers, ^?, SADT, Steve Case, Tools, RECCEX, Telex, OTAN, monarchist, NMIC, NIOG, IDB, MID/KL, NADIS, NMI, SEIDM, BNC, CNCIS, STEEPLEBUSH, RG, BSS, DDIS, mixmaster, BCCI, BRGE, SARL, Military Intelligence, JICA, Scully, recondo, Flame, Infowar, Bubba, Freeh, Archives, ISADC, CISSP, Sundevil, jack, Investigation, JOTS, ISACA, NCSA, ASVC, spook words, RRF, 1071, Bugs Bunny, Verisign, Secure, ASIO, Lebed, ICE, NRO, Lexis-Nexis, NSCT, SCIF, FLiR, JIC, bce, Lacrosse, Flashbangs, HRT, IRA, EODG, DIA, USCOI, CID, BOP, FINCEN, FLETC, NIJ, ACC, AFSPC, BMDO, site, SASSTIXS, NAVWAN, NRL, RL, NAVWCWPNS, NSWC, USAFA, AHPCRC, ARPA, SARD, LABLINK, USACIL, SAPT, USCG, NRC, ~, O, NSA/CSS, CDC, DOE, SAAM, FMS, HPCC, NTIS, SEL, USCODE, CISE, SIRC, CIM, ISN, DJC, hemd, SGC, UNCPCJ, CFC, SABENA, DREO, CDA, SADRS, DRA, SHAPE, bird

Les profiles type du pirate?

Le piratage amateur

Le piratage professionnel

Les employés de l'entreprise

Les motivations d'un pirate ?

- Le gain financier
- Vengeance
- Besoin de reconnaissance
- Curiosité, recherche d'émotion forte
- L'ignorance

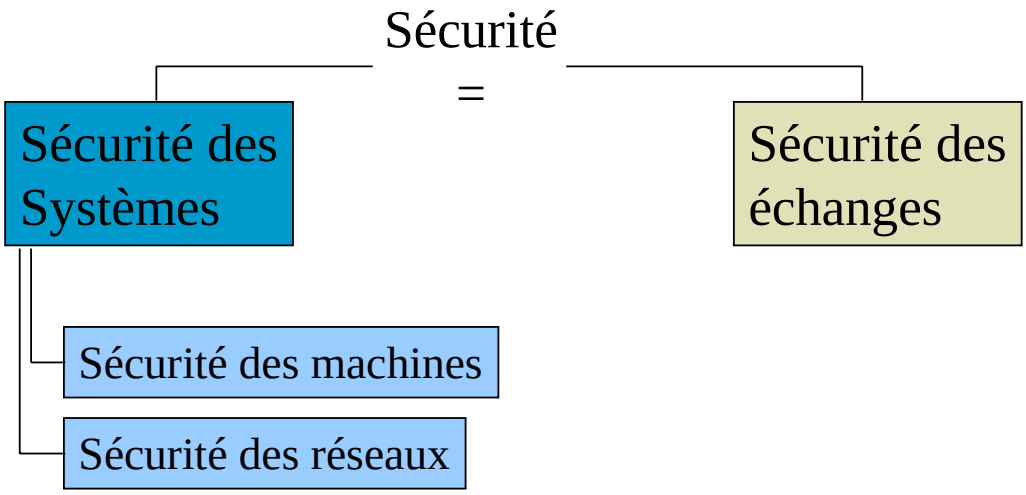
Comment est perçue la sécurité dans les entreprises?

La sécurité n'apporte aucune valeur ajoutée

>> les grandes entreprises

Budget

Sécurité de quoi?



Sommaire

Sécurité des systèmes

- Les attaques
- Les virus
- Les protocoles à risques
- Les services à risques
- Les gardes-barrières

Infiltration par mots de passe

Les failles:

mauvais choix de mot de passe

Négligence des administrateurs système

- Connaissance d'un couple <nom de log, mpasse>

  ex: <Domain,guest>
- Vol d'un fichier /etc/passwd
- Attaque par dictionnaire

  Solution : le salage.

Types d'attaques():
L'ingénierie sociale

Ex1: Par E-mail

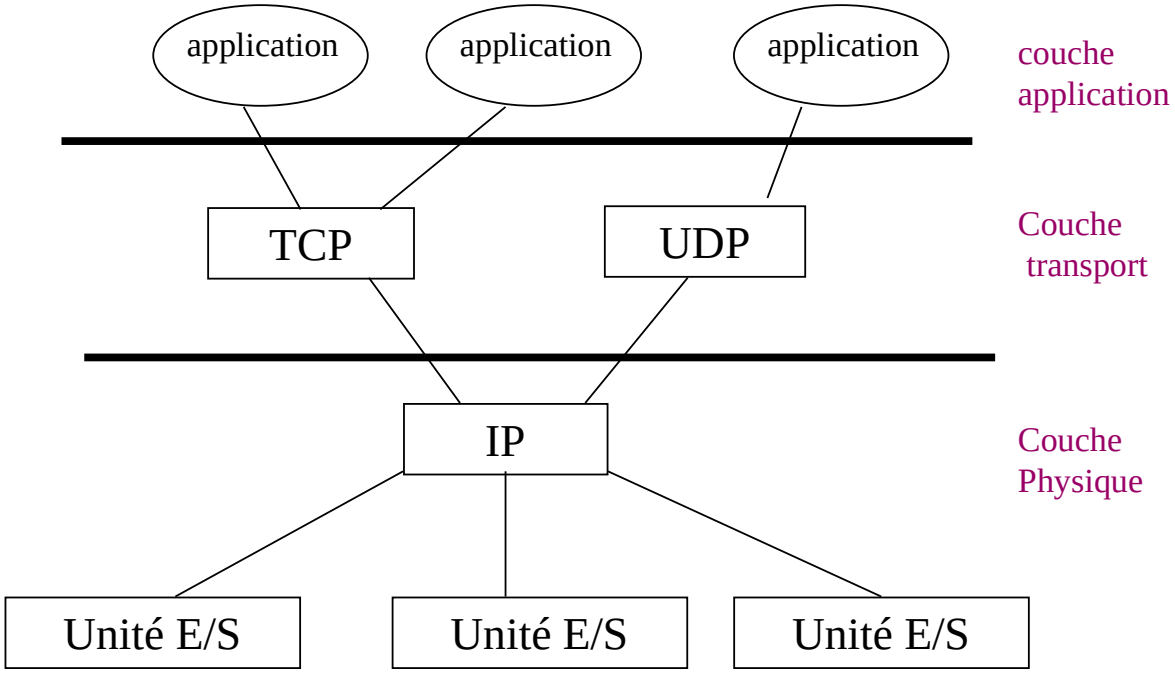
```
From : chf@organisation.com
To : empl@organisation.com
Subject: Le nouveau technicien

Eric,
Pourriez vous demander à l'administrateur système de créer un
nouveau log pour le technicien de chez Sun: Utiliser de préférence le même
mot de passe haché suivant:
pxf:5bHD/k5k2mTTs:2043:148:Pat:/home/pat:/bin/sh
```

Ex2: Installation de logiciels

Turbo Tetris

Le protocole TCP/IP

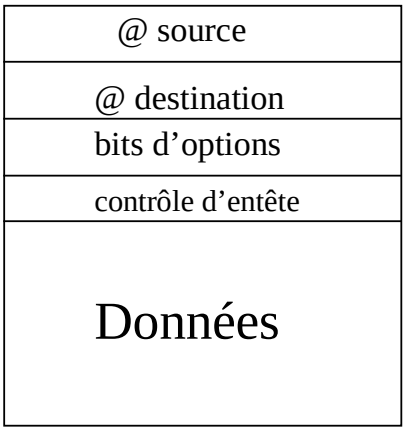


Le protocole TCP/IP

La couche IP

Un message IP

Un paquet IP



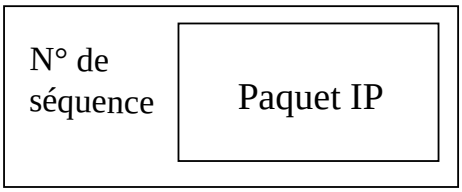
Limites d'IP

- IP ne gère pas la continuité transmission des paquets
- Aucune vérification de l'@ source

Le protocole TCP/IP

La couche TCP

Cohérence de la transmission des paquets IP grâce à des numéros de séquence

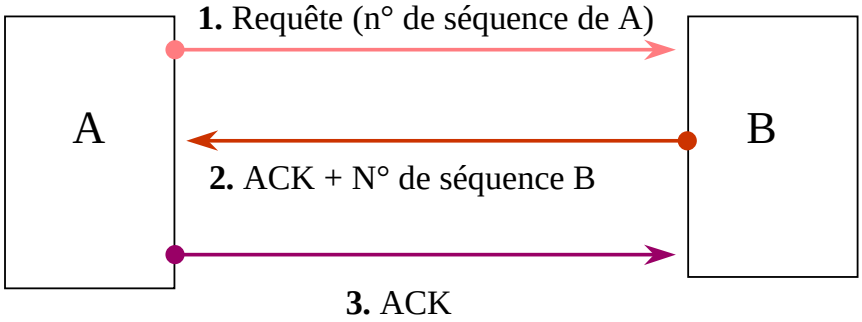


=> Les numéros de séquence sont générés aléatoirement par la couche TCP de la machine source

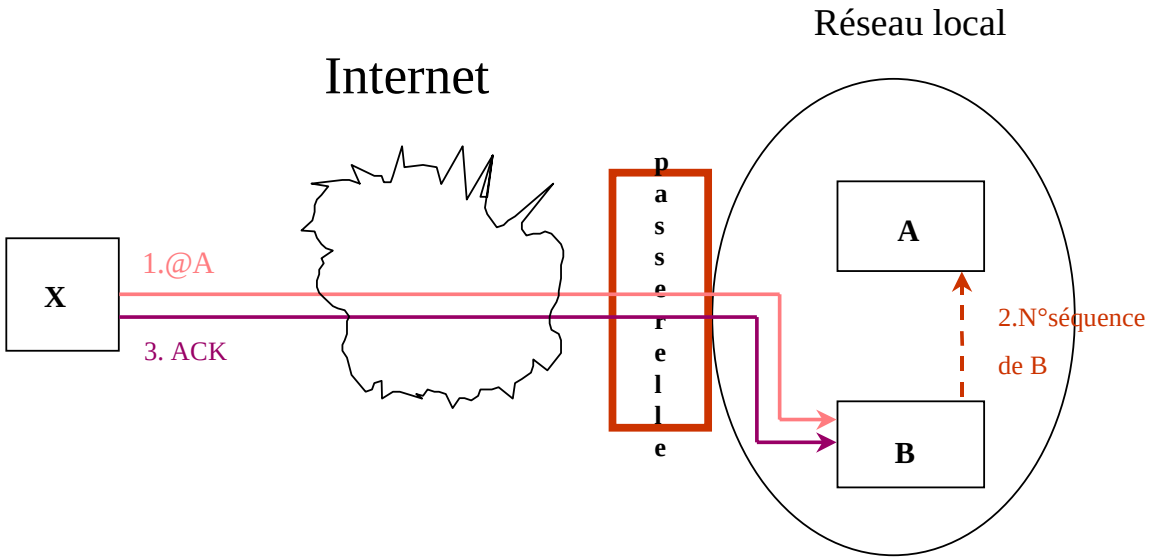
Types d'attaques():

Le trucage d'adresse

Protocole classique d'une connexion



Types d'attaques():
Le trucage d'adresse(2)



Types d'attaques():
Le trucage d'adresse(3)

- Interdire l'accès par confiance pour les machines externes.
- Refuser toute requête externe en provenance d'une machine interne
- Améliorer le procédé de génération des numéros de séquence (procédés cryptographiques)

Types d'attaques():
Le détournement de session

- Contrôle d'une machine intermédiaire

Procédés:

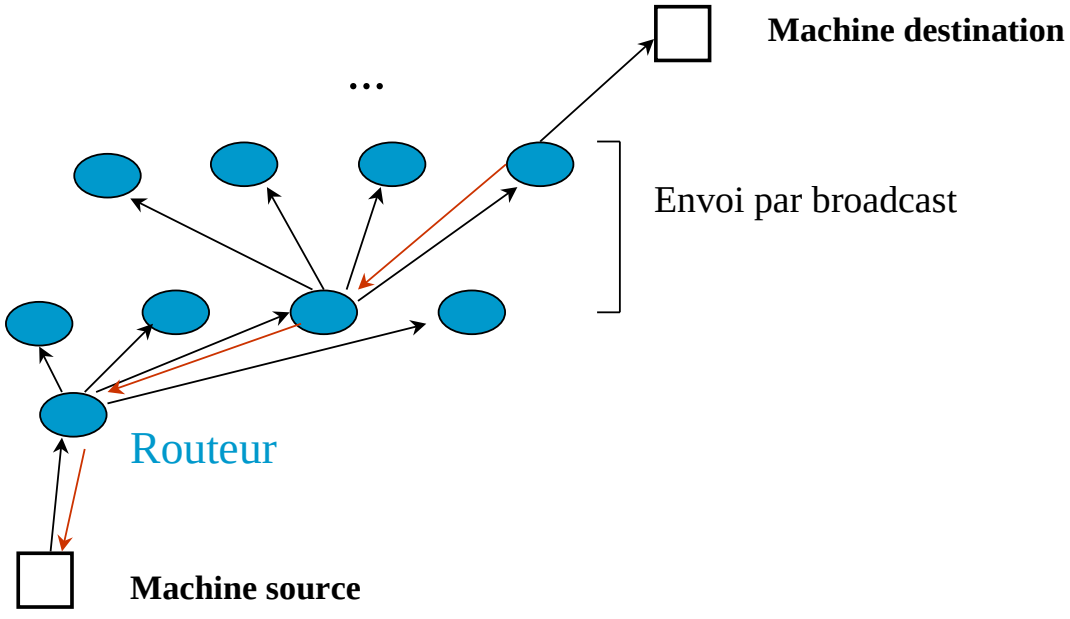
attaque par mot de passe, ingénierie sociale

➡ Trucage IP

Solution: Le chiffrement

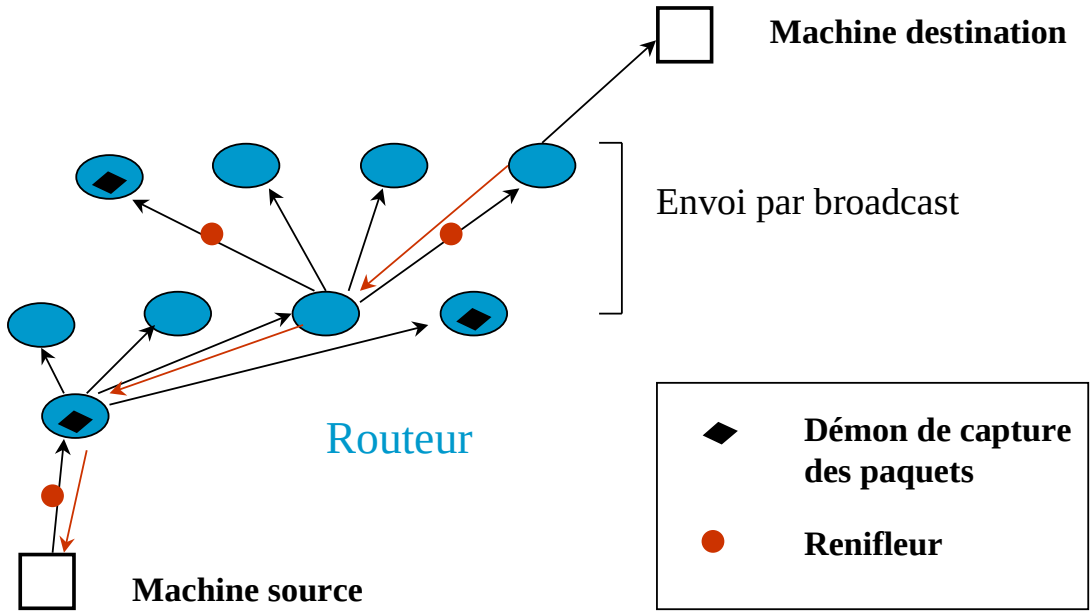
Types d'attaques():
L'observation du réseau

Le routage des paquets IP



Types d'attaques():
L'observation du réseau

Le routage des paquets IP



Types d'attaques():
L'observation du réseau

Les solutions ?

- Mécanismes d'authentification forte

  Ex: les mots de passe à usage unique.

- Inspection physique => peu efficace
- Technologie des répartiteurs de paires torsadées

- La cryptographie

Virus & Autres programmes malveillants

- Les plus insidieux:

  Virus furtifs,Virus polymorphes

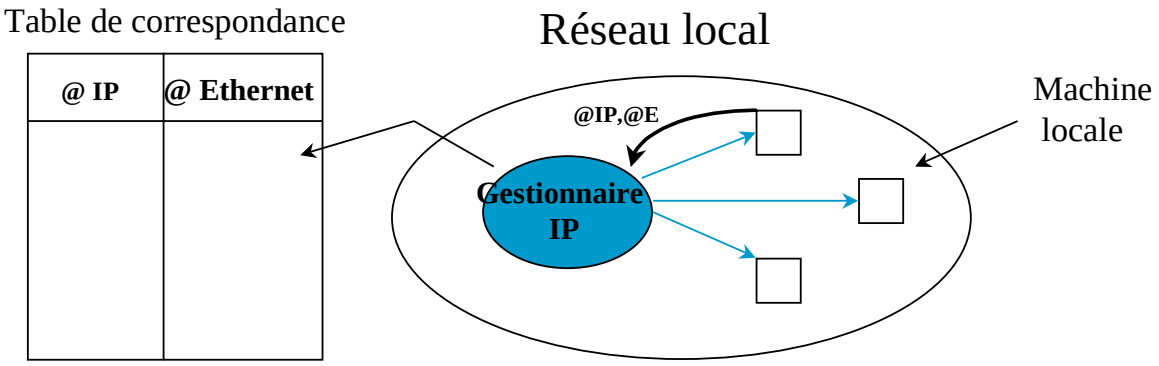
- Les chevaux de Troie
- Les worms
- Les bombes logiques et à retardement

Internet: Accroit les risques de contamination:
E-mail, Applets,...etc

Menaces & risques

Déviation du trafic vers une machine pirate(1)

- Le protocole ARP (Adress Résolution Protocol)



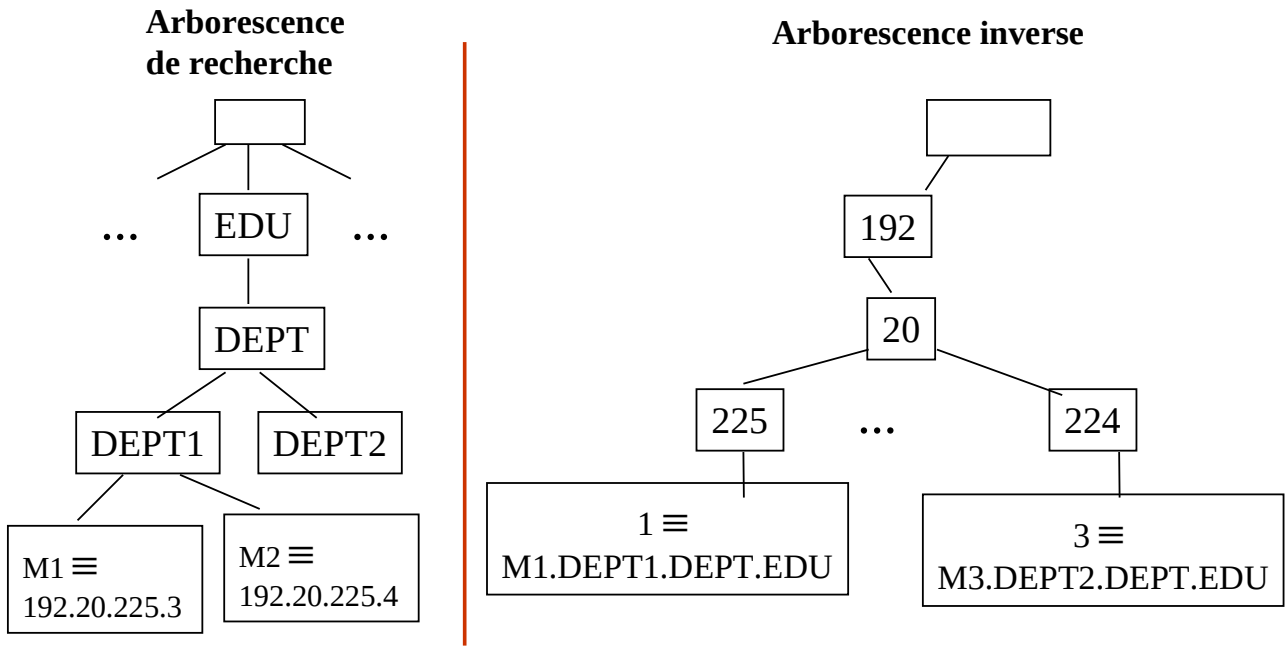
- Traduction des @ IP (32 bits) en @ Ethenet(48 bits)

  => Utilisation d'une table de correspondance

Menaces & risques

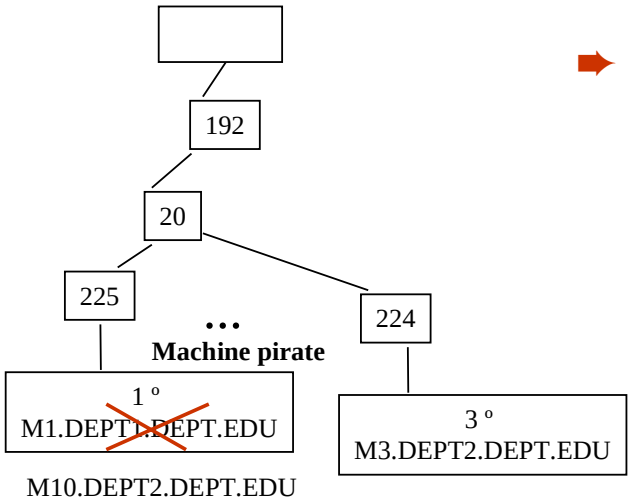
Déviation du trafic vers une machine pirate(2)

- Le système DNS (Domain Name System)



Menaces & risques

Déviation du trafic vers une machine pirate(2)



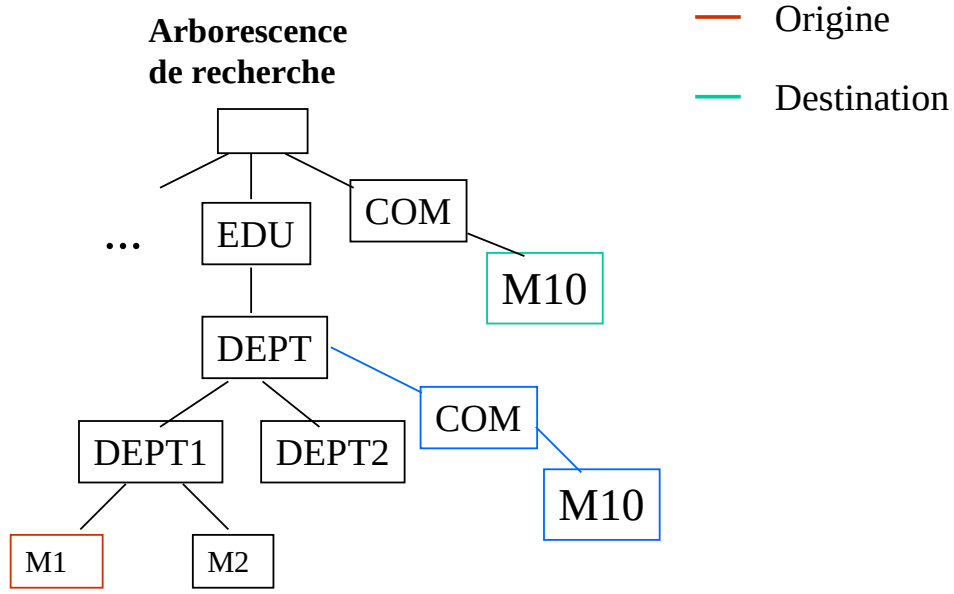
- La machine pirate peut maintenant tenter un rlogin réussi sur M3.DEPT2.DEPT.EDU !

Solution : Vérification de l'adresse IP dans la première arborescence.

Hypothèse :
M3.DEPT2.DEPT.EDU a confiance en M10.DEPT2.DEPT.EDU

Menaces & risques

Déviation du trafic vers une machine pirate(2)



Le serveur RPC (Remote Procedure Call)

Requêtes externes de services locaux:

- Risque de falsification des requêtes

  => RPC sécurisé: DES

- L'appel direct

Autres services réseaux à risques

- Les montages NFS (Network File system)

  ☛ Risque de perte ou de modification de fichiers sensibles

- Le système NIS (Network Information Service)

Solutions

Services protégés par un garde barrière.

Les protocoles à risques

Les protocoles de connexion à distance

- Telnet
- rlogin
- rsh

Pourquoi sont-ils risqués?

- Absence de confidentialité, d'intégrité
- Absence d'authentification
- Accès direct à un shell sur la machine distante.

  ➡ facilite le contrôle illicite.

Solutions

Bloquer l'accès illimité

Authentification forte

Chiffrement

Les protocoles à risques

La messagerie électronique

- SMTP

  Problèmes : confidentialité,intégrité,
  authentification, non répudiation

  Menace sur les systèmes

  - Utilisation de MIME(Multipurpose Internet Mail Extension)
    - Virus,
    - chevaux de Troie,
    - commandes illicites

Les protocoles à risques

La messagerie électronique(2)

- Sendmail

  ➢ Menaces sur les systèmes
  - Exécution en accès privilégié
  - Trop de bugs

  ➢ Accessible par telnet
  - Problème d'intégrité.
  - Authentification des mails

Les protocoles à risques

La messagerie électronique(3)

Les solutions :

Cryptographie à clé publique

Ex: PEM (Privacy Enhanced mail)
PGP (Pretty and Good Privacy)
MOSS (MIME Object Security Service)
S/MIME

Les protocoles à risques

les news

- NNTP (Network News Transfert Protocol)

Les menaces

➢ Exécution en accès privilégié

➢ Accessible par telnet

Perturbation de la diffusion des news

Pas d'authentification

Les protocoles à risques

les news(2)

- NNTP (Network News Transfert Protocol)

Les solutions

- ☛ Utilisation d'un firewall
- ☛ Signature des articles :
  Pb d'authentification
- ☛ Le chiffrement

Sécuriser les machines

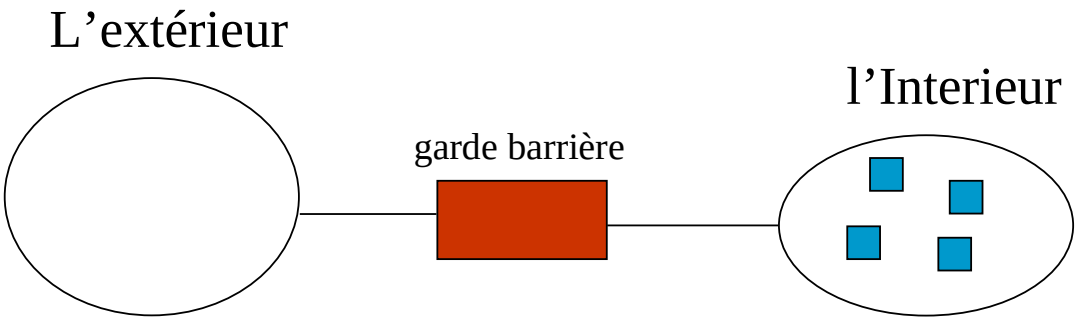
Quelques outils indispensables

- Filtres de mots de passe > crack
- Validité de la configuration système > COPS
- Contrôle des ports de communications >

  TCP-Wrapper, Xinetd
- Contrôle de l'intégrité du sytème >

  TAMU

Les gardes-barrières



Fonctionnement?

Les gardes-barrières

- Avantages
  - Point de contrôle unique pour la protection du réseau
  - Administration de la sécurité
  - Audit du trafic
- Inconvénients
  - Goulot d'étranglement
  - Compromission => multiplier les gardes barrières
  - Intégrité, authentification

Les types de gardes-barrières

- Filtres de paquets
- Les serveurs délégués
  - Filtres applications → Spécifiques / Génériques
  - Filtres circuits

Les filtres de paquets

Principe & fonctionnement

- Principe

  Filtrage des paquets IP

Ex de ports

SMTP:	25
Telnet :	23
ftp:	20,21
X11:	6000~ 6100

Contenu d'un paquet IP:

- La source, la destination
- Ports source & destination
- Protocole utilisé: IP,TCP,UDP...
- L'état: pour un paquet TCP

Rq : les application systèmes sont affectés à des ports < 1024

Les filtres de paquets

Principe & fonctionnement (2)

- Fonctionnement

  Les listes d'accès

Pseudo syntaxe:

<n° liste> | ***<Accepté/refusé>***| ***<Protocole>*** | ***<Source>*** | ***<destination>***

Exemple:

Liste 1	**Accepté**	**TCP**	*****	**Port 23**

L'ordre d'évaluation est important!

Liste 1	**Refusé**	**TCP**	*****	**Port 23**
Liste 1	**Accepté**	**TCP**	**128.18.30.2**	**Port 23**

Les filtres de paquets

le pb de retour des requêtes

Règle exclusive

Liste 1	**Accepté**	**TCP**	**interne**	*****	
Liste 1	**Refusé**	**TCP**	*****	**interne**	

Solution 1 :

Liste 1	**Accepté**	**TCP**	*****	**>1023**

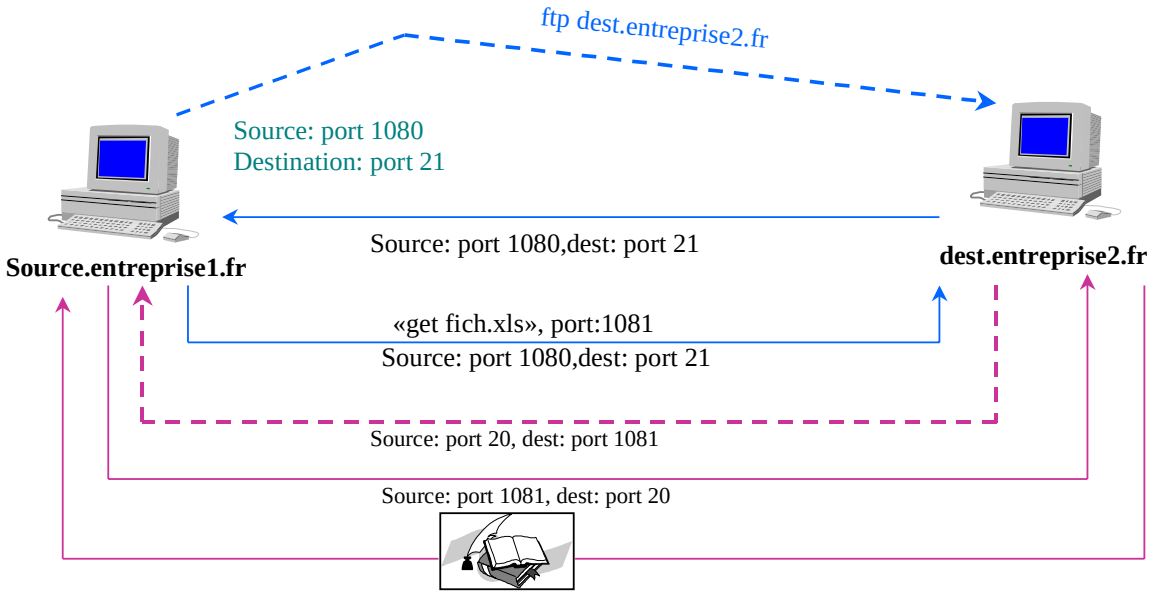
Solution 2: Utilisation du champ état

Liste 1	**Accepté**	**TCP**	**Interne**	*****		
Liste 1	**Accepté**	**TCP**	*****	**Interne**	**ACK**	

Les filtres de paquets

Les cas particuliers

Les requêtes FTP



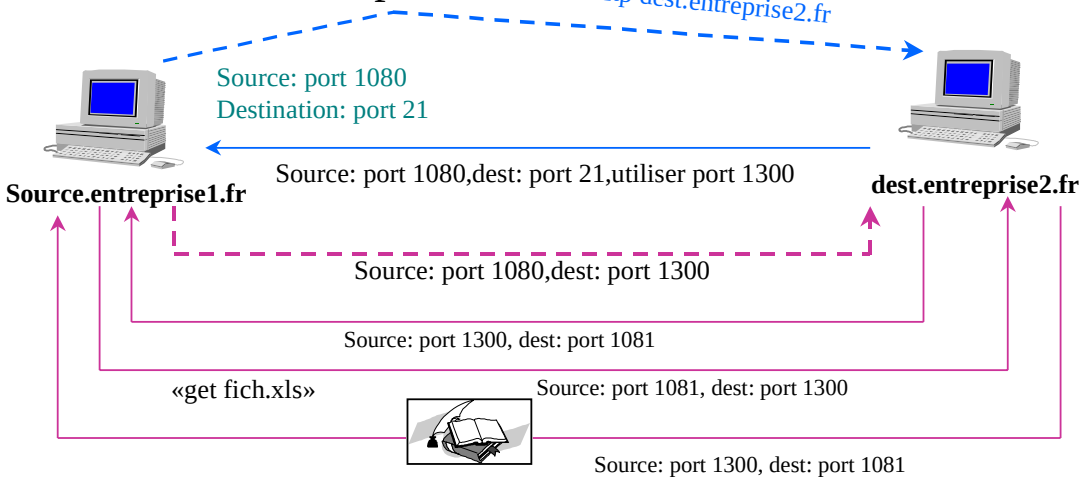
Les filtres de paquets

Le cas FTP (suite)

Solution 1

Liste 1	**Accepté**	**TCP**	***.port20**	**intérieur . >1023**

Solution 2 : le FTP passif



Les filtres de paquets

Mise en oeuvre

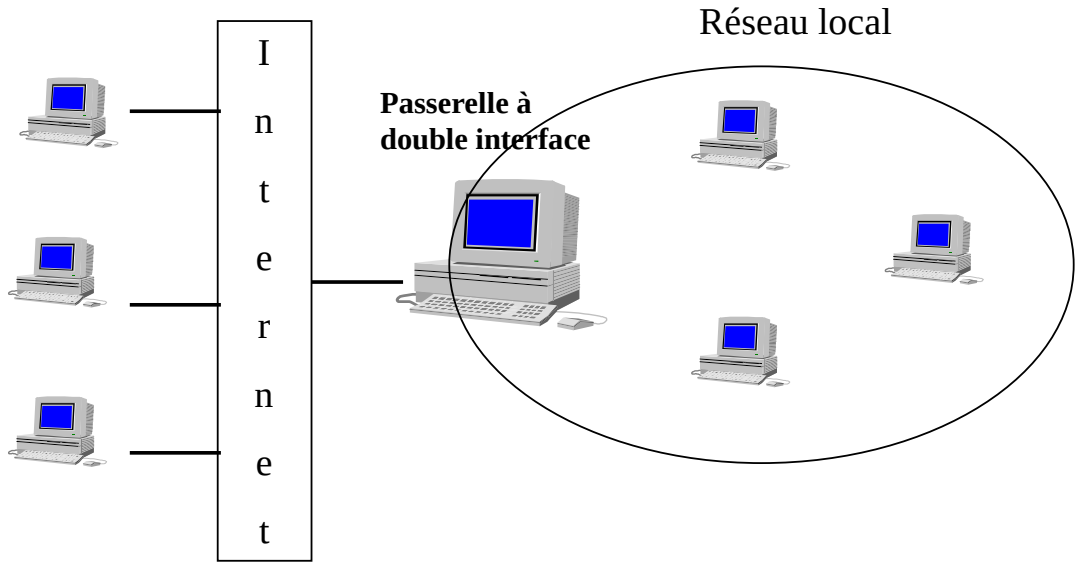
- Routeur
  - •Edition des listes d'accès
  - •L'audit du trafic
- Machine filtre
- Filtre intelligent
  - •Interface graphique conviviale
  - •Détection des incohérences
  - •Plusieurs niveaux d'audit
  - •Authentification
  - •Traitement des requêtes ftp, X11

Les serveurs délégués

Les serveurs délégués

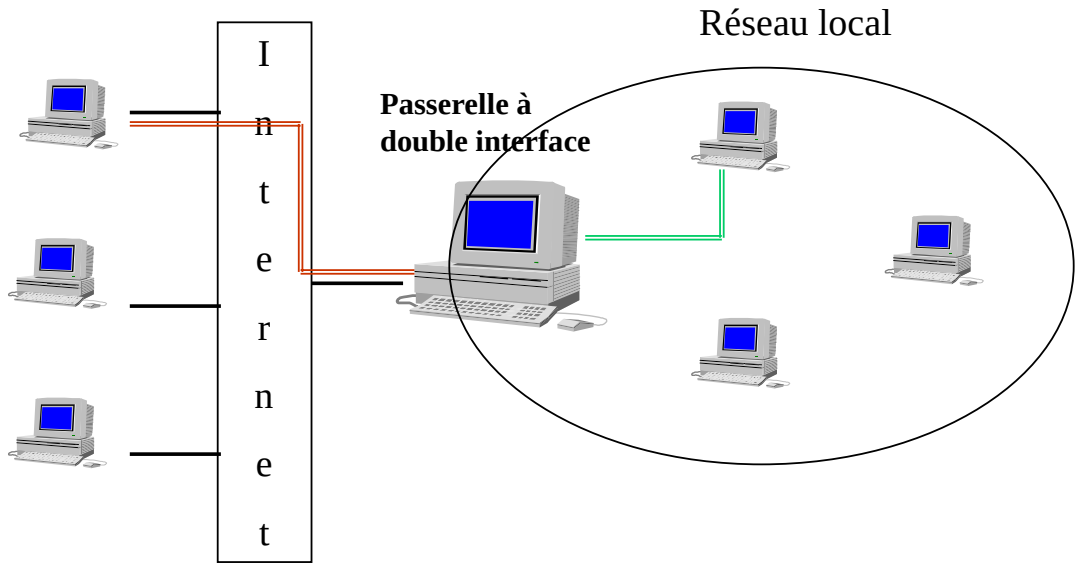
Qu'est ce ?

Passerelle à double interface



Les serveurs délégués

Deux Connexions



Les serveurs délégués

- Rôle de la passerelle
  - Les machines du réseau interne sont cachées.
  - Authentification frontale
- Rôle du serveur délégué
  - Transparence de la connexion
  - Pas de connexion shell sur la passerelle

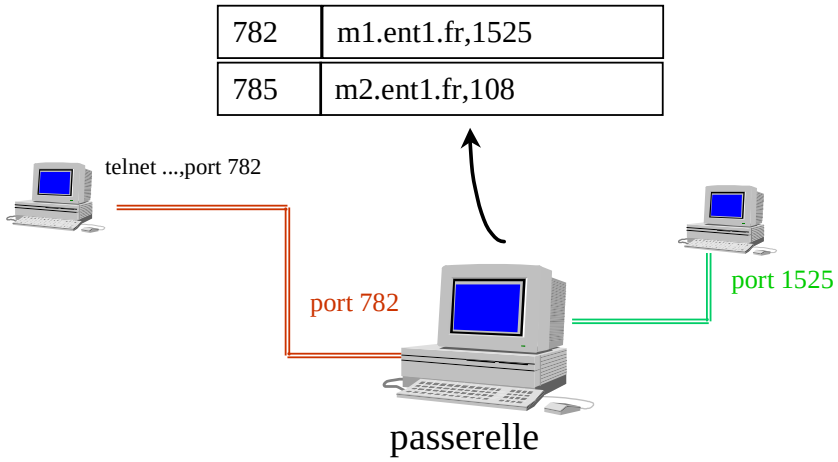
Les serveurs délégués

serveurs d'applications

Un serveur / application

Intérêt: s'adapte aux spécificités de l'application

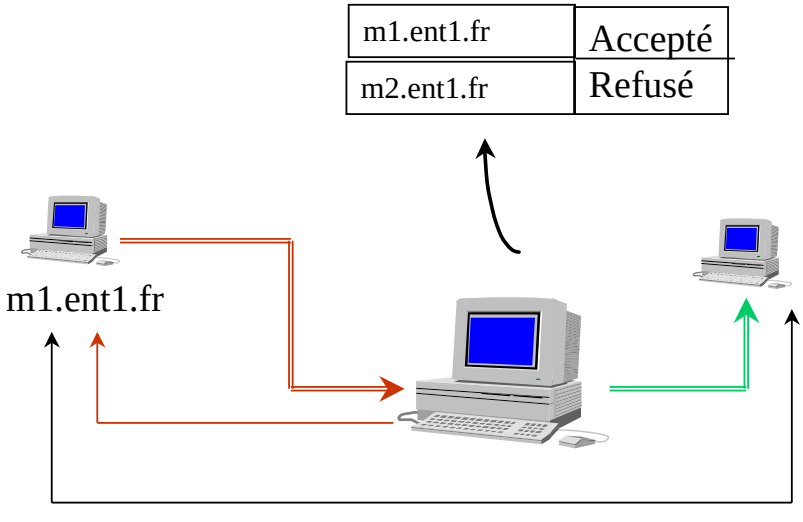
Serveur générique



Les serveurs délégués

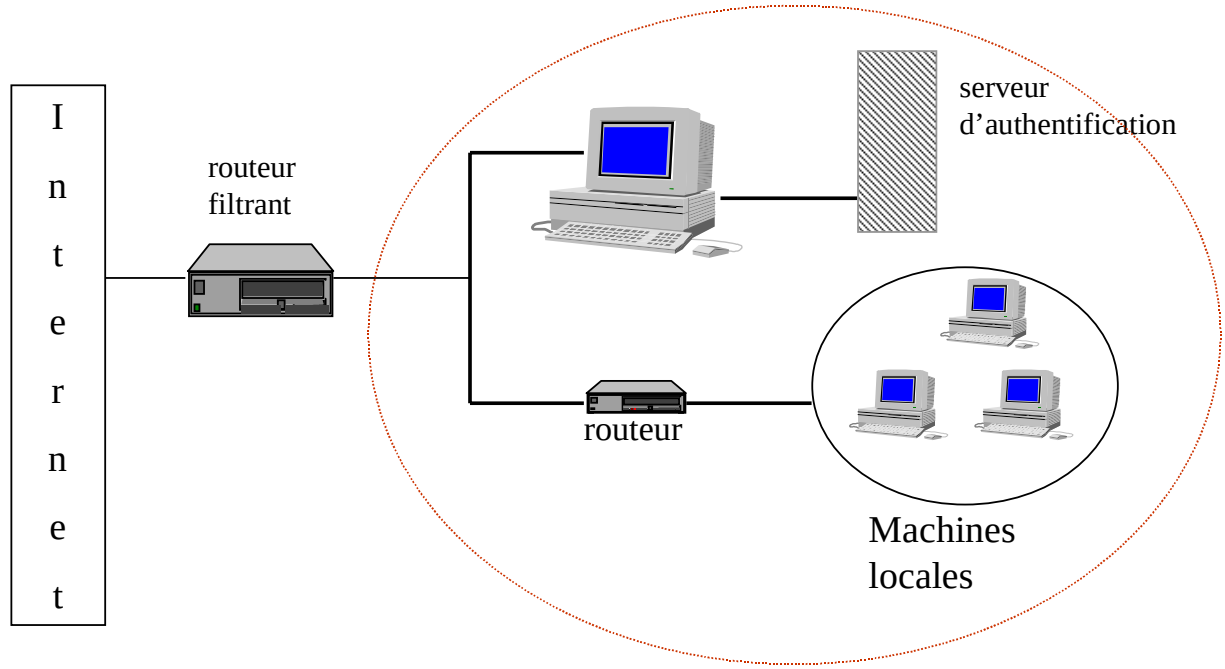
Filtres de circuit

- SOCKS



Architecture des gardes-barrières

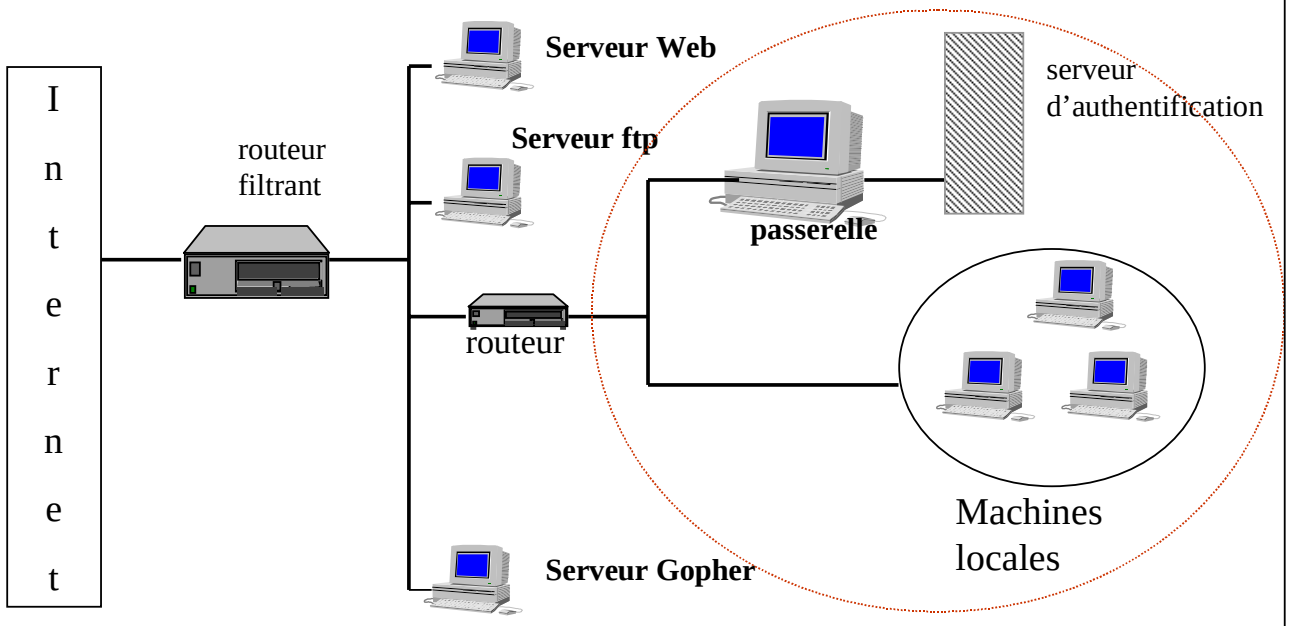
La passerelle filtrante



L'intérieur

Architecture des gardes-barrières

Le sous réseau filtrant

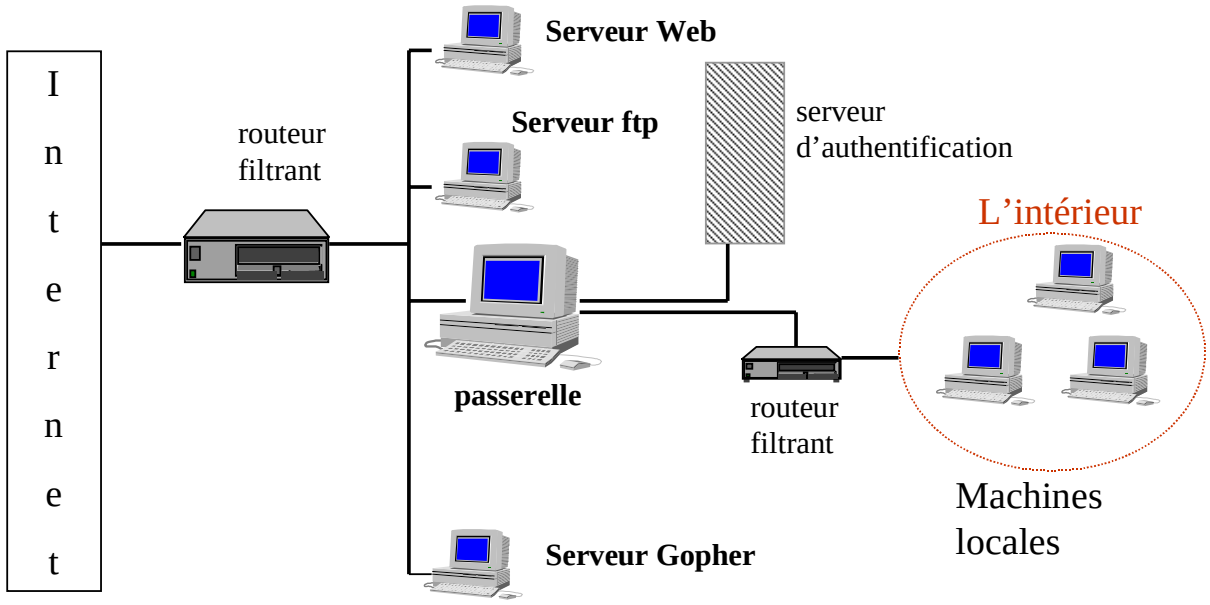


Sous réseau
Filtrant

L'intérieur

Architecture des gardes-barrières

Le garde-barrière «ceinture et bretelles»



Bibliographie (i)

- Cryptographie

  Applied Cryptography, by Bruce Schneier (Wiley), ISBN 0-471-59756-2 (ISBN 2-84180-036-9 en VF)

- Législation

  www.cnil.fr

  Echange de Données Informatisé : Contrôle et audit d'un système EDI, AFNOR & EDIFRANCE 1994, ISBN 2-12-481312-9.

  G. Beaure d'Augère, P. Bresse, S. Thuillier, «Paiement numérique sur Internet», Ed ITP France, 1997, ISBN 2-84180-160-8

Bibliographie (ii)

- Sécurité des Systèmes UNIX
  - Unix System Security: A Guide for Users and System Administrators by David Curry, O'Reilly
  - Practical Unix Security, by Simson Garfinkel and Gene Spafford,O'Reilly,ISBN 0-937175-72-2
- Internet Security Alerts
  - RISKS
    - Forum on Risks to the Public in Computers and Related Systems, http://catless.ncl.ac.uk/Risks
  - CERT
    - ftp://ftp.cert.org/pub/cert_advisories/

Bibliographie (iii)

- Sécurité des Serveurs Web
  - How to Set Up and Maintain a World Wide Web Site: The Guide for Information Providers, by Lincoln D. Stein (Addison-Wesley), ISBN 0-201-63389-2
  - Managing Internet Information Systems, by Cricket Liu, Jerry Peek, Russ Jones, Bryan Buus, and Adrian Nye (O'Reilly), ISBN 1-56592-051-1
- Firewalls
  - Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steven M. Bellovin,Addison-Wesley, ISBN 0-201-63357-4
  - Building Internet Firewalls, by D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly, 1st Edition September 1995, ISBN 1-56592-124-0

Bibliographie (iv)

- CORBA

  CORBA 2.1, «Security Service Specifications», OMG 1997

Vos suggestions et vos remarques

- Merci de me les retourner à
  - Didier DONSEZ, donsez@univ-valenciennes.fr, Fax 03 27 14 11 83
- Avez vous trouvé ce cours instructif ?
  - Est il complet ?
  - Qu 'est qu 'il manque ?
  - Qu 'est que vous auriez aimé voir plus développé ?
  - Est il bien organisé ?
  - ...
- Quels sont votre fonction et votre domaine d 'activité ?