sécurité des infrastrutures de télécommunication

- protocole IP
- intranet: sécurité contre les risques internes
- internet: sécurité contre les risques externes
- confidentialité

IP V4

- aucun mécanisme de sécurité
- aucun mécanisme d'authentification
- pas de gestion de la qualité de service
- aucun mécanisme pour la confidentialité
- le protocole contient des éléments facilement exploitables (désactivés de nos jours)
- conséquences:
  - sécurité géré au niveau application (ssh, https, ...)
  - vpn ,ipsec

exemple d'attaque: dhcp

- neutraliser un serveur dhcp
- le remplacer
- devenir routeur (Man In the Midle)
- serveur dns (phishing)

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
  - VLAN, 802.1X
  - coupe feu

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
  - filtrage par adresses MAC ou IP
  - portail captif
  - analyse distante des postes
  - 802.1X

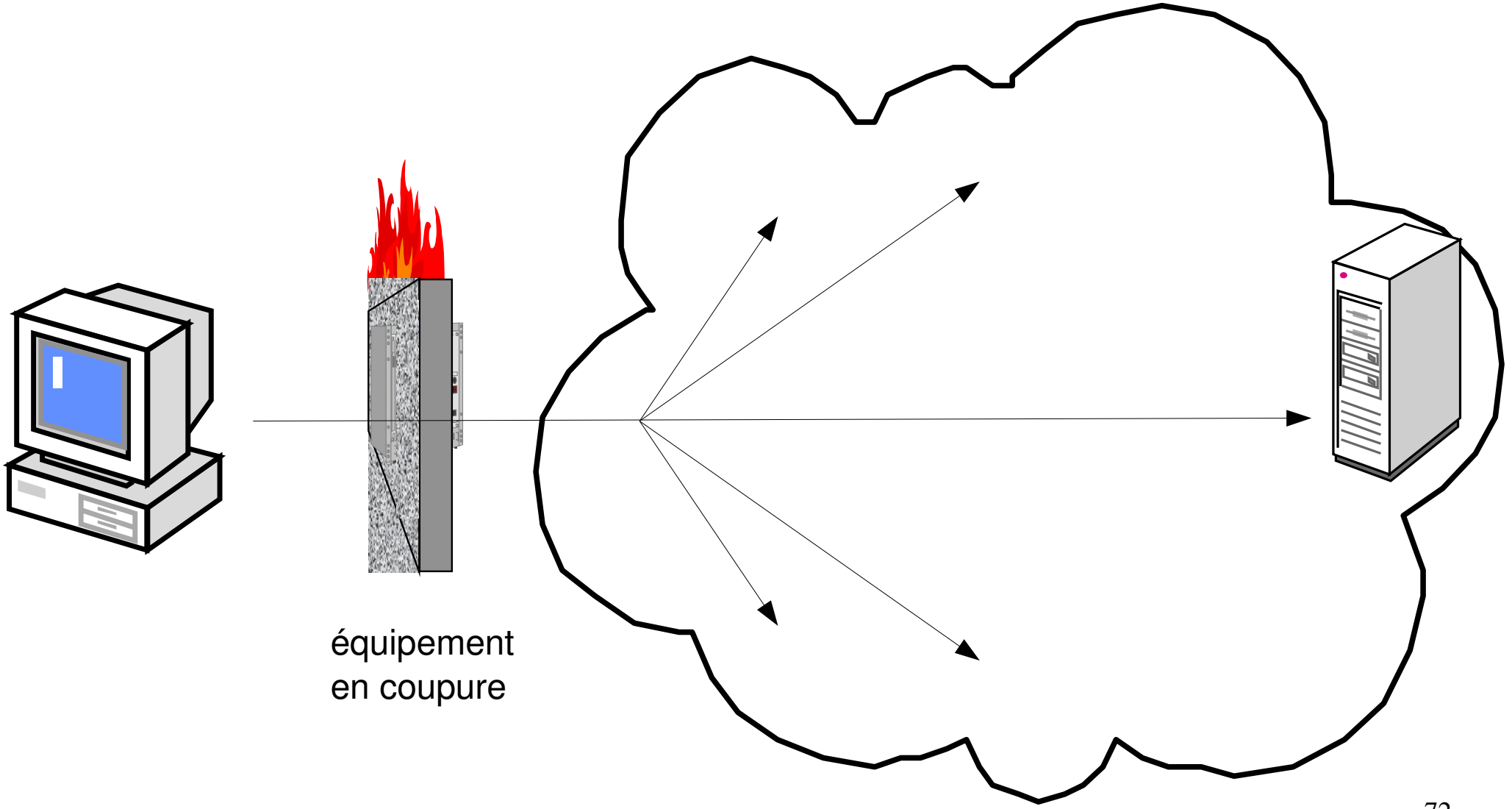
NAC: brassage à la demande

- brassage et activation de ports à la demande
  - éviter les prises libres utilisables
  - coûteux en ressources humaines
  - protection très faible : ne peut rien contre l'utilisation d'une prise utilisée

NAC: brassage à la demande

- contrôle des adresses MAC:
  - affectation d'adresses MAC par ports :
    - le port est coupé si le matériel qui est branché n'a pas l'adresse MAC déclarée
    - fastidieux à gérer :saisie des données, déblocage des ports bloqués par erreur
  - gestion globale des adresse MAC sur l'entreprise
  - facilement contournable (MAC écrite sur les postes, faciles à changer)

•NAC: équipement en coupure



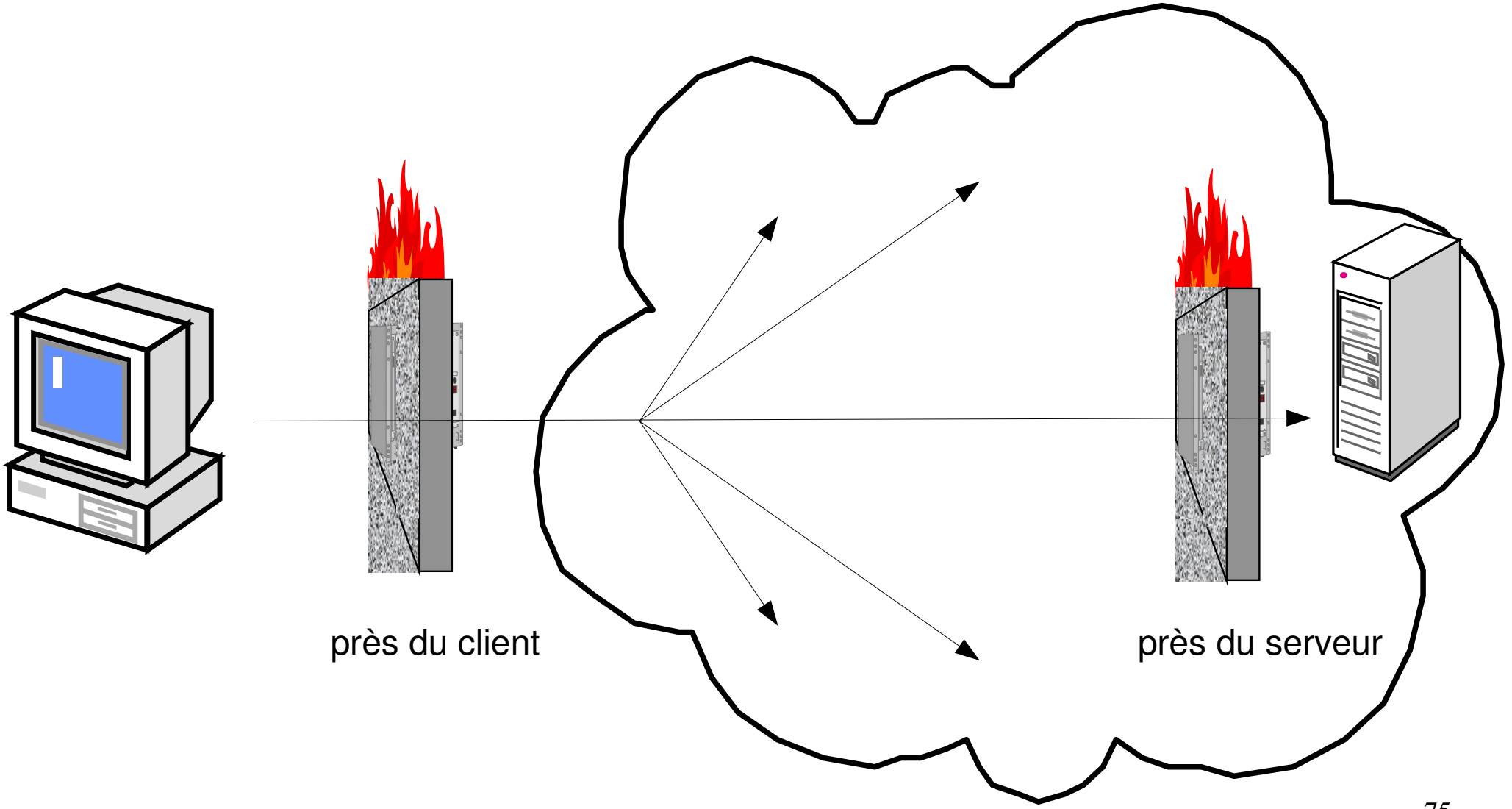
•NAC: Contrôle via un équipement en coupure

- l'accès réseau n'est autorisé qu'après authentification sur un équipement en coupure
  - par une connexion directe sur l'équipement (http, ssh, telnet, ...). Exemple: authpf (OpenBSD, PacketFilter)
  - par une redirection automatique : proxy transparent et portail captif
- succès de l'authentification => chargement de règles de filtrage, de VLAN spécifiques
- méthode « moderne » facilitant une gestion centralisée

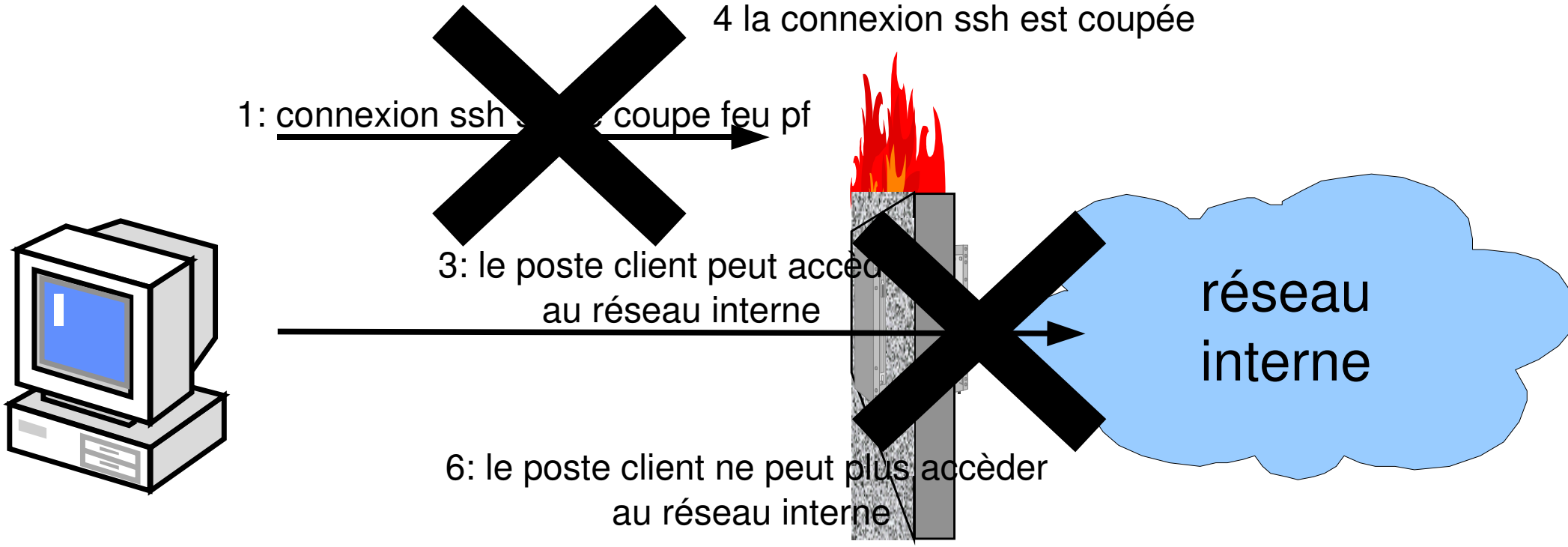
•NAC: positionnement de l'équipement en coupure

- positionnement de l'équipement en coupure:
  - seul ce qui est après l'équipement est protégé
  - ce qui est avant est exposé
  - positionnement proche du client:
    - pour réguler un accès au réseau de l'entreprise
    - de nombreux type de flux vont devoir être autorisés
  - positionnement proche du serveur :
    - pour réguler l'accès à un unique type d'applications
    - permet de filtrer de façon fine le trafic (on sait plus précisément de quoi devra être constitué le trafic)

•NAC: positionnement de l'équipement en coupure



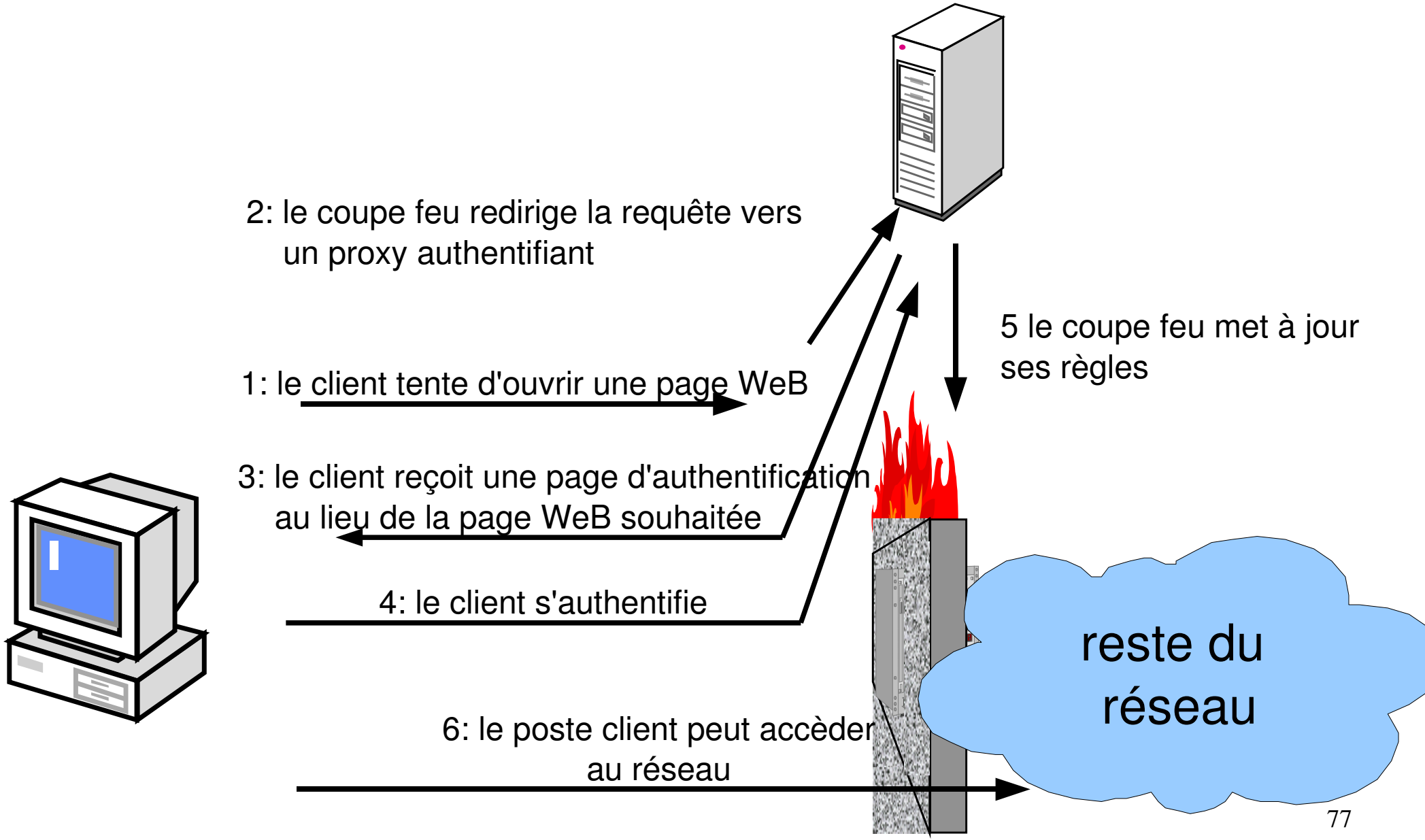
•NAC: authPF



2: le coupe feu charge des règles spécifiques autorisant l'accès au réseau interne

5: le coupe feu décharge les règles spécifiques autorisant l'accès au réseau interne

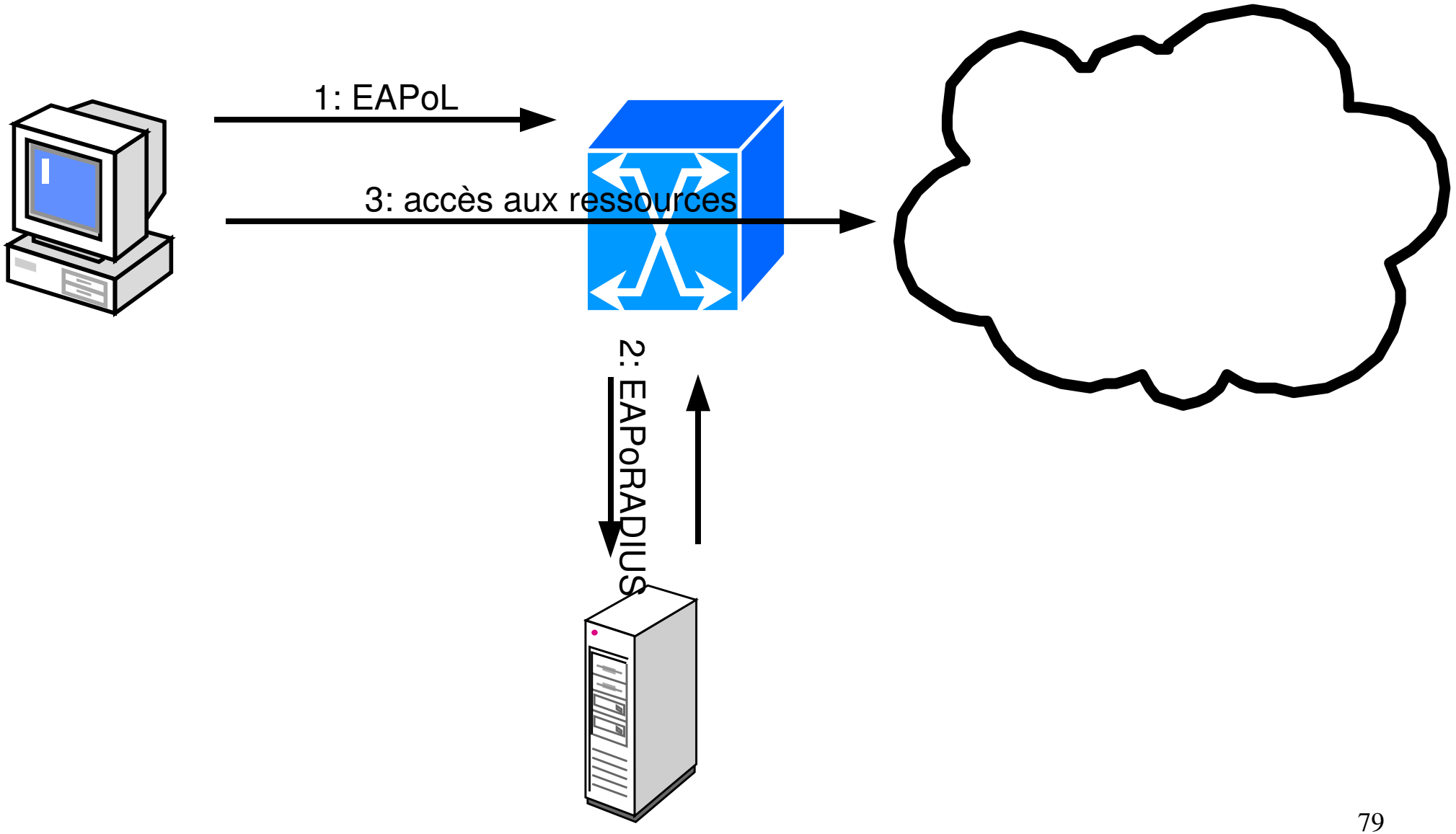
•NAC: portail captif WeB



•NAC: Contrôle par un équipement en coupure niv. 3

- Pb: possibilité d'usurpation d'IP, MAC, ... pour emprunter les droits d'une connexion active
  - authentification périodique pour valider la présence du client authentifié
    - portail WeB:
      - la page d'authentification se recharge périodiquement
      - si la page est fermée ou ne se recharge pas, l'accès est coupé au bout d'un temps paramètrable
  - ou utilisation d'un protocole en mode connecté (connexion coupée => perte de l'accès)
    - authpf: coupure de la connexion ssh => coupure immédiate de l'accès (si timeout ssh paramètré)

•NAC: 802.1X, contrôle au niveau 2



802.1X: contrôle niveau 2

- 3 éléments entrent en jeux :
  - le client (« supplicant ») qui souhaite un accès au réseau
  - le point de contrôle (« authenticator ») à l'entrée du réseau local (commutateur, borne WiFi en général)
  - le serveur d'authentification (« authentification server ») radius

802.1X: cinématique

- le client transmet des informations d'authentification et sa posture de sécurité (éléments de conformité)
- le point d'accès valide ces informations avec le serveur radius qui lui retourne éventuellement des éléments de configuration (VLAN , ...)
- en fonction de la réponse obtenue, l'accès est autorisé dans les conditions précisées dans la réponse (notamment le VLAN du client) ou interdit

802.1X:

- le port du commutateur ne laisse passer vers le commutateur que les trames EAPoL (EAP encapsulé dans de l'ethernet)
- le commutateur encapsule la requête EAP dans un paquet EAPoRADIUS
- sécurité: pas de communication directe entre client et serveur d'authentification

802.1X: points de mise en oeuvre

- continuité de service: point clef: le serveur radius
- support 802.1X par les équipements réseau, par les postes clients
- impact du choix de la méthode d'authentification EAP:
  - authentification de la machine/de l'utilisateur (quid de l'accès réseau pendant le boot)
  - type d'authentification (certificat, OTP, ...)

802.1X: points de mise en oeuvre

- gestion de périphériques passifs (imprimantes, ...)
- impact sur la facilité d'administration du parc (WakeUpOnLan, ...)
- sécurité de la zone de quarantaine
  - vis à vis du reste du réseau
  - à l'intérieur de la zone (interdire les connexions entre postes)

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 (NAT, REDIRECT, mandataire transparent, ...)

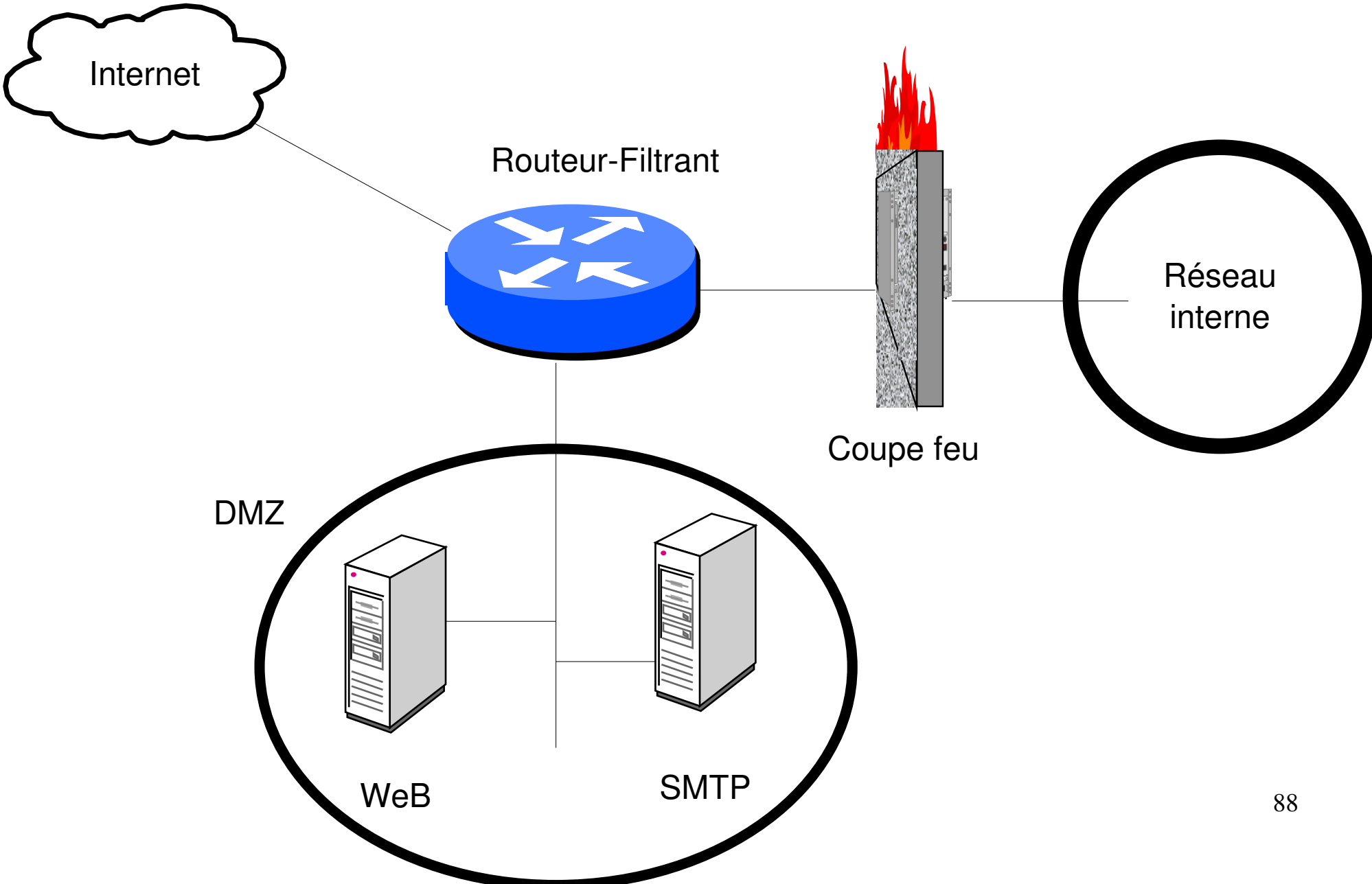
Divers types de coupes-feux

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

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 smtp 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

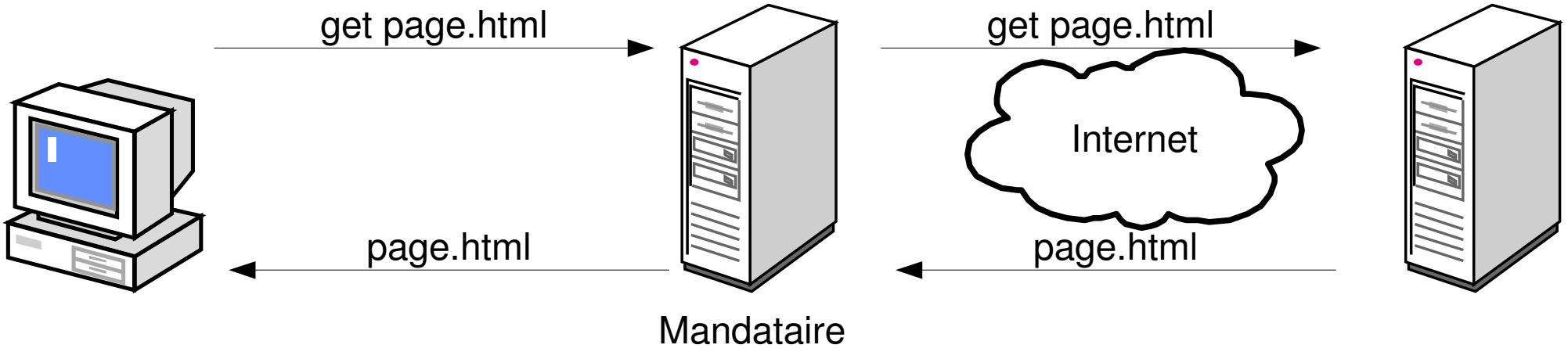
défense en profondeur

- 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)

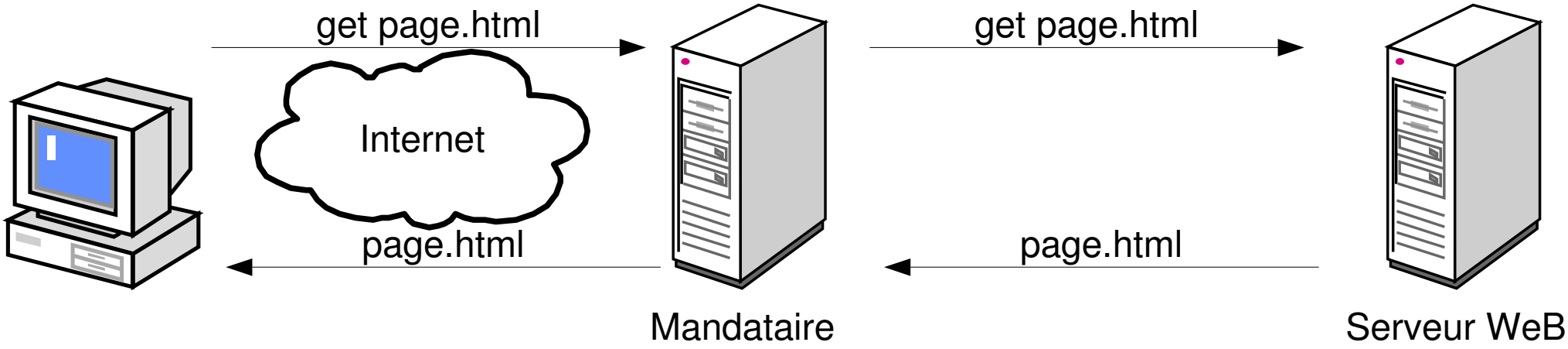


- le mandataire peut effectuer
  - un travail de nettoyage sur les données reçues (antivirus, ...)
  - un filtrage ou un nettoyage sur les données transmises
  - une journalisation des requètes
  - une demande d'authentification des utilisateurs

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, SMTP 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

proxy variés :

- proxy transparent:
  - proxy couplé avec un firewall qui détourne les requêtes vers le proxy sans que le client le sache
- proxy http / https
  - https est chiffré
  - les proxies https déchiffrent et rechiffrent les données au vol (gare aux problèmes légaux)

coupe feu personnel

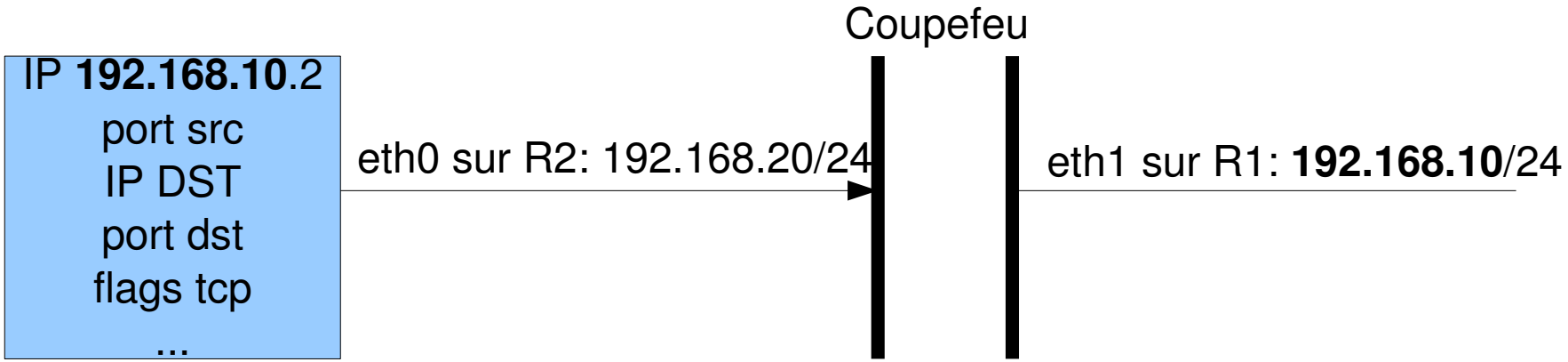
- sur le poste de travail
- filtre le trafic entrant
- filtre le trafic sortant en fonction de l'application qui l'a généré

Filtre de paquet

- analyse les paquets indépendamment les uns des autres
- critères de filtrage:
  - paquet IP: IP src, IP destination, ports sources et destination
  - interface réseau sur laquelle se présente le paquet

Filtre de paquet: exemples typiques (1)

- filtrage de paquet avec une source sur un sous-réseau incorrect:
  - le coupe feu ne doit pas accepter sur eth0 des paquets ayant une IP source sur R1 (eth1)



Filtre de paquet: exemples typiques (2)

- autorisation des accès au WeB (http: tcp/80, https: tcp/443)
- en sortie: paquet vers le port 80 de toute machine externe
- paquet retour: paquet depuis le port 80 de toute machine externe
- Problème: tout paquet venant de l'extérieur et ayant le port 80 comme port source sera autorisé.
- dans la vraie vie, on utilise un mandataire WeB (proxy WeB) qui est la seule machine visible de l'extérieur

Filtre de paquets: bilan

- analyse paquet par paquet
- simple à implémenter
- syntaxe simple s'appuyant sur les propriétés du paquet (interface réseau entrante comprise)
- pas de suivi de l'historique des paquets
  - => manque de souplesse pour les autorisation
  - choix entre trop fermer (ne pas rendre le service) ou trop ouvrir (ne plus protéger)
  - cf exemple accès WeB sortant

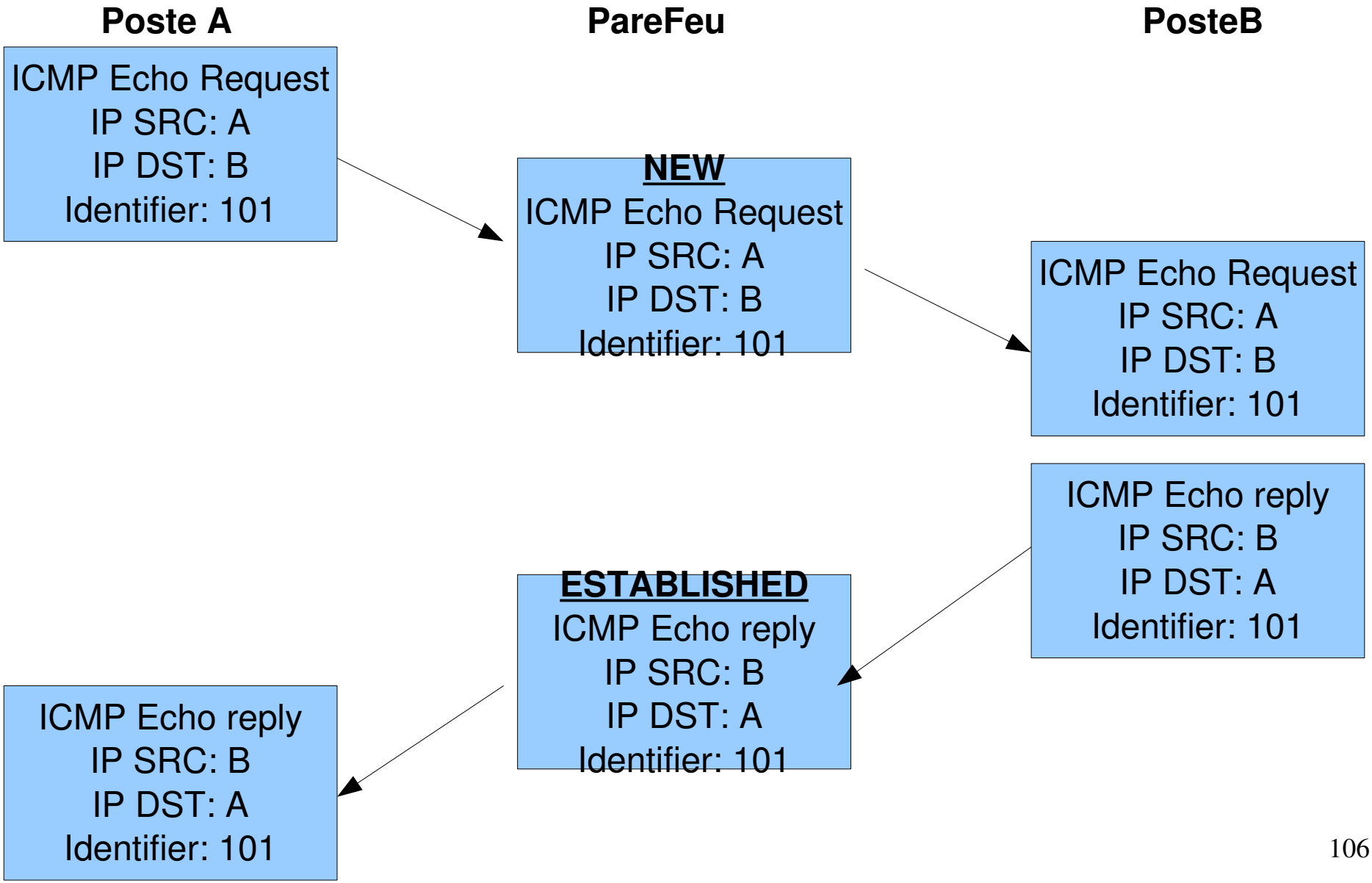
coupefeu à états

- termes équivalents: coupefeu dynamique, à états, par suivi de connexion, « Statefull Packet Inspection»
- enrichit le filtrage des paquets par la mémorisation de l'état des sessions,d'échanges de données en fonction des paquets déjà vus
- analyse s'appuyant sur l'historique des sessions
- session
  - naturel avec tcp
  - la connaissance des couches réseau, transport, voire application permet d'en gérer avec udp et icmp

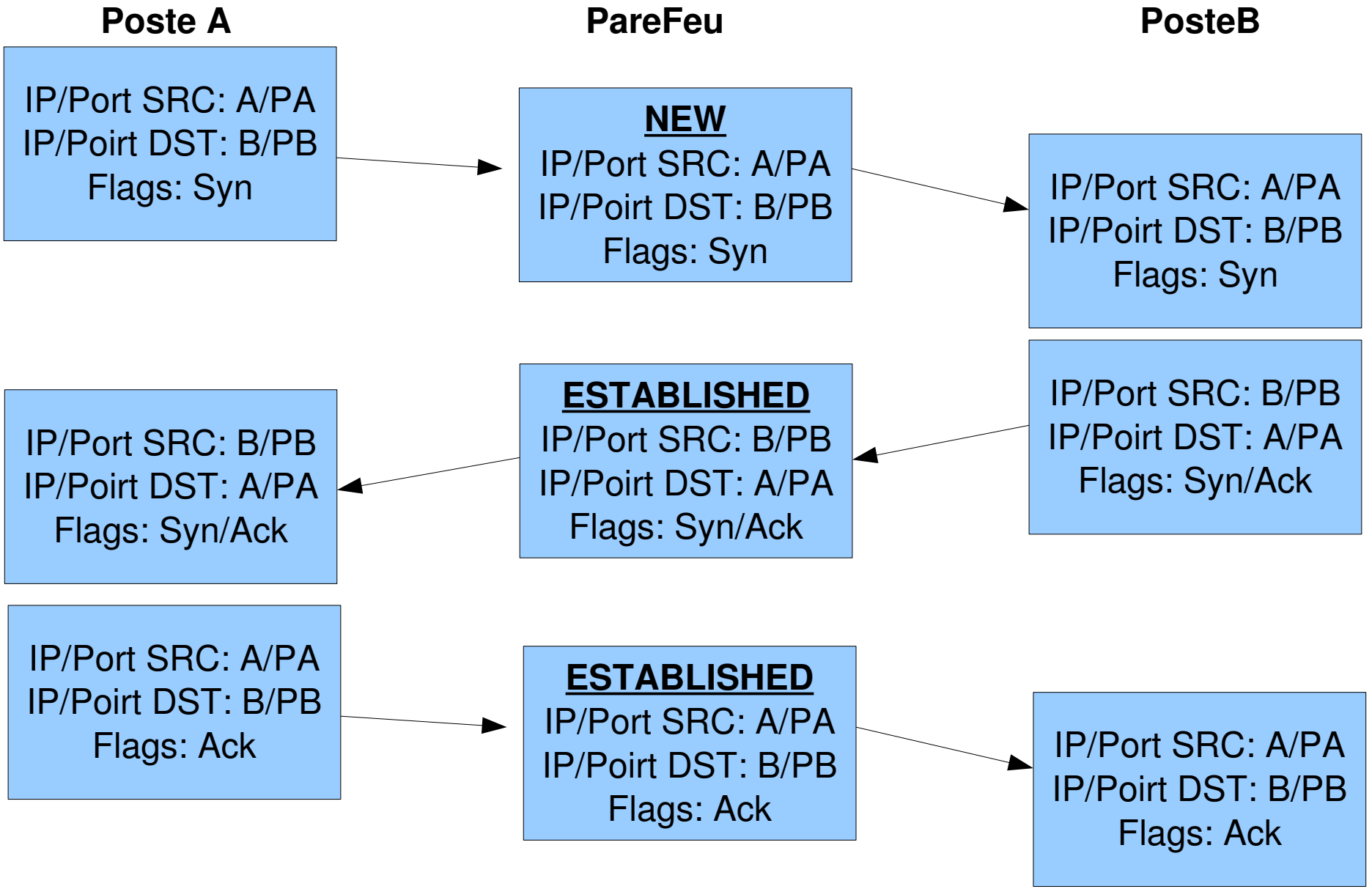
parefeu à état: état d'une session

- avec le parefeu NetFilter (Linux 2.4+), un paquet faisant partie d'une session peut être l'un des 4 états suivants :
  - New: ne correspond à aucune entrée de la table des états. Création d'une nouvelle entrée
  - Established: le paquet fait partie d'une connexion existante (entrée existante dans la table des états)
  - Related: le paquet fait partie d'une nouvelle connexion faisant partie d'une session existante.
  - Invalid: paquet dont l'état n'a pu être déterminé
- il y a des états internes plus détaillés accessibles par « cat /proc/net/ip_conntrack »

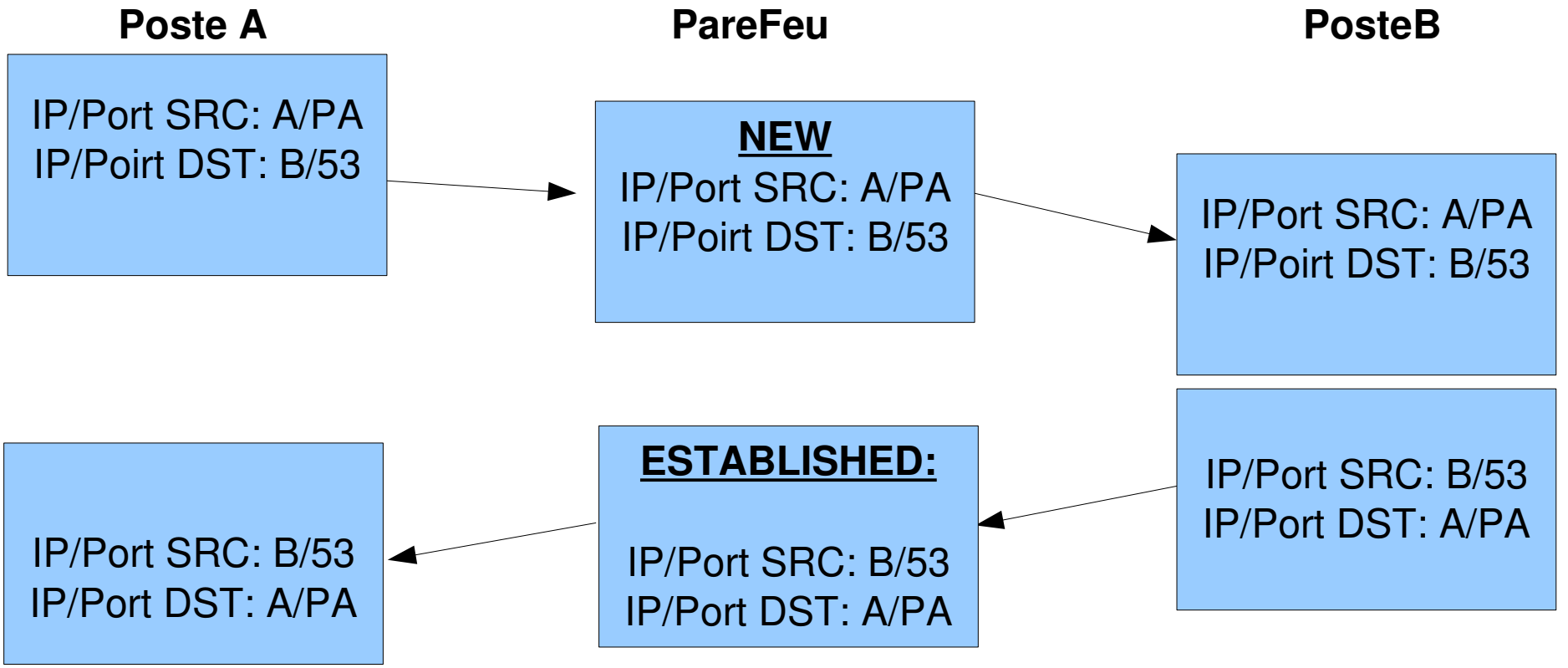
exemple de sessions: icmp echo



exemple de sessions: tcp



exemple de session: udp (dns)



coupe feu à états: exemple typique

- autorisation des accès au WeB (http: tcp/80, https: tcp/443)
- en sortie: paquet vers le port 80 de toute machine externe
- en entrée: paquet correspondant à une connexion sortante:
  - machine/port sources et destinations
  - tcp/udp
  - éventuellement d'autres paramètres:
    - numéros de séquences