Configurare Squid con HAVP e Clamav

Nel precedente articolo abbiamo visto come aggiungere la funzionalità di anti-virus ad un proxy-web. In questo articolo indichiamo i principali passi per la configurazione di Squid con HAVP e Clamav. Assumiamo che Squid, HAVP e Clamav siano installati sulla stessa macchina. La compilazione ed installazione di questi programmi è standard, indichiamo solo che per la compilazione di HAVP sono necessarie sia le librerie di Clamav normali che quelle di sviluppo (devel).

La configurazione

La configurazione di Squid ed HAVP può creare confusione poiché vogliamo che HAVP si comporti come un programma *helper* di Squid. In particolare vogliamo che HAVP sia per Squid il parent-proxy per tutte le richieste provenienti dai client, mentre Squid sia il parent-proxy per HAVP stesso. Inoltre le richieste dei client non devono essere trattenute nella cache di Squid, mentre le richieste di HAVP devono essere mantenute nella cache. La Fig. 1 illustra questo processo.

La configurazione di HAVP è abbastanza semplice, in Tabella 1 indichiamo i principali parametri del file `/etc/havp/havp.config`. In questa configurazione abbiamo indicato sia Squid come parent-proxy che di attendere richieste solo sulla porta 8080 della macchina locale. Inoltre la dimensione massima di un file da scansire è di 400MB mentre, solo per motivi dimostrativi del funzionamento di HAVP, abbiamo posto la dimensione della parte bloccata del file sino al termine della scansione anti-virus a 100KB (si veda il precedente articolo per la discussione di questa caratteristica di HAVP). I file temporanei sono creati nella directory `/var/havp/tmp/` che deve essere montata su di un filesystem con l'opzione *mandatory* (`-o mand`). Se non abbiamo a disposizione una partizione fisica che possiamo montare con questa opzione, possiamo o utilizzare dei ram-disk che offrono anche la massima velocità, oppure una partizione all'interno di un file che si può creare come indicato in Tabella 2.

La configurazione di Squid è in realtà abbastanza complessa, ne indichiamo in Tabella 3 solo i punti essenziali ma richiede comunque parecchia attenzione. In questa configurazione indichiamo che Squid deve ascoltare richieste sia dai client nella rete locale (192.168.1.0/24) che sulla stessa macchina (HAVP). Inoltre creiamo due ACL, una per i client interni ed una per specificare il protocollo HTTP. Infatti in questo esempio abbiamo deciso di far filtrare da HAVP solo il protocollo HTTP, non HTTPS, FTP eccetera (traffico che invece può attraversare Squid), e dobbiamo quindi poter distinguere questo tipo di traffico dal resto. A questo punto indichiamo che sulla porta 8080 della stessa macchina è presente un parent-proxy che va utilizzato come default, e che gli oggetti ricevuti da questo parent-proxy non devono essere posti in cache (opzione `proxy-only`). Le opzioni `always-direct` e `never-direct` sono sintatticamente più complesse. Le prime indicano che tutte le richieste ad eccezione di quelle HTTP proveniente dalla rete locale, devono essere soddisfatte direttamente senza passare dal parent-proxy. Le seconde al contrario indicano che tutte le richieste di tipo HTTP provenienti dalla rete locale devono essere inviate al parent-proxy. Infine l'ultima istruzione riafferma che non deve essere fatta una cache locale delle richieste e risposte provenienti direttamente dai client della rete locale, mentre vengono messe in cache le richieste provenienti dalla stessa macchina, ovvero quelle di HAVP.

Il funzionamento

Per verificare che tutto funzioni correttamente abbiamo eseguito alcune prove. In Tabella 4. riportiamo i log della prima prova: come si vede quando il client chiede per la seconda volta la stessa pagina, Squid non la fornisce dalla cache (TCP_MISS) ma la chiede al parent-proxy, mentre la richiesta di HAVP è soddisfatta dalla cache (TCP_REFRESH_HIT). Per motivi di spazio abbiamo tralasciato alcuni campi dei messaggi di log di Squid, quelli indicati sono: l'indirizzo da cui proviene la richiesta, il risultato della richiesta, la dimensione dei dati inviati come risposta, il metodo HTTP, la pagina richiesta, il modo ed a chi è stata inviata la richiesta, il tipo di file

richiesto. Nei log di Squid prima vengono indicati i dati ricevuti dal server esterno ed inviati a HAVP (righe che cominciano per 127.0.0.1) e poi i dati ricevuti da HAVP ed inviati al client interno (righe che cominciano per 192.168.1.3), ovvero nell'ordine di invio dei dati e non delle richieste ricevute.

In Tabella 5 mostriamo un test di funzionamento dell'anti-virus, si noti in questo caso come la dimensione dei dati inviati al client (terzo campo della seconda riga) sia molto maggiore rispetto ai dati ricevuti dal server (terzo campo della prima riga). Il motivi è che HAVP invece di inviare al client il virus, ha inviato la pagina illustrata in Fig. 2.

Infine nella Tabella 6 indichiamo il comportamento del sistema quando viene scaricato un virus di dimensioni superiori a 100KB[1]: si noti come Squid abbia inviato a HAVP (terzo campo della prima riga del log) dati per 240KB, mentre abbia ricevuto da HAVP ed inviato al client solo 140KB (terzo campo della seconda riga del log). Il client ha ricevuto perciò 140KB del virus (in questo caso un dialer di accesso ad un sito pornografico) ma i 100KB mancanti hanno reso del tutto innocuo ed inutile il file scaricato, che infatti non è stato riconosciuto da alcun anti-virus sul client. Il file era un archivio zip corrotto e del tutto inutilizzabile. Ovviamente per evitare che anche una piccola parte del file contenente un virus vengano inviati al client, bisogna porre nella configurazione di HAVP il parametro `KEEPBACKBUFFER` uguale a `MAXSCANSIZE`, il sistema sicuramente perderà molto di prestazioni nello scarico di file di grandi dimensioni, ma aumenterà il livello di sicurezza.

Andrea Pasquinucci

pasquinucci@ucci.it

Riferimenti Bibliografici

[1] Squid http://www.squid-cache.org/

1 Sono ovviamente state cambiate le URL del sito dialer preso ad esempio, la transazione è però autentica.

[2] HAVP http://www.server-side.de/

[3] Clamav http://www.clamav.net/

```
#/etc/havp/havp.config
USER  havp
GROUP havp
SCANTEMPFILE /var/havp/tmp/havp-XXXXXX
PARENTPROXY localhost
PARENTPORT 3128
PORT 8080
BIND_ADDRESS 127.0.0.1
MAXSCANSIZE 400000000
KEEPBACKBUFFER 100000
ENABLECLAMLIB true
```

Tabella 1. Configurazione di HAVP

```
mkdir -p /var/havp/tmp/
cat <<EOF >>/etc/fstab
/var/havp/havp.img /var/havp/tmp ext2 loop,mand 0 0
EOF
dd if=/dev/zero of=/var/havp/havp.img bs=1M count=512
mke2fs -F -q -m0 /var/havp/havp.img
mount /var/havp/tmp
chown -R havp:havp /var/havp
chmod -R 750 /var/havp
```

Tabella 2. Creazione di un filesystem su file montato su loopback con opzione -mand

```
#/etc/squid/quid.conf
http_port 192.168.1.254:3128
http_port localhost:3128
#
acl local_net src 192.168.1.0/255.255.255.0
acl HTTP proto HTTP
#
cache_peer localhost parent 8080 0 no-query no-digest no-netdb-exchange\
           default proxy-only
#
always_direct deny local_net HTTP
always_direct allow all
never_direct allow local_net HTTP
never_direct deny all
#
no_cache deny local_net HTTP
```

Tabella 3. Configurazione di Squid

```
#/var/log/squid/access.log
#Primo tentativo
127.0.0.1 TCP_MISS/304 184 GET http://www.server-side.de/\
    DIRECT/212.227.109.197 -
192.168.1.3 TCP_MISS/304 221 GET http://www.server-side.de/\
    DEFAULT_PARENT/localhost -
#Secondo tentativo
127.0.0.1 TCP_REFRESH_HIT/304 184 GET http://www.server-side.de/\
    DIRECT/212.227.109.197 -
192.168.1.3 TCP_MISS/304 221 GET http://www.server-side.de/\
    DEFAULT_PARENT/localhost -
```

Tabella 4. Verifica funzionamento Squid

```
#/var/log/squid/access.log
127.0.0.1 TCP_MISS/200 471 GET http://www.eicar.org/download/eicar.com\
          DIRECT/83.246.65.3 application/x-msdos-program
192.168.1.3 TCP_MISS/200 1307 GET http://www.eicar.org/download/eicar.com\
          DEFAULT_PARENT/localhost text/html
#/var/log/havp/access.log
127.0.0.1 http://www.eicar.org/download/eicar.com Virus: Eicar-Test-Signature
#/var/log/havp/havp.log
Virus Eicar-Test-Signature in file /var/havp/tmp/havp-sFF0Fy detected!
```

Tabella 5. Verifica funzionamento HAVP

```
#/var/log/squid/access.log
127.0.0.1 TCP_MISS/200 240823 GET http://www.dialer.com/Dialer.zip\
          DIRECT/66.235.219.114 application/zip
192.168.1.3 TCP_MISS/200 141690 GET http://www.dialer.com/Dialer.zip\
          DEFAULT_PARENT/localhost application/zip
#/var/log/havp/access.log
Virus Dialer-568 in file /var/havp/tmp/havp-uMA6Ey detected!
#/var/log/havp/havp.log
127.0.0.1 http://www.dialer.com/Dialer.zip Virus: Dialer-568
```

Tabella 6. Verifica con un virus di dimensioni superiori a 100KB

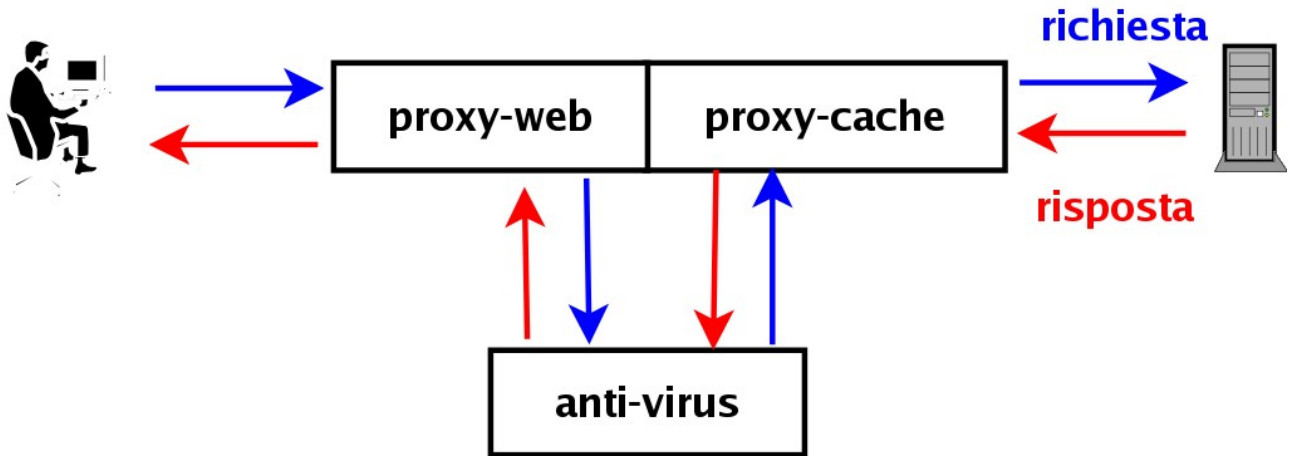

Fig 1. AV come helper del proxy

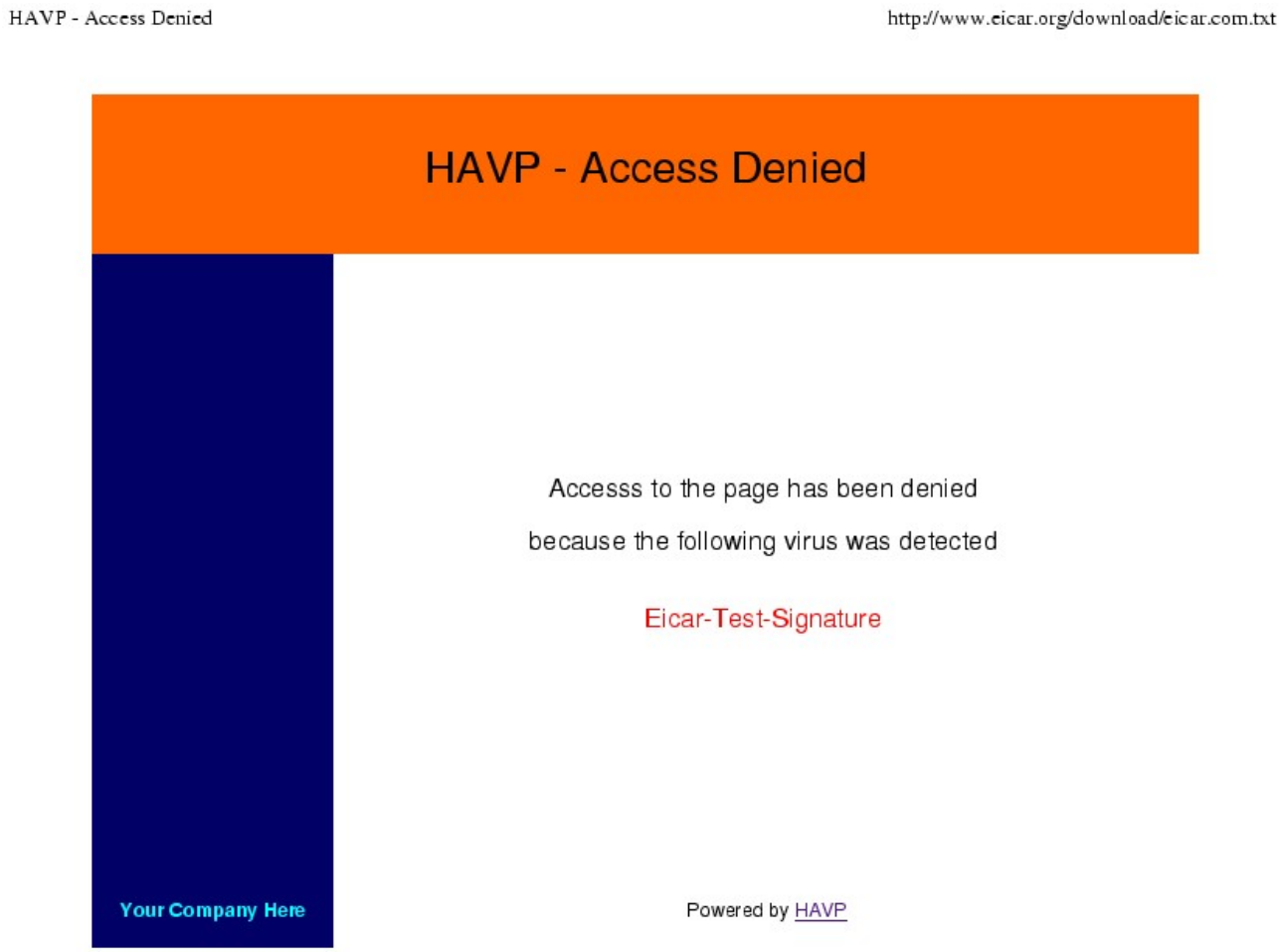

Fig. 2 Pagina inviata da HAVP invece del virus