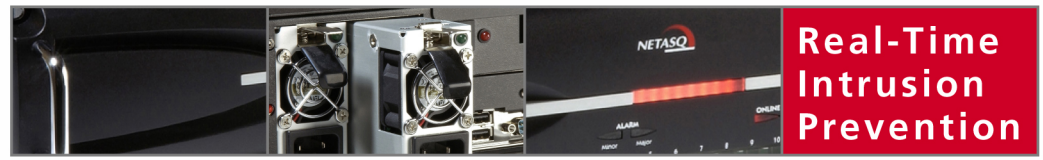
ASQ

Version 3.0

NETASQ

Secure Internet Connectivity



Multiples Méthodes

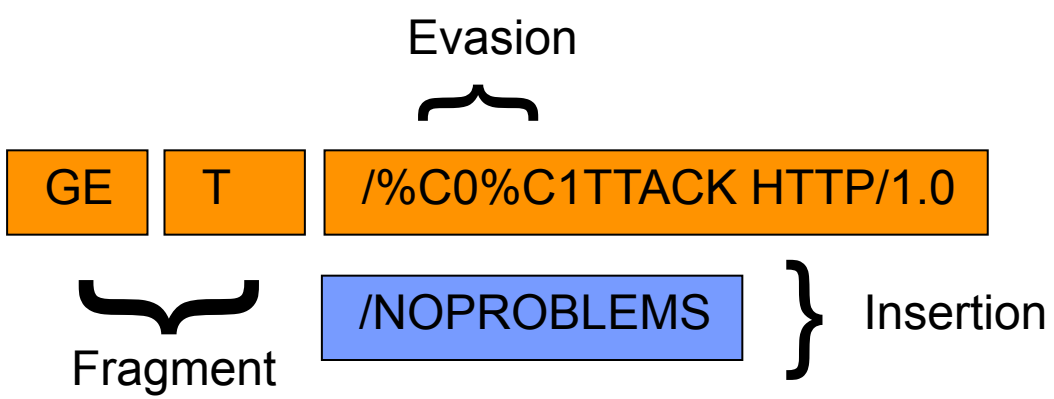
- [x] Analyse protocolaire
- [ ] Signatures contextuelles
- [ ] Statistiques et heuristiques

Analyse protocolaire

- Respect des RFC
  - Malformation (recouvrement de fragment)
  - Utilisation hors contexte (réponse sans demande)
- Protection contre l'évasion par la normalisation
  - Fragment
  - TCP
  - URL
- "Buffer overflow"
- ...

Cas d'étude

- Requête HTTP qui comporte 3 attaques protocolaires
  - GET /ATTACK HTTP/1.0
    - Fragment
    - TCP Insertion
    - Evasion UTF-8 (A -> %C0%C1)

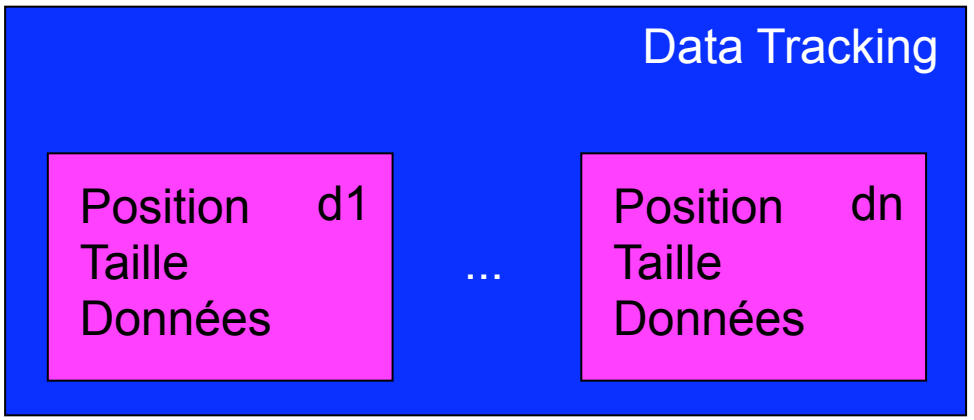


Etapes de l’analyse

- Analyse IP
  - Fragment
- Analyse TCP
  - Reconstruction du flux
  - Plugin
    - Analyse HTTP

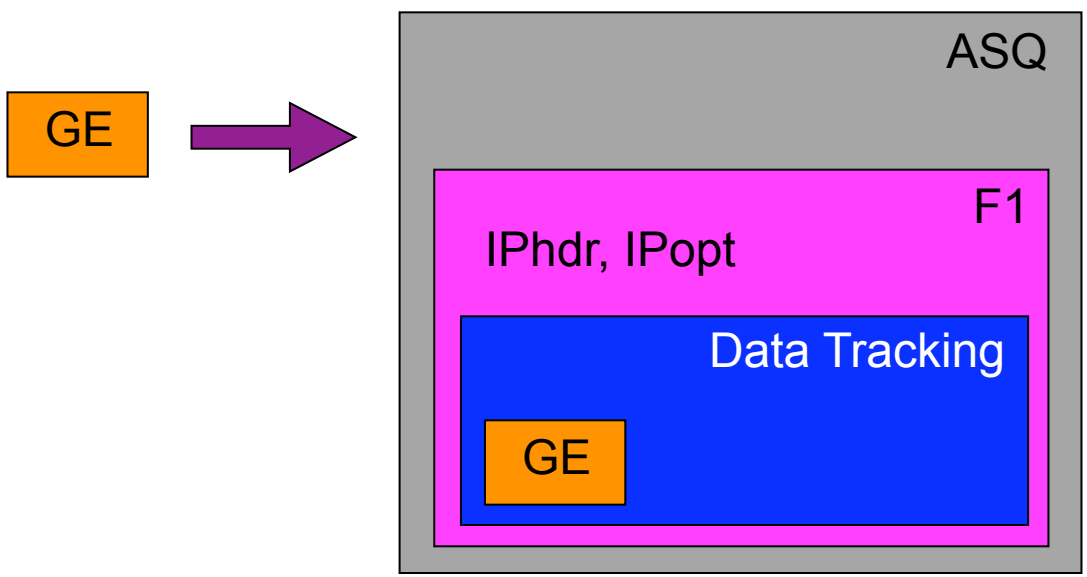
Suivi de données

- Module générique
  - Vérifier la cohérence
    - Bornes (Offset pour les fragments, Séquence pour TCP)
    - Données (Comparaison)
  - Stockage des données (Virtualisation de flux)



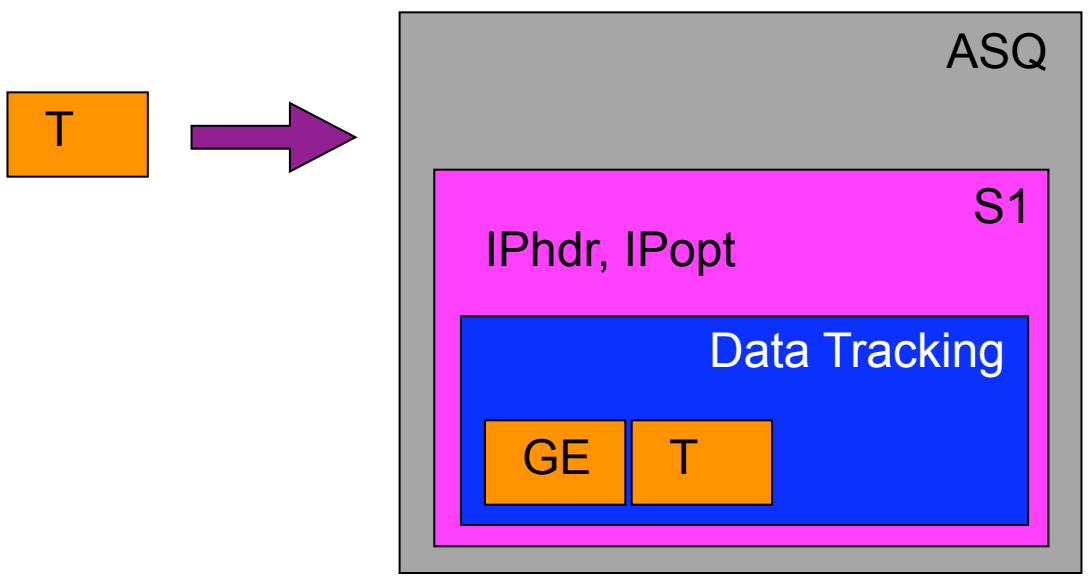
Fragment

- Premier fragment
  - Création de l'état
  - Mémorisation de l'entête IP et des options
  - Création d'une unité de suivi de données



Fragment

- Dernier fragment
  - Recomposition du paquet
  - Analyse TCP

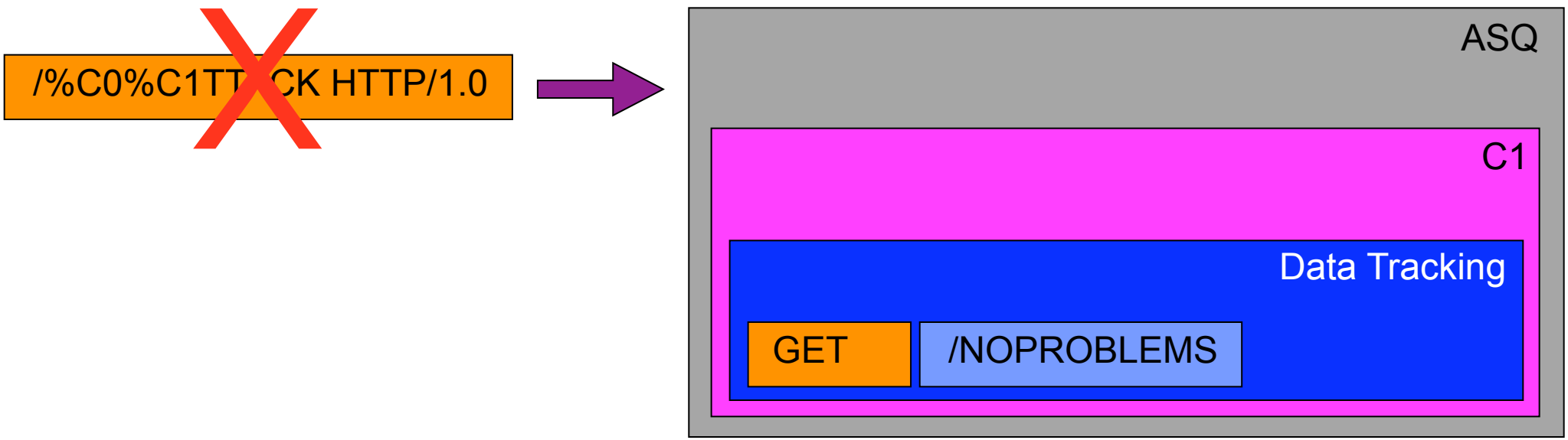


Fragment

Transforme les fragments en paquets virtuels

Reconstruction du flux TCP

- Utilise un module de suivi de données par connexion
  - Vérification des séquences
  - Normalisation des données
  - Abstraction du flux pour les plugins

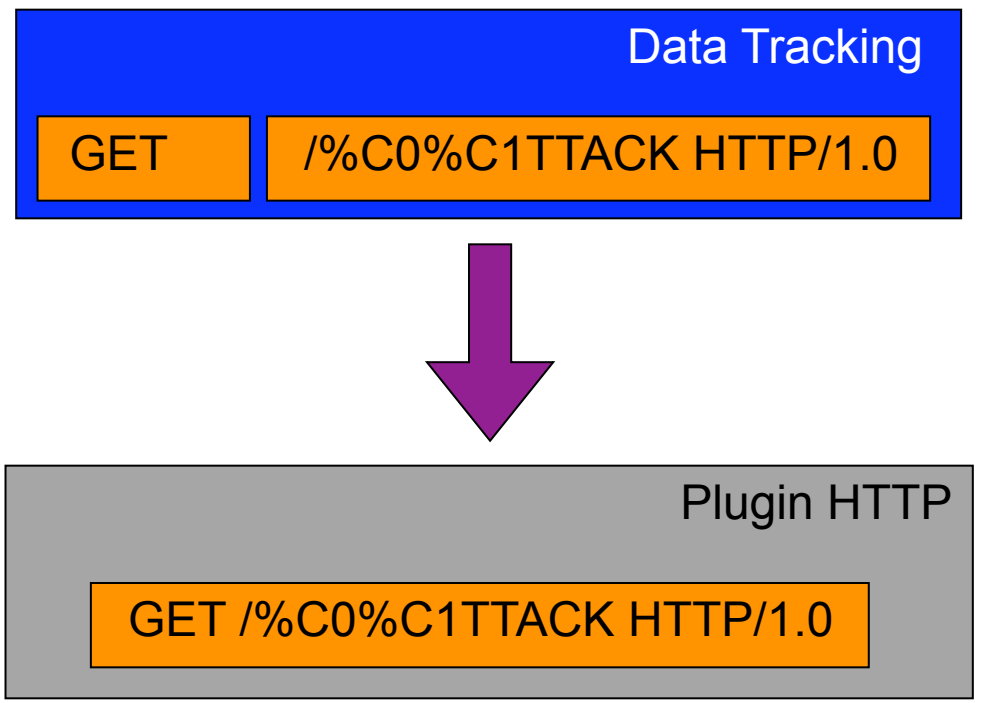


Reconstruction du flux TCP

Normalise le flux de données TCP

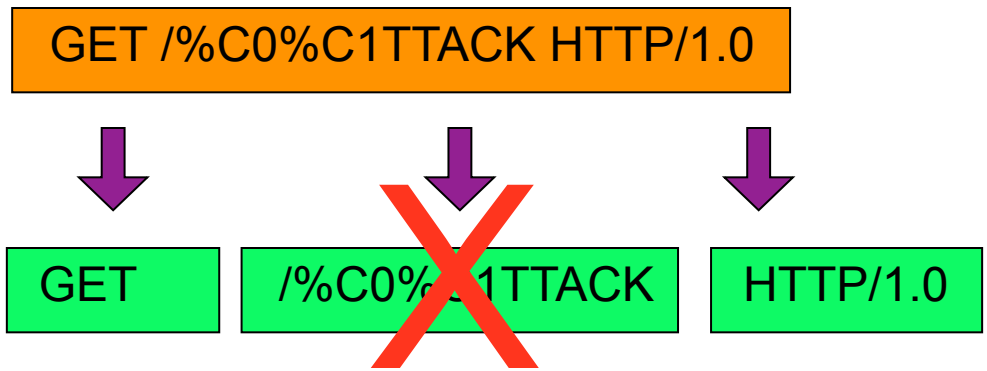
Plugin

- Utilise le module de suivi de données
  - Réalise une analyse ligne par ligne



Plugin

- Analyse de la requête
  - Protocole (HTTP/1.0)
  - Opération (GET)
  - Décodage de l'URL ("%", "%u", ...)
  - Vérification de l'URL (UTF-8, ...)



Cas pratique (Vulnérabilité serveur IPswitch)

- Faille publié le 30 novembre 2004
  - Permet a un attaquant de prendre le contrôle du serveur
  - 4 commandes différentes sont concernées
- IPswitch publie un correctif le 20 décembre
  - Client sans solution ni protection pendant 20 jours

Cas pratique (Vulnérabilité serveur IPswitch)

- L'analyse protocolaire permet le blocage depuis plus d'un an
  - Version 5.0 de Juillet 2003

ftp	Bloquer	Ne rien faire.	✔	Mineure	Attaque FTP bounce possible
	Bloquer	Ne rien faire.	✔	Majeure	Tentative d'insertion de commande FTP PASV
	Bloquer	Ne rien faire.	✔	Majeure	Commande FTP inconnue
	Bloquer	Ne rien faire.	✔	Majeure	Débordement en FTP sur les commandes USER
	Bloquer	Ne rien faire.	✔	Majeure	Débordement en FTP sur une commande
	Bloquer	Ne rien faire.	✔	Majeure	Attaque en force brute sur mot de passe FTP
	Bloquer	Ne rien faire.	✔	Majeure	Exécution de commande via SITE EXEC
	Bloquer	Ne rien faire.	✔	Majeure	FTP PASV DoS
	Bloquer	Ne rien faire.	✔	Majeure	Protocole FTP invalide

Cas pratique (Vulnérabilité serveur IPswitch)

- Quelle réaction sans analyse protocolaire ?
  - Création d'une signature par commande (4 en tout)
  - 9 jours sans protection (solution à base de signatures)

Cas pratique (Autres)

- Vulnérabilité des applications PHP (Juillet 2004)
- Vulnérabilité des serveurs IIS (Juillet 2004)
- Vulnérabilité des serveurs Apache (Octobre 2004)

Questions

Multiples Méthodes

- ☐ Analyse protocolaire
- ☑ Signatures contextuelles
- ☐ Statistiques et heuristiques

Pourquoi ?

- Complémentaires
  - Réagir rapidement
  - Attaque valide au niveau du protocole
- Faux positifs
  - Utilise l'analyse protocolaire
- Performances
  - Algorithme parallèle
  - Eviter l'évaluation hors contexte
- Mise à jour régulière
  - Téléchargement automatique "Active Update"

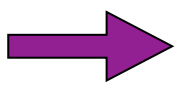
Comment

- Algorithme simple trop couteux
  - Evaluer 100 signatures sur 100 octets = 10000 évaluations
- Compile sous forme complexe les signatures
  - Permet l'évaluation en une seule passe
  - 100 signatures sur 100 octets presque équivalent a une signature sur 100 octets
- Algorithme utilisé dans le filtrage URL
  - Evaluation de plusieurs millions URLs
  - Temps d'évaluation inférieur à la milliseconde sur un F200

Comment

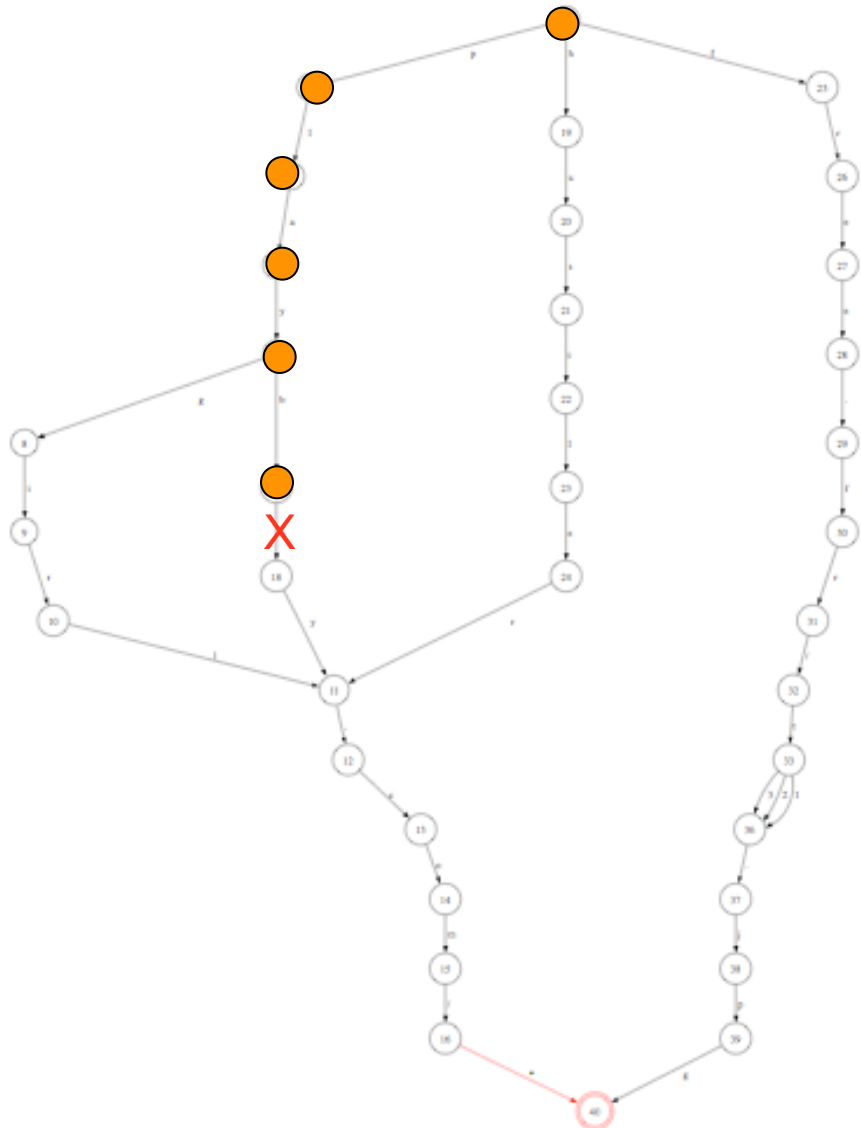
- Construction du graphe

playboy.com/|*
playgirl.com/|*
hustler.com/|*
free.fr/t1.jpg
free.fr/t2.jpg
free.fr/t3.jpg

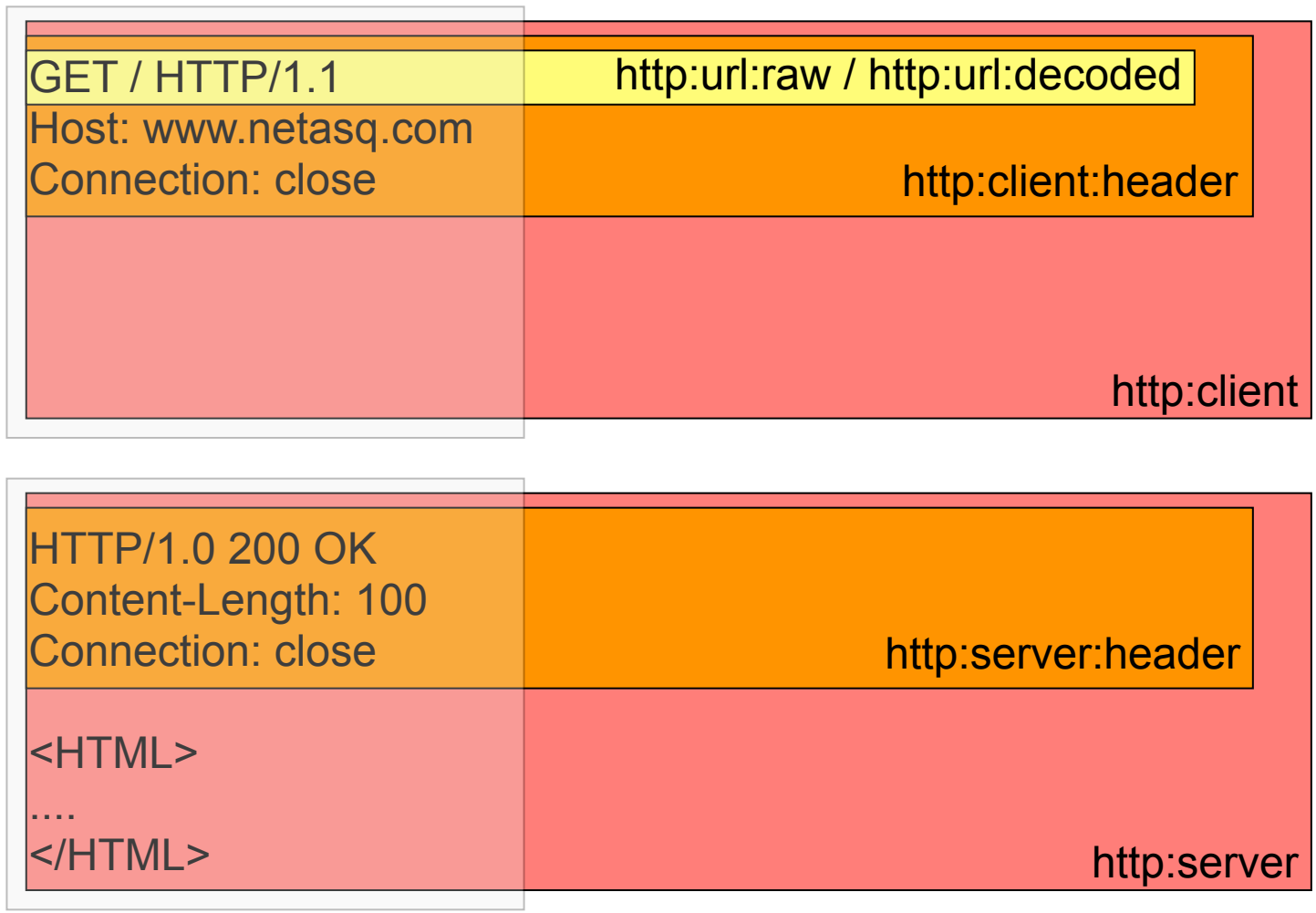


Comment

- Evaluation



Ou ? (Contexte protocolaire HTTP)



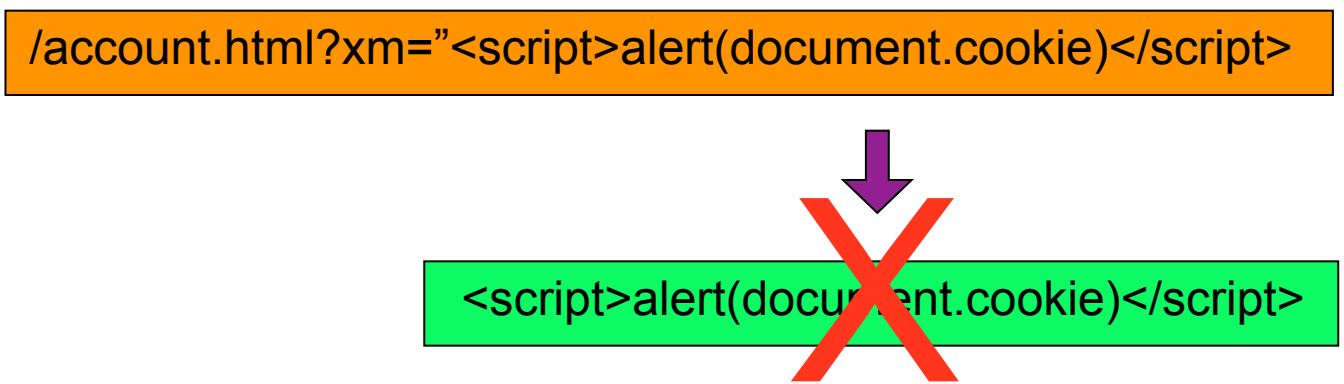
Etapes de l’analyse

- Analyse IP
  - Fragment
- Analyse TCP
  - Reconstruction du flux
  - Plugin
    - Analyse HTTP

IDENTIQUE

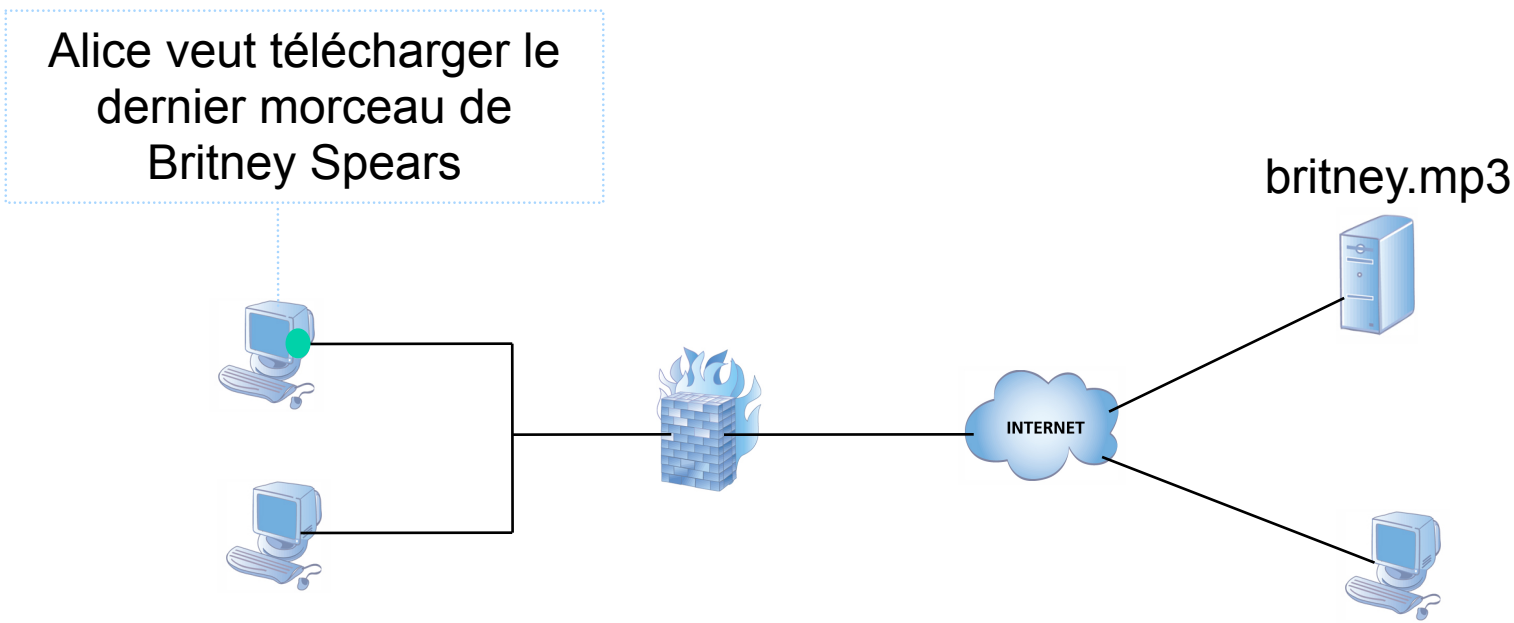
Signature

- Evaluation contexte “http:url:decoded”
  - Signature “*<script>*</script>*”



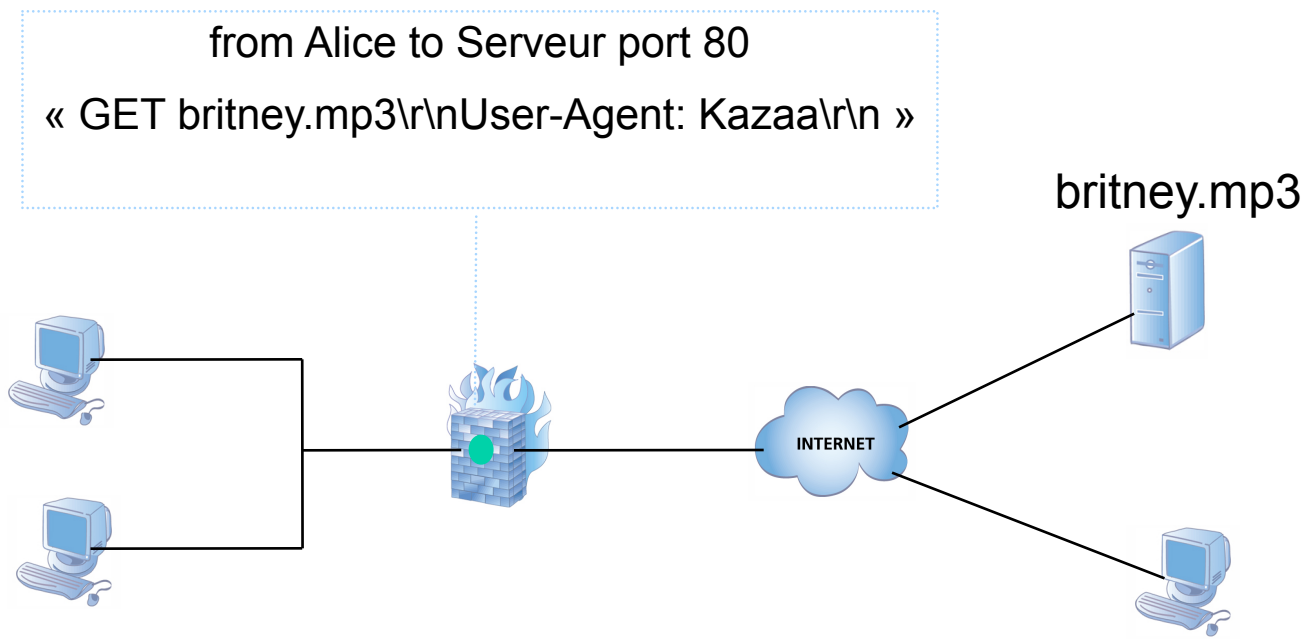
Cas pratique (Kazaa)

- Signature classique



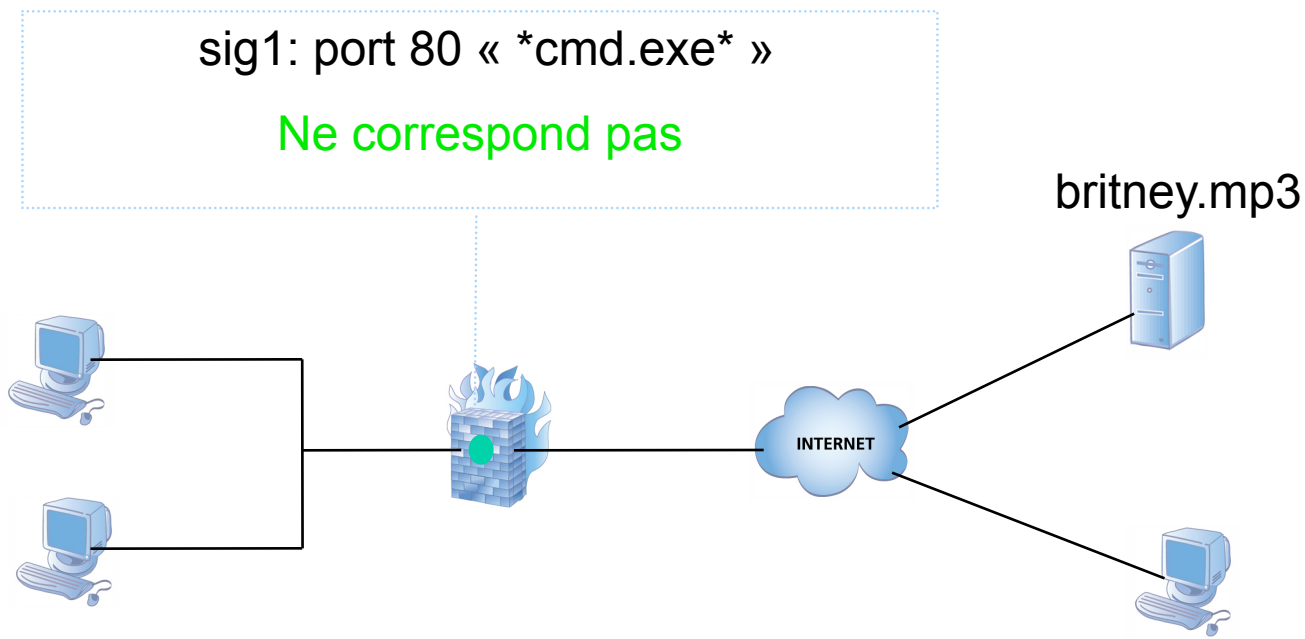
Cas pratique (Kazaa)

- Signature classique



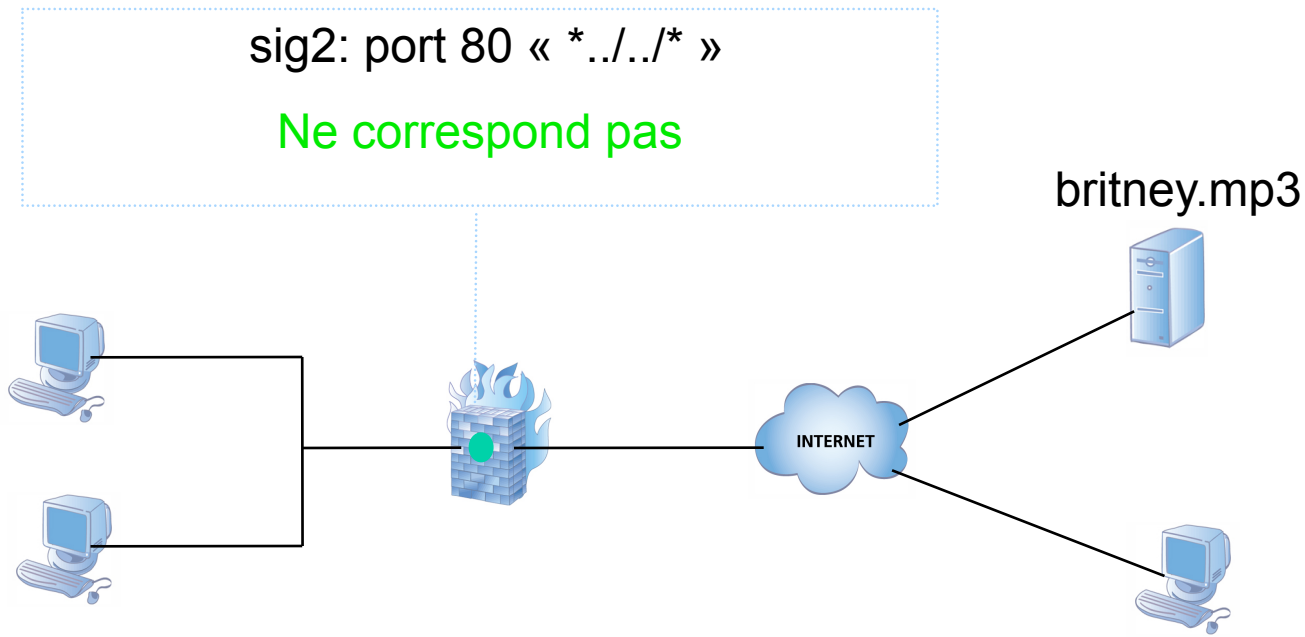
Cas pratique (Kazaa)

- Signature classique



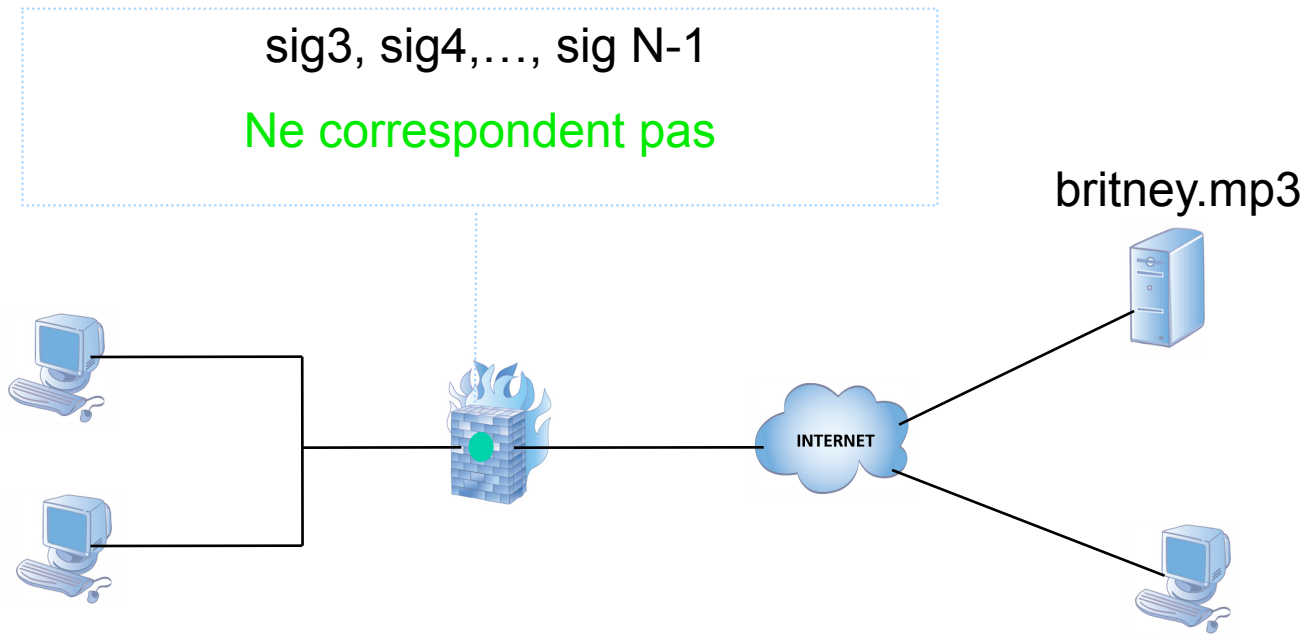
Cas pratique (Kazaa)

- Signature classique



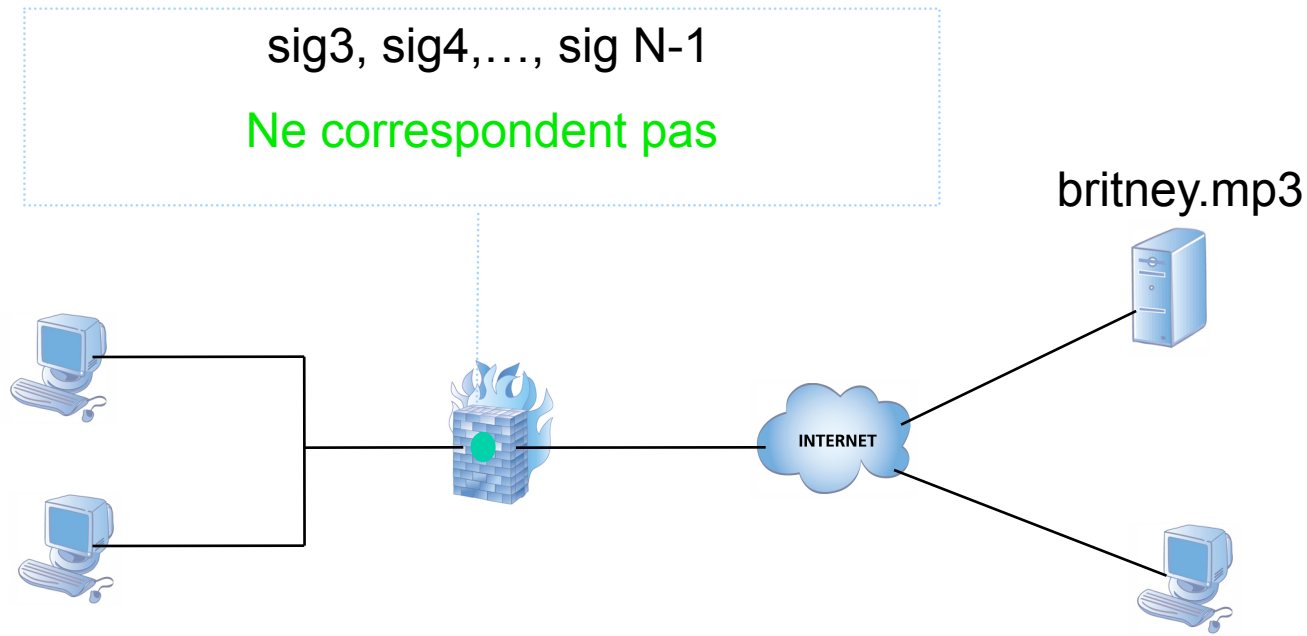
Cas pratique (Kazaa)

- Signature classique



Cas pratique (Kazaa)

- Signature classique

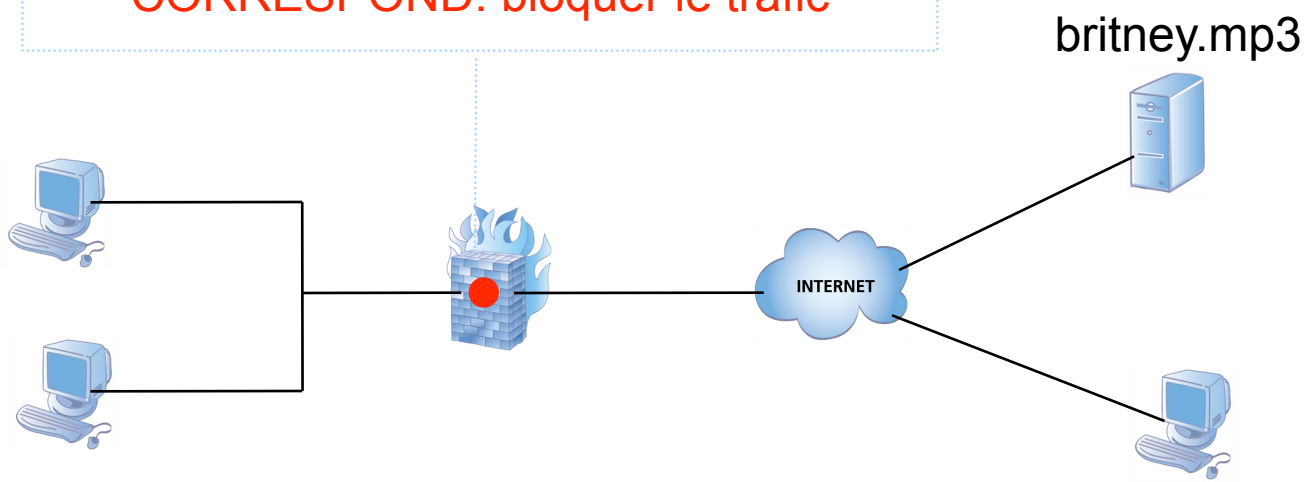


Cas pratique (Kazaa)

- Signature classique

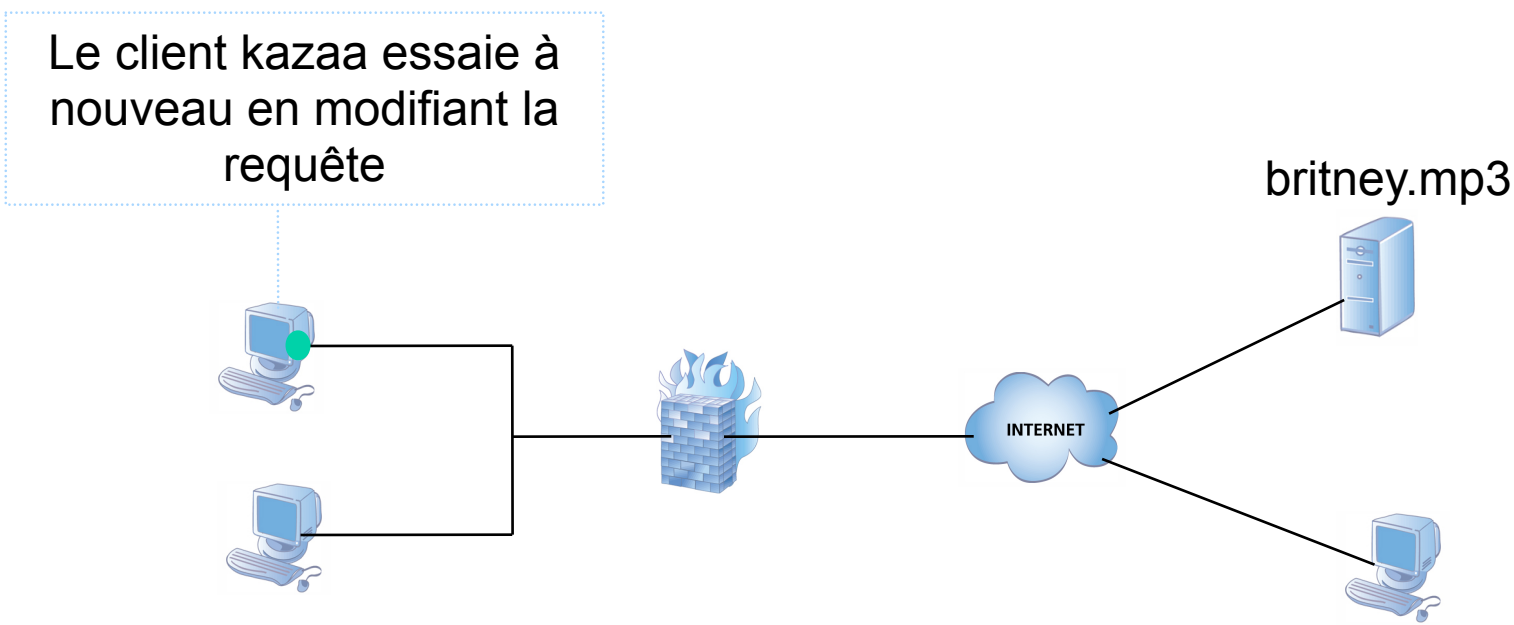
sig N: port 80 « *User-Agent: Kazaa* »

CORRESPOND: bloquer le trafic



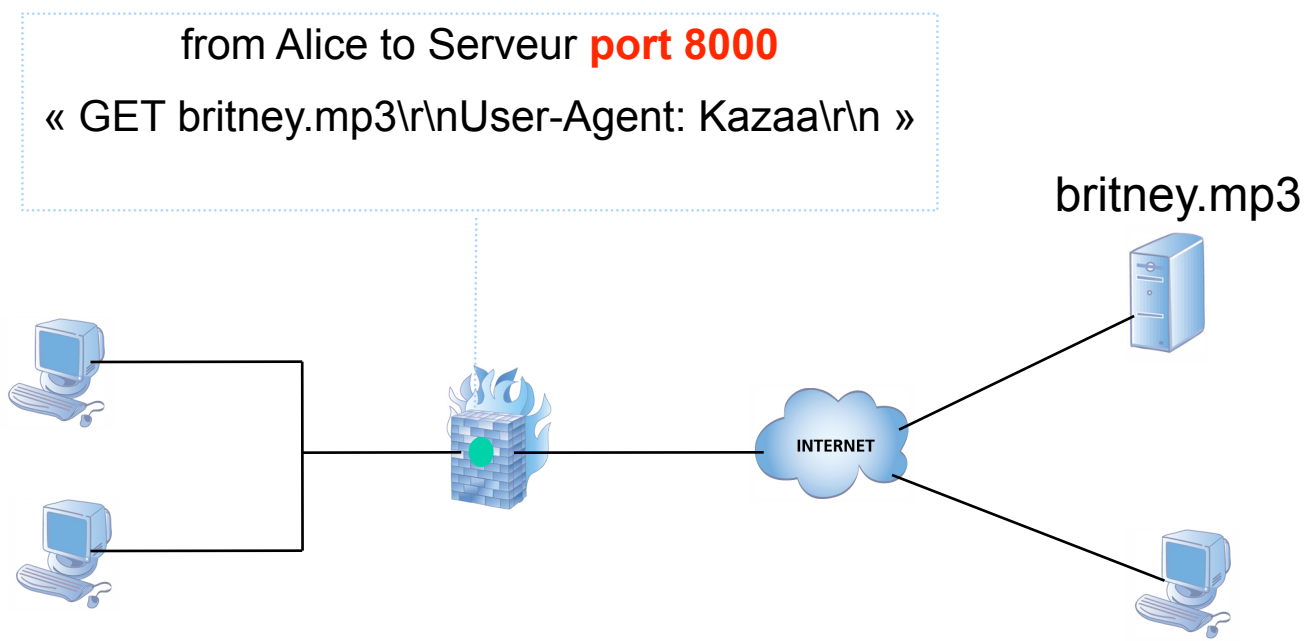
Cas pratique (Kazaa)

- Signature classique



Cas pratique (Kazaa)

- Signature classique

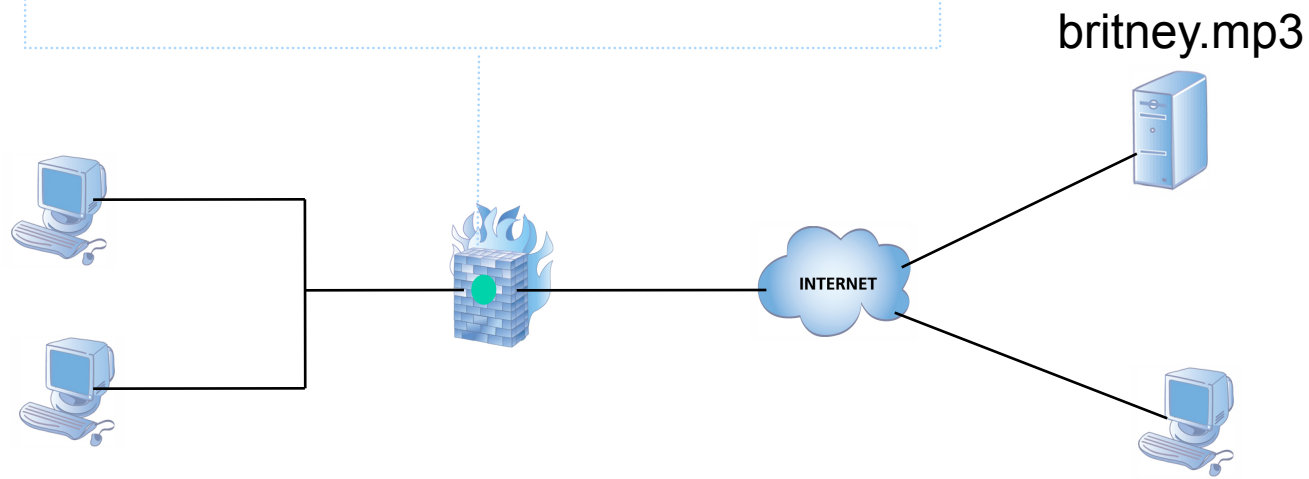


Cas pratique (Kazaa)

- Signature classique

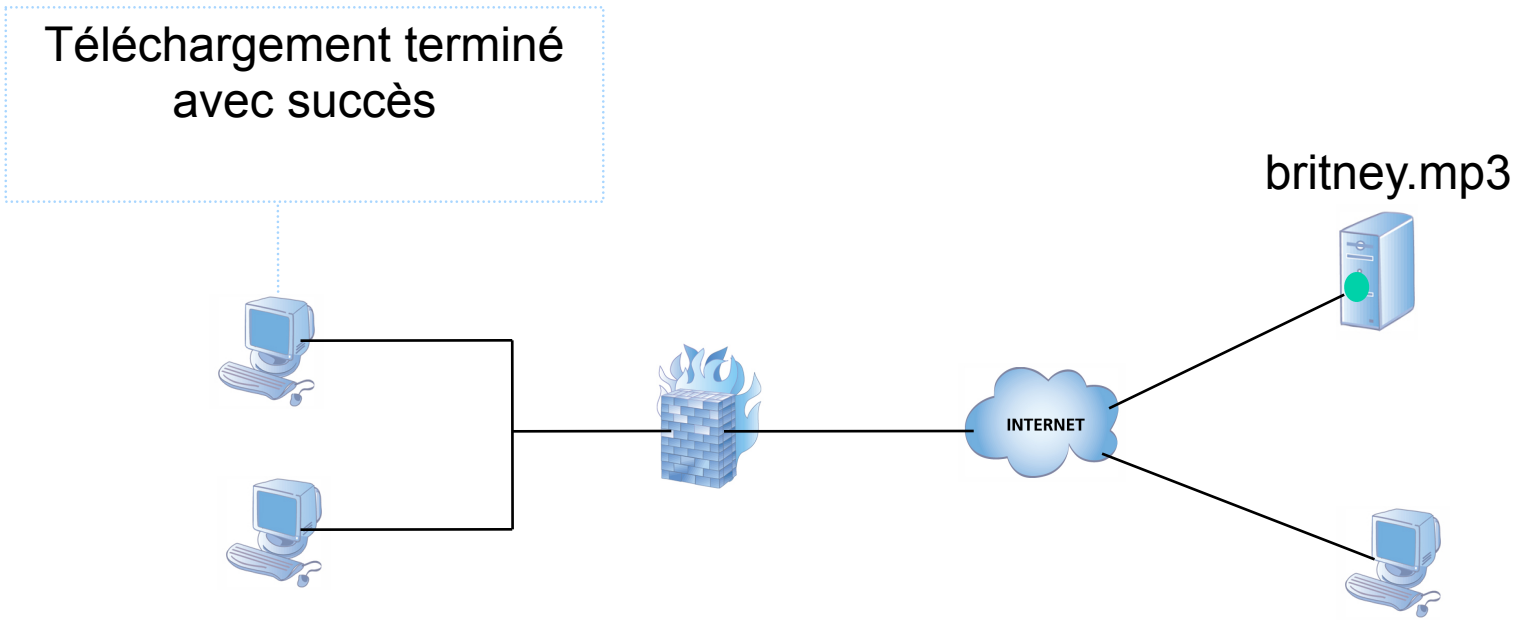
sigN: port 80 « *User-Agent: Kazaa* »

Ne correspond pas (port 8000 ≠ 80)



Cas pratique (Kazaa)

- Signature classique



Cas pratique (Kazaa)

- Signature classique

Une signature plus générale est nécessaire

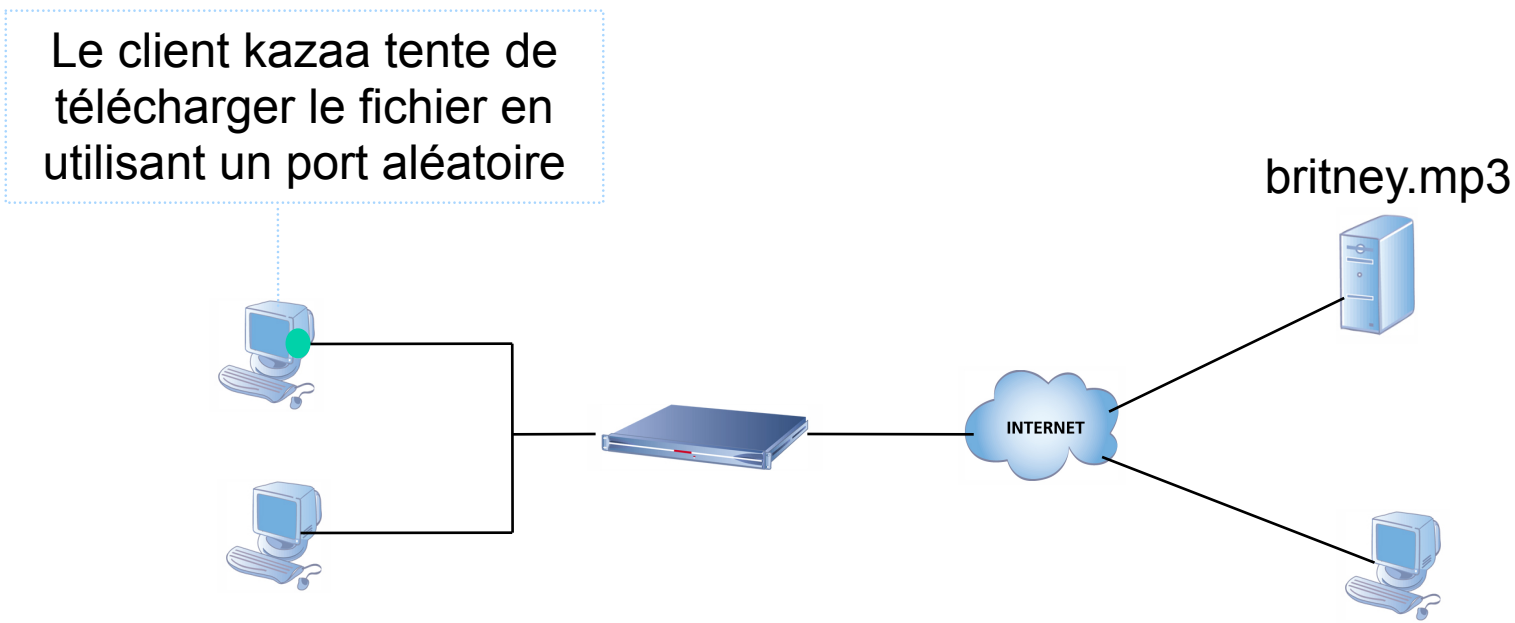
- port any « *User-Agent: Kazaa* »
- cette nouvelle signature déclenchera une fausse alerte « Kazaa » lors de l'envoi de cette présentation, par FTP ou par mail

Exemple 2: port 80 « *cmd.exe* »

- déclenchera une fausse alerte lors d'une recherche de cmd.exe dans un moteur de recherche (Google par exemple)

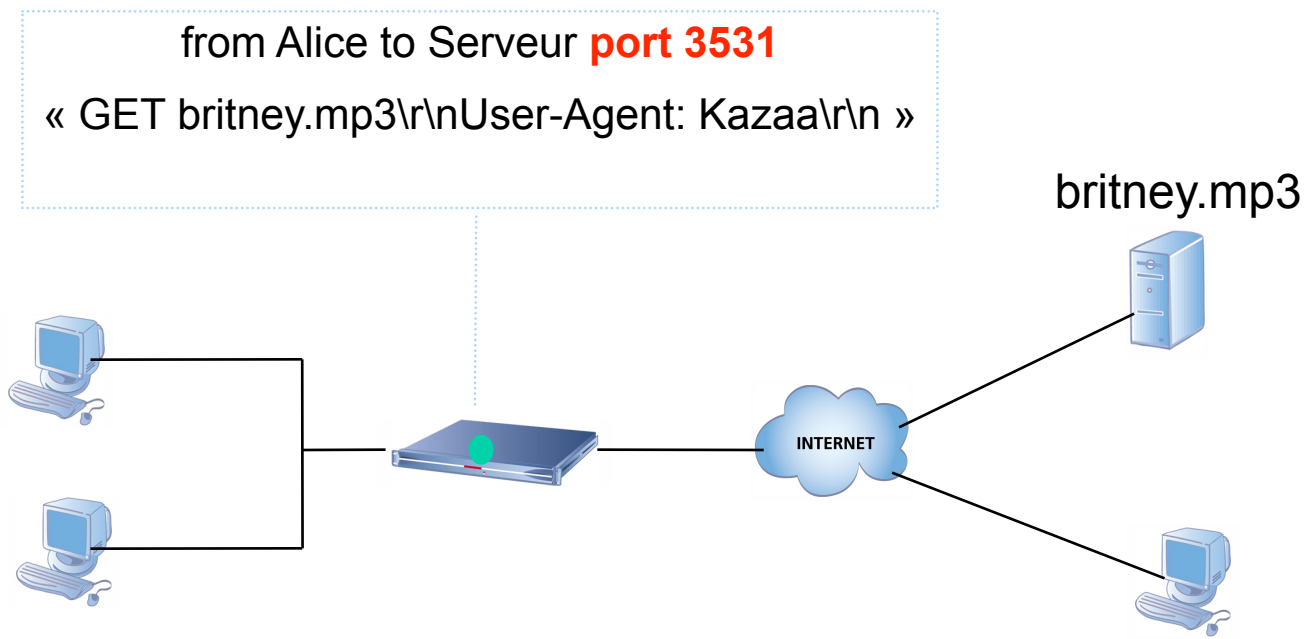
Cas pratique (Kazaa)

- Collaboration des méthodes ASQ



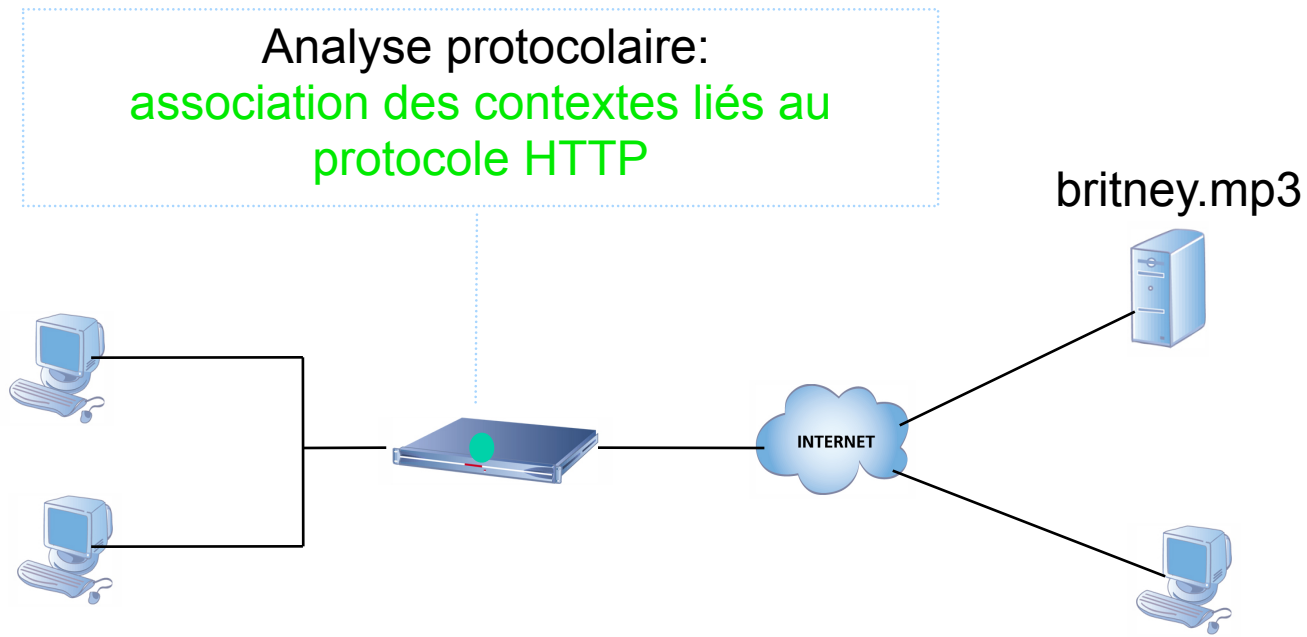
Cas pratique (Kazaa)

- Collaboration des méthodes ASQ



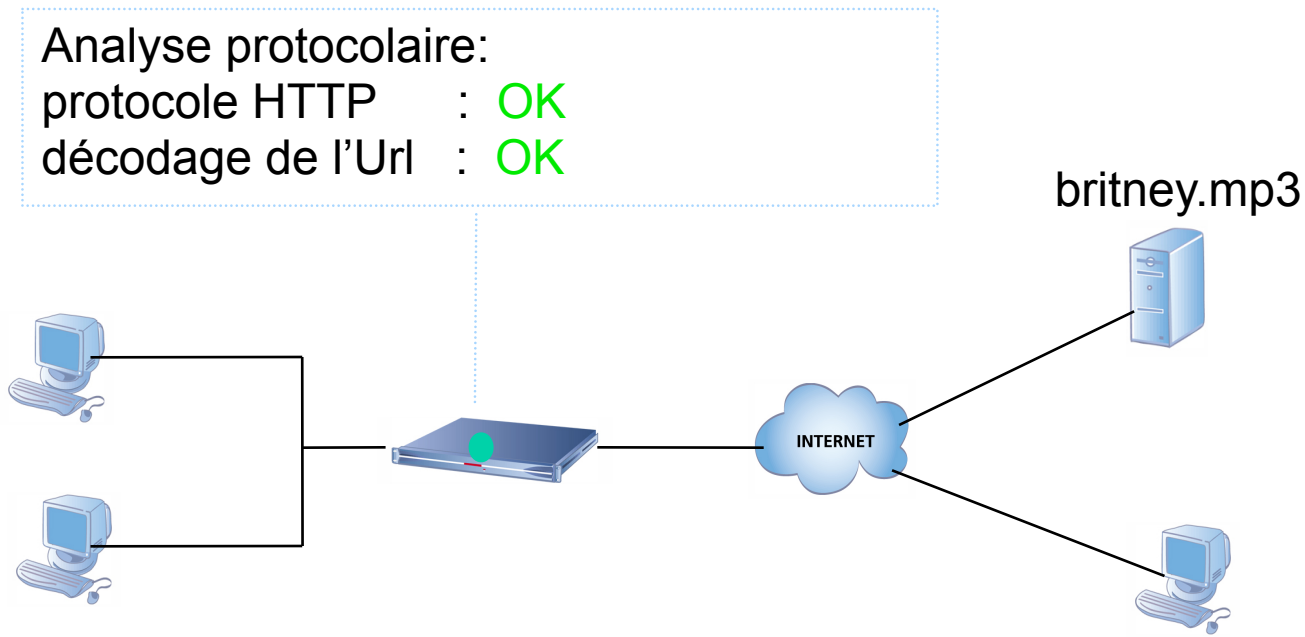
Cas pratique (Kazaa)

- Collaboration des méthodes ASQ



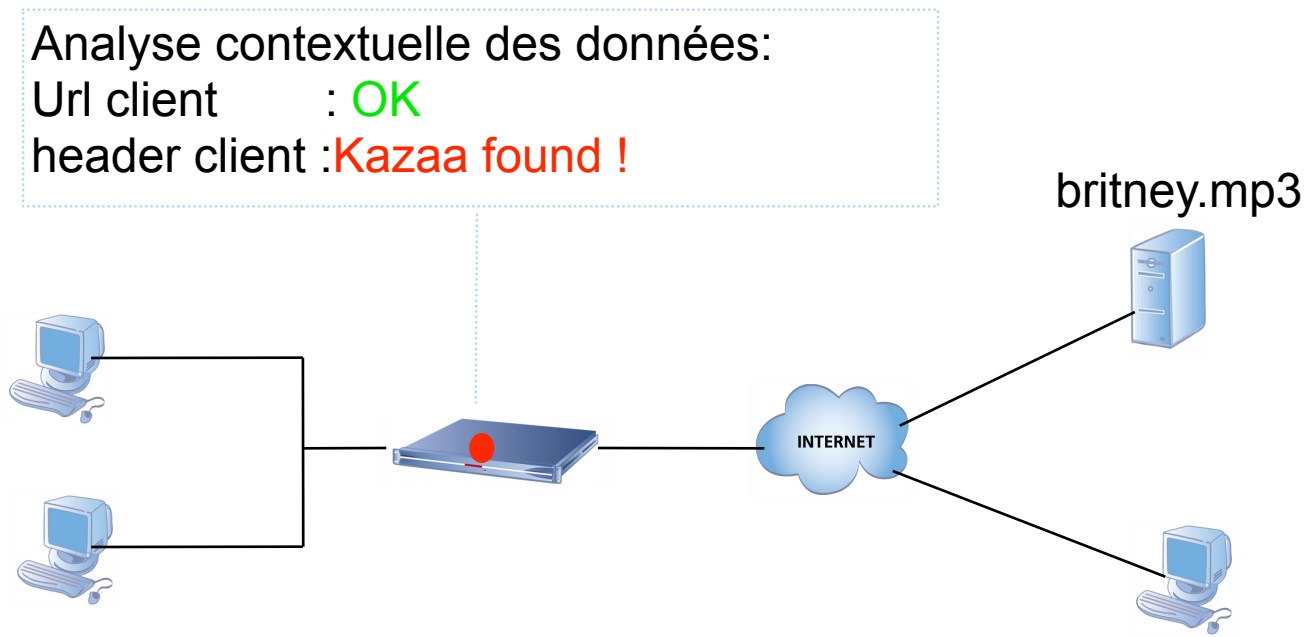
Cas pratique (Kazaa)

- Collaboration des méthodes ASQ



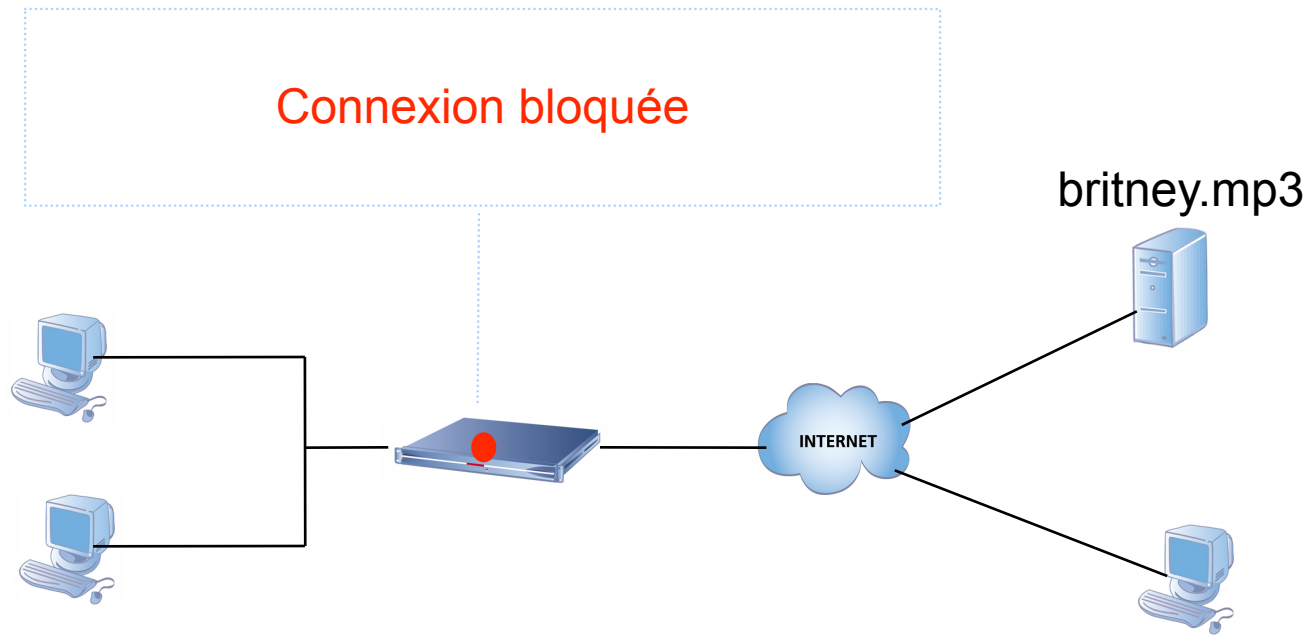
Cas pratique (Kazaa)

- Collaboration des méthodes ASQ



Cas pratique (Kazaa)

- Collaboration des méthodes ASQ



Cas pratique (Kazaa)

- Collaboration des méthodes ASQ

Les contextes permettent d'affiner l'analyse

- La base correspondant à l'entête HTTP ne sera jamais confrontée aux données d'une page web !
- l'envoi de cette présentation par mail ou par FTP ne déclenchera pas de fausse alerte « Kazaa »

La combinaison des analyses améliore les performances

- chaque analyse est faite sur une fraction des données

Autres applications

- Détection des services vulnérables
- Protection contre les XSS
- Protection contre les logiciels espions (Spyware)
- Protection contre les injections SQL
- ...

Questions

Multiples Méthodes

- ☐ Analyse protocolaire
- ☐ Signatures contextuelles
- ☑ Statistiques et heuristiques

Détection de backdoor

Nomade (trojan)

Connexion SSH, HTTP, ...
Valide au niveau de la politique

Attaquant

Serveur

Firewall

Nomade (trojan)

Règle	Date	Action	Interface	Protoc...	Source	Destination	Port ...	Message	Aide
	01/02/2005	block	in	tcp	BOB	BADSERVER	http	Détection d'une connexion interactive	
	01/02/2005	block	in	tcp	BOB	BADSERVER	http	Détection d'une connexion interactive	

Détection de backdoor

- Indicateurs statistiques sur la connexion
  - Taille des paquets
  - Organisation des paquets dans le temps
- Calcul d'un indice pour déterminer les connexions interactives
- Dialogue avec l'analyse protocolaire
  - Détermine les seuils (SSH différent de HTTP)

Résumé

Protection

- Protocolaire
  - Ethernet, IP, TCP, UDP, ...
  - Plugins applicatifs (HTTP, FTP, ...)
  - 100 classes d'alarmes
- Signatures avec contextes protocolaires
  - Mise à jour automatique avec ActiveUpdate
- Statistique et heuristique
  - Port scan
  - Détection backdoor

Performance

- Mode kernel
  - Pas de copie kernel -> user -> kernel
- Pas d'interruption
  - Mode polling
- Pas de réécriture des paquets
  - Le paquet n'est pas dupliqué
- Algorithmes évolués de vérification
  - Contextuel et parallèle

Questions