

Notes: ICAP en milieu Hétérogène

Frédéric Bourgeois <http://www.traceroot.fr>

13 janvier 2005

V 1.0

1 -Théorie.....	2
1.1 - ICAP.....	2
1.1.1 -Fonctionnement.....	2
2 - Utilisation différente du protocole.....	3
2.1 - Scanneur de fichiers.....	4
2.1.1 -Prototype.....	4
2.1.2 -Utilisation	7
2.1.3 -Avantages.....	7
2.1.4 -Inconvénients.....	7

1 –Théorie

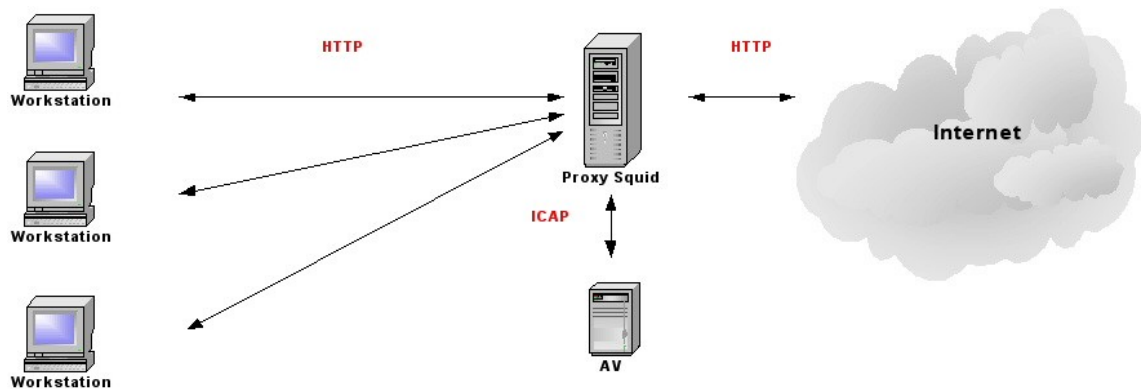
1.1 -ICAP

Définition :

ICAP est un protocole permettant la circulation de données HTTP. Il s'appuie sur des serveurs Proxies compatibles au protocole ICAP, de manière à ce que les services et l'accès rapide aux contenus Web soient possibles. Par exemple si vous combinez des produits Antivirus et un proxy Squid, ce dernier se charge du cache et de la requête sur Internet, alors que les fonctions relatives au filtrage se déroulent sur un serveur à part communicant en parallèle avec Squid à l'aide de ICAP.

1.1.1 -Fonctionnement

Transfert HTTP



2 – Utilisation différente du protocole

Grâce au filtrage de contenu, la sécurité offerte par le proxy est donc considérablement accrue:

- La possibilité de rediriger les URLs, utile si on veut empêcher le téléchargement de fichier (.exe ou .mp3 par exemple)

- Une analyse de contenu. Ainsi, pour chaque flux HTTP reçu depuis Internet, le proxy ne se contente pas seulement de travailler sur l'URL, mais examine le contenu de la trame toute entière en l'envoyant dans un antivirus.

Puisqu'il est possible, en appliquant des règles spécifiques, de filtrer certains contenus considérés comme potentiellement dangereux en HTTP, je me suis posé la question de la possibilité d'une utilisation de ce protocole dans une architecture différente, en l'occurrence dans la situation de scanneur de fichiers antivirus pour un simple poste de travail.

2.1 -Scanneur de fichiers

Pour pouvoir valider la théorie, il me fallait confirmer l'analyse par un antivirus d'un fichier hors de l'environnement HTTP.

J'ai trouvé le projet de plug-in, Samba-vscan, qui permet une analyse antivirale lors de l'écriture d'un fichier sur un partage Samba.

Dans ce projet il y a un programme qui permet de tester le protocole ICAP avec l'antivirus Symantec.

2.1.1 -Prototype

En modifiant les sources de ce logiciel j'ai pu réaliser un petit client Linux pour Kaspersky ICAP Server.

J'ai d'abord analysé les réponses de Kaspersky Antivirus dans différentes situations pour comprendre le fonctionnement du protocole avec ce logiciel.

Exemple:

Demande client :

```
./icap-client test.txt -scr  
ICAP exemple client  
Fred test 1
```

```
RESPMOD icap://127.0.0.1/ ICAP/1.0  
Allow: 204  
Host: localhost  
Encapsulated: req-hdr=0, res-hdr=25, res-body=104
```

```
GET test.txt HTTP/1.1
```

```
HTTP/1.1 200 OK  
Content-Type: application/octet-stream  
Content-Length: 14
```

```
e  
fichier texte  
0
```

```
Scan result: File test.txt is clean
```

Réponse du serveur:

```
./icap-client test.txt -ssr  
ICAP exemple client  
Fred test 1
```

```
ICAP/1.0 204 No Content  
ISTag: KAVICAP-1312006  
Date: Fri, 13 Jan 2006 09:54:32 GMT  
Encapsulated: null-body=0
```

Fichier infecté:

```
./icap-client eicar.com -scr  
ICAP exemple client  
Fred test 1
```

```
RESPMOD icap://127.0.0.1/ ICAP/1.0  
Allow: 204  
Host: localhost  
Encapsulated: req-hdr=0, res-hdr=26, res-body=105
```

```
GET eicar.com HTTP/1.1
```

```
HTTP/1.1 200 OK  
Content-Type: application/octet-stream  
Content-Length: 68
```

```
44  
X5O!P%@AP[4\PZX54(P^7CC)7}$EICAR-STANDARD-ANTIVIRUS-  
TEST-FILE!$H+H*  
0
```

```
INFECTED: 200 OK
```

Ce programme permet l'analyse de tous les fichiers locaux contenus sur le disque dur de ma machine.

2.1.2 -Utilisation

En conclusion, il semble parfaitement possible d'utiliser ICAP dans des situations différentes, fichiers locaux, serveur HTTP, SMTP, etc.

En effet, il suffit de développer un client sur chacun de ces serveurs afin de pouvoir analyser leurs fichiers locaux.

2.1.3 -Avantages

- Administration centralisée et complète d'un parc de machines (postes clients, serveurs)
- L'ensemble est très modulaire : chaque fonctionnalité (filtrage, refus de types MIME, suppression de Javascript, ...) est une option du serveur central. On peut donc rajouter un filtre sans modification générale.
- Un moteur d'analyse unique simplifie les mises à jours.

2.1.4 -Inconvénients

- Il s'agit d'un prototype, afin d'être confronté à la réalité il est fort probable que des modifications et des tests doivent être apportés
- Pour limiter le trafic sur le réseau, il est important d'avoir un moteur qui n'envoie que les fichiers ayant subi une modification ou nouvellement créés
- Le client doit être spécifique à chaque application (FTP, SMTP, HTTP, partage de fichiers, etc.) mais le protocole de communication reste unique