Università degli Studi di Milano Bicocca
Scuola di Scienze
Dipartimento di Informatica, Sistemistica e Comunicazione
Corso di Laurea Magistrale in Informatica

Sistemi e Servizi di Telecomunicazione

Prestazioni dei firewall realizzati con appliance dedicate: Dipendenza dal numero di regole e ottimizzazioni

Autore:
Michele Salanti 793091

Anno Accademico 2019–2020

Indice

Capitolo 1

Introduzione

1.1 Firewall

Un firewall è un dispositivo di rete solitamente interposto tra due reti per filtrare il traffico tra loro secondo una certa politica di sicurezza. Un firewall fornisce protezione eseguendo controlli basati su regole ai pacchetti. I firewall possono essere hardware, software od una combinazione dei due. Un firewall hardware può essere un componente di un dispositivo dedicato od un componente di un router a banda larga:

- Un ***firewall hardware*** è in genere implementato sul gateway principale che collega una rete interna protetta e il resto della rete.
- Un ***firewall software*** è un software in esecuzione su un computer, che protegge il suddetto computer limitandone i tentativi esterni di accesso.

I firewall hardware tendono ad offrire una protezione e delle prestazioni migliori rispetto ai firewall software. Essi possono avere funzioni di filtraggio di pacchetti in modalità stateless a vere e proprie applicazioni stateful:

- I filtri ***stateless*** di pacchetti applicano regole di filtro per accettare o rifiutare singoli pacchetti senza esaminare la relazione tra di loro. Il filtraggio dei pacchetti senza stato fornisce un controllo meno efficace ma al contempo mostra prestazioni elevate.
- Le applicazioni ***stateful*** applicano meccanismi di sicurezza a specifiche applicazioni tenendone traccia dei vari stati. Il controllo specifico di un'applicazione è piuttosto efficace, al costo però di una sensibile degradazione generale delle prestazioni rispetto ad un filtro stateless.

1.2 Motivazioni

Nonostante i vantaggi, i firewall hardware presentano tre principali inconvenienti:

- I firewall hardware sono spesso *costosi*.
- I costi di manutenzione e aggiornamento dei firewall hardware sono in genere associati a configurazioni complicate e specifiche del fornitore.

- L'interoperabilità tra i firewall hardware realizzati da diversi fornitori non può sempre essere facilmente raggiunta.
- I guasti sui firewall hardware possono comportare la sostituzione e la riconfigurazione di più unità hardware al fine di garantire una politica coerente su una rete.

Questi inconvenienti potrebbero essere alleviati sostituendo i firewall hardware con alternative flessibili ed a basso costo; il paradigma di rete emergente SDN (Software Defined Networking) è un buon candidato.

I firewall hardware orientati a SDN sono in grado di preservare alte prestazioni sul traffico e consentire un controllo estremamente flessibile sul traffico.

Pertanto, le normative sul traffico possono essere eseguite su un gran numero di switch SDN-oriented senza incorrere in elevati costi di manutenzione.

In questo testo ci baseremo sul prototipo di un firewall hardware SDN-abilitato (con stati) e che fa uso di OpenFlow come protocollo di comunicazione. Ci focalizzeremo dell'impatto che può avere sulle prestazioni il numero di regole applicate su di un firewall e parleremo delle pratiche da adottare (o da evitare) per ridurre il più possibile questo impatto.

In sostanza questo lavoro si baserà principalmente sulle ricerche del team di Collings[1] e di Khaled[2].

Capitolo 2

Implementazione

2.1 Struttura

Il firewall controller può potenzialmente essere posizionato in un qualsiasi punto della rete. Le regole sono specificate nella tabella di flusso che sono gestite sia dallo switch che dal firewall controller (vedi tabella 2.1). Una voce nella tabella di flusso corrisponde ad una regola che gestisce il flusso del traffico. Lo switch agisce come un banale inoltratore di pacchetti basato sulle regole di sicurezza definite nella sua tabella di flusso. Il firewall controller utilizza la sua tabella di flusso per tenere traccia delle decisioni intraprese sul traffico.

Un canale di comunicazione dedicato viene mantenuto tra lo switch e il controller del firewall. Attraverso questo canale, lo switch invia le informazioni sui flussi di traffico non identificati al controller per l'ispezione e il controller invia le decisioni allo switch.

Interface	Src. MAC	Dst. MAC	Network Type	Src. IP	Dst. IP	Layer 4 Protocol	Src. Port	Dst. Port	Action
*	*	*	*	*	*	UDP	*	*	Out on port 2
Port 4	*	*	IP	192.168.10.0/24	*	TCP	13576	80	Send to ctrl
*	*	*	*	*	*	*	*	*	Drop

Figura 2.1: Esempio di Tabella di Flusso (Flow Table)

2.2 Modalità Permissiva e Restrittiva

Sono state presenti due modalità per specificare le azioni di controllo predefinite in base al traffico:

- ***Modalità permissiva:*** rifiuto selettivo dei flussi. Ossia che il traffico viene normalmente inoltrato di default a meno che non venga esplicitamente negato.

- ***Modalità restrittiva:*** autorizzazione selettiva dei flussi. Ossia che il traffico viene negato di default a meno che esplicitamente consentito.

2.3 First Deny Last Allow

Un controller firewall adotta una metodologia *"first deny last allow"* per determinare un'azione di controllo su un flusso.

Un controller privilegia flusso che "matcha" (corrisponde) ad una regola di rifiuto (deny rule) rispetto a una regola di permissiva (allow rule). La precedenza delle regole di rifiuto sulle regole di consenso allevia il rischio per la sicurezza derivante da regole potenzialmente in conflitto nella tabella di flusso del controller ed anche evita che i pacchetti debbano percorrere un'intero set di regole prima di essere scartati.

2.4 Posizione delle regole: Valutazione delle performances

In seguito verranno brevemente presentate le prestazioni di un firewall di rete basato su regole. In genere, e come mostrato nella Figura 2.3b1, i pacchetti in entrata che trasportano richieste arrivano al firewall e vengono messi in coda per l'elaborazione in più fasi:

1. La prima fase prevede l'esecuzione di funzionalità di collegamento dati e livello di rete.
2. Successivamente viene attivato il motore di ricerca delle regole del firewall per elaborare i pacchetti in entrata.

Salah cita da un'altra fonte [2] che è stato dimostrato che le regole in fondo alla tabella possono essere scoperte da un aggressore esterno. Un utente malintenzionato può quindi lanciare un attacco che prenda di mira principalmente le regole di in fondo alla tabella e degradi efficacemente e rapidamente le prestazioni di un firewall con una serie di attacchi DoS a basso volume di traffico. Questo tipo di attacco viene chiamato "attacco di complessità algoritmica" (Complexity-algorithmic attacks), è una classe di attacchi DoS a bassa velocità che sfruttano le carenze algoritmiche nella progettazione del software [2].

Risulta quindi importante capire che impatto possono avere questi attacchi sulle prestazioni dei firewall in modo da trovare modi per mitigare il problema.

2.4.1 Misure prese

Il tema di Salah ha effettuato le misurazioni sottoponendo il firewall a due tipi di traffico: traffico normale e traffico DDoS indirizzato a regole diverse situate in posizioni diverse nell'insieme di regole del firewall.

In base all'hardware a disposizione del team è stato misurato che:

- Il valore medio era di circa 0,5 ms per l'interrogazione di 10.000 regole, ossia 0,05 microsecondi per singola regola.
- Il tempo medio di elaborazione del kernel del driver del dispositivo e dell'elaborazione IP ed è stato riscontrato che il valore medio è di circa 2,65 microsecondi.

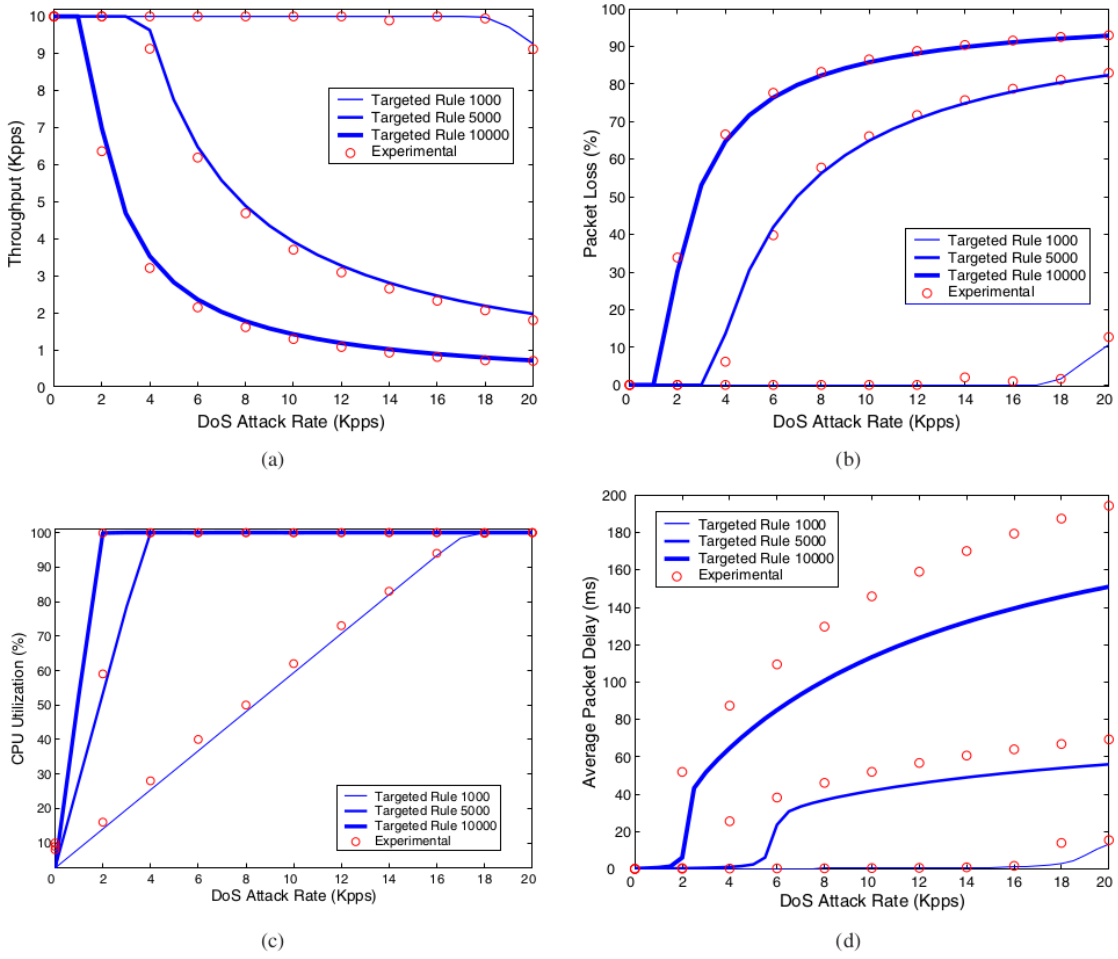


Figura 2.2: L'impatto dei flussi di traffico DoS che colpiscono diverse regole sul firewall

La Figura 2.2 mostra l'impatto sulle prestazioni che il firewall subisce quando si lanciano attacchi DoS con velocità diverse che colpiscono posizioni diverse delle regole. L'impatto è stato misurato

facendo in modo che venga generato un normale flusso di traffico UDP costante a una velocità di 10 Kpps.

Abbiamo misurato il degrado delle prestazioni in termini di perdita di pacchetti (packet loss), velocità effettiva, utilizzo della CPU e ritardo unidirezionale quando si invia traffico normale e quando si sottopone il firewall a flussi di attacchi DoS di velocità diverse e prendendo di mira regole diverse.

2.4.2 Osservazioni

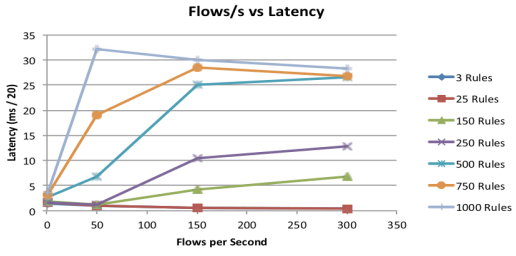
Dai grafici mostrati in Figura 2.2 emerge chiaramente che un leggero degrado si manifesta quando gli attacchi DoS prendono di mira le regole più importanti (quelle in cima), mentre un notevole degrado si manifesta quando gli attacchi DoS colpiscono regole meno importanti (quelle in fondo) come quelle posizionate a 5.000 e 10.000. Più specificamente, quando si prendono di mira le regole meno importanti, si può osservare un degrado grave e evidente con attacchi DoS a velocità relativamente bassa di circa 1 Kpp e 3 Kpp quando si prendono di mira regole posizionate rispettivamente a 10.000 e 5.000. Tuttavia, quando si prende di mira una regola posizionata a 1000, il degrado si manifesta solo con attacchi DoS ad alta velocità di circa 18 Kpps.

Pertanto, si può concludere che le regole di targeting nella parte inferiore del set di regole possono essere gravemente dannose per le prestazioni del firewall. Le prestazioni del firewall sono accettabili quando gli attacchi DoS (fino a una velocità di 18 Kpps) mirano a regole posizionate intorno a 1.000, ma non a regole superiori.

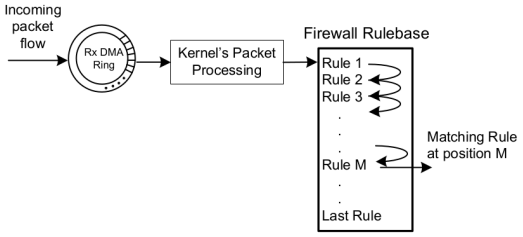
2.5 Conotroller: Valutazione delle performances

Nella valutazione, il team di Collins fa uso di una configurazione restrittiva con insiemi di regole composte completamente da regole permissive (allow rules). Ciò rappresenta il caso di regole base peggiore perché il controller del firewall è costretto a tentare di accettare ogni flusso di traffico non identificato.

Il numero di regole nelle configurazioni varia da un minimo di 3 a un massimo di 1000.



(a) Crescita della latenza media



(b) Schema di interrogazione delle regole del firewall per i pacchetti in arrivo

Dal grafico 2.3a si osserva che la latenza media aumenta linearmente con il tasso di arrivo di nuovi flussi di traffico quando la dimensione del set di regole è 150. Le latenze medie mostrano improvvisi aumenti di latenza con un numero più alto di arrivi di flussi quando le dimensioni del set di regole è a 250 e 500. La latenza media smette di crescere quando il set di regole è a 750 e 1000.

Questa interruzione di crescita, secondo Collins può essere dovuta principalmente a due motivi:

1. Molti nuovi flussi di traffico hanno pattern molto simili, quindi dopo un iniziale processamento da parte del controller le regole per quel pattern vengono applicate allo switch. Questa cosa viene osservata spesso in molti flussi di traffico di un gateway principale dove per esempio, molte connessioni Web tentano di visitare lo stesso insieme di server (per esempio portali di News molto frequentati).

2. Molti flussi vengono scartati (dropped) a causa dello spazio di coda limitato per contenere i pacchetti dei flussi non identificati quando i tassi di arrivo dei flussi sono elevati. La latenza media mostrata in tabella non copre i flussi persi.

Capitolo 3

Note Finali

Il team di Salah ha dimostrato che le regole di targeting nella parte inferiore (in basso) di un set di regole relativamente ampio possono essere gravemente dannose per le prestazioni di un firewall. Come buona pratica di progettazione e contromisura vitale contro gli attacchi DoS che prendono di mira le regole in fondo al set, il team consiglia di ridurre al minimo le dimensioni del set di regole del firewall o di riorganizzare dinamicamente le regole in modo che le regole più in basso possano essere spostate nella parte superiore del set di regole, rendendolo così più difficile lanciare attacchi algoritmici di tale complessità che colpiscono le regole inferiori.

Il lavoro del team di Collins, a parere dell'autore di questo testo, sembra in parte inconclusivo su questo fronte, ma mostra chiaramente l'impatto della dimensione del set di regole sulle prestazioni d un firewall ed accenna (o da una breve introduzione) a problematiche nuove introdotte dal paradigma SDN che vengono approfondite da ricerche come quella del team di Shin [3] e dal team di Porras [4] (in breve: Garbage collection delle regole mandate agli switch ed ottimizzazione e risoluzione di conflitti).

Oltretutto, ***come nota personale***, l'autore di questo testo si sente di aggiungere che la metodologia *"first deny last allow"* descritta da Collins ed usata anche dal team di Bakker [5] può essere una buona tecnica da tenere in mente quando si progettano set di regole di un firequall, indipendentemente che sia SDN-based o meno. Questo, oltre a conferire un ovvio vantaggio sulla mantenibilità da parte degli amministratori di rete, permette anche di garantire prestazioni ottimali dovuto ad un set ridotto di regole.

Bibliografia

[1] Jake Collings and Jun Liu. An openflow-based prototype of sdn-oriented stateful hardware firewalls. In *2014 IEEE 22nd International Conference on Network Protocols*, pages 525–528. IEEE, 2014.

[2] Khaled Salah, Khalid Elbadawi, and Raouf Boutaba. Performance modeling and analysis of network firewalls. *IEEE Transactions on network and service management*, 9(1):12–21, 2011.

[3] Seung Won Shin, Phillip Porras, Vinod Yegneswara, Martin Fong, Guofei Gu, Mabry Tyson, et al. Fresco: Modular composable security services for software-defined networks. In *20th Annual Network & Distributed System Security Symposium*. Ndss, 2013.

[4] Philip Porras, Seungwon Shin, Vinod Yegneswaran, Martin Fong, Mabry Tyson, and Guofei Gu. A security enforcement kernel for openflow networks. In *Proceedings of the first workshop on Hot topics in software defined networks*, pages 121–126, 2012.

[5] Jarrod N Bakker, Ian Welch, and Winston KG Seah. Network-wide virtual firewall using sdn/openflow. In *2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 62–68. IEEE, 2016.