分散ファイアウォールにおける負荷の軽減

木下研究室　　大畑　嵩（201002678）

1　まえがき

セキュリティ対策としてファイアウォールは重要である. ファイアウォールの設置方法は集中型と分散型の 2 種類があり、分散型は柔軟で強固なセキュリティの実現ができ、セキュリティ強化として注目されているが、負荷による通信速度の遅延が問題となっている.

本稿では、スループットによる負荷の総和が最小となるルールチェーンを最適と定義し、負荷という観点からルールの削減、移動を行う. 分散環境下に属する各ファイアウォール間で遅延による負荷の大きさを求め、マッチング回数の多いルールを負荷の大きいファイアウォールから小さいファイアウォールへ移動する. また、上位層と下位層での共通ルールを上位層に配置することで下位層のルール数を削減しマッチング回数を減らす.

2　提案手法

2.1　ルールの統合

スループットとルール数の関係性の測定から、スループットはある行 K まではほぼ一定のスループットを保つことがわかる (図 1). しかしながら、K 行目以上のルールでマッチング処理が行われるとスループットは大きく低下する. ルールの統合を行うことは、ファイアウォールにかかる負荷の減少につながる.

ルール統合の際、統合の前後でセキュリティポリシーが変化しないように以下の条件を与える.

・プロトコル及び操作が同じである

・連続しているルールである

上記の条件を両方とも満たしたルール間でのみルールの統合を行うことができる.

ルールの統合には、Quine-McClaskey の方法を使用する. 論理式の加法標準形を IP アドレスと考えると、この手法を用いることで IP アドレスを基にルール数を削減できる.

2.2　上位層と下位層での共通ルール

分散環境下でのルールの移動はセキュリティポリシーの整合性の問題が起こると考えられる. 上位層と下位層間でのルールの受け渡しをすることによって、セキュリティポリシーを崩すことなく各ファイアウォールでのルールのマッチング回数を減少させることができる.

ルールの並び替えを行った後に、ルールの上下を比べることで、同じルール、同意義のルールを見つけられる。ここでルール統合の処理を行ってルール数自体を減らす.

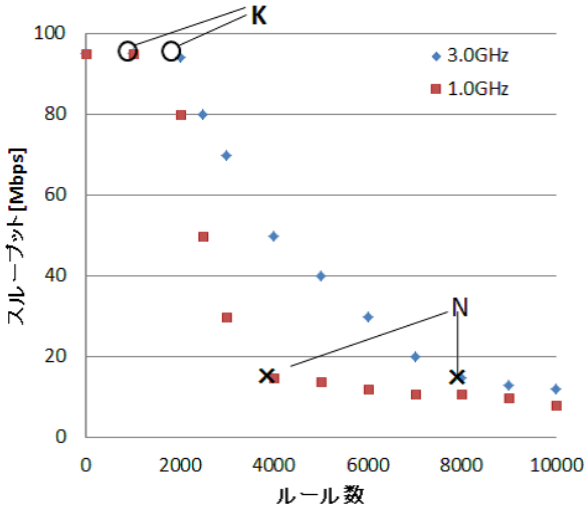

図 1: スループットとルール数の関係

2.3　ルールの移動

ファイアウォールの処理能力を x[GHz] としたとき、K 行目をスループットが落ち始める行番号、N 行目をスループットが低下しきって、低いスループットで一定値を取り始める行番号とする. この時、スループットの低下率 T が求められる.

$$T = \frac{|K_s - N_s|}{|K - N|} \tag{1}$$

K から N までの値を比較し値の大きいファイアウォールから小さいファイアウォールへルールを移動させる. ルールの移動を行うファイアウォールは (2) 式を基に選ぶ.

$$Y_i = \frac{1}{N-K} \sum_{i=K}^{N} M_i \cdot T \cdot i \tag{2}$$

・ルールチェーンの設定行番号 $i(1 \leq i \leq \mathrm{N})$

・各行におけるマッチング回数 $M_i(1 \leq i \leq \mathrm{N})$

スループットによる負荷の観点から、次式が最小になったとき、分散環境下での最適なルール配置と定義できる.

$$E = \sum_{j=1}^{s} Y_j \tag{3}$$

分散環境下のファイアウォールの数を $\mathrm{j}(1 \leq \mathrm{j} \leq \mathrm{s})$ とする.

2.4　実験・結果

iptables を用いてルールの並び替えを行い、同意義のルールを見つける動作を行うプログラムを作成した.(2) 式に基づいて、各ファイアウォールに返し、設定することで分散ファイアウォールの連携を行い、(3) 式の値が小さくなれば負荷は軽減したといえる.