

Proteksi LAN dari Virus internet dengan Squid dan C-ICAP server

By

Henry Saptono <boypyt@gmail.com>

januari 2011

Salah satu cara efektif untuk dapat melindungi jaringan komputer Anda dari serangan virus yang berasal dari internet atau jaringan adalah dengan melakukan scanning virus saat user mendownload suatu file dari internet, dan juga tentunya saat user mengupload file ke jaringan atau internet. Umumnya user melakukan download file melalui layanan http/web, begitu juga saat mengupload suatu file ke sebuah web site. Akses web(http) dapat Anda sediakan untuk user user dalam jaringan LAN Anda dengan memasang sebuah http proxy server yang umumnya berfungsi sebagai web cache guna meningkatkan respon time akses web, dan juga sebagai filtering akses web. Sehingga akses web yang dilakukan user tidak secara langsung namun melalui sebuah service proxy. Dengan proxy ini Anda tentunya dapat melakukan adaptasi content web seperti filtering content web dan scanning virus. Aplikasi http proxy yang dapat digunakan untuk maksud tersebut diantaranya adalah squid (<http://www.squid-cache.org>). Squid menjadi standar aplikasi proxy server yang disertakan dalam berbagai distro Linux.

Sebenarnya squid tidak serta merta dapat langsung melakukan adaptasi content web. Untuk dapat memfungsikan squid seperti demikian dibutuhkan mekanisme adaptasi content web seperti ICAP, ClientStreams, eCAP, Squid ACL, dan penggunaan program Redirector (lihat di <http://wiki.squid-cache.org/SquidFaq/ContentAdaptation>).

Salah satu cara untuk memungkinkan squid melakukan adaptasi content web, content filtering dan scanning virus adalah dengan menerapkan mekanisme ICAP(Internet Content Adaptation Protocol) . Mulai squid versi 3.0 keatas, dukungan akan mekanisme ICAP telah tersedia. Untuk itulah penulis dalam tulisannya kali ini akan membahas bagaimana menerapkan mekanisme ICAP pada squid untuk memungkinkan melakukan scanning virus terhadap file file yang didownload oleh user via http (dari web site di internet) dan file file yang diupload oleh user ke web tertentu dalam jaringan atau internet.

Dalam menerapkan mekanisme adaptasi content web dengan ICAP, ada beberapa perangkat lunak yang dibutuhkan diantaranya aplikasi icap server yaitu C-ICAP, Clamav Antivirus, serta Squid. Dalam tulisan ini penulis akan menggunakan squid versi 3.0.STABLE19-1, dan c_icap-0.1.4 serta c_icap_modules-0.1.3, dan clamav- 0.96. Dalam tulisan ini penulis menggunakan distribusi Linux Ubuntu 10.04, dan sebagai gambaran bahwa service squid dan icap server serta clamav diinstal pada komputer yang sama yaitu komputer yang akan difungsikan sebagai proxy server.

ICAP (Internet Content Adaptation Protocol)

Internet Content Adaptation Protocol , adalah protokol yang bertujuan menyediakan konten vectoring sederhana berbasis obyek untuk layanan HTTP (RFC3507, <http://www.rfc-editor.org/rfc/rfc3507.txt>). ICAP pada dasarnya adalah sebuah protokol ringan untuk mengeksekusi sebuah "remote procedure call" pada pesan-pesan HTTP. Hal ini memungkinkan ICAP klien untuk memberikan pesan HTTP ke server ICAP untuk beberapa jenis transformasi atau processing lainnya ("adaptasi"). ICAP server mengeksekusi layanan transformasi pada pesan pesan yang dikirimkan oleh klien dan kemudian mengirim kembali tanggapan kepada klien, biasanya dengan pesan yang telah diubah. Pesan tersebut bisa pesan permintaan atau tanggapan HTTP

Beberapa aplikasi proxy populer, termasuk squid, memiliki dukungan ICAP. Jika algoritma adaptasi content berada (dilakukan) pada ICAP server, maka proses adaptasi ini dapat bekerja dalam berbagai lingkungan dan tidak akan tergantung pada sebuah produk proxy atau vendor. Dan tidak diperlukan modifikasi kode sumber proxy untuk dapat melakukan adaptasi content web menggunakan ICAP.

Sebuah proxy server bisa saja mengakses beberapa ICAP server, dan sebuah ICAP server bisa saja diakses oleh beberapa proxy server. Sebuah ICAP server bisa saja secara fisik berada dalam mesin yang sama dengan squid server atau berjalan pada sebuah mesin remote. Tergantung pada konfigurasi dan konteksnya, beberapa kegagalan yang terjadi pada ICAP server dapat di bypass, sehingga membuat ICAP server tak terlihat oleh user pengguna.

Beberapa perangkat lunak icap server diantaranya adalah sebagai berikut:

- C-ICAP (C)
- Traffic Spicer (C++)
- ICAP-Server (Python)
- POESIA (Java)

C-ICAP

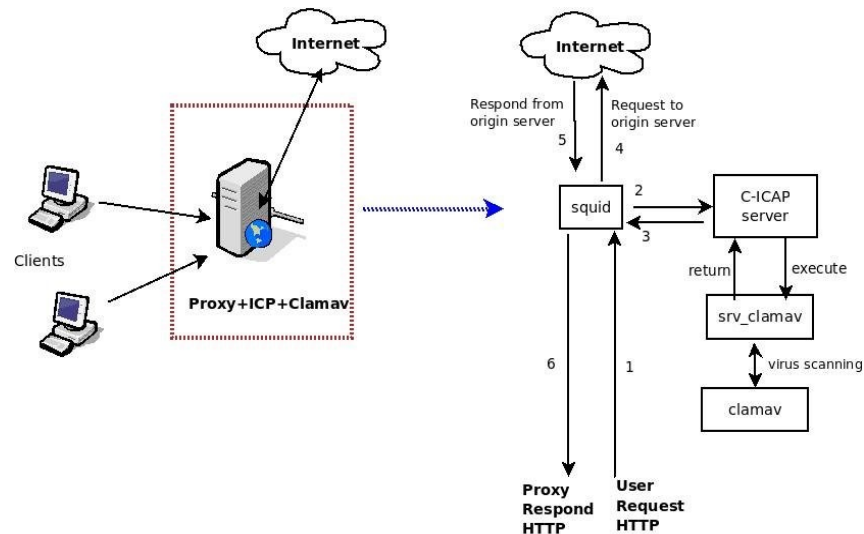
C-ICAP adalah sebuah implementasi dari sebuah ICAP server. Dapat digunakan oleh HTTP proxy yang mendukung protokol ICAP untuk menerapkan *content adaptation* dan *filtering services*.

Sebagian besar aplikasi HTTP proxy komersial pasti mendukung protokol ICAP. HTTP Proxy open source yang telah mendukung protokol ICAP adalah [Squid 3.x](#) .

Dalam tulisan ini kita akan menggunakan icap server C-ICAP beserta modul-modulnya, yang dapat diperoleh dari <http://c-icap.sourceforge.net/>

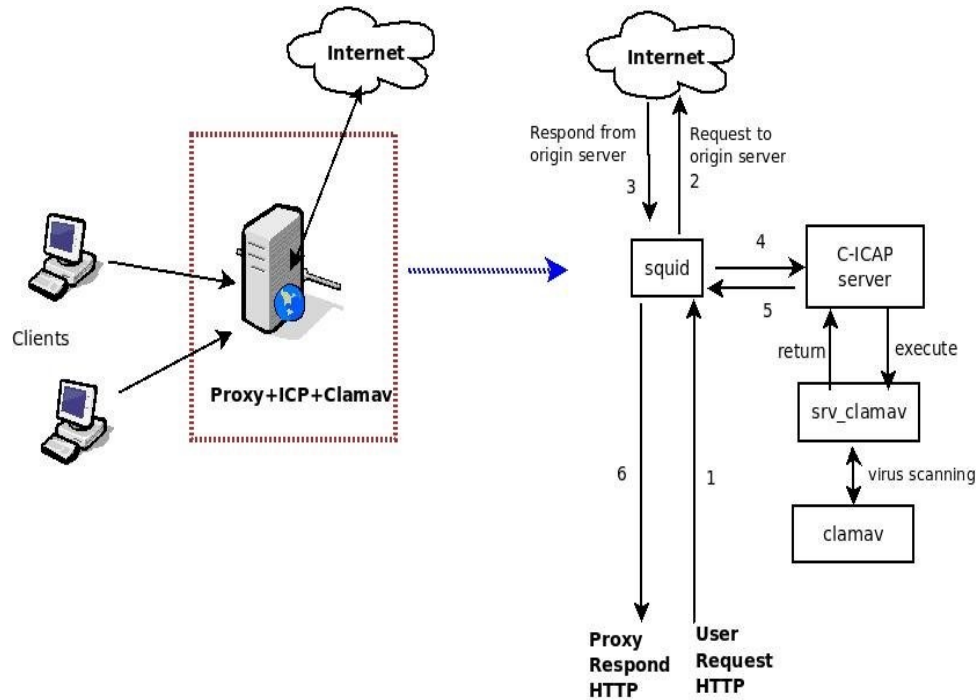
Proses Adaptasi content (scanning virus)

Proses adaptasi content web dengan mekanisme ICAP terdiri dari dua mode , yaitu request mode (reqmod, gambar-1) dan respond mode (respmod, gambar-2).



Gambar 1. Ilustrasi proses adaptasi content - request mode

Dari gambar-1, tampak bahwa seluruh request http dari klien ditujukan/menjuhi komputer proxy server, dimana pada proxy server juga terinstal icap server dan clamav antivirus. Pesan permintaan atau request dari klien diterima oleh squid proxy server kemudian, proxy mengirimkan/meneruskan pesan permintaan dari klien tersebut kepada C-ICAP server untuk diproses oleh service yang tersedia pada C-ICAP server dalam hal ini service scanning virus (disediakan oleh modul C-ICAP yaitu **srv_clamav**). Selanjutnya srv_clamav melakukan scanning virus terhadap pesan http dari klien, kemudian hasil pesan hasil scanning dikirimkan kembali ke C-ICAP server yang kemudian di kirimkan kembali kepada squid.



Gambar 2. Ilustrasi proses adaptasi content – respond mode

Dalam respond mode (gambar-2), pesan permintaan atau request dari klien diterima oleh squid proxy server yang kemudian, proxy mengirimkan/meneruskan permintaan ke original server, dan selanjutnya menerima pesan dari original server yang dikirimkan ke ICAP server untuk diadaptasi oleh service yang tersedia pada C-ICAP server dalam hal ini service scanning virus (disediakan oleh modul C-ICAP yaitu *srv_clamav*). Selanjutnya *srv_clamav* melakukan scanning virus terhadap pesan http dari klien, kemudian hasil pesan hasil scanning dikirimkan kembali ke C-ICAP server yang kemudian di kirimkan kembali kepada squid.

Instalasi squid

Jika squid versi 3 belum terinstal pada komputer Anda maka segera instal, dan jika sebelumnya sudah terinstal squid versi 2 sebaiknya squid versi 2 di uninstal dahulu. Untuk instalasi squid versi 3 Anda dapat menggunakan perintah berikut ini:

```
ibad@master:~$ sudo apt-get install squid3
```

Instalasi clamav

Clamav diperlukan sebagai aplikasi antivirus. Untuk instalasi clamav lakukan seperti perintah berikut ini:

```
ibad@master:~$ sudo apt-get install clamav libclamav-dev clamav-freshclam
```

Perlu diperhatikan, setelah instalasi clamav secara otomatis akan dijalankan service update database antivirus clamav ke mirror mirror clamav di internet, yaitu service freshclam. Terkadang proses update gagal sehingga file database antivirus clamav tidak terbentuk (tidak ada). Untuk mengatasi hal ini berdasarkan pengalaman penulis, maka sebaiknya dijalankan perintah berikut ini:

```
ibad@master:~$ sudo dpkg --configure -a
```

Instalasi C-ICAP

Jika c-icap server dan modulnya telah Anda download dari http://sourceforge.net/projects/c-icap/files/c-icap/0.1.x/c_icap-0.1.4.tar.gz/download, maka lakukan langkah berikutnya yaitu instalasi. Berikut ini adalah proses instalasi c-icap server:

```
ibad@master:~$ sudo su -
root@master:~# tar -xzvf c_icap-0.1.4.tar.gz
root@master:~# cd c_icap-0.1.4
root@master:c_icap-0.1.4# ./configure --prefix=/opt/c-icap --enable-large-files
root@master:c_icap-0.1.4# make
root@master:c_icap-0.1.4# make install
```

Opsi --prefix menunjukkan lokasi direktori tempat nantinya hasil kompilasi(build) c-icap diinstal.

Selanjutnya download c-icap module dari http://sourceforge.net/projects/c-icap/files/c-icap-modules/0.1.x/c_icap_modules-0.1.3.tar.gz/download, kemudian instal dengan langkah langkah sebagai berikut:

```
ibad@master:~$ sudo su -
root@master:~# tar -xzvf c_icap_modules-0.1.3.tar.gz
root@master:~# cd c_icap_modules-0.1.3
root@master:c_icap_modules-0.1.3# ./configure --with-c-icap=/opt/c-icap
root@master:c_icap_modules-0.1.3# make
root@master:c_icap_modules-0.1.3# make install
```

Opsi --with-c-icap menunjukkan dimana lokasi direktori c-icap server, dalam contoh ini adalah /opt/c-icap

Konfigurasi C-ICAP server

Agar icap server berfungsi sebagaimana yang diharapkan maka lakukanlah konfigurasi icap server, dengan mengatur konfigurasi yang tersimpan dalam file /opt/c-icap/etc/c-icap.conf, aturlah agar entri konfigurasi c-icap server seperti berikut ini:

```
PidFile /var/run/c-icap/c-icap.pid
CommandsSocket /var/run/c-icap/c-icapctl
Timeout 300
MaxKeepAliveRequests 100
KeepAliveTimeout 600
StartServers 3
MaxServers 10
MinSpareThreads 10
MaxSpareThreads 20
ThreadsPerChild 10
MaxRequestsPerChild 0
Port 1344
User proxy
Group proxy
ServerAdmin henry@overflow.web.id
ServerName icap.overflow.web.id
TmpDir /var/tmp
MaxMemObject 131072
DebugLevel 1
ModulesDir /opt/c-icap/lib/c_icap
ServicesDir /opt/c-icap/lib/c_icap
TemplateDir /opt/c-icap/share/c_icap/templates/
TemplateDefaultLanguage en
LoadMagicFile /opt/c-icap/etc/c-icap.magic
RemoteProxyUsers off
RemoteProxyUserHeader X-Authenticated-User
RemoteProxyUserHeaderEncoded on
acl localnet src 192.168.1.0/255.255.255.0
acl localhost src 127.0.0.1/255.255.255.255
acl all src 0.0.0.0/0.0.0.0
```

```
icap_access allow localnet
icap_access allow localhost
icap_access deny all
ServerLog /opt/c-icap/var/log/server.log
AccessLog /opt/c-icap/var/log/access.log
Service echo srv_echo.so
Module logger sys_logger.so
Logger sys_logger
sys_logger.Prefix "C-ICAP:"
Include srv_clamav.conf
Include srv_url_check.conf
```

Diasumsikan bahwa LAN Anda memiliki network address 192.168.1.0/24 . Selanjutnya konfigurasi service srv_clamav, dengan mengatur konfigurasi pada file /opt/c-icap/etc/srv_clamav.conf, dan entri konfigurasinya seperti berikut ini:

```
Service antivirus_module srv_clamav.so
ServiceAlias avscan srv_clamav?allow204=on&sizelimit=off&mode=simple
srv_clamav.ScanFileTypes TEXT DATA EXECUTABLE ARCHIVE GIF JPEG MSOFFICE
srv_clamav.SendPercentData 5
srv_clamav.StartSendPercentDataAfter 2M
srv_clamav.MaxObjectSize 5M
srv_clamav.ClamAvTmpDir /var/tmp
srv_clamav.ClamAvMaxFilesInArchive 0
srv_clamav.ClamAvMaxFileSizeInArchive 100M
srv_clamav.ClamAvMaxRecLevel 5
```

Selanjutnya konfigurasi service srv_url_check, dengan mengatur konfigurasi pada file /opt/c-icap/etc/srv_url_check.conf, dan entri konfigurasinya minimal seperti berikut ini:

```
Service url_check_module srv_url_check.so
```

Selanjutnya membuat direktori /var/run/c-icap, serta file /var/run/c-icap/c-icap.ctl, seperti berikut ini:

```
root@master:~#mkdir /var/run/c-icap
root@master:~#chown proxy /var/run/c-icap
root@master:~#echo -n "" > /var/run/c-icap/c-icap.ctl
```

Mengaktifkan C-ICAP server

Untuk mengaktifkan atau menjalankan c-icap server Anda dapat menggunakan perintah berikut ini:

```
root@master:~# /opt/c-icap/bin/c-icap -f /opt/c-icap/etc/c-icap.conf -N -D -d 2
```

atau jika ingin menjalankan c-icap server sebagai daemon , maka perintahnya seperti berikut ini:

```
root@master:~# /opt/c-icap/bin/c-icap -f /opt/c-icap/etc/c-icap.conf -D -d 2
```

Untuk merestart c-icap server sebagai berikut:

```
root@master:~#echo -n "reconfigure" > /var/run/c-icap/c-icapctl
```

Untuk mematikan service c-icap server sebagai berikut:

```
root@master:~#echo -n "stop" > /var/run/c-icap/c-icapctl
```

Setelah mematikan c-icap server untuk dapat mengaktifkan kembali c-icap server , maka Anda harus menjalankan perintah berikut:

```
root@master:~#echo -n "" > /var/run/c-icap/c-icapctl
```

Menguji C-ICAP server

Jika c-icap server sudah berjalan coba Anda uji dengan menjalankan perintah berikut:

```
root@master:~# /opt/c-icap/bin/c-icap-client
```

Jika berhasil maka Anda akan mendapatkan output seperti berikut ini:

```
ICAP server:localhost, ip:127.0.0.1, port:1344
```

OPTIONS:

```
Allow 204: Yes
Preview: 1024
Keep alive: Yes
```

ICAP HEADERS:

```
ICAP/1.0 200 OK
Methods: RESPMOD, REQMOD
Service: C-ICAP/0.1.4 server - Echo demo service
ISTag: CI0001-XXXXXXXXXX
Transfer-Preview: *
Options-TTL: 3600
Date: Mon, 03 Jan 2011 19:39:23 GMT
Preview: 1024
```

```
Allow: 204
X-Include: X-Authenticated-User, X-Authenticated-Groups
Encapsulated: null-body=0
```

Konfigurasi Squid

Untuk mengatur konfigurasi squid versi 3 Anda dapat mengedit file /etc/squid3/squid.conf, konfigurasi pertama adalah mendefinisikan access control list, untuk itu tambahkan entri konfigurasi berikut ini pada file /etc/squid/squid.conf (dibawah baris komentar yang bertuliskan “#INSERT YOUR OWN RULE.....”):

```
acl localnet src 192.168.1.0/24
http_access allow localnet
```

Selanjutnya cari baris komentar yang bertuliskan #ICAP OPTIONS, kemudian tambahkan entri berikut ini dibawahnya:

```
icap_enable on
icap_service service_req reqmod_precache 1 icap://127.0.0.1:1344/avscan
icap_class class_req service_req
icap_access class_req allow all

icap_service service_resp respmod_precache 0 icap://127.0.0.1:1344/avscan
icap_class class_resp service_resp
icap_access class_resp allow all
```

Mengaktifkan squid

Untuk mengaktifkan service squid gunakan perintah berikut ini:

```
root@master:~# /etc/init.d/squid3 start
```

Dan untuk merestart service squid, gunakan perintah berikut:

```
root@master:~# /etc/init.d/squid3 restart
```

atau

```
root@master:~# squid3 -k reconfigure
```

Dan untuk mematikan service squid, sebagai berikut:

```
root@master:~# /etc/init.d/squid3 stop
```

Uji coba mendownload File virus

Untuk uji coba gunakan aplikasi firefox web browser namun sebelumnya pastikan agar web browser selalu terhubung ke proxy server setiap kali mengakses web, untuk itu setting dahulu koneksinya melalui proxy server dengan memilih menu Edit | Preferences | Advanced | Network | Settings . kemudian pada window settings pilih “Manual Proxy Configuration” selanjutnya isi bagian HTTP Proxy dengan alamat IP proxy server Anda dan portnya (3128) dengan benar.

Selanjutnya coba Anda download sebuah file sample virus dari url berikut <http://www.eicar.org/download/eicarcom2.zip>

Kemudian amati seharusnya jika squid dan c-icap server bekerja maka Akan didapat pesan seperti tampak pada gambar 3.



Gambar 3. Pesan error saat download file virus

Anda dapat juga melakukan verifikasi setiap aksi download ataupun upload file bervirus dengan mengamati file log, yang dapat Anda lihat melalui file /var/log/daemon.log atau /var/log/syslog pada server proxy.

Selamat mencoba