Présentation:

- Pascal PETIT
- sécurité informatique
- pascal.petit@shayol.org
- http://www.ibisc.fr/~petit puis M2 CCA

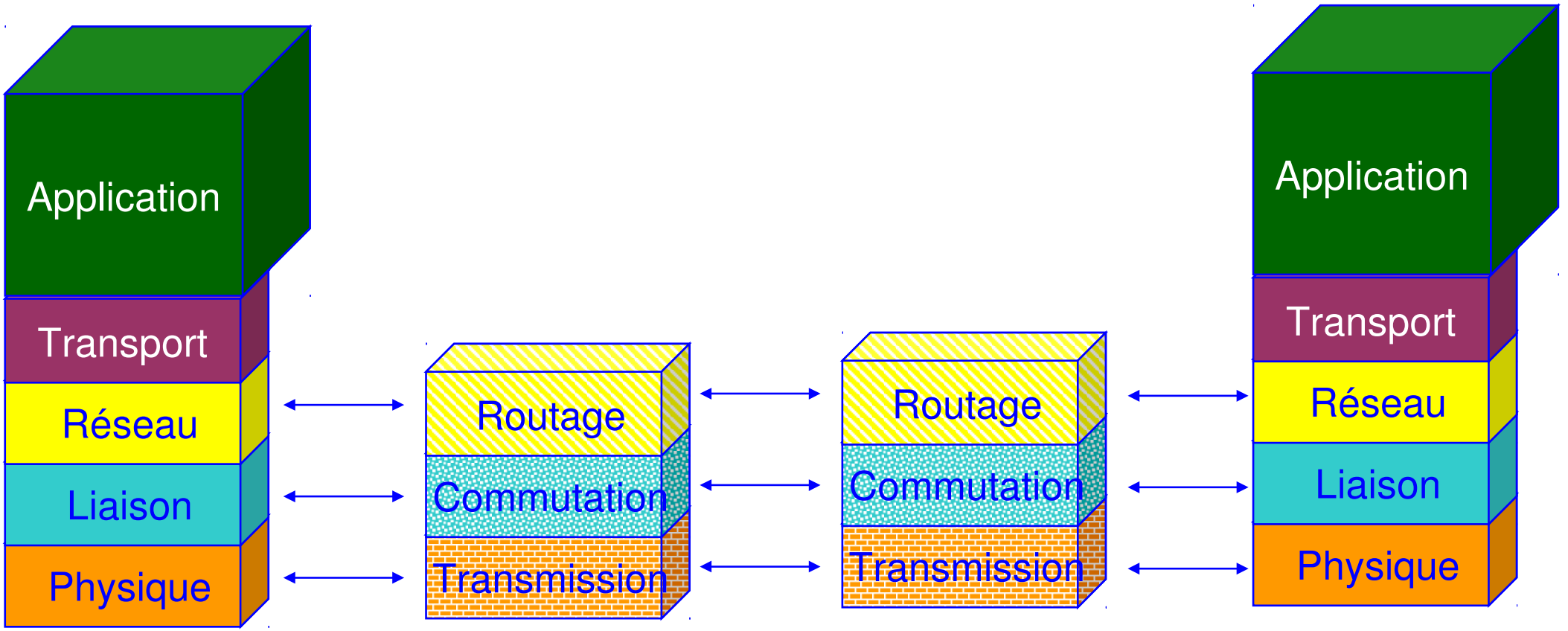
Plan

- notion sur les réseaux IP
  - architecture en couche
  - routage IP
  - notion de port
- éléments classiques d'une architecture d'entreprise sécurisée

Licence de ce document

- licence créative common BY-SA
- cf http://creativecommons.org/licenses/by-sa/4.0/
- pour réaliser ce document, j'ai utilisé le travail d'autres personnes que je remercie et qui sont citées :
  - soit directement si leur travail est utilisé tel quel
  - soit en bibliographie si leur travail m'a permis d'améliorer ma compréhension du domaine sans être utilisé directement
- un retour normal est de permettre à quiconque d'utiliser les éléments de ce document

architecture en couche



architecture en couche

- couche liaison :
  - permet à des machines directement connectées de communiquer
- couche réseau (IP)
  - permet à des machines non directement connectées de communiquer
  - routage, adresse IP
- couche transport
  - permet à des programmes situé sur des machines de communiquer
  - notion de port

routage, notion de réseau IP

- IP V4 : toute machine a une adresse IP
- ex. 194.199.90.1
- partie réseau, partie hôte
- 2 machines sont directement connectées si leur adresse a la même partie réseau
- indiquer la taille de la partie réseau :
  - le masque
  - partie réseau : nombre = 255
  - ex : 255.255.255.0 : 3 premiers nombres dans la partie réseau
  - /24 : les 24 premiers chiffres en base 2
  - 24=3*8 = les 3 premiers nombres en base 10

types de réseau historiques

- classe A : la partie réseau, c'est le premier nombre
- classe B : la partie réseau, c'est les 2 premiers nombres
- classe C : la partie réseau est constituée des 3 premiers nombres
- notions obsolètes

types de réseau actuels

- on travaille en base 2
- une adresse IP, c'est 4 nombres de 8 chiffres en base2
- une adresse IP, c'est 32 chiffres en base 2
- la taille de la partie réseau est exprimée en nombre de chiffres en base2
- ex.
  - classe A : /8
  - classe B : /16
  - classe C : /24
  - mais aussi /10 ou /22 …

structure des réseaux d'entreprise

- sortir d'un réseau : passer par une machine intermédiare appelée routeur (ou passerelle)
- à la maison : la box adsl est le routeur du réseau interne et permet l'accès à internet
- 2 machines situées sur un même réseau peuvent communiquer sans intermédiaire
- placer des machines sur des réseaux différents permet de filtrer leur trafic

attribution d'adresses IP :dhcp

- 2 machines différentes ne doivent pas avoir la même adresse IP
- attribution d'adresse ip :
  - soit par configuration manuelle
  - soit par obtention automatique auprès d'un serveur d'adresses ip appelé serveur DHCP
- DHCP : Dynamic Host Configuration Protocol

Intranet: risques

- bon dimensionnement et bonne gestion du réseau interne de l'entreprise
- idem pour les serveurs hébergeant les applications
- contrôler l'accès aux données
- contrôler l'accès physique au réseau
- protéger les serveurs des attaques
- une clef: cloisonnement et contrôle d'accès
  - outils : 802.1X, portail captif, coupe feu

Coupe Feu: généralités

- termes équivalents : parefeu, coupefeu, garde barrière (US: firewall)
- élément d'une politique de sécurité :
  - Buts possibles:
    - protéger les postes internes des attaques, cloisonnement
    - interdire la fuite des données de l'entreprise (cas d'un espion en interne)
    - contrôler les accès réseau des programmes présents sur un poste de travail (firewall perso)
  - Moyens:
    - filtrer/interdire le trafic non autorisé/dangereux,
    - laisser passer le trafic légitime
    - modifier les paquets

Divers types de coupes-feux

- terme recouvrant des réalités variées :
  - filtre de paquet
  - coupe feu à état ou suivi de connexion ou SPI
  - mandataire (proxy applicatif)
  - coupe feu personnel
- agissant à des niveaux variés:
  - couche liaison
  - couche réseau/transport
  - couche application

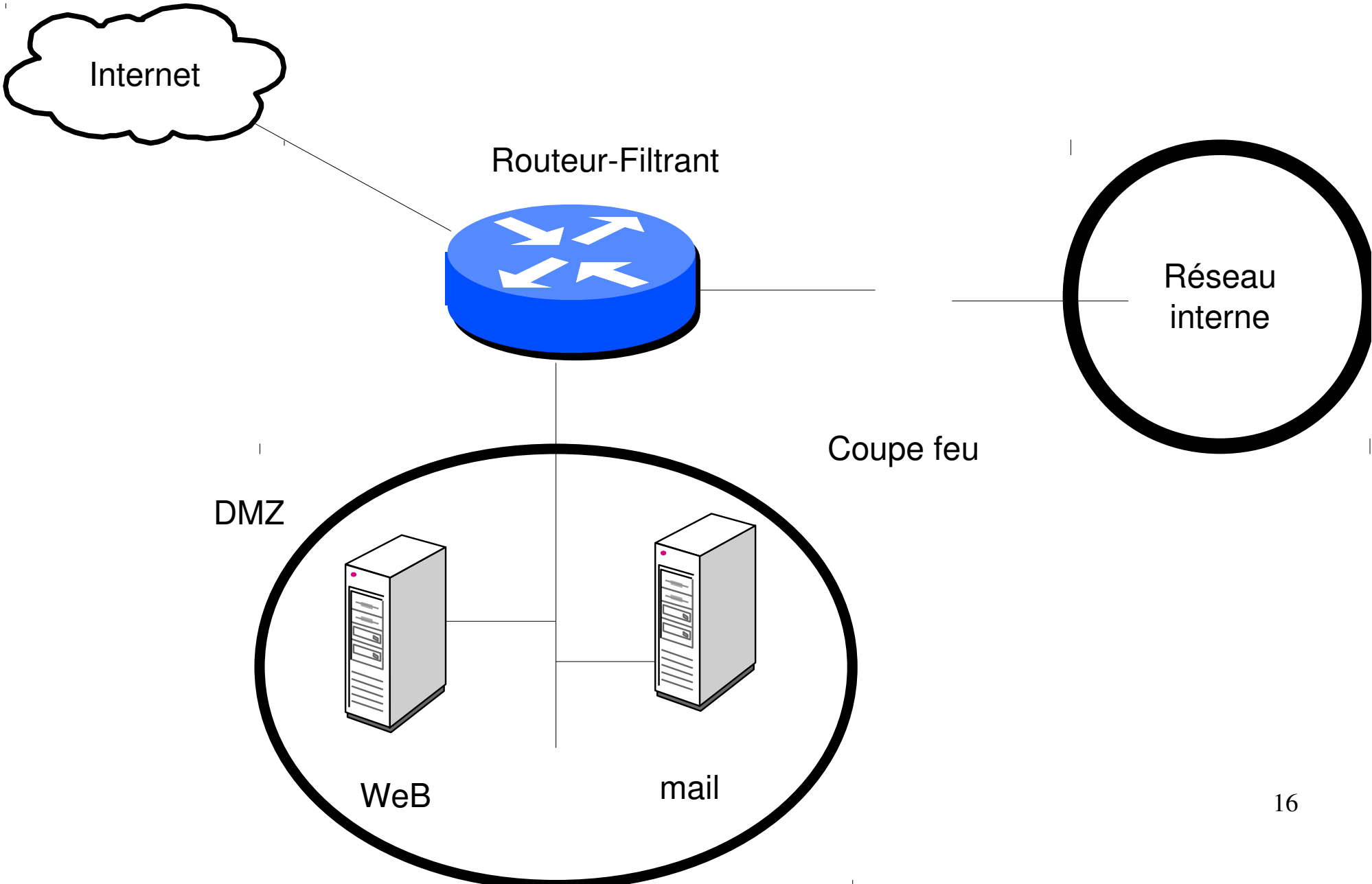
coupe feu/routeur filtrant

- positionner sur un nœud du réseau
- filtre le trafic
- filtre de paquet : filtre les paquets un par un sans historique
- coupe feu à suivi de connexion : garde un historique qui lui permet d'associer les paquets à une connexion
- exemple :
  - autoriser les paquets sortants
  - autoriser les paquets retours des paquets sortants

coupe feu pour sécurité périmétrique

- sécurité périmétrique
- indispensable mais insuffisante contre les ennemis de l'intérieur:
    - WeB, mail,portable ramenés à la maison puis dans l'entreprise, vpn, ...
  - ces accès directs aux postes clients nécessitent des mesures spécifiques pas forcément compatibles avec les demandes des utilisateurs:
    - mandataire WeB avec antivirus & Co
    - relais mail entrant avec antivirus
    - politique de sécurité stricte sur les portables, sous-réseau dédié en interne, ...

Architecture classique:



Architecture classique:

- machine bastion:
  - machine directement exposée aux attaques
  - ex.: machine ayant une adresse ip publique, serveur smtp entrant, serveur WeB, ...
- dmz
  - zone intermédiaire entre le réseau interne et le réseau externe non maîtrisé
  - contient des machines bastion
  - isole des machines publiques du réseau interne

Architecture classique

- But :
  - limiter/interdire l'accès direct de/vers l'extérieur aux postes/serveurs internes
  - réserver l'accès de/vers l'extérieur à des machines ciblées, surveillées et configurées en conséquence avec la plus petite surface d'attaque possible : les machines bastion
- Limitations:
  - supprime les accès réseau directs
  - mais pas les entrées de contenu malicieux via WeB ou mail (virus & Co)

Surface d'attaque

- diminuer la surface d'attaque: les attaques ont souvent lieu par l'exploitation de faille de logiciels
- => limiter les services accessibles sur une machine
  - en désactivant les services inutiles
  - en répartissant les services sur plusieurs machines
- Exemple historique: windows 2000 installé avec le serveur WeB IIS installé et actif

défense en profondeur

- défense globale et dynamique, coordonnant plusieurs lignes de défense couvrant toute la profondeur du système d'information
- traduction: ceinture et bretelles
  - la sécurité périmétrique seule ne suffit pas
  - l'hétérogénéité des systèmes permet d'éviter la faille qui troue tout (à opposer aux problèmes de compétence des équipes système qui incitent à homogénéiser)
- pour plus d'informations:
  http://www.ssi.gouv.fr/fr/confiance/documents/Methodes/mementodep-v1.1.pdf

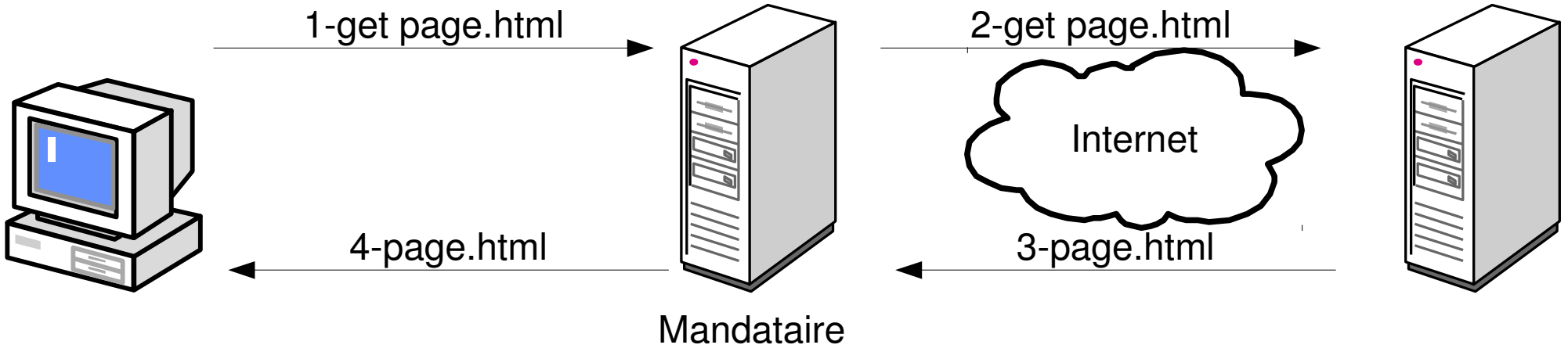
défense en profondeur

- exemples de mesure y participant
  - routeur filtrant ou firewall d'entrée de marque A
  - dmz, firewall d'entrée de l'intranet de marque B
  - blindage des OS, firewall local sur les serveur
  - cloisonnement de l'intranet
  - système de détection d'intrusion
  - antivirus sur les mandataires WeB, smtp entrant
  - antivirus, firewall personnel sur les postes de travail
  - ...

Architecture classique

- quoiques insuffisantes, ces architectures avec protection périmétrique ont quand même quasiment fait disparaître les attaques directes
- Elles peuvent être complétées par d'autres mécanismes que nous allons voir maintenant
- A noter que l'amélioration de la qualité de systèmes d'exploitation a largement fait baisser les problèmes d'exploitation directes à distance (cf http://hack.lu/images/4/45/Renaud_Hack_Lu.pdf)

Mandataire (proxy)

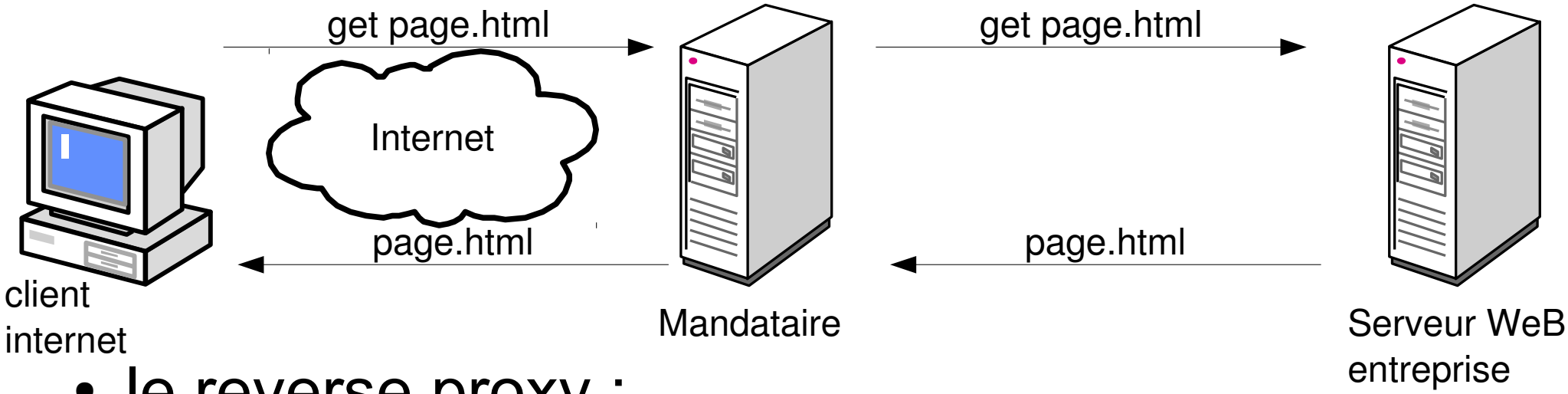


- le mandataire peut effectuer
  - un travail de nettoyage sur les données reçues (antivirus, ...)
  - un filtrage ou un nettoyage sur les données transmises
  - une journalisation des requètes
  - une demande d'authentification des utilisateurs

Mandataire (proxy)

- permet à un client des connexions indirectes à des serveurs externes
- fonctionnement
  - le client transmet sa requête au mandataire
  - le mandataire interroge le serveur distant
  - le mandataire transmet la réponse au client
- Avantages :
  - travail au niveau application
  - permet du filtrage en entrée (antivirus, ...) et en sortie (interdire certaines requêtes)
  - permet journalisation des requêtes, authentification.
- Cas courante: WeB, mail entrant/sortant

Reverse proxy

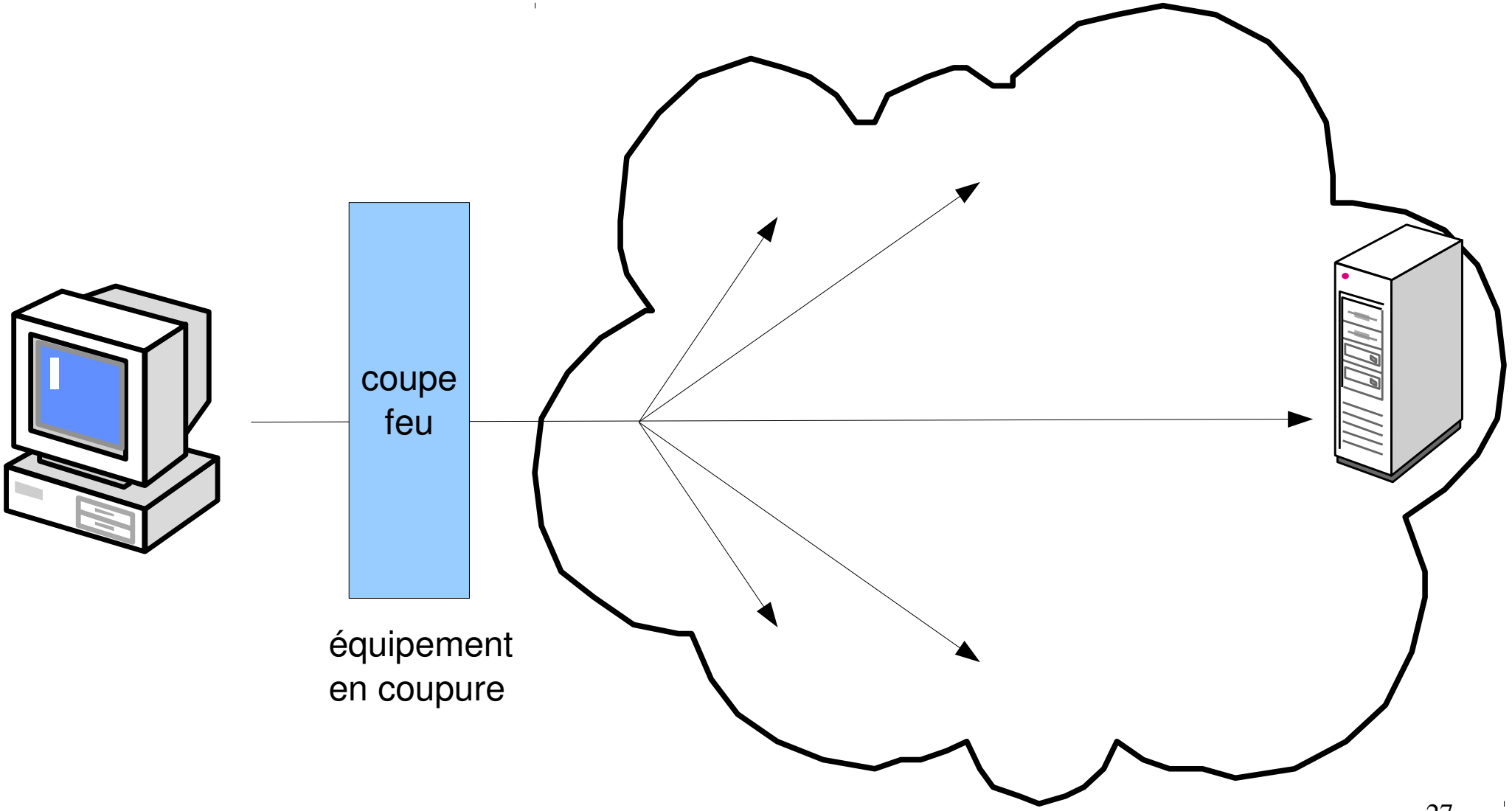


- le reverse proxy :
  - peut protéger un OS un peu faible des accès directs
  - peut effectuer un filtrage ou un nettoyage sur les requêtes transmises pour palier la faiblesse d'un logiciel serveur WeB
  - peut demander une authentification

Contrôler l'accès au réseau (NAC)

- interdire l'accès au réseau interne des postes non autorisés
- but: éviter des attaques/vol d'informations d'un visiteur agissant de l'intérieur (filaire, WiFi)
- divers méthodes :
  - sécurité physique (accès aux locaux)
  - brassage à la demande (pour info, pas au programme)
  - filtrage par adresses MAC ou IP (idem)
  - portail captif (au programme)
  - 802.1X

•NAC: équipement en coupure



•NAC: Contrôle via un équipement en coupure

- l'accès réseau n'est autorisé qu'après authentification sur un équipement en coupure
  - exemple : par une redirection automatique : proxy transparent et portail captif
  - cas du WiFi etudiant de l'université d'Evry
- succès de l'authentification => chargement de règles de filtrage autorisant certains accès
- méthode « moderne » facilitant une gestion centralisée

•NAC: portail captif WeB