分散ファイアウォールの連携

木下研究室　　国崎　大地 (200502780)

1　まえがき

現在、生活の一部としてネットワークは欠かせないものになった。その中で、外部ネットワークを通じて第三者の侵入による、データの盗み見・破壊などの被害が出ている。この様な被害を防ぐため、外部との境界を流れるデータを監視し、不正なアクセスを検出・遮断するシステムがファイアウォールである。

ファイアウォールの目的は、必要な通信のみを通過させ、不要な通信を遮断することである。上記のようなルールをファイアウォールに設定し、システムを実現させる。本稿では、仮想マシンを用いたネットワークを提案し、ファイアウォールのセキュリティーポリシー（ルール）をほかのファイアウォールと連携させることにより、全体としてのルール数を減らし、負荷の要因となるマッチング回数軽減によるファイアウォールの処理能力向上について考察する。

2　分散ファイアウォール

外部ネットワークとの境界のみにファイアウォールを設置する従来の集中型と呼ばれる方法では一箇所で制御しているので管理はしやすいが、部署ごとの異なるセキュリティーポリシーに対応できない、内部からの攻撃に対処できないなどの問題点がある。

上記の集中型に対して、外部ネットワークとの境界のみでなく内部ネットワークの部署単位でもファイアウォールを設置する方法を分散型と呼ぶ。分散型なら集中型で挙げた問題も解決できる上に、部署ごとに異なるセキュリティーポリシーを設定できるので柔軟で強固なセキュリティーを実現できる。

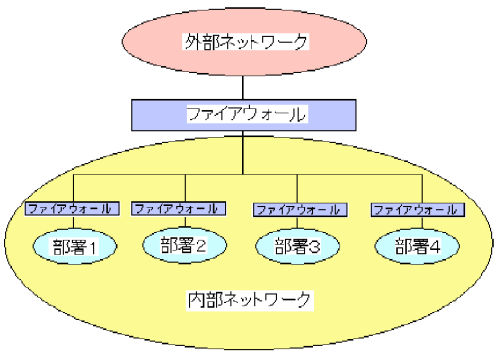

図 1: 分散型ファイアウォール

3　提案システム

ファイアウォールの処理能力に影響を及ぼす負荷の要因として、受信パケットのサイズ、送られて来たパケットと設定したルールとのマッチング処理、経路情報の増加、などが考えられる。本稿では、ルールとのマッチング処理に注目した。各ファイアウォールに設定するルール数を減らすことにより、ルールのマッチングの最適化に努め、ファイアウォールのメモリ使用量の軽減、パケットが通過する際の遅延時間減少が見込める。分散環境下にあるファイアウォールとその上にあるファイアウォールとの間でルールの受け渡しをすることによって、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事が出来る。ルール数とスループットは反比例の関係にあるため、ルール数が減少することで、各ファイアウォールのマッチング回数が減り、負荷の軽減につながる。

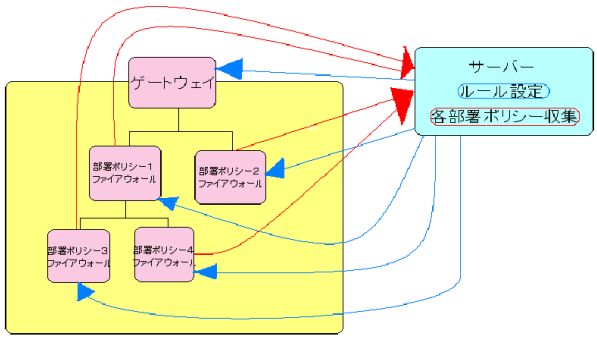

図 2: システム概要

3.1　ルール統合の手順

部署ごとのセキュリティポリシーを集める。
集めたセキュリティポリシーに基づいてルールの統合し最適化を行う。
最適化の論理式に基づいて各ファイアウォールにルールを返し、設定する。
部署ごとのセキュリティポリシーに変更があった場合は　～　をやり直す。

4　実装したネットワーク

本稿では２台のホストＰＣと４台のルータを用いて分散ファイアウォールの実装検証を行った。ネットワークの構築を容易にするためにホスト PC とルータの計６台を、仮想マシンモニター（QEMU）を用いて、１台の PC の仮想マシン上にまとめた。