Usare un Anti-Virus per la Navigazione Web

Ci siamo già occupati in precedenti rubriche del problema della sicurezza della navigazione web. Abbiamo considerato sia il filtraggio delle URL, ovvero degli indirizzi delle pagine richieste dai browser degli utenti, che del filtraggio sul tipo di contenuti inviato dal server in risposta. I filtri di cui abbiamo parlato sono però statici e molto generici, ad esempio i filtri sui contenuti possono rimuovere gli applet Java o Active-X, oppure i banner pubblicitari.

La navigazione Web sta però diventando il principale metodo di invio di virus ed altri programmi nocivi. Perciò è ormai necessario trattare la sicurezza della navigazione allo stesso modo della sicurezza della posta elettronica. Se possiamo equiparare il filtraggio degli indirizzi dei siti all'anti-spam, è necessario aggiungere al proxy-web aziendale la funzionalità di anti-virus.

Proxy-web ed anti-virus

In linea di principio non è per nulla difficile aggiungere ad un proxy-web aziendale anche la funzionalità di anti-virus. Per quanto riguarda l'anti-virus possiamo spesso utilizzare direttamente quello che usiamo già per la posta elettronica, anche se su di un'altra macchina, quella dedicata al proxy-web. Infatti molti produttori di anti-virus includono anche le firme dei virus che possono essere scaricati via web in quanto molti prodotti anti-virus non sono solamente per la posta elettronica, ma pensati in modo generale per qualunque tipo di virus che possa arrivare sul nostro personal computer.

I problemi che sorgono aggiungendo un anti-virus alla servizio di proxy-web sono principalmente di due tipi. Il primo riguarda il problema della interattività. Quando l'anti-virus su di un server di posta agisce sui messaggi di posta elettronica, non ha problemi di tempi di risposta verso l'utente finale perché l'utente non si accorge se il messaggio di posta arriva con un minuto di ritardo. Il servizio web è invece interattivo e non è possibile introdurre un grande ritardo nella consegna delle

pagine senza che l'utente finale si lamenti. Utilizzare un macchina più potente non è da sola la soluzione a questo problema. Oltre ad utilizzare hardware di potenza adeguata, è necessario che il programma che svolge il compito di anti-virus adotti tecniche opportune per velocizzare il più possibile il controllo dei dati in transito. Discuteremo più avanti un possibile modo per farlo.

Il secondo problema riguarda il posizionamento della funzionalità di anti-virus rispetto al proxy-web. Ricordiamo che un proxy-web svolge molte funzioni utili alla navigazione: dalla cache dei dati per velocizzare la navigazione e ridurre il traffico in internet, all'implementazione di complesse regole di autenticazione, autorizzazione e filtraggio delle destinazioni consentite. Inoltre, il traffico web è caratterizzato dalla richiesta del client verso il server nella quale è specificato di norma solo quale pagina il client chiede al server, e la risposta del server che invia il documento richiesto. In questo caso il controllo anti-virus deve essere fatto sicuramente sui dati inviati dal server al client. Più raramente anche il client invia dati al server, tipicamente quando si fa l'upload di un documento o si compila una form on-line, ed ovviamente anche in questi casi i dati devono essere controllati. Chiaramente la situazione più pericolosa è quella dei dati inviati dal server al client. Dove possiamo allora inserire il filtraggio anti-virus? Abbiamo 3 possibilità:

1. possiamo porre l'anti-virus a monte del proxy-web: in questo caso l'ordine è client <=> proxy-web <=> anti-virus <=> server e quindi tutti i dati inviati dal server prima passano dall'anti-virus e poi dal proxy-web. Il problema di questa soluzione è nel fatto che il proxy-web mantiene in cache, anche per lungo tempo, i dati inviati dai server e li distribuisce ai client senza riscaricarli dal server orginario. Visto che il database degli anti-virus è aggiornato periodicamente, ma sempre *dopo* la comparsa di un virus, se un virus riesce a passare l'anti-virus prima dell'arrivo della relativa firma rischia di rimanere nella cache del proxy-web ed essere distribuito ai client per molto tempo [fig. 1].
2. Possiamo mettere l'anti-virus a valle del proxy-web: in questo caso l'ordine è client <=> anti-virus <=> proxy-web <=> server. Si risolve il problema precedente ma se ne produce un altro: gli anti-virus non hanno tutte le funzionalità di autenticazione, controllo degli accessi eccetera tipiche di un proxy-web, e visto che i client si connettono direttamente

all'anti-virus queste funzionalità sarebbero perse [fig. 2].

3. L'ultima possibilità è la configurazione a sandwich nella quale sdoppiamo il proxy-web: logicamente l'ordine è client <=> proxy-web <=> anti-virus <=> proxy-cache <=> server, ove il proxy-web attua tutte le politiche di controllo degli accessi sui client, filtro delle URLs eccetera ma non fa alcuna cache dei dati, mentre il proxy-cache fa esclusivamente cache per i client dei dati inviati dai server. Il problema di questa soluzione è che i dati ora devono fare 3 attraversamenti e non più solo 2, con l'ovvio aumento delle richieste di calcolo e tempi di ritardo [fig. 3].

La terza soluzione è quella che offre le maggiori garanzie di sicurezza, in quanto tutti i dati inviati verso i client sono sempre prima controllati dall'anti-virus, anche se provengono dalla cache locale, ed al contempo il proxy-web può attuare tutte le usuali politiche di controllo.

Inoltre non è veramente necessario utilizzare due proxy-web per realizzare questa configurazione. Infatti possiamo vedere l'anti-virus come una applicazione *helper* del proxy-web. In pratica il proxy-web passa all'anti-virus i dati da controllare che li restituisce una volta svolto il controllo. Questo può essere realizzato utilizzando la struttura ad albero dei proxy, in pratica utilizzando la possibilità per un proxy di inviare la richiesta non direttamente al server ma ad un proxy *parent*, cioè di livello più alto nella gerarchia delle cache. A sua volta il proxy-parent, in questo caso l'anti-virus, invia la richiesta ad un altro parent, che non è altro che il proxy originale. La differenza è che nel proxy-web i due traffici vengono trattati in modo diverso, il primo per la parte di controllo, il secondo per la cache [fig. 4].

La soluzione SQUID con HAVP

Per esemplificare questa configurazione, consideriamo il ben noto Squid [1], di cui abbiamo già parlato in questa rubrica, come proxy-web, ed HAVP [2], ovvero *HTTP AntiVirus Proxy*, come anti-virus. Dobbiamo segnalare che HAVP è un prodotto molto nuovo, e quindi non ancora maturo[1]

1 Sconsigliamo vivamente di utilizzarlo in ambienti di produzione, anche se nei test da noi effettuati il prodotto si è comportato bene.

ma che si adatta bene alla nostra discussione.

Nel prossimo articolo illustreremo come installare e configurare Squid con HAVP, qui ci limitiamo a discutere dell'approccio scelto da HAVP per velocizzare l'operazione di scansione dei dati.

HAVP può utilizzare le librerie di vari anti-virus, di norma Clamav, ma anche F-Prot, Trophie, Sophos, Kaspersky ed altri. HAVP può essere usato come proxy-anti-virus-web isolato oppure insieme ad un altro proxy-web, come nel caso Squid.

Quando HAVP riceve una richiesta da un client (o da un proxy di livello inferiore) invia la richiesta direttamente al server od al proxy di livello superiore. All'arrivo dei dati in risposta (qualunque tipo di dati, pagine html, immagini ecc.), HAVP scrive tutti i dati in un file temporaneo. A questo punto il processo in esecuzione pone un hard-lock sugli ultimi 200KB[2] del file temporaneo in modo che questa parte del file non possa essere inviata al client sino al termine della scansione anti-virus. Si noti che la maggior parte delle pagine web e delle immagini sono di dimensioni inferiori a 100KB, ed in tutti questi casi tutto il file viene bloccato. Viene quindi attivato un altro processo che attiva la scansione anti-virus sul file. Per i primi 5 secondi (parametro modificabile) della scansione, HAVP non invia nulla al client a meno che la scansione non sia terminata. Dopo 5 secondi di scansione, se il file è di dimensioni superiori a 200KB (o del valore impostato) la prima parte dei dati viene inviata al client ad eccezione della parte bloccata che viene inviata solo dopo la fine della scansione e solo se non viene trovato un virus [fig. 5]. Appena viene trovato un virus, l'invio viene interrotto e la scansione terminata.

Ovviamente questa soluzione permette di velocizzare lo scaricamento di file particolarmente grossi, anche a rischio che parte o tutto il virus venga inviato al client. Il fatto però che l'ultima parte del file contenente il virus non venga mai inviata al client, forza il browser del client ad abortire il download ed a cancellare i dati scaricati. Nella peggiore delle ipotesi, il virus viene comunque scaricato sulla macchina del client, ma in un file incompleto e quindi difficilmente utilizzabile. Ovviamente, per ottenere la massima sicurezza si può impostare ad un valore molto alto la

2 Questo è comunque un parametro modificabile e può essere impostato uguale alla dimensione massima dei file da scansire, imponendo così che tutti i file siano bloccati interamente sino al termine della scansione anti-virus.

dimensione della parte del file da tenere bloccato in modo che nulla venga inviato al client prima del termine della scansione. Questo però rallenta notevolmente lo scaricamento di file di grandi dimensioni, quali documenti, immagini ecc.

Andrea Pasquinucci

pasquinucci@ucci.it

Riferimenti Bibliografici

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

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

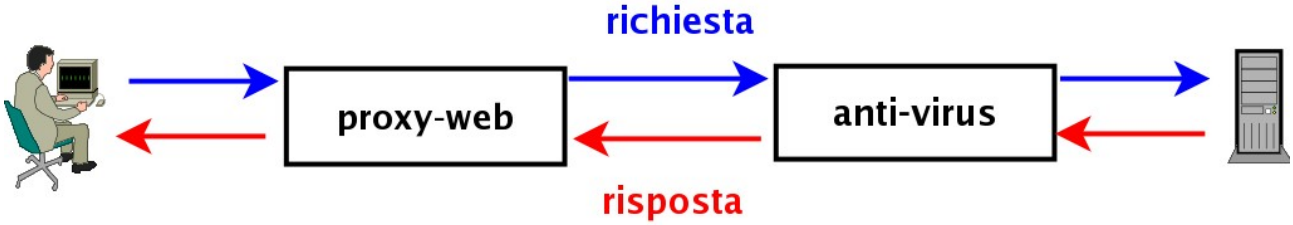

Fig. 1 Configurazione con AV a monte

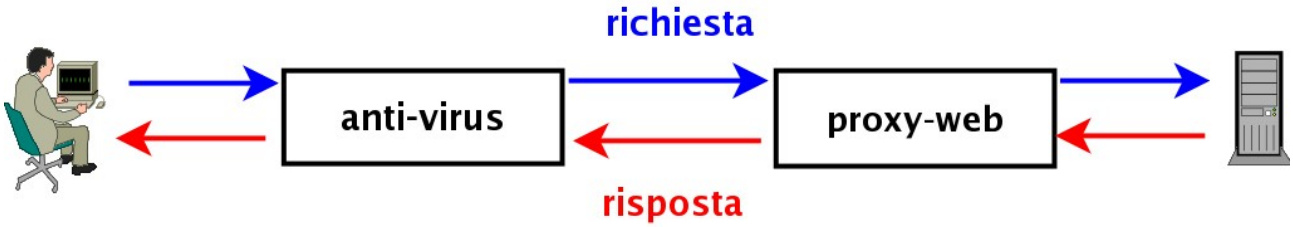

Fig. 2 Configurazione con AV a valle

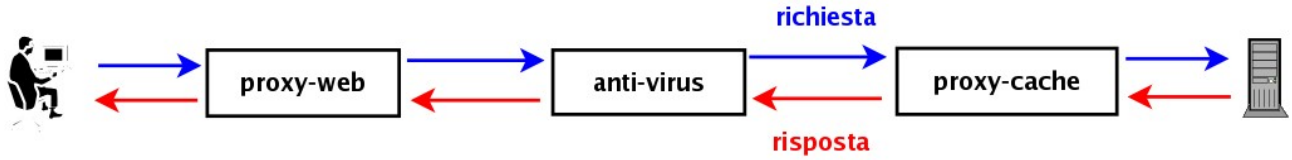

Fig. 3 Configurazione Sandwich

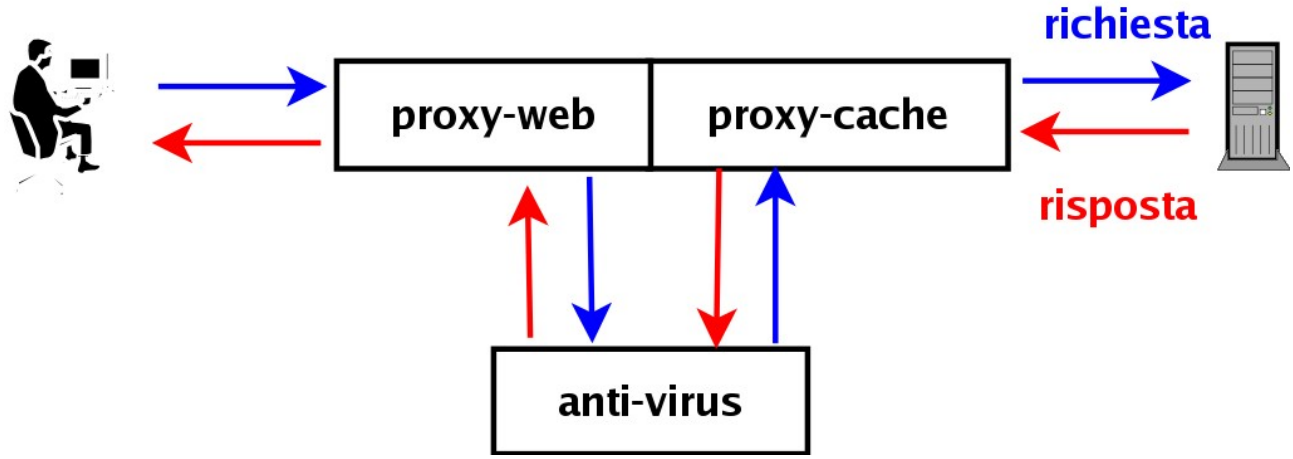

Fig. 4 Configurazione con AV helper del proxy

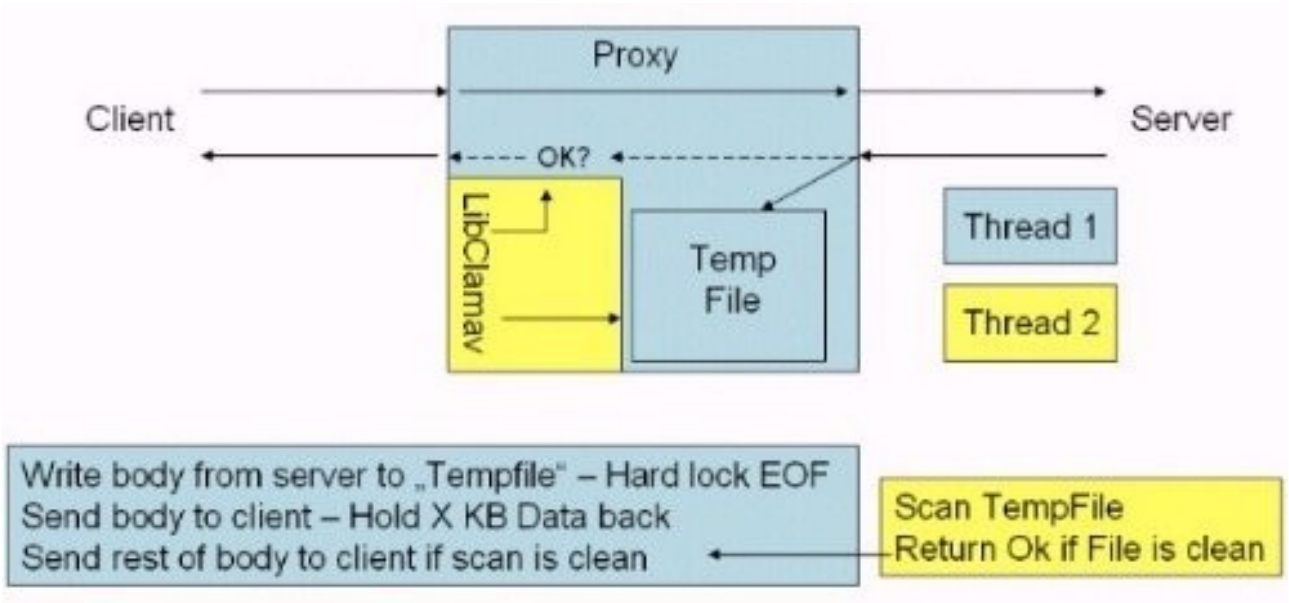

Fig. 5 Logica di HAVP