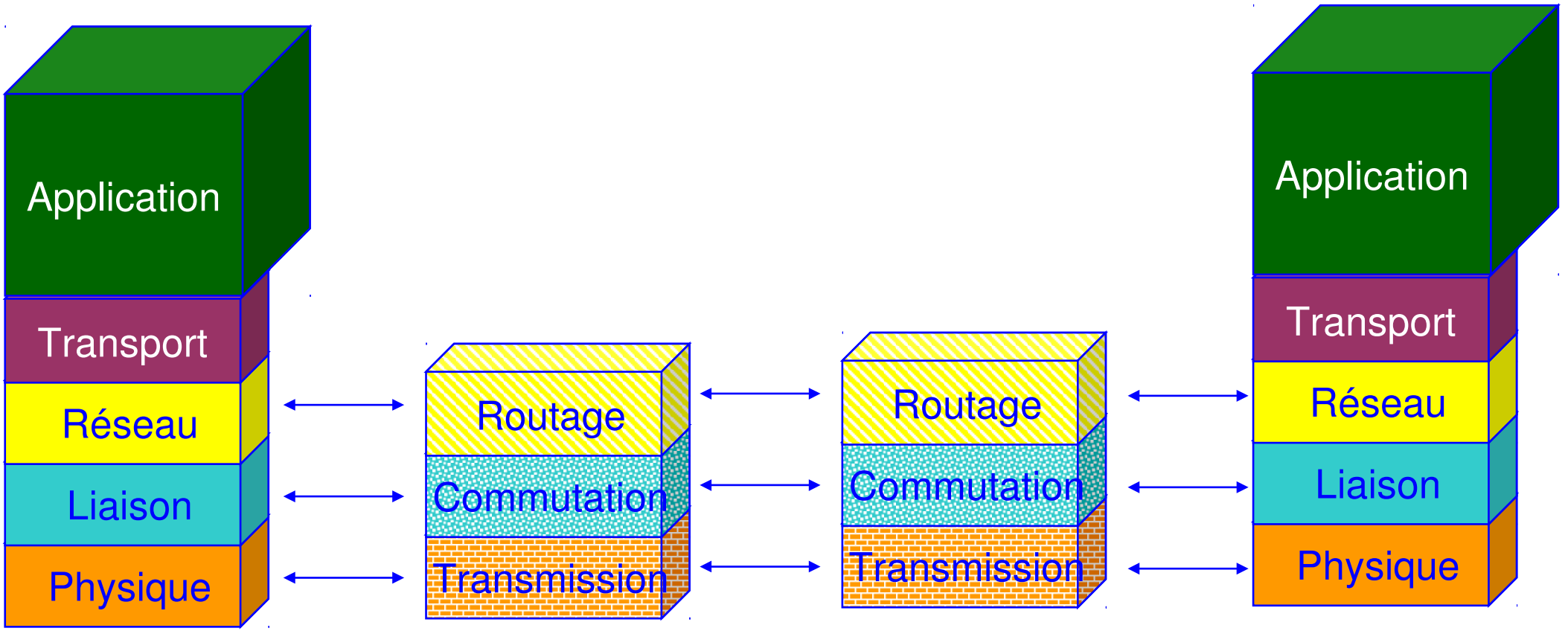
Présentation:

- Pascal PETIT
- sécurité informatique
- pascal.petit@shayol.org

Plan

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

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

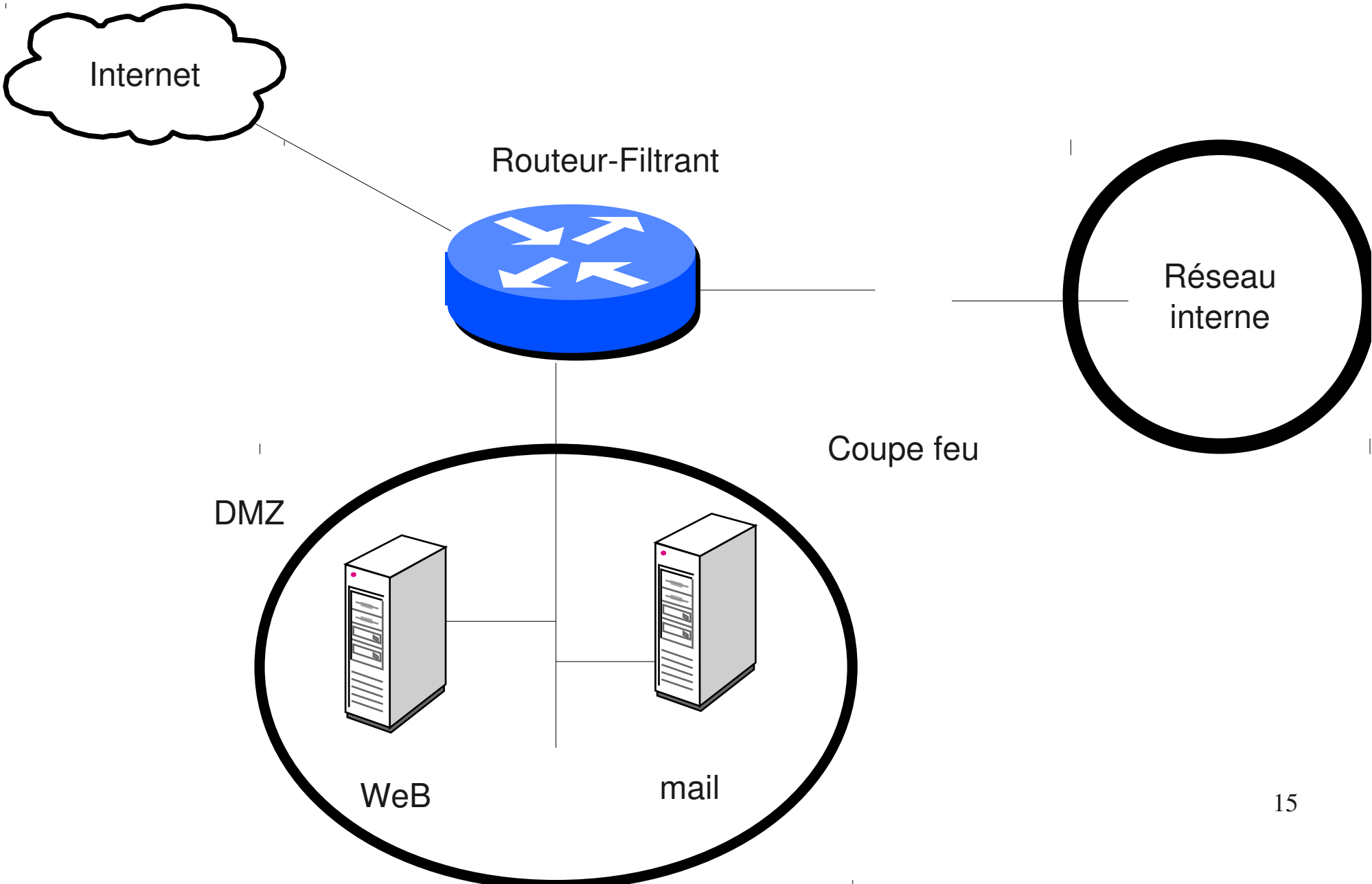
coupe feu/routeur filtrant

- 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

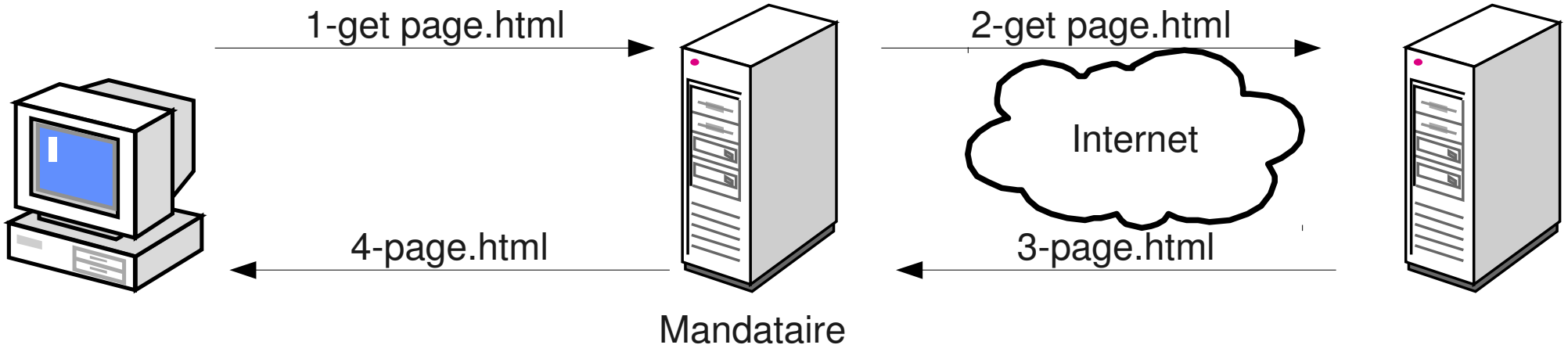
défense en profondeur

- 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)

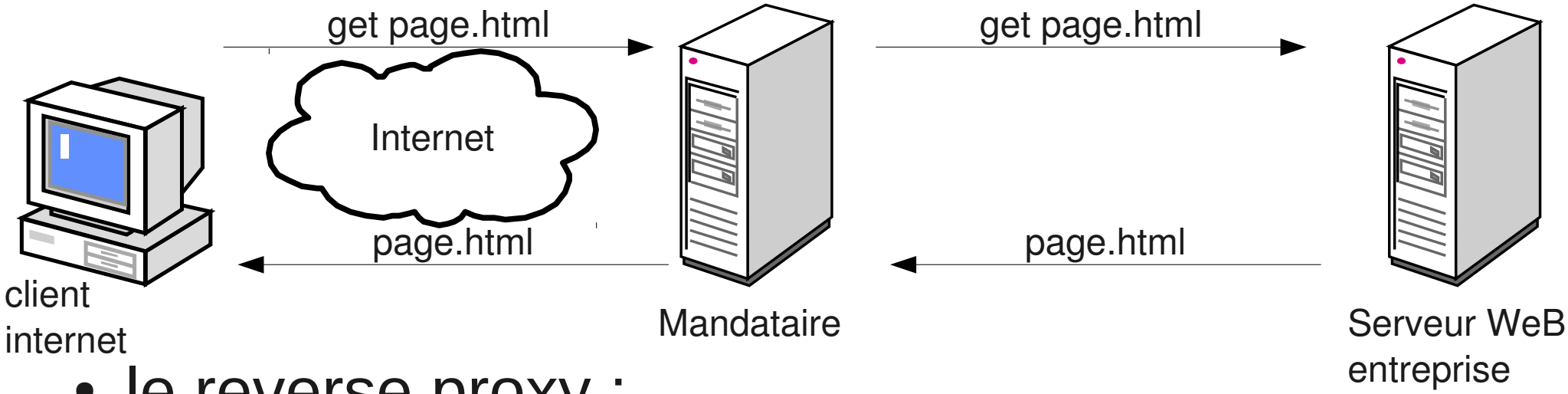


- le mandataire peut effectuer
  - un travail de nettoyage sur les données reçues (antivirus, ...)
  - un filtrage ou un nettoyage sur les données transmises
  - une journalisation des requètes
  - une demande d'authentification des utilisateurs

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

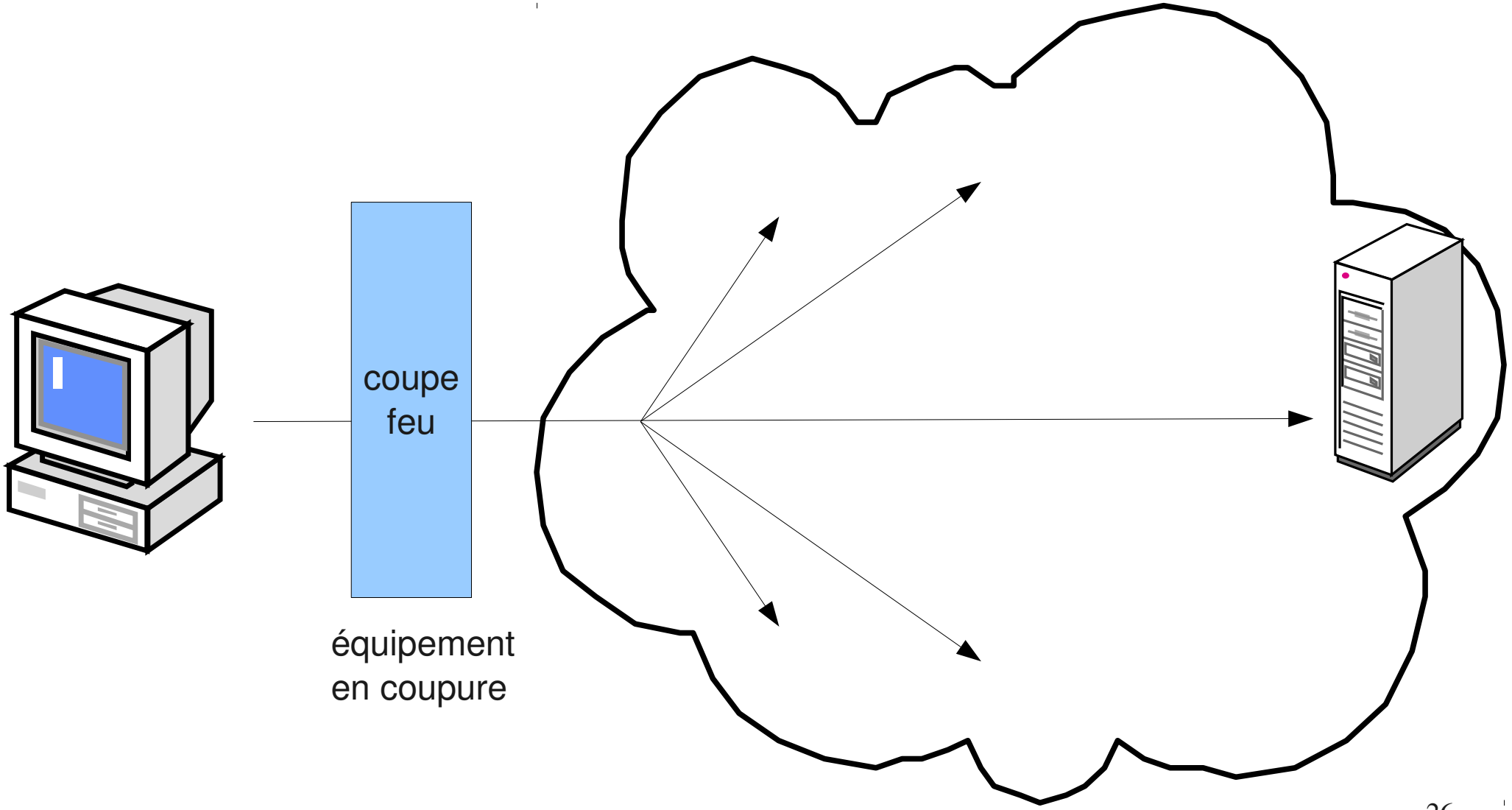


- le reverse proxy :
  - peut protéger un OS un peu faible des accès directs
  - peut effectuer un filtrage ou un nettoyage sur les requêtes transmises pour palier la faiblesse d'un logiciel serveur WeB
  - peut demander une authentification

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

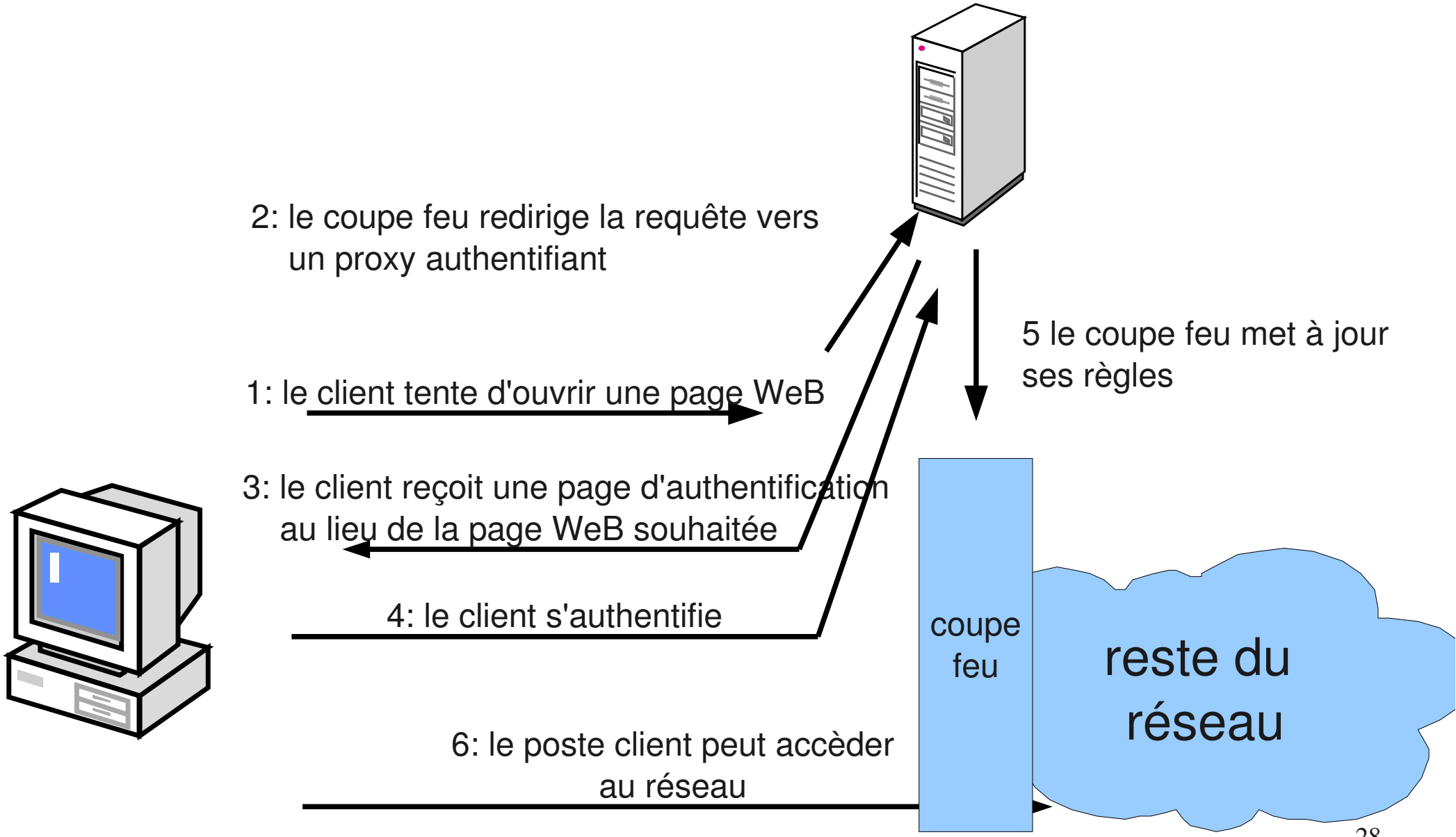
•NAC: équipement en coupure



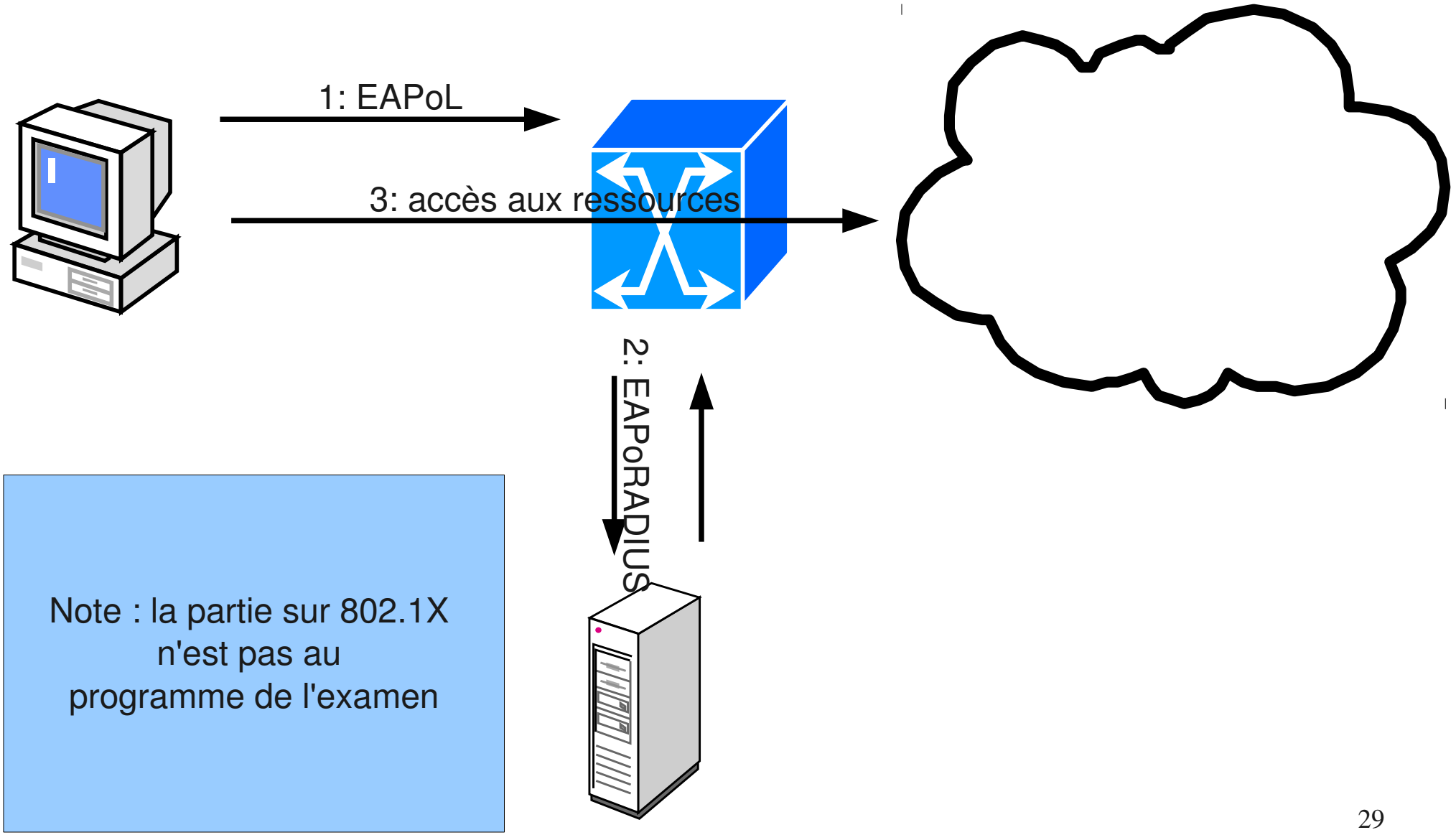
•NAC: Contrôle via un équipement en coupure

- 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



•NAC: 802.1X, contrôle au niveau 2



Note : la partie sur 802.1X n'est pas au programme de l'examen

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

Note : la partie sur 802.1X n'est pas au programme de l'examen

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

Chiffrement: robustesse

- cryptanalyse: analyser une information chiffrée pour la déchiffrer(dont méthodes en force brute, ...)
- algo public
- la sécurité repose sur :
  - la non divulgation de la clef
  - la robustesse de l'algorithme
  - la taille de la clef (gare aux comparaisons entre algo différents)
  - l'utilisation de clefs différentes pour chiffrer des messages différents limite la quantité d'information à la disposition de l'attaquant

chiffrement: taille des clefs

- attaques en force brute: tenter une partie importante de l'espace des clefs
- temps dépend du nombre de clefs possibles et donc de la taille de la clef:
  - 10 bits : 1024 clefs possibles
  - 56 bits: 2^56=7 10^16
  - dépendance exponentielle en fonction de la taille de la clef: 1 bit de plus = 2 fois plus de temps
- la taille critique dépend de l'algo (et de sa vitesse, de ses faiblesses, ...)

algorithme de chiffrement

- chiffrement symétrique/asymétrique
  - symétrique:
    - les algo classiques sont rapides
    - **la même clef sert au chiffrement et au déchiffrement**
    - souvent utilisé via une clef de session
      - clef de session: transmise via algo asymétrique (on parle d'enveloppe digitale)
      - session: chiffrée par un algo symétrique et la clef transmise

algorithme de chiffrement

- chiffrement symétrique/asymétrique
  - asymétrique:
    - les algo classiques sont lents
    - **couple de clef publique/clef privée**
      - clef publique: peut être connue de tous
      - clef privée: tenue cachées
      - ce qui est chiffré avec l'une ne peut être déchiffré qu'avec l'autre

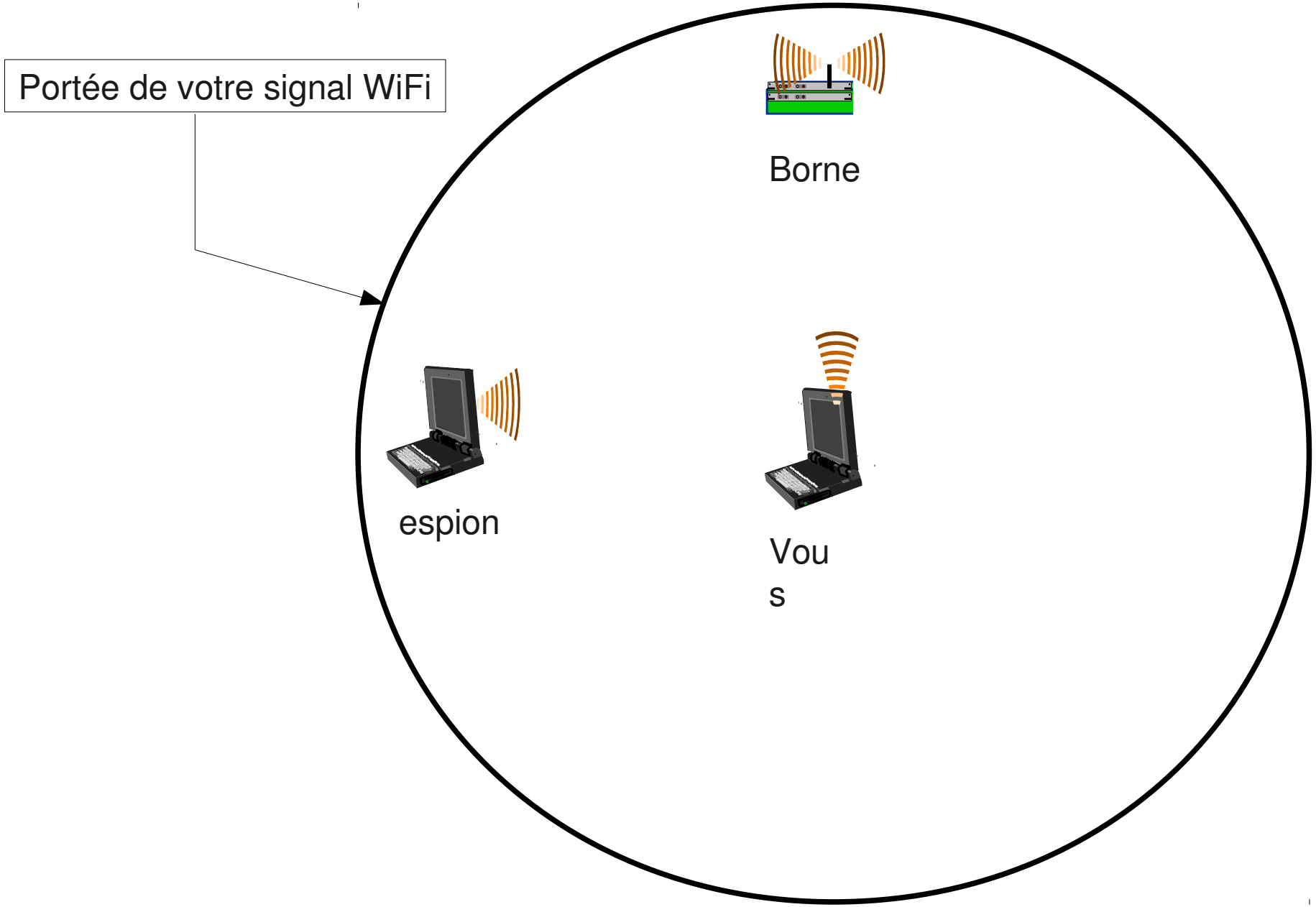
services offerts par le chiffrement:

- confidentialité
- intégrité
- signature numérique
- authentification
- Single Sing On
- non répudiation

WiFi : enjeux

- Utilisation du réseau par un utilisateur non légitime
  - Pour rebond
  - Pour réseau local
  - Pour attaque des autres postes WiFi
    - Solution : interdire les connexions entre postes WiFi (réglage point d'accès)
- Espionnage des données échangées :
  - Sites consultés
  - Mot de passe
  - ...

WiFi : enjeu



WiFi : sécurité

- Ouvert : pas de chiffrement. En général associé à un portail d'authentification
- WEP : chiffrement MAIS cassable en quelques minutes par un non informaticien
- WPA1/WPA2 personnal : chiffrement solide (si clef solide) MAIS clef commune
- WPA2 entreprise + 802.1X + méthode génératrice de clef : chiffrement solide, clef unique par poste
- Exemples : google cars.

Solutions :

- utiliser une méthode solide (WPA2)
- chiffrer ses communications
  - https
  - VPN
- Utiliser https partout où c'est possible
  - Trafic chiffré entre votre navigateur et le serveur
  - Authentification du serveur
- Extension firefox : httpseverywhere (https://www.eff.org/https-everywhere)

Certificats, https

Carte d'identité

Pascal PETIT

Certificats, https

Certificats :

- Un certificat :
  - Identité,
  - clefs publique
  - Certifiés par une autorité de certification
- Permet l'authentification d'un site
  - Le site possède la clef privée associée
  - Le site indiqué par le certificat est bien celui auquel on se connecte
- Permet la mise en place d'un tunnel chiffré : protège contre l'espionnage des communications

certificats et hameçonnage

- Du phishing pour identifier les opposants à Bachar El-Assad
  - faute site youtube annonçant une fausse mise à jour de flash
    - => installation d'un logiciel espion
  - faux site facebook ou youtube
    - récupérer login et mot de passe (y compris des personnes qui mettent des commentaires)
- source : Numerama, 30 mars 2012 :
  http://www.numerama.com/magazine/22197-du-phishing-pour-identifier-les-opposants-a-bachar-el-assad.html

limite de https

- vigilance des utilisateurs (cf exemple syrien)
- fiabilité des autorités de certification
  - que penser d'une AC liée à un pays
  - impact possible
    - créer un faux certificats reconnu comme valide par le navigateur
    - l’hameçonnage sans détection possible
- solutions :
  - aucune pour l'instant

Dropbox

- avril 2011 : changement des conditions d'utilisation de dropbox
- avant, dropbox vantait la qualité de son chiffrement AES 256bits
- détection de doublon
  - pour gagner de la place
  - suppose que dropbox puisse déchiffrer les fichiers chiffrés
- BIBLIO :
  - http://www.cnetfrance.fr/news/dropbox-induisait-en-erreur-sur-la-confidentialite-des-donnees-et-le-cryptage-39760824.htm

Dropbox : solution

- chiffrer les données soit même
- via true crypt :
  - pénible car suppose le transfert de tout le contener à chaque modification
  - soit avec des solutions fichiers par fichiers à la encfs
    - pcimpact : http://www.pcinpact.com/dossier/chiffrement-cloud-encfs-boxcryptor-dropbox/209-1.htm
    - http://korben.info/dropbox-chiffrer-crypter-securiser.html
    - http://korben.info/boxcryptor-dropbox-crypte.html

Protection des disques durs

- Mot de passe du bios
  - Peut être supprimé par un voleur
  - Ne l'utiliser que pour empêcher l'utilisation du portable en votre absence
- Mot de passe du disque dur
  - Le mot de passe est stocké dans l'électronique du disque
  - Beaucoup plus résistant
  - Plusieurs niveaux de sécurité (récupérable par le constructeur ou non)
- Chiffrement de partitions ou de disques

Truecrypt : références

- Le FBI se serait cassé les dents dessus : http://sid.rstack.org/blog/index.php/400-pbkdf2-a-l-epreuve-du-fbi
- Rapport de certification de la version 6.0a : http://esec.fr.sogeti.com/FR/documents/presse/tc_dcssi.pdf
- Site officiel : http://www.truecrypt.org/

True crypt fonctionnalités

- Peut chiffrer un disque virtuel dans un fichier
- Peut chiffrer une partition (y compris la partition où est installé windows)
- Le chiffrement est transparent et automatique
- Permet de la stéganographie (méfiance : des travaux récents permettent de détecter les conteneurs truecrypt)
- Fournit des mécanismes de déni plausible en cas de fourniture forcée du mot de passe

encfs/box cryptor

- outils de chiffrement de dossier
- chiffre fichiers par fichiers
- plus efficace en cas de synchronisation entre dossiers sauvegardés
- les outils :
  - encfs/cryptkeeper : sous linux
  - boxcryptor : sous windows

Mail & Co : bonnes pratiques

- Mail : gare à la diffusion involontaire d'information
- Informations contenues dans les documents pdf, m$-office & Co

Mail : du danger de la citation

- Guerre de religions avec 2 sectes :
  - Le dinosaures : Ceux qui répondent au dessous du texte cité
  - Ceux qui répondent au dessus du texte cité
  - ràf : un exemple de chaque

Mail : du danger de la citation

- Citer l'intégralité du courrier auquel on répond
- Au fil des échanges, ajouter des destinataires
- => danger
- Exemple : cf ràf
- Bonne pratique :
  - Choisir sa secte (pas important)
  - Relire la partie citée
  - En supprimer les parties non pertinentes du courrier cité

mail : stockage, diffusion

- avoir accès au serveur où sont vos boîtes aux lettres permet de lire vos mails
- toute machine où passent vos mails est un point où ils peuvent être espionnés
- gmail : google analyse le contenu de vos mails pour vous profiler
- conseil : soyez paranoïaques
  - des solutions techniques et des adresses différentes selon les activités (prof. perso, syndicales, …)
  - utilisez le chiffrement des courriers

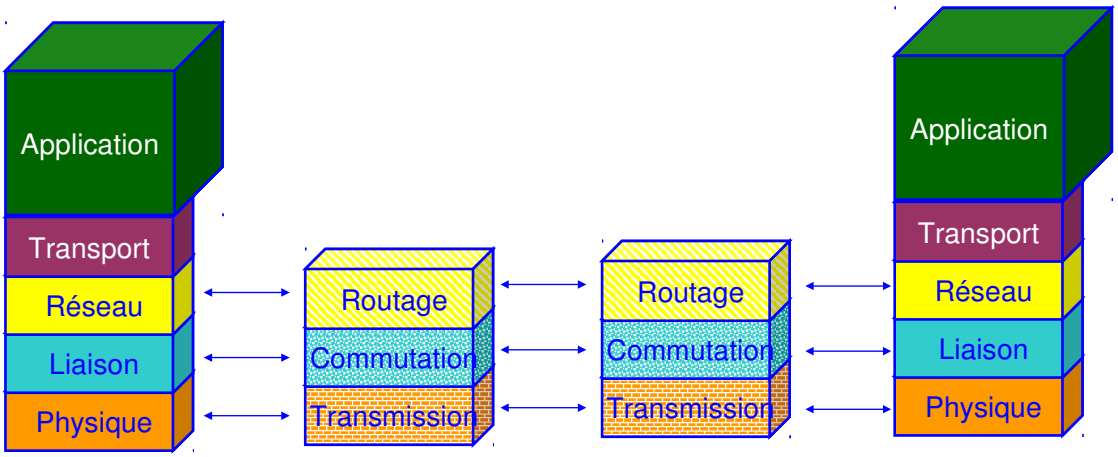
Présentation:

- Pascal PETIT
- sécurité informatique
- pascal.petit@shayol.org

Plan

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

architecture en couche



3

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

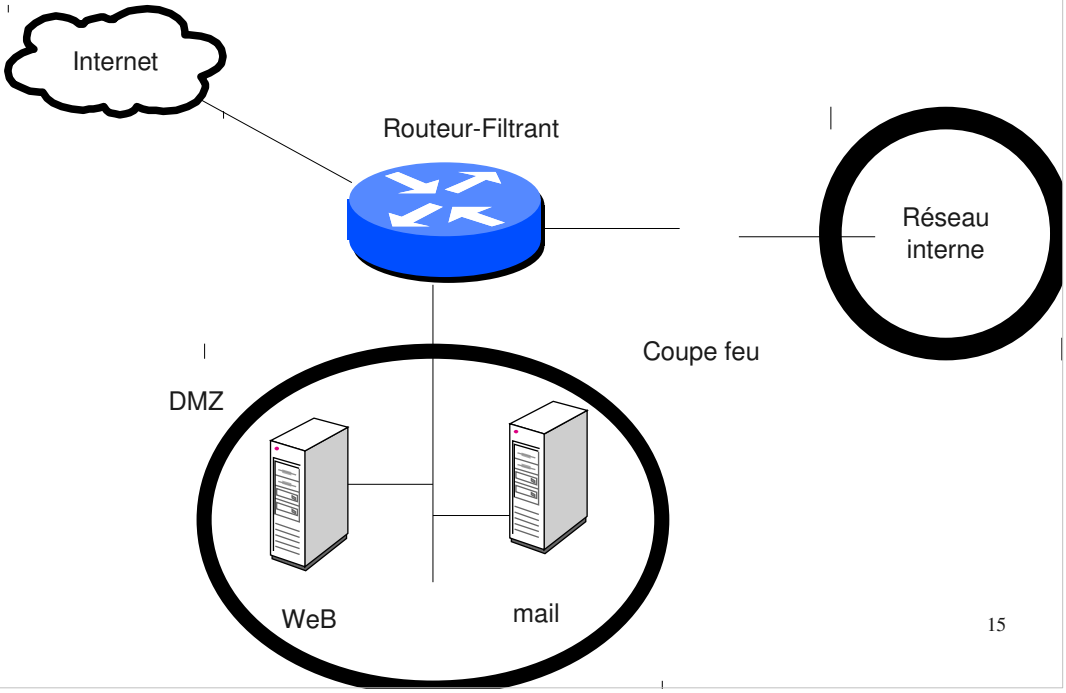
coupe feu/routeur filtrant

- 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:



15

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

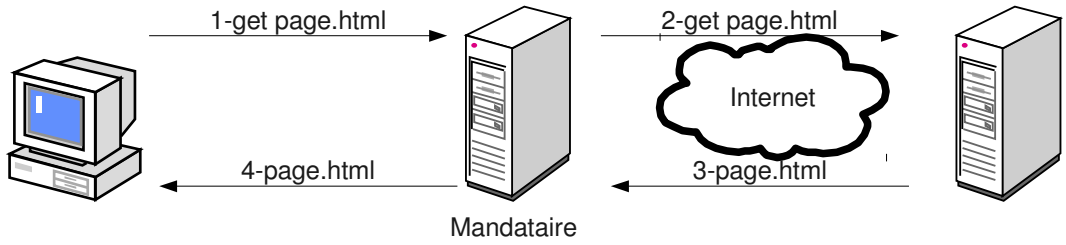
défense en profondeur

- 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)

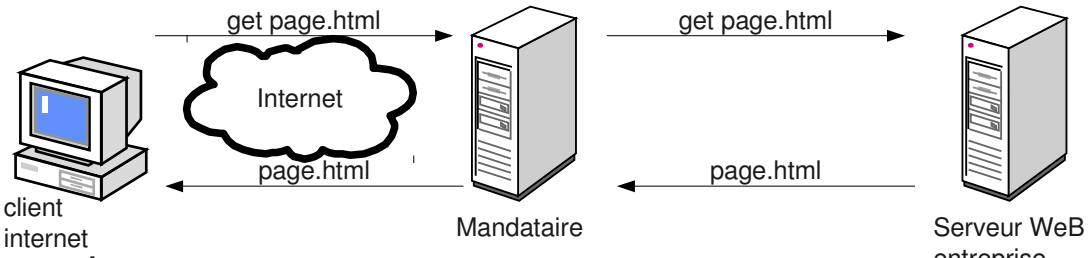


- le mandataire peut effectuer
  - un travail de nettoyage sur les données reçues (antivirus, ...)
  - un filtrage ou un nettoyage sur les données transmises
  - une journalisation des requètes
  - une demande d'authentification des utilisateurs

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

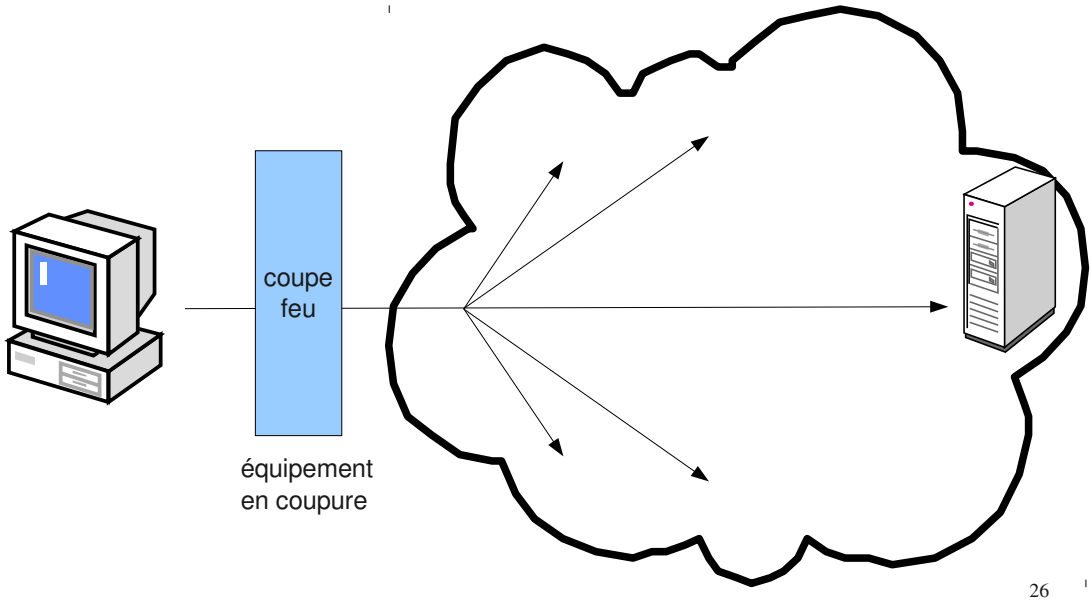


- le reverse proxy :
  - peut protéger un OS un peu faible des accès directs
  - peut effectuer un filtrage ou un nettoyage sur les requêtes transmises pour palier la faiblesse d'un logiciel serveur WeB
  - peut demander une authentification

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

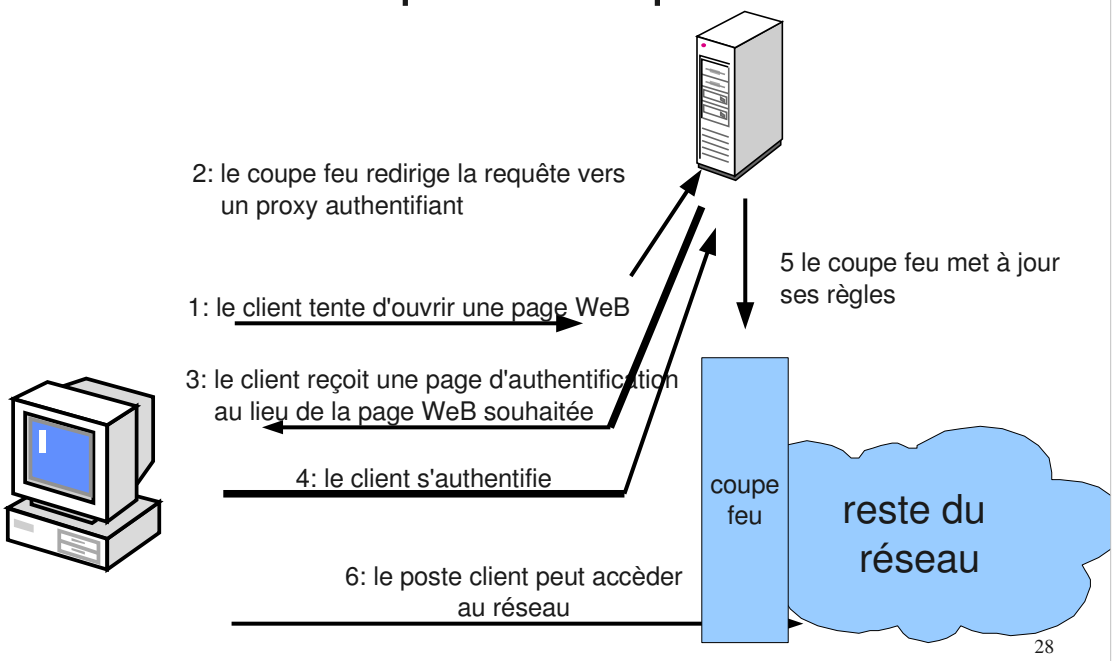


26

•NAC: Contrôle via un équipement en coupure

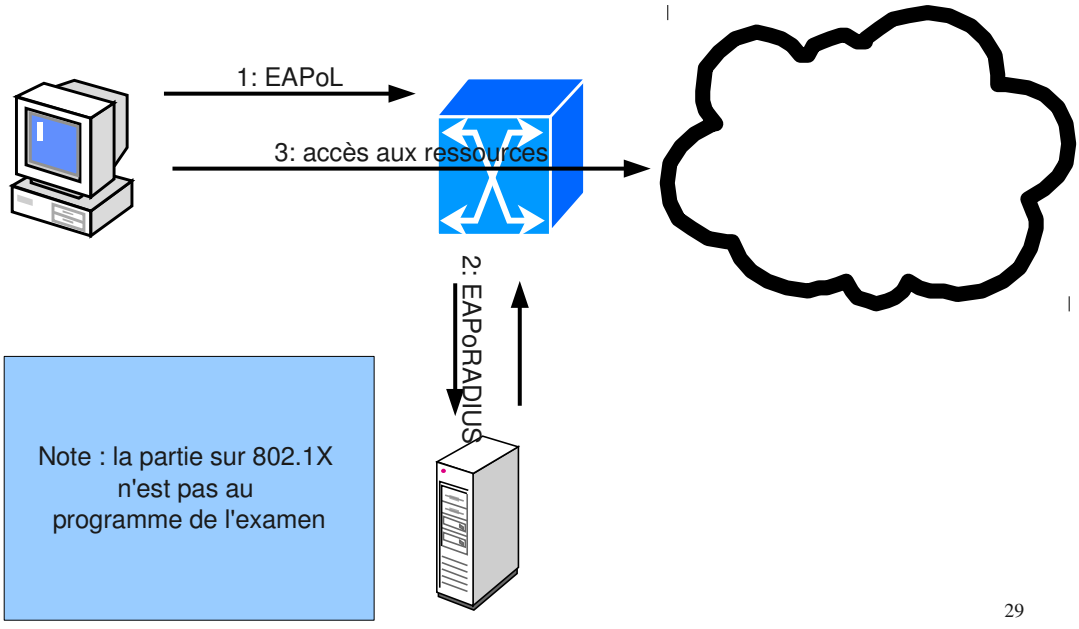
- l'accès réseau n'est autorisé qu'après authentification sur un équipement en coupure
  - exemple : par une redirection automatique : proxy transparent et portail captif
  - cas du WiFi etudiant de l'université d'Evry
- succès de l'authentification => chargement de règles de filtrage autorisant certains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

•NAC: portail captif WeB



28

•NAC: 802.1X, contrôle au niveau 2



Note : la partie sur 802.1X n'est pas au programme de l'examen

Server radius

29

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

Note : la partie sur 802.1X n'est pas au programme de l'examen

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

Chiffrement: robustesse

- cryptanalyse: analyser une information chiffrée pour la déchiffrer(dont méthodes en force brute, ...)
- algo public
- la sécurité repose sur :
  - la non divulgation de la clef
  - la robustesse de l'algorithme
  - la taille de la clef (gare aux comparaisons entre algo différents)
  - l'utilisation de clefs différentes pour chiffrer des messages différents limite la quantité d'information à la disposition de l'attaquant

chiffrement: taille des clefs

- attaques en force brute: tenter une partie importante de l'espace des clefs
- temps dépend du nombre de clefs possibles et donc de la taille de la clef:
  - 10 bits : 1024 clefs possibles
  - 56 bits: 2^56=7 10^16
  - dépendance exponentielle en fonction de la taille de la clef: 1 bit de plus = 2 fois plus de temps
- la taille critique dépend de l'algo (et de sa vitesse, de ses faiblesses, ...)

algorithme de chiffrement

- chiffrement symétrique/asymétrique
  - symétrique:
    - les algo classiques sont rapides
    - **la même clef sert au chiffrement et au déchiffrement**
    - souvent utilisé via une clef de session
      - clef de session: transmise via algo asymétrique (on parle d'enveloppe digitale)
      - session: chiffrée par un algo symétrique et la clef transmise

algorithme de chiffrement

- chiffrement symétrique/asymétrique
  - asymétrique:
    - les algo classiques sont lents
    - **couple de clef publique/clef privée**
      - clef publique: peut être connue de tous
      - clef privée: tenue cachées
      - ce qui est chiffré avec l'une ne peut être déchiffré qu'avec l'autre

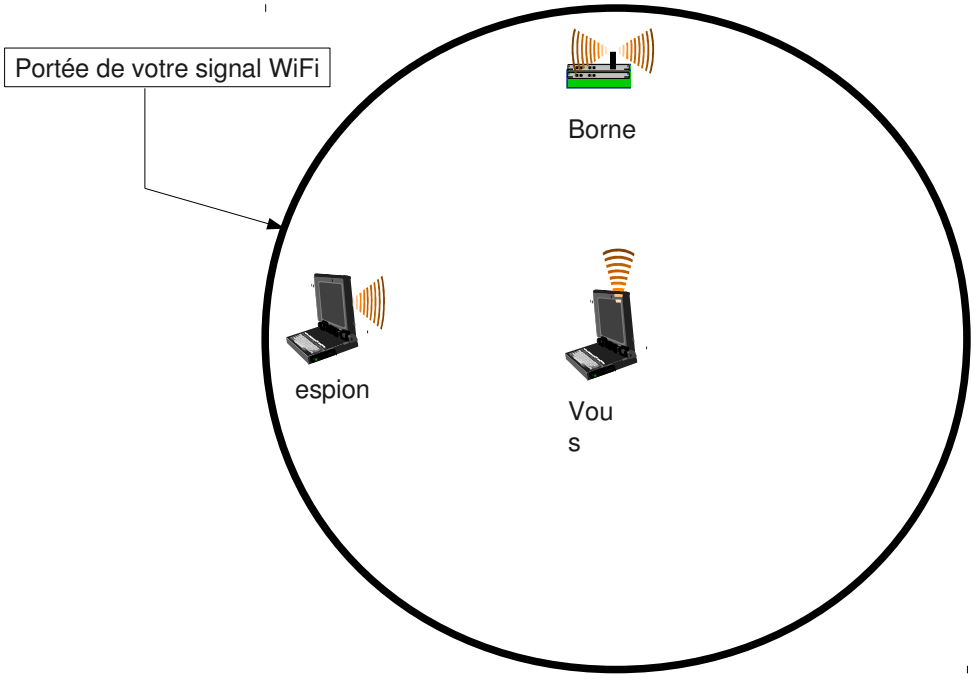
services offerts par le chiffrement:

- confidentialité
- intégrité
- signature numérique
- authentification
- Single Sing On
- non répudiation

WiFi : enjeux

- Utilisation du réseau par un utilisateur non légitime
  - Pour rebond
  - Pour réseau local
  - Pour attaque des autres postes WiFi
    - Solution : interdire les connexions entre postes WiFi (réglage point d'accès)
- Espionnage des données échangées :
  - Sites consultés
  - Mot de passe
  - ...

WiFi : enjeu



WiFi : sécurité

- Ouvert : pas de chiffrement. En général associé à un portail d'authentification
- WEP : chiffrement MAIS cassable en quelques minutes par un non informaticien
- WPA1/WPA2 personnal : chiffrement solide (si clef solide) MAIS clef commune
- WPA2 entreprise + 802.1X + méthode génératrice de clef : chiffrement solide, clef unique par poste
- Exemples : google cars.

Solutions :

- utiliser une méthode solide (WPA2)
- chiffrer ses communications
  - https
  - VPN
- Utiliser https partout où c'est possible
  - Trafic chiffré entre votre navigateur et le serveur
  - Authentification du serveur
- Extension firefox : httpseverywhere (https://www.eff.org/https-everywhere)

Certificats, https

Carte d'identité

Pascal PETIT

Certificats, https

Certificats :

- Un certificat :
  - Identité,
  - clefs publique
  - Certifiés par une autorité de certification
- Permet l'authentification d'un site
  - Le site possède la clef privée associée
  - Le site indiqué par le certificat est bien celui auquel on se connecte
- Permet la mise en place d'un tunnel chiffré : protège contre l'espionnage des communications

certificats et hameçonnage

- Du phishing pour identifier les opposants à Bachar El-Assad
  - faute site youtube annonçant une fausse mise à jour de flash
    - => installation d'un logiciel espion
  - faux site facebook ou youtube
    - récupérer login et mot de passe (y compris des personnes qui mettent des commentaires)
- source : Numerama, 30 mars 2012 :
  http://www.numerama.com/magazine/22197-du-phishing-pour-identifier-les-opposants-a-bachar-el-assad.html

limite de https

- vigilance des utilisateurs (cf exemple syrien)
- fiabilité des autorités de certification
  - que penser d'une AC liée à un pays
  - impact possible
    - créer un faux certificats reconnu comme valide par le navigateur
    - l’hameçonnage sans détection possible
- solutions :
  - aucune pour l'instant

Dropbox

- avril 2011 : changement des conditions d'utilisation de dropbox
- avant, dropbox vantait la qualité de son chiffrement AES 256bits
- détection de doublon
  - pour gagner de la place
  - suppose que dropbox puisse déchiffrer les fichiers chiffrés
- BIBLIO :
  - http://www.cnetfrance.fr/news/dropbox-induisait-en-erreur-sur-la-confidentialite-des-donnees-et-le-cryptage-39760824.htm

Dropbox : solution

- chiffrer les données soit même
- via true crypt :
  - pénible car suppose le transfert de tout le contener à chaque modification
  - soit avec des solutions fichiers par fichiers à la encfs
    - pcimpact : http://www.pcinpact.com/dossier/chiffrement-cloud-encfs-boxcryptor-dropbox/209-1.htm
    - http://korben.info/dropbox-chiffrer-crypter-securiser.html
    - http://korben.info/boxcryptor-dropbox-crypte.html

Protection des disques durs

- Mot de passe du bios
  - Peut être supprimé par un voleur
  - Ne l'utiliser que pour empêcher l'utilisation du portable en votre absence
- Mot de passe du disque dur
  - Le mot de passe est stocké dans l'électronique du disque
  - Beaucoup plus résistant
  - Plusieurs niveaux de sécurité (récupérable par le constructeur ou non)
- Chiffrement de partitions ou de disques

Truecrypt : références

- Le FBI se serait cassé les dents dessus : http://sid.rstack.org/blog/index.php/400-pbkdf2-a-l-epreuve-du-fbi
- Rapport de certification de la version 6.0a : http://esec.fr.sogeti.com/FR/documents/presse/tc_dcssi.pdf
- Site officiel : http://www.truecrypt.org/

True crypt fonctionnalités

- Peut chiffrer un disque virtuel dans un fichier
- Peut chiffrer une partition (y compris la partition où est installé windows)
- Le chiffrement est transparent et automatique
- Permet de la stéganographie (méfiance : des travaux récents permettent de détecter les conteneurs truecrypt)
- Fournit des mécanismes de déni plausible en cas de fourniture forcée du mot de passe

encfs/box cryptor

- outils de chiffrement de dossier
- chiffre fichiers par fichiers
- plus efficace en cas de synchronisation entre dossiers sauvegardés
- les outils :
  - encfs/cryptkeeper : sous linux
  - boxcryptor : sous windows

Mail & Co : bonnes pratiques

- Mail : gare à la diffusion involontaire d'information
- Informations contenues dans les documents pdf, m$-office & Co

Mail : du danger de la citation

- Guerre de religions avec 2 sectes :
  - Le dinosaures : Ceux qui répondent au dessous du texte cité
  - Ceux qui répondent au dessus du texte cité
  - ràf : un exemple de chaque

Mail : du danger de la citation

- Citer l'intégralité du courrier auquel on répond
- Au fil des échanges, ajouter des destinataires
- => danger
- Exemple : cf ràf
- Bonne pratique :
  - Choisir sa secte (pas important)
  - Relire la partie citée
  - En supprimer les parties non pertinentes du courrier cité

mail : stockage, diffusion

- avoir accès au serveur où sont vos boîtes aux lettres permet de lire vos mails
- toute machine où passent vos mails est un point où ils peuvent être espionnés
- gmail : google analyse le contenu de vos mails pour vous profiler
- conseil : soyez paranoïaques
  - des solutions techniques et des adresses différentes selon les activités (prof. perso, syndicales, …)
  - utilisez le chiffrement des courriers