Da IDS a IPS

Nel numero 23 del Maggio 2004, avevamo già accennato alle problematiche di filtraggio del traffico in tempo reale e della relazione tra Intrusion Detection System (IDS) e Intrusion Prevention System (IPS). Oggi sembra che chi non ha un IPS nel proprio sistema di sicurezza di rete non sia al passo con i tempi.

Cercheremo quindi di capire cosa sia veramente un IPS e nel prossimo articolo vedremo come costruirne uno molto semplice utilizzando Snort.

Un'idea, un prodotto od una caratteristica tecnica?

Non esiste una vera e condivisa definizione di cosa sia un IPS, in pratica ogni Vendor ne da una interpretazione diversa. Se guardiamo al marketing dei prodotti di sicurezza, potremmo dire che un IPS è genericamente un tipo di firewall avanzato. In questa sede però ci interessano per lo più gli aspetti tecnici, quindi daremo di IPS una definizione tecnica ben precisa, che in molti casi però non coincide con quello che viene inteso da alcuni Vendor.

La nostra definizione di IPS è quella di *reactive-IDS*, ovvero un Intrusion Detection System in grado non solo di segnalare attacchi o traffico nocivo, ma anche di reagire automaticamente alle minacce. Anche se in parole la differenza tra IDS e reactive-IDS (o IPS) è minima, in pratica per realizzare un IPS di questo tipo bisogna riconsiderare completamente il concetto stesso di IDS perché altrimenti è molto facile realizzare uno strumento poco utile o con serie limitazioni di funzionamento.

Da IDS a IPS

Un Intrusion Detection System funziona principalmente in maniera analoga ad un anti-virus.[1] Un

1 Vi sono IDS non basati sulle *firme* degli attacchi ma ad esempio sul riconoscimento di traffico non usuale, in questa sede consideriamo solo il caso più semplice di IDS basati su firme.

IDS analizza i dati che gli vengono forniti e li confronta con un database, che deve essere mantenuto aggiornato, di *firme* (o regole), ovvero stringhe di caratteri o caratteristiche dei dati che sono ritenuti nocivi. Quando un IDS trova una corrispondenza tra una firma ed il dato che sta analizzando, la segnala emettendo un *Alert*, ovvero inviando un allarme alla *console* di gestione. L'allarme segnalato dall'IDS deve poi essere gestito da altre procedure, manuali od automatiche.

I dati su cui agisce un IDS sono i pacchetti, di norma TCP/IP, che attraversano una rete. Un IDS non si limita a considerare gli header dei pacchetti TCP/IP (lavorando quindi a livello 4 della pila ISO/OSI) ma considera il pacchetto nella sua interezza esaminandone anche i dati trasportati, lavorando quindi anche a livello 7 della pila ISO/OSI. Un sistema IDS è generalmente composto da alcune sonde, che svolgono il lavoro appena descritto e sono dislocate in punti strategici della propria rete, e di una console alla quale tutte le sonde inviano gli allarmi. Il lavoro di un IDS è molto oneroso, anche perché per non perdere pacchetti deve almeno in media essere in grado di svolgere il proprio compito alla stessa velocità della rete. Ad esempio, una sonda connessa ad un cavo FastEthernet sotto carico deve essere in grado di esaminare pacchetti ad almeno 80Mbps. Non solo, anche il sistema di reporting deve essere proporzionato in modo da poter ricevere e registrare gli allarmi in tempo reale, senza perderne o rallentare le sonde. Si noti che le sonde IDS di solito lavorano su *copie* dei pacchetti mentre i pacchetti originali proseguono il loro cammino, in questo modo non intralciando il traffico.

Un problema tipico degli IDS è la sensibilità delle regole utilizzate che spesso porta a molti falsi positivi, ovvero segnalazioni di pacchetti ritenuti nocivi che in realtà non lo sono. D'altra parte il non utilizzo di regole molto sensibili (o non sufficientemente precise da individuare univocamente un attacco) potrebbe aumentare il numero dei falsi negativi, ovvero di veri attacchi non rilevati. Nel caso di un IDS si cerca di compensare i falsi positivi con un analisi degli allarmi fatta alla console, cercando di eliminare quasi del tutto i falsi negativi usando tutte o quasi le firme a disposizione.

Se passiamo a considerare un reactive-IDS ci troviamo subito con un problema, quale azione deve essere effettuata automaticamente e dove? Il classico sistema IDS composto da molte sonde ed una

sola console per gli allarmi deve essere riconsiderato alla luce del problema di dove eseguire le azioni. Una possibilità è la seguente: associare ogni sonda ad un firewall e fare in modo che la rilevazione di un attacco da parte di una sonda abbia come reazione automatica la creazione di una regola sul firewall che impedisca il passaggio del traffico nocivo o anche solamente sospetto. A parte il problema di mettere la sonda a monte od a valle del firewall, questa soluzione ha molti problemi.
Per prima cosa, almeno il primo pacchetto nocivo sicuramente attraversa il firewall e giunge a destinazione, solamente i pacchetti successivi al primo possono essere bloccati dalla nuova regola sul firewall. Inoltre la creazione di una nuova regola sul firewall può portare al blocco di molto traffico lecito (sino al completo blocco del traffico, ovvero un attacco di Denial of Service auto-inflitto). Se la nuova regola immessa sul firewall è molto specifica, ad esempio indicando sia gli indirizzi sorgenti/di destinazione che le porte del traffico TCP, questa bloccherà solo una particolare connessione ed un secondo attacco di nuovo vedrà il primo pacchetto passare. Inoltre in questo modo il firewall si potrebbe velocemente riempire di un grandissimo numero di regole molto specifiche, il che può anche portare a notevoli rallentamenti dello stesso. D'altra parte se invece la regola inserita nel firewall è molto generica, ad esempio viene specificato solo l'indirizzo sorgente del pacchetto nocivo, molto traffico lecito proveniente da quell'indirizzo (si pensi a casi di grandi reti dietro NAT) può essere bloccato.
La soluzione a questo problema è di inserire l'IPS direttamente nel firewall. Consideriamo infatti un firewall stateful, che lavora sino al livello 4 della pila ISO/OSI e quindi non filtra il contenuto dei pacchetti. Possiamo aggiungere un IPS, ovvero una sonda IDS reattiva, direttamente sulla stessa macchina facendo in modo che i pacchetti che hanno già attraversato il firewall, e che quindi sono permessi dalle regole che implementano le politiche di sicurezza al livello 4, prima di uscire dalla macchina debbano attraversare la sonda IDS. Si noti come in questo caso la sonda lavori direttamente sul pacchetto e non su di una copia. La *reattività* della sonda IDS in questo caso è di *droppare*, ovvero cancellare il pacchetto e non permetterne l'uscita dal firewall. Il problema dell'inserimento delle regole nel firewall è evitato, poiché nessuna regola è inserita, e solo i pacchetti ritenuti no-

civi dall'IPS sono droppati, gli altri non nocivi, eventualmente anche appartenenti alla stessa connessione[2], possono attraversare il firewall+IPS.

Limiti di un IPS

Abbiamo appena visto che il nostro IPS riceve i pacchetti accettati dal firewall stateful (a livello 4), li confronta con le firme e droppa quelli che ritiene nocivi. Il problema dei falsi positivi degli IDS diventa molto preoccupante per gli IPS, infatti un falso positivo per un IPS vuol dire che una connessione lecita viene bloccata. E' necessario quindi utilizzare solo le firme che danno la massima garanzia di non avere alcun falso positivo, ma come abbiamo visto questo vuol dire non utilizzare firme di minore precisione e quindi avere un maggior numero di falsi negativi, ovvero di pacchetti illeciti non bloccati.

Se la modalità di funzionamento di un IDS è comunemente quella di limitare i falsi negativi accettando anche parecchi falsi positivi (falsi allarmi), un IPS al contrario deve limitare al massimo i falsi positivi accettando anche parecchi falsi negativi (attacchi non bloccati). Quindi da questo punto di vista IPS e IDS funzionano in modalità opposta.

Un altro problema dell'IPS è quello di lavorare sul pacchetto originale e non su di una copia come fa l'IDS. L'IPS deve svolgere anche parecchio lavoro per analizzare il pacchetto e confrontarlo con tutte le firme rilevanti, e quindi il pacchetto potrebbe essere trattenuto nell'IPS per parecchio tempo creando dei ritardi anche sensibili per l'utente nel caso di comunicazioni in tempo reale. Per ridurre i ritardi si possono adottare varie strategie: la prima è di implementare l'IPS con dell'hardware dedicato, la seconda di ridurre al minimo il numero di firme da confrontare, ed infine di selezionare solo alcuni tipi di traffico per la scansione dell'IPS.

Ad esempio potremmo decidere di non far scansire dall'IPS il traffico di posta elettronica poiché comunque tutti i messaggi di posta elettronica passeranno successivamente attraverso l'anti-virus e l'anti-spam. Meglio ancora, possiamo decidere di far scansire dall'IPS solo il traffico web, ovvero

2 Volendo l'IPS può anche bloccare l'intera connessione a cui appartiene un pacchetto illecito, opzionalmente inviando un Reset al mittente/destinatario per cercare di bloccare il flusso dei dati.

quello in porta 80, usando solo firme relative a possibili attacchi a server o client http. In questo modo possiamo fare una selezione molto accurata del tipo di traffico da scansire e delle firme da confrontare, limitando al massimo i ritardi introdotti dall'IPS e la possibilità di falsi positivi, ovvero blocco di traffico lecito.

Un IPS in pratica

Ora che abbiamo visto come funziona il nostro IPS, ci possiamo chiedere a cosa veramente ci può servire. Certamente non ci serve per sostituire il firewall, i proxy/ALG, gli anti-virus/anti-spam eccetera. Ma allora a cosa serve? Vi sono sicuramente alcune situazioni in cui un IPS può dare un contributo alla sicurezza del nostro sistema informatico. Consideriamo sempre il caso di un IPS che controlli il traffico http e che aggiorni ogni poche ore il database delle firme (come un qualunque anti-virus). Questo IPS sarebbe in grado di bloccare un worm come *code-red* appena scaricata la relativa firma e proteggere il server web sino all'installazione della patch di sicurezza. Infatti nel caso di vulnerabilità gravi del software, ad esempio un server http, è difficile che gli altri elementi della infrastruttura di sicurezza siano in grado a priori di bloccare l'attacco, che a loro di solito appare come traffico lecito.

Un'altra simile applicazione di un IPS è a protezione di una applicazione *legacy* con vulnerabilità note ma non eliminabili[3] e per le quali si possono creare firme apposite.

Concludendo, all'interno della infrastruttura di sicurezza di rete possiamo possiamo posizionare l'IPS tra il firewall stateful a livello 4 ed i proxy/ALG (quali anti-virus/anti-spam ecc.) a livello 7. Come abbiamo visto un IPS non sostituisce un IDS che rimane un elemento di controllo del traffico nella propria rete. Inoltre possiamo pensare a due diversi utilizzi di un IPS: il primo un IPS generalista, che analizza tutto il traffico confrontandolo con le firme dei più pericolosi attacchi in atto al momento, il secondo un IPS specialistico che filtra solamente il traffico di un certo tipo, ad esempio http, lavorando prima del relativo proxy (vedi figure 1 e 2).

3 Questo caso è purtroppo troppo frequente nella realtà dei sistemi informativi aziendali.

Andrea Pasquinucci

pasquinucci@ucci.it

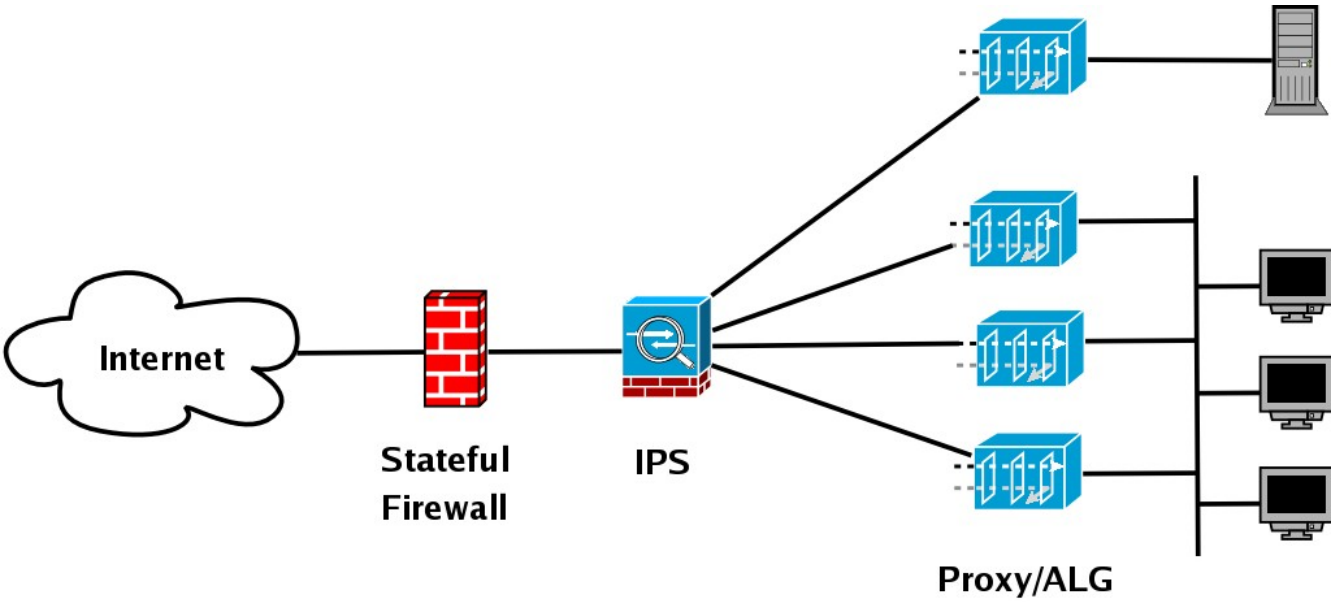

Figura 1. Schema logico di posizionamento di un IPS 'generalista'

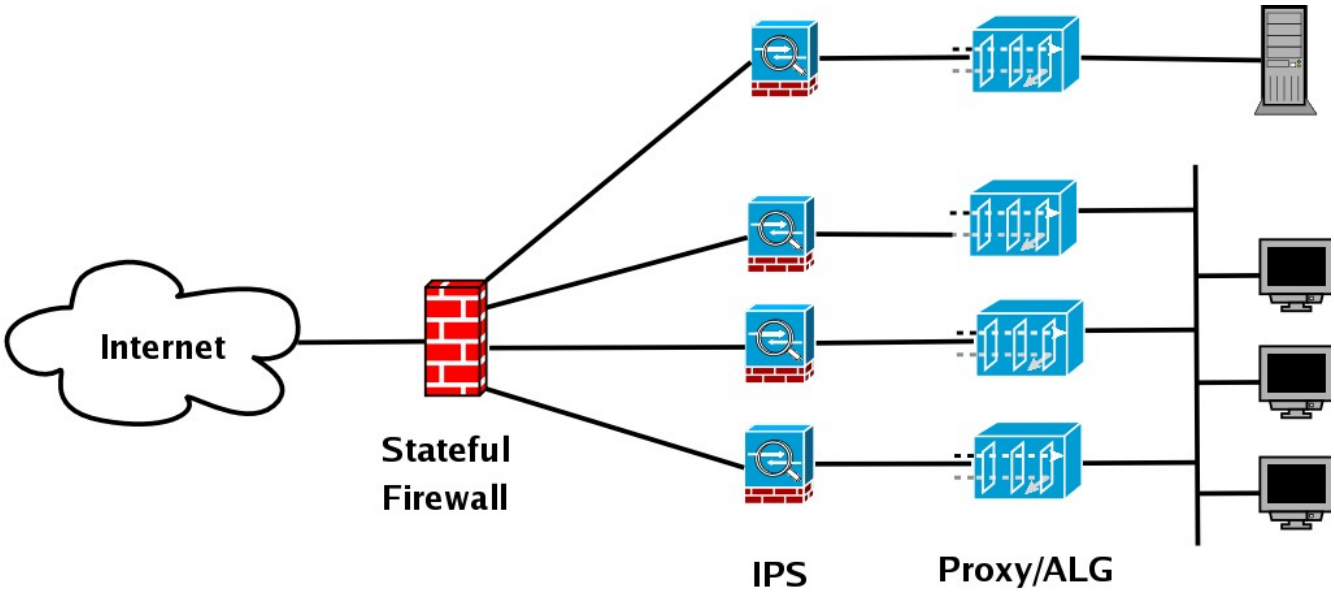

Figura 2. Schema logico di posizionamento di IPS 'specialistici'