Maggiore sicurezza nelle reti

DAVID CHU*

Motori di ricerca di rete in applicazioni VPN

La rete non è più sicura come un tempo. Collegarsi alla rete di ufficio da un sito remoto non è più così facile. Non lo è neppure collegare tra loro due reti remote, in modo sicuro e affidabile. Garantire la sicurezza dei dati trasmessi in rete è importante tanto quanto garantire la sicurezza di una rete privata contro eventuali attacchi di malintenzionati. Le reti private virtuali (VPN, Virtual Private Networks) sono state sviluppate proprio per rispondere alle esigenze di chi ha bisogno di collegamenti remoti affidabili e sicuri. Si tratta di reti che spesso utilizzano protocolli di crittografia e codifica, per garantire la validità e l'origine dei dati trasmessi in una rete pubblica. Uno di questi protocolli, Internet Protocol Security (IPSec), verrà discusso nel corso di questo articolo. Tuttavia, protocolli di sicurezza di questo tipo aggiungono un'ulteriore complicazione alla rete che proteggono. È necessario effettuare svariate operazioni di classificazione, a livello dei singoli pacchetti, ad entrambi i capi della rete, per determinare in che modo codificare o decodificare un pacchetto. Questo compito, piuttosto oneroso, deve essere svolto dal sottosistema di ricerca, che è parte integrante della soluzione utilizzata per l'elaborazione dei pacchetti. Oggi la maggior parte delle operazioni di classificazione sono gestite dal sottosistema di ricerca, collegato al processore di pacchetti. Il sottosistema di ricerca può essere un motore di ricerca di rete (NSE, Network Search Engine) di tipo TCAM o un banco di memoria (SRAM, DRAM) utilizzato per memorizzare i dati. Quando un pacchetto transita dalla sezione che si occupa dell'elaborazione dei pacchetti, in una scheda di linea, è necessario eseguire la classificazione in tempi estremamente rapidi, per determinare la natura del pacchetto.

Nel mondo IPSec le politiche e le modalità di collegamento tra i nodi di rete sono definite da due tipi di tabella del sottosistema di ricerca: il cosiddetto security association database (SAD) e il security protocol database (SPD). L'header dei pacchetti che devono essere inviati lungo una connessione di rete sicura (network ingress) dovrà essere analizzato dallo SPD per determinare il tipo di protocollo di sicurezza da applicare. I pacchetti che seguono il percorso inverso (network egress) dovranno essere analizzati dal SAD, che deve determinare la bontà del collegamento e il tipo di protocollo di sicurezza necessario per decrittografare il pacchetto. Le chiavi di ricerca sono lunghe tipicamente 128 - 144 bit. Queste due operazioni di ricerca, di per se stesse, non comportano alcuna difficoltà anche a frequenze di trasmissione di 10G, tanto nel caso di soluzioni hardware che software. Tuttavia la tendenza ad evolvere verso funzionalità di tipo IPv6 e VNP nei gateway di rete dei fornitori di servizi, aggiunge un ulteriore livello di complessità al problema. L'adozione di IPv6 implica un aumento delle dimensioni degli header utilizzati per l'identificazione dei pacchetti, che raggiungono una larghezza sempre crescente (l'identificatore IP di destinazione passa da 32 a 128 bit).

SISTEMI SOFTWARE PER LA CLASSIFICAZIONE

Per parecchio tempo, nella classificazione dei pacchetti di rete sono stati utilizzati algoritmi di tipo software. Sebbene ne esistano in circolazione una grandissima varietà, la maggior parte ricadono nella categoria degli algoritmi di tipo tipo m-trie o hashing implementation. Gli algoritmi m-trie operano su un "trie" che è costruito dinamicamente in base alle entries della struttura. Normalmente vengono utilizzate delle implementazioni "hashing" per ridurre il numero di bit dell'header di pacchetto da analizzare, riducendoli a un numero gestibile, tramite meccanismi di manipolazione aritmetica (come il checksum). In questo modo è possibile memorizzare un numero di entries relativamente elevato in una memoria di dimensioni sufficientemente ridotte.

COME MIGLIORARE QUALCOSA CHE DÀ GIÀ BUONI RISULTATI

Le prestazioni di un'operazione possono variare notevolmente, in base all'algoritmo e alle dimensioni della memoria utilizzata per implementare il database. Nella maggior parte dei casi saranno comunque di natura non deterministica, poiché è necessario risolvere differenti situazioni di match o collisione. Le collisioni sono prevalenti soprattutto nelle applicazioni IPSec quando lo SPD lookup genererà, in base alla configurazione d'utente, un numero variabile di indifferenze nella chiave di ricerca, ottenendo come risultato molti hits o operazioni parallele di lookup. È in questo caso che torna utile un NSE. Gli NSE sono sistemi basati su TCAM, utilizzati per classificare i pacchetti paragonando simultaneamente una chiave di ricerca con tutte le entries di un database. Questi sistemi hanno un'elevatissima velocità di ricerca (fino a centinaia di milioni di ricerche al secondo) e una latenza decisamente ridotta e deterministica. L'architettura parallela di questi dispositivi permette di effettuare operazioni di ricerca back-to-back senza che sia necessario attendere il risultato di una ricerca prima di iniziare quella successiva. In questo modo il progettista di sistema può prevedere meglio il numero dei buffer di pacchetto e la latenza complessiva dei pacchetti in un sistema. Gli NSE rappresentano un sistema di classificazione ad alte prestazioni. Permettono all'utente di analizzare i pacchetti anche a frequenze di trasmissione di linea decisamente veloci. Si tratta di sistemi molto adatti per applicazioni in cui la sicurezza, la gestione delle politiche (policy) e la classificazione vengono effettuate simultaneamente, senza richiedere operazioni algoritmiche complesse da parte del processore. Tuttavia, anche con l'elevata frequenza di ricerca resa disponibile da un NSE, vi sono applicazioni, soprattutto quelle di forwarding di pacchetto, che utilizzano soluzioni algoritmiche, che hanno il vantaggio di permette un compattamento delle entries. Una soluzione NSE non sempre è ottimale, ma deve essere considerata una possibile alternativa ai processi tradizionali di classificazione. ■

*David Chu (DCU) - Kong Hoei Susanto (KHS)