修 士 論 文

ラベルスイッチング技術を用いたネットワークにおける ファイヤウォールの実現

指導教官　篠田陽一 助教授

北陸先端科学技術大学院大学
情報科学研究科情報システム学専攻

宇多 仁

平成 11 年 2 月 15 日

要 旨

本論文では、ラベルスイッチング・ネットワークにおいて、その特性を生かしたファイヤウォールの実現方法について提案する。ラベルスイッチング・ルータにおいては、その特性から、パケット・フィルタリング機能を効果的に提供する事が困難であった。そこで、本論文では、これを実現するための手法として、

- 擬似的なカットスルーを用いる方式
- フィルタリング処理をエッジ・ルータへ委託する方式

を提案し、議論する。さらに、これらの方式の応用方法等についても議論する。

目 次

図 目 次

表 目 次

第 1 章

序論

1.1 本研究の背景と目的

今日では、インターネットは非常に大規模なものへ拡大し、さらに、爆発的な勢いで拡大し続けている。インターネットの利用により、利用者は、世界中の情報にアクセスし、世界中に向けて情報の発信が可能である。インターネットは、世界的な超巨大情報メディアであると言える。

1.1.1 背景 1: 広帯域・低遅延ネットワークへの要求

インターネットで流通される情報は、その黎明期はテキストベースの電子メールや Net-News 等が中心であった。現在では、高画質の動画や音声を始めとする、より情報量の多いものも増えつつある。また、インターネットの即時性を利用した遠隔会議システム等に代表されるような双方向型の情報流通も増えつつある。このような情報流通が増えるにしたがって、エンド・ユーザ間での広帯域・低遅延の情報通信環境が求められている。

エンド・ユーザ間での広帯域・低遅延の情報通信を可能とする技術の 1 つとして、ラベルスイッチング技術が提案され、議論されている。

1.1.2 背景 2: ネットワーク上の情報や資源の保護への要求

世界的な情報流通媒体であるインターネットは、情報の汚染や破壊などにも利用できる脅威である。インターネットは、情報流通のための画期的なメディアとして利用者に恩恵を与えるネットワークであり、かつ、情報や資源の汚染や破壊に用いられ利用者に脅威を

与えるネットワークであるという 2 つの側面を持っている。このため、インターネット上におかれた情報や資源の保護が大きな課題となっている。

インターネットへ接続しつつ、自らの情報や資源を保護するための技術として、ファイヤウォールを構築する方法が多く用いられている。ファイヤウォールは、一定のセキュリティーを維持しつつ、ネットワークをインターネットへ接続するための 1 つの有効な保護手段である。

1.1.3 研究目的

広帯域・低遅延の情報通信環境下においても、情報や資源の保護が重要な課題である事は言うまでもない。ところが、先に述べたラベルスイッチング技術を用いて構築したネットワークは、そのネットワーク的特性からファイヤウォールとの親和性に乏しい。

そこで、本研究では、ラベルスイッチング技術を用いたネットワークにおいて、ラベルスイッチングの長所を生かしつつ、ファイヤウォールを実現することを目的とする。

1.2 本論文の構成

本論文は、全 10章から構成される。各章の内容は以下の通りである。

- 第 2章、第 3章では、ラベルスイッチング、ファイヤウォールそれぞれの技術について、個別にその概要を述べる。
- 第 4章では、ラベルスイッチング・ネットワーク上にファイヤウォールを構築する際の問題点を検討し、さらにその解決方法として 2 つの方式を提案する。
- 第 5章、第 6章では、第 4章で提案した解決方法について、その実現のための具体的手法、それぞれの方法の特徴などを詳しく述べる
- 第 7章では、本研究で行ったプロトタイプ実装について述べる。
- 第 8章では、本研究で提案した方式について性能改善・応用方法に関する議論を含めて考察を行う。
- 第 9章では、本研究での提案に対する今後の課題を述べる。
- 第 10章では、むすびとして本研究をまとめる。

第 2 章

ラベルスイッチング技術

インターネットでの情報流通において、高画質の動画や音声を始めとする、より情報量の多いものも増えつつある。また、インターネットの即時性を利用した遠隔会議システム等に代表されるような双方向型の情報流通も増えつつある。このような情報流通が増えるにしたがって、エンド・ユーザ間での広帯域・低遅延の情報通信環境が求められている。

エンド・ユーザ間での広帯域・低遅延の情報通信を可能とする技術の 1 つとして、ラベルスイッチング技術が提案され、議論されている。本章では、このラベルスイッチング技術について、その概要と特徴を述べる。

2.1 ラベルスイッチング技術の概要

ラベルスイッチング技術を用いたラベルスイッチルータは第 3 層のパケットの転送に、

- 従来の第 3 層アドレスを用いて転送する方法
- 第 3 層アドレス情報に対応させた固定長ラベルを用いて転送する方法

を併用する。

ラベルは、第 2 層のアドレス (ATM の場合は VPI/VCI、Ethernet 等の場合は MAC アドレス) に直接対応しており、固定長ラベルを用いた転送を行うことにより高性能パケット転送が実現できる。

従来の第 3 層アドレスを用いて転送する方法をホップ・バイ・ホップ状態での転送と呼び、固定長ラベルを用いて転送する方法をカット・スルー状態での転送と呼ぶ。それぞれについて、図 2.1で説明する。

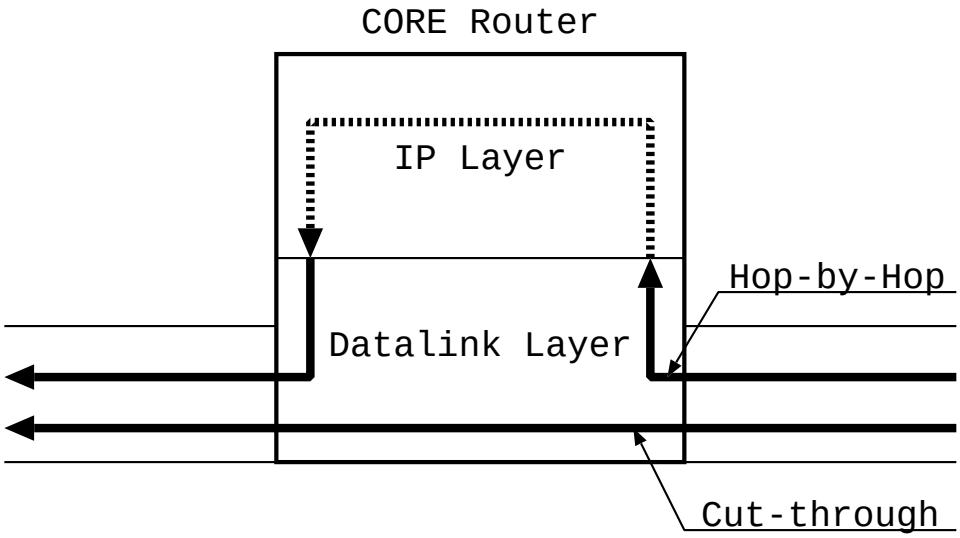

図 2.1: ホップ・バイ・ホップ状態とカット・スルー状態

ホップ・バイ・ホップ状態でのパケットの転送は、ルータの第 3 層の機能によって実現される。ルータでは、

1. 受け取ったデータグラムをパケットに再構成する。
2. パケットヘッダの宛先アドレスを用いてルーティングテーブルを検索し、出力すべきインタフェースを判断する。
3. パケットを再びデータグラム化し、適当なインタフェースへ出力する。

という手順によりパケットが転送される。これは、通常のルータにおけるパケット転送処理と全く同一である。

一方、カット・スルー状態でのパケットの転送は、ルータの第 2 層の機能によって実現される。ルータでは、

1. 受け取ったデータグラムのラベルより転送先を判断し、そのままデータグラムを転送する。

という手順によりパケットが転送される。この、第 2 層の処理のみでパケットが転送される経路をカット・スルー経路と呼ぶ。

カット・スルー状態でのパケットの転送処理は、ホップ・バイ・ホップ状態でのパケットの転送処理と比べ、処理内容が非常に単純である。このため、カット・スルー状態では、

広帯域・低遅延なパケットの転送が可能である。この、カット・スルー状態での転送こそが、ラベルスイッチルータの特徴と言える。

2.2 ラベルの割り当てトリガ

カット・スルー経路生成のトリガの違いにより、ラベルスイッチルータは 2 種類に大別できる。

2.2.1 トポロジ・ドリブン方式

トポロジ・ドリブン方式のラベルスイッチルータでは、経路エントリの生成をトリガとしてカット・スルー経路が生成される。カット・スルー経路の解放は、経路エントリの消滅時に行われる。

この方式では、パケットが流れる前に、既にカット・スルー経路が生成されているため、パケットは常にカット・スルー状態で転送される。しかし、この方式では経路エントリの数のラベルが必要となる。

2.2.2 フロー・ドリブン方式

フロー・ドリブン方式のラベルスイッチルータでは、特定の特徴を持つパケットの通過をトリガとしてカット・スルー経路が生成される。カット・スルー経路の解放は、該当カット・スルー経路に一定時間トラフィックが流れない時に行われる。

この方式では、カット・スルー経路が生成される以前のパケットは、カット・スルー状態での転送ができないために、ホップ・バイ・ホップ状態で転送を行わなければならない。しかし、この方式ではその時点で存在するフローの数だけしかラベルを必要としない。

2.3 ラベルの割り当て方針

ラベルの割り当て方針は、現在、以下のようなものが提案されている。

- TDP[1]で定義されているもの
  - ラベル割り当てトリガは、トポロジ・ドリブン方式

[1] Tag Distribution Protocol

  - 宛先ネットワーク毎にラベルを割り当てる。

- IFMP[2]で定義されているもの
  - ラベル割り当てトリガは、フロー・ドリブン方式
  - 発信元アドレスと宛先アドレスの組毎にラベルを割り当てる。
- FANP[3]で定義されているもの
  - ラベル割り当てトリガは、フロー・ドリブン方式
  - 発信元アドレスと宛先アドレスの組毎にラベルを割り当てる。

[2]Ipsilon Flow Management Protocol

[3]Flow Attribute Notification Protocol

第 3 章

ファイヤ・ウォール

3.1　ファイヤ・ウォールの必要性

インターネットは、統一的に管理されているネットワークではない。個々の組織の方針に基づいて運営されている自律ネットワークの集合体である。インターネット上の利用者は、組織にとって信頼できる者だけであるとは限らない。

このため、インターネットへの接続により、容易な情報の発信・享受が可能となる反面、情報の破壊などの攻撃を受ける危険にさらされる。そこで、インターネットに接続されているコンピュータを外界から守ることが必要となる。

組織内のコンピュータを、ネットワークを介した外界からの攻撃から守る方法として、大きく分けて次の方法がある。

- **物理的遮断**
  保護対象となるネットワークやコンピュータを外部ネットワークと物理的に接続しない。この方法は最も安全であるが、インターネットから何も恩恵は受けられない。

- **ホスト・セキュリティー**
  保護対象となる全てのコンピュータのセキュリティーを万全なものとする。この方法では、守らなければならないコンピュータの数が多いと多大な労力が必要となる。また、多くのコンピュータのセキュリティーを一定以上に保つことは容易ではない。

- **ネットワーク・セキュリティー**
  保護対象のネットワークと外部との間の通信に制限を加える。通信に制限を加えるためのシステム群を総称してファイヤ・ウォールと呼ぶ。この方法では、攻撃のた

めの通信は、ファイヤ・ウォールにより制限され、保護対象のコンピュータまでは到達しない。

どの方法を選択するかは、管理方針による。インターネットからの恩恵を享受しつつ、低い管理コストでセキュリティーが維持できるために、ファイヤウォールを構築する方法が広く使われている。

3.2 ファイヤ・ウォールの構成手法

ファイヤウォールの構築においては、次のような手法が主に用いられる。以後、特に断らない場合、「内部ネットワーク」とは保護対象のネットワークを、「外部ネットワーク」とは、それ以外、特にインターネットを指すものとする。

3.2.1 デュアルホーム・ホストを用いる方法

外部ネットワークと内部ネットワークの双方にインターフェイスを持つデュアルホーム・ホストで、「IP 転送機能」を禁止する事によりファイヤウォールを実現する。

この方法では、外部ネットワークと内部ネットワークの間で直接通信を行う事はできない。デュアルホーム・ホストは、サービスを proxy 化するか、利用者に直接デュアルホーム・ホストにログインさせる事によってのみサービスを提供する。

3.2.2 パケット・フィルタリングを用いる方法

パケット・フィルタリング機能はルータにより提供される。IP パケットには、パケットの始点・終点アドレスをはじめ、サービス等を識別するための情報が含まれる。パケット・フィルタリング機能を提供するルータは、各パケットについてこの情報を解析し、フィルタリング・ルールを適用することにより、内部ネットワークと外部ネットワークの間の通信を制限する。

フィルタリング・ルールは、組織のセキュリティー方針をもとに作成する。フィルタリング・ルールには、特定のアドレスやサービスに関するパケットの通過を許すかどうかを記述する。

パケット・フィルタリング機能は、利用者から見て透過的に設置される機能である。許可されているサービスを用いる限り、利用者はパケット・フィルタリングの存在を全く意識しなくてよい。また、利用者の理解を必要とせずに、ある程度のネットワーク・セキュリティーを実現できる。

しかしながら、パケット・フィルタリング機能は万能ではない。パケット・フィルタリングでは、特定のサービスに関するパケットの通過を制御するだけである。サービス内の個々の操作の制限は困難である。この問題に対し、Proxy サービスと組み合わせて用いるという方法が多く用いられる。

3.2.3 proxy サービス

proxy サービスは、内部ネットワーク上の利用者と外部サービスとの間に、ある程度透過的に設置されるサービスである。proxy サービスは、利用者とインターネット・サービスとの間の通信を中継する。

利用者の要求は、proxy サービスによって中継されるため、その中継を制御する事も可能である。proxy サービスにおいて、セキュリティー方針に基づいた要求の処理が可能である。これは、パケット・フィルタリングでは困難であった、サービス内の個々の操作の制御が可能である事を意味する。

proxy サービスは、先に述べたデュアルホーム・ホストを用いる方法やパケット・フィルタリングを用いる方法と組み合わせて利用する。

3.3 パケット・フィルタリング

実際のファイヤウォールの構築では、パケット・フィルタリング機能が必要不可欠である。このことから、ファイヤウォールを構築するにあたり、パケット・フィルタリング機能を有するルータは、重要な地位を占める。

ルータの主要な動作は、パケットを受け取り、終点アドレスをもとに経路表を索き、適切なインターフェイスへ出力する事である。パケット・フィルタリング機能を提供するルータでは、この通常の動作に加えて、

1. パケットの特徴解析
2. フィルタリング・ルールの適用

を行う。

3.3.1 パケットの特徴解析

パケット・フィルタリング機能を提供するルータにおいては、IP 層でのパケット転送処理の過程で、パケットの特徴解析を行う。これは、パケット内の IP ヘッダや、上位プ

ロトコルのヘッダから、

- パケットの始点アドレス
- パケットの宛先アドレス
- IP フラグメント情報
- IP オプション
- 上位プロトコル種別
  - ICMP
    - ICMP メッセージ・タイプ
  - TCP
    - TCP 始点ポート番号
    - TCP 宛先ポート番号
    - TCP フラグ群
  - UDP
    - UDP 始点ポート番号
    - UDP 宛先ポート番号
- 入力インターフェイス
- 出力インターフェイス

などの情報を抽出するものである。

3.3.2 フィルタリング・ルールの適用

パケットの特徴解析によって得られた、各種情報にフィルタリング・ルールを適用する。フィルタリング・ルールは、あらかじめ管理者によってセキュリティー方針に従って設定される。フィルタリング・ルールは、基本的には、パケットの特徴に応じた転送の許否の設定の集合である。

ルータによっては、さらに高度なパケット・フィルタリング機能も持つ。基本的なパケット・フィルタリングでは、処理はパケット毎に行われ、パケット間の因果関係はない。

高度なパケット・フィルタリング機能では、非コネクション型の通信 (UDP など) やレイヤ違反のプロトコル (ftp など) について、パケットの詳しい内容や前後関係をもとにした動的なフィルタリングも可能である。

しかし、パケットフィルタリング機能を実現する上で、最も基礎となる技術は、パケットの特徴解析とパケット転送の制御である。特徴解析が可能であれば、解析結果にフィルタリング・ルールを適用しパケット転送を制御できる。パケットの内容解析やパケット転送の制御が不可能な場合、パケット・フィルタリングは実現できない。

第 4 章

ラベルスイッチングとファイヤ・ウォール

高速ネットワークへの対応としてラベルスイッチング技術が注目されている。内部ネットワーク、外部ネットワーク共にラベルスイッチング・ネットワークとなれば、ラベルスイッチング・ネットワーク上でのファイヤウォール構築技術が必要である。しかしながら、ラベルスイッチング・ネットワーク上での効率的なファイヤウォールの構築手法については、研究されていない。

4.1 ファイヤ・ウォールを実現する上での課題

前章で述べたように、ファイヤウォール実現のためにデュアルホーム・ホストを用いる方法がある。この方法においては、全ての通信は、アプリケーション層での中継により行われるため、ラベルスイッチング・ネットワークを用いている事を意識する必要はない。しかし、デュアルホーム・ホストのみでファイヤウォールを構築する事は稀である。

一方、パケット・フィルタリングを用いる方法では、

- ラベルスイッチング・ネットワークにおいては、カット・スルー状態では、ラベルをもとに第 2 層におけるデータグラム転送を行う。
- パケットフィルタリングを行うためには、第 3 層以上の情報を用いて、パケットの転送を制御しなくてはならない。

という双方の特徴から実現が難しい。(図 4.1)

これは、カット・スルー状態で第 2 層におけるデータグラム転送が行われると、流れるパケットの内容解析、そして、転送の制御が全くできないためである。

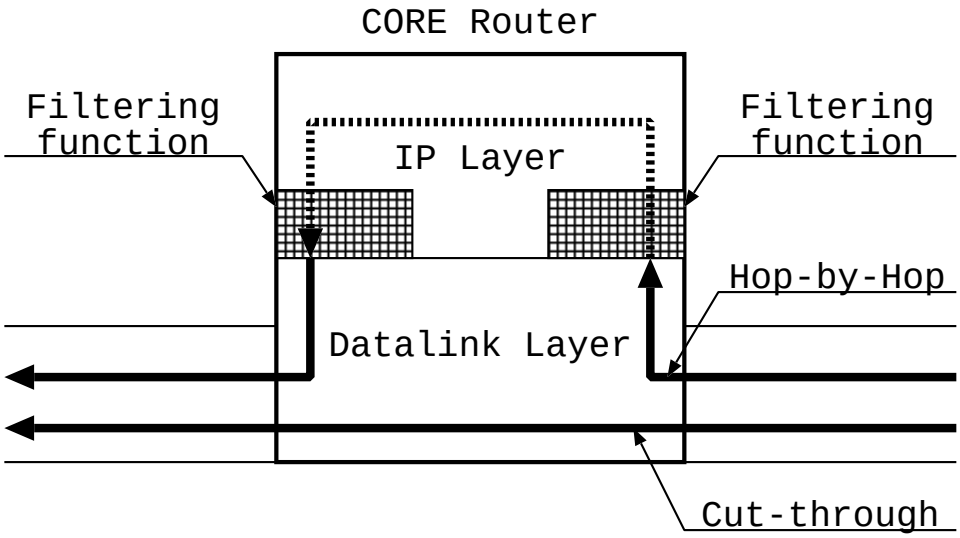

図 4.1: カット・スルーとパケット・フィルタ

特に、ラベルスイッチルータでは、高速なデータグラム転送を実現するために、一般的にハードウェア・スイッチを用いる。カットスルー状態においては、データグラムは、ハードウェア・スイッチのみを通過する事により転送される。ハードウェア・スイッチでは、ラベルのみを評価することによって高速なデータグラム転送を実現している。しかし、先に述べたように、パケット・フィルタリングでは、ラベル以外の情報も用いて、パケット転送を制御しなくてはならない。このため、ラベルスイッチルータではパケットの内容解析や転送の制御が困難なのである。

そこで、本研究では、ラベルスイッチング・ネットワークにおいてパケットフィルタリングの実現を目標とする。

4.2 カット・スルーの禁止による方法

パケット・フィルタリング処理を行うルータにおいて、カット・スルーを禁止する事によって実現する。この方法では、全てのカット・スルー経路はパケットフィルタリング処理を行うルータで終端される。つまり、全てのパケットは IP 層における通常の方式で処理される。(図 4.2)

この方法の実現は非常に容易である。パケットフィルタリング処理を行わせたいルータにおけるカット・スルー動作を完全に禁止するだけでよい。カット・スルーが禁止された

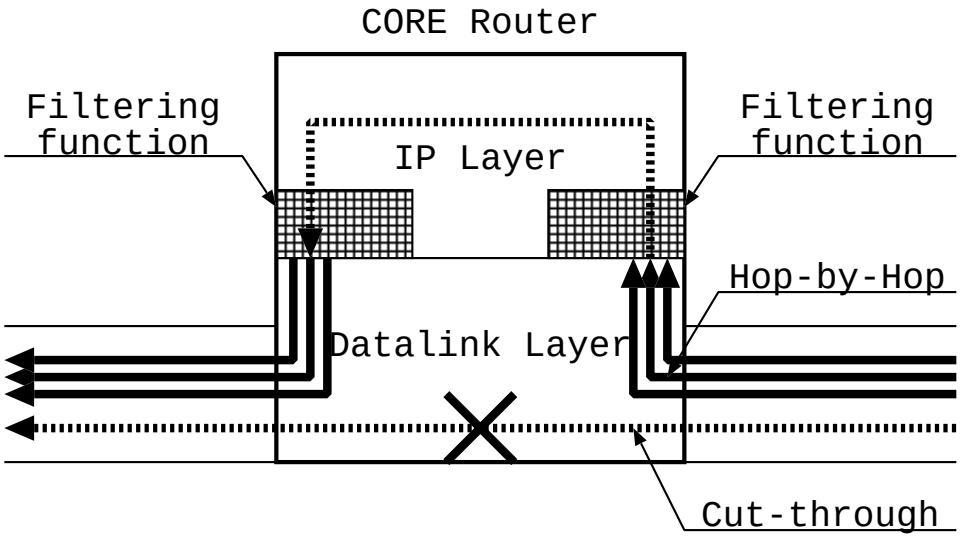

図 4.2: カット・スルーの禁止による方法

ラベルスイッチルータは、全てのパケットを通常の第 3 層による IP 転送の方式で処理する。カット・スルーを行う事のできないラベルスイッチング・ルータでのフィルタリング処理は、通常のルータでのフィルタリング処理と何ら変わりない。

ラベルスイッチング・ネットワークの最も大きな特徴は、カット・スルーにより高速・高帯域なパケット転送が可能である点である。しかしながら、本方式においては、カット・スルーを行う事は不可能である。よって、この方法はラベルスイッチング・ネットワークの利点を失っていると言える。

本研究では、ラベルスイッチング・ネットワークの利点を生かしつつ、パケットフィルタリングを実現する方法を提案する。

4.3 効率的なパケットフィルタリングの実現方式

ラベルスイッチング・ネットワークの特徴を生かしつつ、パケットフィルタリングを実現する方法として、大きく分けて 2 種類の方式を提案する。

4.3.1 擬似的なカット・スルーを用いる方式

本方式では、パケット・フィルタリング機能を提供するラベルスイッチルータにパケット転送モジュール (以下では PFM と呼ぶ) を組み込む。PFM は、入力データグラムに対

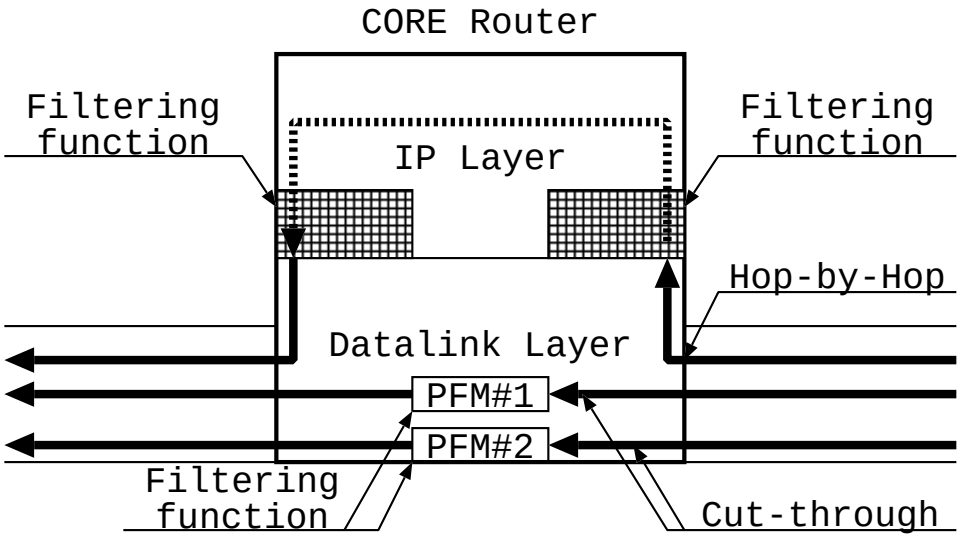

図 4.3: PFM による方式

しフィルタリング・ルールを適用し、転送が許可されればデータグラムを出力する。

ルータでは、カット・スルー経路の生成時に、通常のカット・スルー経路を生成するかわりに PFM へ迂回する「擬似カットスルー経路」を生成する。これにより、全てのデータグラムは PFM を介して転送されることとなる。(図 4.3)

本方式では、パケットフィルタリング処理を提供するルータだけの変更で処理が可能となる。また、カット・スルーを禁止する方式と比較すると、パケット転送のための経路探索等の、フィルタリング処理に本来必要としない処理を行う必要がないという利点がある。詳細は、第 5章で述べる。

4.3.2 フィルタリング処理をエッジ・ルータへ委託する方式

ラベルスイッチング・ネットワークにおいて、カット・スルー状態でもカット・スルー経路の端点においては IP 層でのパケット転送が行われる。本方式は、フィルタリング処理をカット・スルー経路の端点までスライドさせるものである。(図 4.4)

本方式では、完全なカット・スルーが可能となる。詳細は、第 6章で述べる。

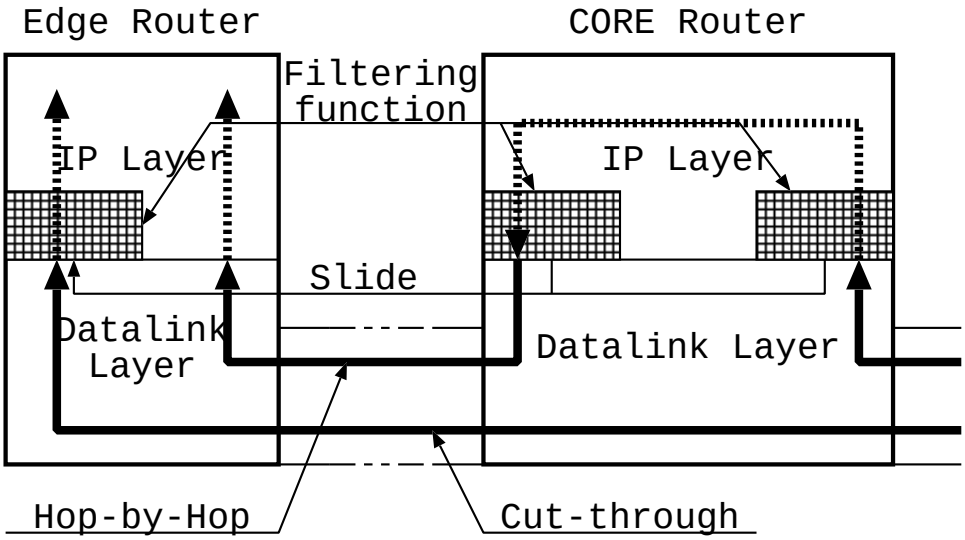

図 4.4: フィルタリングを行う位置をスライドさせる方式

第 5 章

擬似的なカットスルーを用いる方式で実現できる機能

本章では、擬似的なカットスルーを用いる方式について詳しく言及する。

5.1 構成法

本方式の構成法について解説する。

5.1.1 PFM の導入

PFM はデータリンク層におけるデータグラム転送を行うためのモジュールである。本モジュールは、カット・スルー経路の生成時に、カット・スルー経路毎に生成する。

本モジュールは、

- 第 2 層でデータグラムを転送
- 内部的にパケットを再構成
- パケット情報を取得
- フィルタリング・ルールの適用

の機能を持つ。

フィルタリング・ルールの設定は、各 PFM の生成時に行う。このため、各 PFM は独立したフィルタリング・ルールを持つことが可能となる。

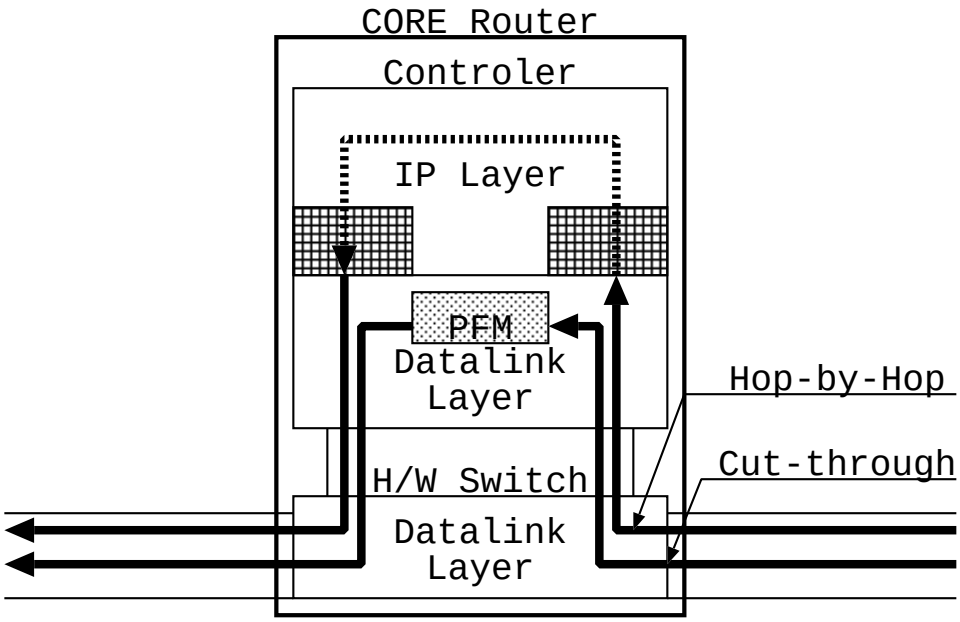

図 5.1: 擬似カット・スルー

5.1.2 擬似カット・スルー

カット・スルー経路の生成時に、完全なカット・スルー経路を生成する代わりに PFM へ迂回する経路を生成する。これを、擬似カット・スルーと呼ぶ事とする。

ラベルスイッチルータは、高速なデータグラム転送を実現するために、ハードウェア・スイッチとコントローラにより構成される。カットスルー状態においては、コア・ルータにおいて、データグラムはハードウェア・スイッチにより転送される。

ハードウェア・スイッチでは、ラベルのみを評価することによって高速なデータグラム転送を実現している。PFM ではラベル以外の情報も用いてフィルタリング・ルールの適用を行うためにハードウェア・スイッチに PFM の機能を組み込む事は困難である。よって、PFM はスイッチとは独立したモジュールとして構築する。(図 5.1)

通常のカット・スルー経路の生成は、カット・スルー要求に対し、スイッチの制御を行う事によって実現されている。擬似カット・スルー経路の生成は、カット・スルー要求に対し、

1. PFM を生成し、適切な設定を行う。

2. スイッチを制御し、経路を PFM へ接続する。

の 2 段階で実現される。

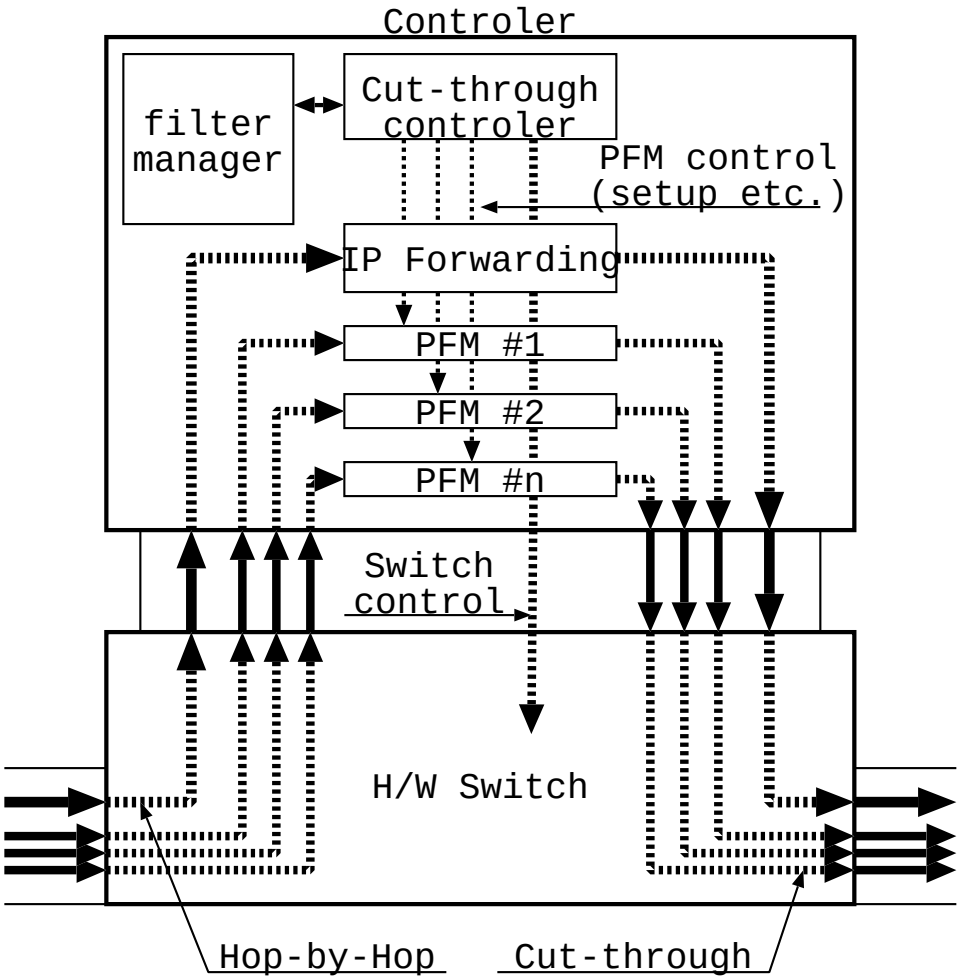

図 5.2: PFM 方式の全体構成

5.1.3 全体構成

本方式を実現するための全体構成モデルを図 5.2に示す。

このモデルの各モジュールについて解説する。以下で、(既存) は既存のラベルスイッチング・ルータに備わっている機能、(新規) は本方式を用いてパケット・フィルタリングを行うために新たに付け加えた機能を示す。

- Cut-through controler
  - (既存) カット・スルー状態への移行などをつかさどる。
  - (既存) ハードウェア・スイッチの制御を行う。

- (新規) PFM の生成/設定/開放を行う。

- filter manager
  - (新規) フィルタリング・ルールを管理し、Cut-throug controler からの要求に応じて、適切なフィルタリング・ルールを提供する。

- Packet Forwarding Module (PFM)
  - (新規) データグラムの解析、フィルタリング・ルールの適用、データグラムの転送等を行う。

5.2 PFM 方式の特徴

本節では、PFM 方式を用いてパケット・フィルタリングを実現した場合の特徴を述べる。

5.2.1 単体完結

パケットフィルタリングは、通常、セキュリティー・ドメインの境界点で行われる。通常のネットワークにおいて、パケットフィルタリング機能を提供するルータは、内部ネットワークと外部ネットワークの境界点に設置される。

PFM を用いる方式を用いた場合、既存のファイヤウォール・アーキテクチャをそのまま用いる事が可能である。PFM を用いる方式では、パケット・フィルタリングの全ての処理は、1 つのコア・ルータで行われる。これは、既存のルータにおけるフィルタリングと等価であると言える。

さらに、PFM を用いる方式は、単一のルータのみで実現が可能である。外部のルータからは、通常のラベルスイッチルータと認識される。

これらの特徴から、容易に導入が可能であると言える。

5.2.2 ラベルを用いたフィルタリング

パケット・フィルタリング・ルータは、発信アドレス・宛先アドレス・サービス種別等の情報を用いて、フィルタリングを実施する。ラベルスイッチング・ネットワークにおいては、これらの情報の他にラベルを用いる事が可能である。

PFM はラベル毎に独立して処理を行う。特定の PFM を流れるパケットに、発信アドレス・宛先アドレス・サービス種別等の点で特徴があれば、該当 PFM では、その特徴に

発信アドレス	宛先アドレス	サービス種別	ポリシ
*	150.65.1.0/25	TCP/POP	reject
*	150.65.3.0/25	ALL	accept
*	150.65.5.0/25	ALL	accept
*	150.65.0.0/16	TCP/TELNET	reject

表 5.1: フィルタリング・ルール全体

発信アドレス	宛先アドレス	サービス種別	ポリシ
*	*	TCP/TELNET	reject
!10.0.0.1	!150.65.190.16	ALL	reject

表 5.2: 縮小されたフィルタリング・ルール

合致したフィルタリング・ルールのみを評価すればよい事になる。特に、フロードリブン方式のラベルスイッチング・ネットワークでは、フローとラベルに関連があるため、この特徴を生かす事ができる。

例えば、フィルタリング・ルールの全体が表 5.1 である場合、

- 発信アドレス 10.0.0.1、宛先アドレス 150.65.190.16

の特徴を持つフローに対するラベルのための PFM では、表 5.2 のフィルタリング・ルールのみを評価すれば良い。

なお、縮小されたフィルタリングルールには、縮小前のフィルタリング・ルールに含まれなかったエントリが追加されている。これは、ラベルを偽る事によってフィルタを通過しようとするパケットを防ぐためのものである。

既に述べている通り PFM はラベル毎に独立して動作する。各 PFM へのフィルタリング・ルールの設定は、該当 PFM の生成時に行われる。よって、PFM の生成時に、対応するラベルを持つ経路の特性に合わせて、フィルタリング・ルールを縮小した上で設定する事が可能である。

フィルタリング・ルールの縮小のための処理は、各 PFM の生成時のみである。一方、フィルタリング・ルールを用いたパケットの評価は、到着した各パケット毎に行われる。このため、フィルタリング・ルール縮小のためのコスト増加よりも、各パケット毎に行わ

れるフィルタリング・ルール評価で削減されるコストの方が遥かに大きくなると期待できる。

5.2.3 クラスタリング

PFM はラベル毎に生成される。各 PFM は互いに独立して処理を行う。このモデルは、マルチプロセッサ・システムやコンピュータ・クラスタでの処理に適している。

先に提案した PFM 方式を、コンピュータ・クラスタに対応させるため図 5.3のように拡張する。擬似カットスルー経路は、コントローラにより各クラスタに割り当てる。このモデルでは、コントローラは自らも PFM を持ちクラスタの役目も果たしている。

この際、各カットスルー経路の流量は同一ではないことに留意しなくてはならない。このため、効率良く各カットスルー経路をクラスタに割り付けるためのアルゴリズムを検討する必要がある。

各カットスルー経路の流量に極端な偏りがないと仮定すると、コンピュータ・クラスタを用いる事により、クラスタの数に応じた帯域のフィルタリング性能が得られる。本モデルでは、各経路が 2 度同一スイッチを通過するため、理論上の最大転送容量はハードウェア・スイッチの 1/2 である。これは、構成変更により、ハードウェア・スイッチの性能に匹敵する最大転送容量を得る事も可能である。

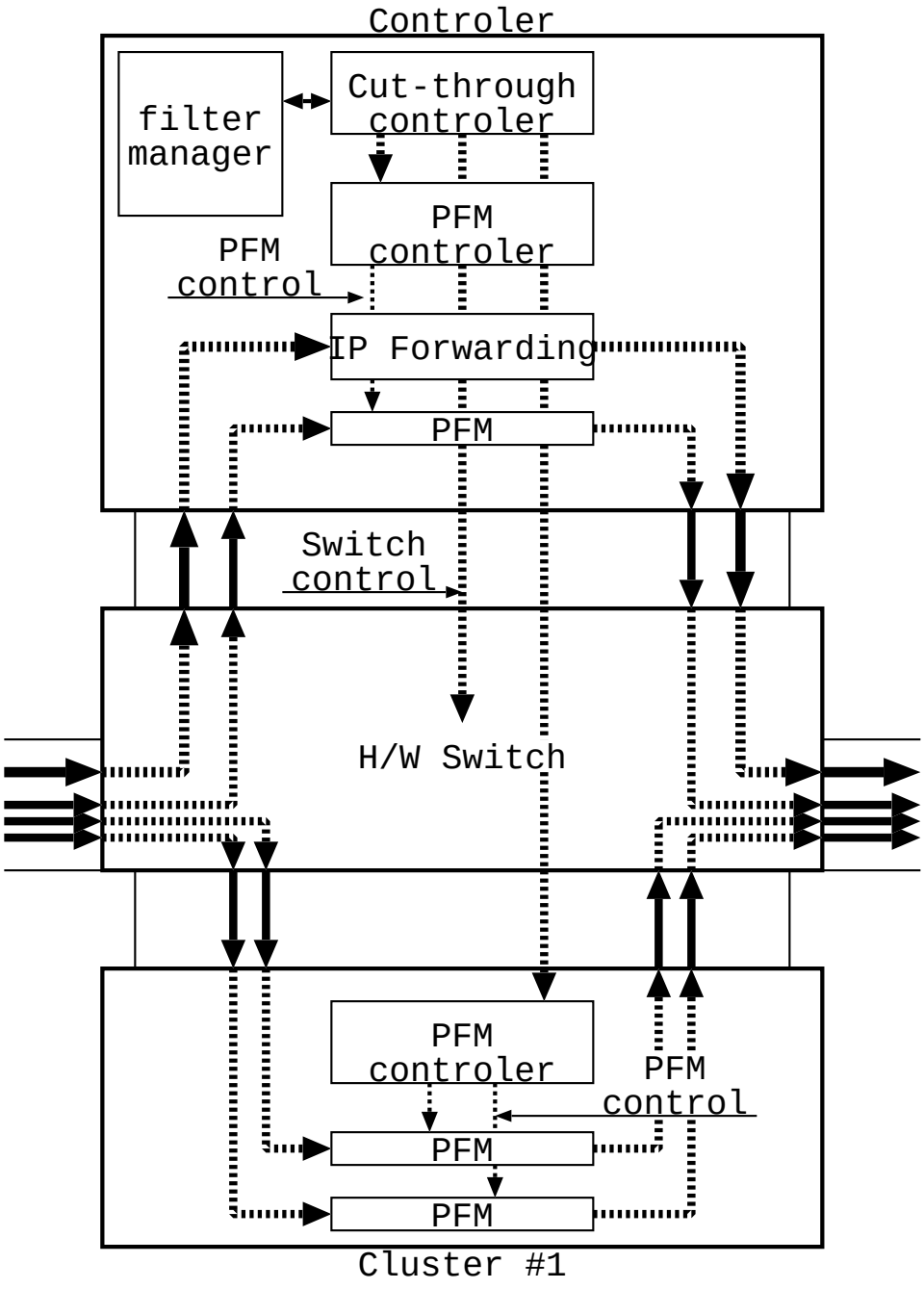

図 5.3: PFM 方式の全体構成 (クラスタリング)

第 6 章

フィルタリング処理をエッジルータへ委託する方式で実現できる機能

ラベルスイッチング・ネットワークにおいて、カット・スルー状態においてもカット・スルー経路の端点では IP 層でのパケット転送が行われる。本章では、フィルタリング処理を、カット・スルー経路の端点であるルータに委託することにより、完全なカット・スルーを行いつつフィルタリング処理を行う方式を提案する。

6.1 次段/前段ルータへの委託

セキュリティードメイン境界のコア・ルータにおいてカット・スルー要求が生じた際に、次段あるいは前段の信頼できるルータにフィルタリング処理を委託する。本方式を連続的に用いる事により、ラベルスイッチング・ネットワークの端点であるエッジ・ルータにフィルタリング処理を委託できる可能性がある。

次段のルータに委託する場合を例として挙げる。コア・ルータが、カット・スルー要求を受けると、次のような処理が行われる。(図 6.1)

1. 次段ルータが信頼できるルータであれば、次段ルータへフィルタリング処理の委託を試みる。

2. フィルタリング処理の委託を受けたルータは、可能であれば該当経路に対し委託されたフィルタを設定する。

    - 依頼を受けたルータが、コア・ルータならば、さらに次段に依頼する事を試みる。

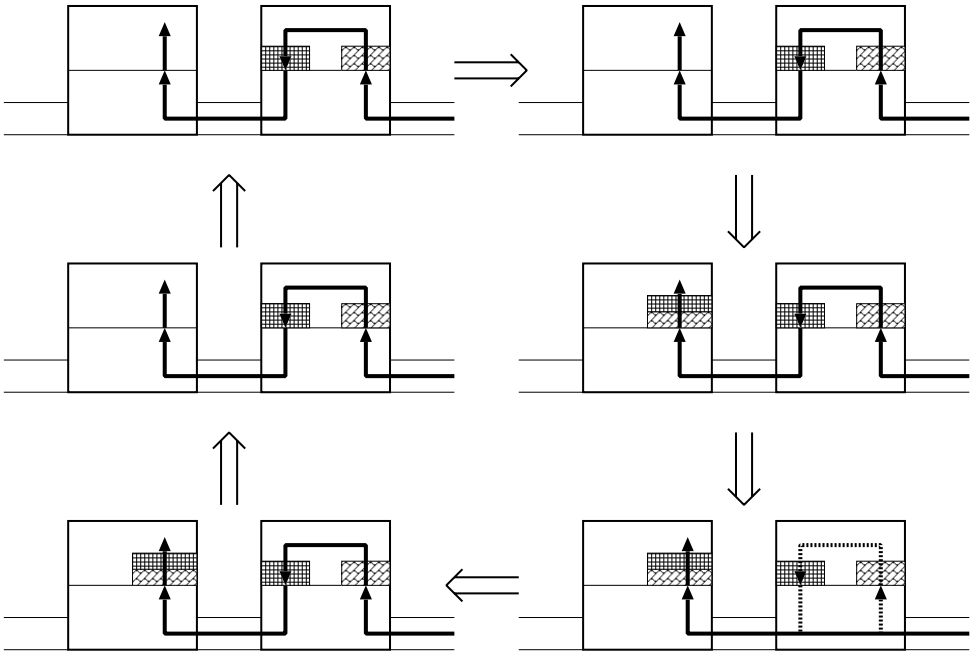

図 6.1: 次段ルータへ委託する場合の状態遷移

3. フィルタの設定が完了すると、その旨を委託元のルータに通告する。

4. 委託が受け入れられると、カット・スルー状態に移行する。

6.1.1 本方式の特徴

本方式では、委託に成功した経路については、該当ルータでは完全なカットスルーが可能となる。エッジ・ルータまで連続的に委託に成功すると、ラベルスイッチング・ネットワークにおける理想状態であるエッジ・ルータまでのカット・スルー経路を生成する事ができる。これは、ラベルスイッチング・ネットワークでパケットの再構成を一切行わないデータグラム転送が可能であることを意味する。

さらに、フィルタリングはカット・スルー経路毎に行われるために、前章で述べたフィルタリング・ルールの縮小が可能である。

しかし、委託を受け入れるルータにもある程度のセキュリティー・レベルが要求される。このため、本方式のみでフィルタリングを行おうとすると、全てのエッジ・ルータに高いセキュリティー・レベルが要求される。これでは、全ての機器にフィルタリング・ルールを記述する必要まではないものの、ホスト・セキュリティーに近いものとなってしまう。

なお、本方式では、委託を受け入れる側のルータが、どのような手法でフィルタリングを行うかは定めていない。よって、委託を受け入れたルータで、先に提案した PFM 方式でフィルタリングを実施する事も可能である。

6.2 任意のルータへの委託

本節では、隣接しないルータにフィルタリング処理を委託する方式について議論する。委託元のルータから委託先のルータまでの経路が、完全に自らの管理ドメイン内である場合は、前節で述べた方式で実現が可能である。しかし、委託元のルータから委託先のルータまでの経路中に、自らの管理ドメイン外のルータが入ると、前節で述べた方法では実現ができない。

本節で提案する方式は、特に、自らの管理ドメイン外に信頼できるルータが存在し、そのルータへフィルタリング処理を委託する事を目的としたものである。

本方式は、カット・スルー経路の生成時に、該当カット・スルー経路を VPN (Virtual Private Network) とするものである。この VPN の一端は、内部ネットワーク内のエッジ・ルータであり、他端は、フィルタリング処理を委託する先の管理ドメイン外ルータとなる。つまり、カット・スルー経路の生成とともに、委託先のルータは、内部ネットワークと外部ネットワークを結ぶ境界ルータの 1 つとなるわけである。

この方式では、内部ネットワークへ宛てられたパケットに対して、自らの管理ドメイン内に到達するより前の段階でフィルタリング処理を行う。このため、ネットワーク帯域やシステム資源を洪れさせることによるサービス不能攻撃に対して非常に有効である。

しかし、本方式には次に示すように課題となる点も多い。

1. **動的 VPN 生成**
   カット・スルー経路は動的に生成されるものである。これに対応して、該当カット・スルー経路を動的に VPN 化しなくてはならない。また、フィルタリング処理を委託される側だけでなく、VPN の両端点が動的 VPN 生成に対応し、一定のセキュリティーが保たれている必要がある。

2. **安全なフィルタリング処理内容の伝達**
   フィルタリング処理内容が外部に露呈する事は、セキュリティー上、非常に危険な事である。また、処理内容は正確に委託先に伝えられなければならない。

3. **スケーラビリティー**
   本方式は、自らの管理ドメイン外に信頼できるルータが存在し、多くのパケットが

そのルータを経由して自らのネットワークに到達する事を仮定している。しかし、ラベルスイッチング・ネットワークが非常に大きなものとなると適用が難しい。

第 7 章

プロトタイプの実装

第 5章で提案した PFM を用いる方式についてプロトタイプを実装した。プロトタイプは、ラベルスイッチルータの実装の 1 つである、CSR[1]を用いて実装した。CSR は、フロー・ドリブン方式を採用し、第 2 層に ATM を用いたラベルスイッチルータである。

7.1 実装目的

本プロトタイプの実装は、第 5章で提案した PFM を用いる方式でのパケットフィルタ処理の実現可能性を示し、その特徴を検証することを目的として行った。

7.2 実装仕様

本プロトタイプは、次の機能・特徴を持つ。

- カット・スルー経路生成要求時に、PFM を生成し、擬似カット・スルー経路を設定する。
- PFM では、データグラム単位でパケットの転送を行う。
- PFM では、各パケットの特徴解析と転送制御機能を持つ。
- 該当ルータで内部完結し、他のルータは既存のものがそのまま利用できる。

[1](株) 東芝: Cell Switch Router

7.3 モジュール構成と動作概要

本プロトタイプでは、PFM を含む全てのモジュールを、ユーザ空間で実装した。PFM がデータグラムの受信・送信に用いるインターフェイスとして、ATM socket を持ちた。モジュール構成を図 7.1で示す。

カットスルー要求は fanpd で生じる。カット・スルー要求が発生すると、次のような動作を行い、擬似カット・スルーを実現する。

1. fanpd はラベルと Flow ID を PFM Controler に送る。Flow ID は該当ラベルを持つパケットが持つ特徴を示す識別子で、実際には、発信元 IP アドレス、宛先 IP アドレスの組で表される。

2. PFM Controler は、Policy Manager に Flow ID を送る。

3. Policy Manager は Flow ID をもとに、該当フローに必要なフィルタリング・テーブルを生成し、PFM Controler に返す。

4. PFM Controler は PFM を生成し、フィルタリング・ルールを設定する。

5. 生成された PFM はフィルタリング・ルールの設定が終ると、ATM Socket に接続し、転送動作を開始する。

6. PFM コントローラは ATM スイッチとカーネルを操作し、該当ラベルを持つデータグラムが ATM socket を介し該当 PFM へ流れるように設定する。

7.4 プロトタイプの評価

本プロトタイプにより、PFM 方式でパケット・フィルタリング機能が実現可能である事が示された。また、PFM 方式の特徴である内部完結性も実証できた。

一方、本プロトタイプではパケット転送能力の検証を目的としなかった。このため、非常に低速な転送しか実現できない。高速なデータグラム転送は、先の図 7.1で示した PFM をカーネル内部に実装し、ATM socket を介さず直接 ATM ドライバを利用する事により可能となる。

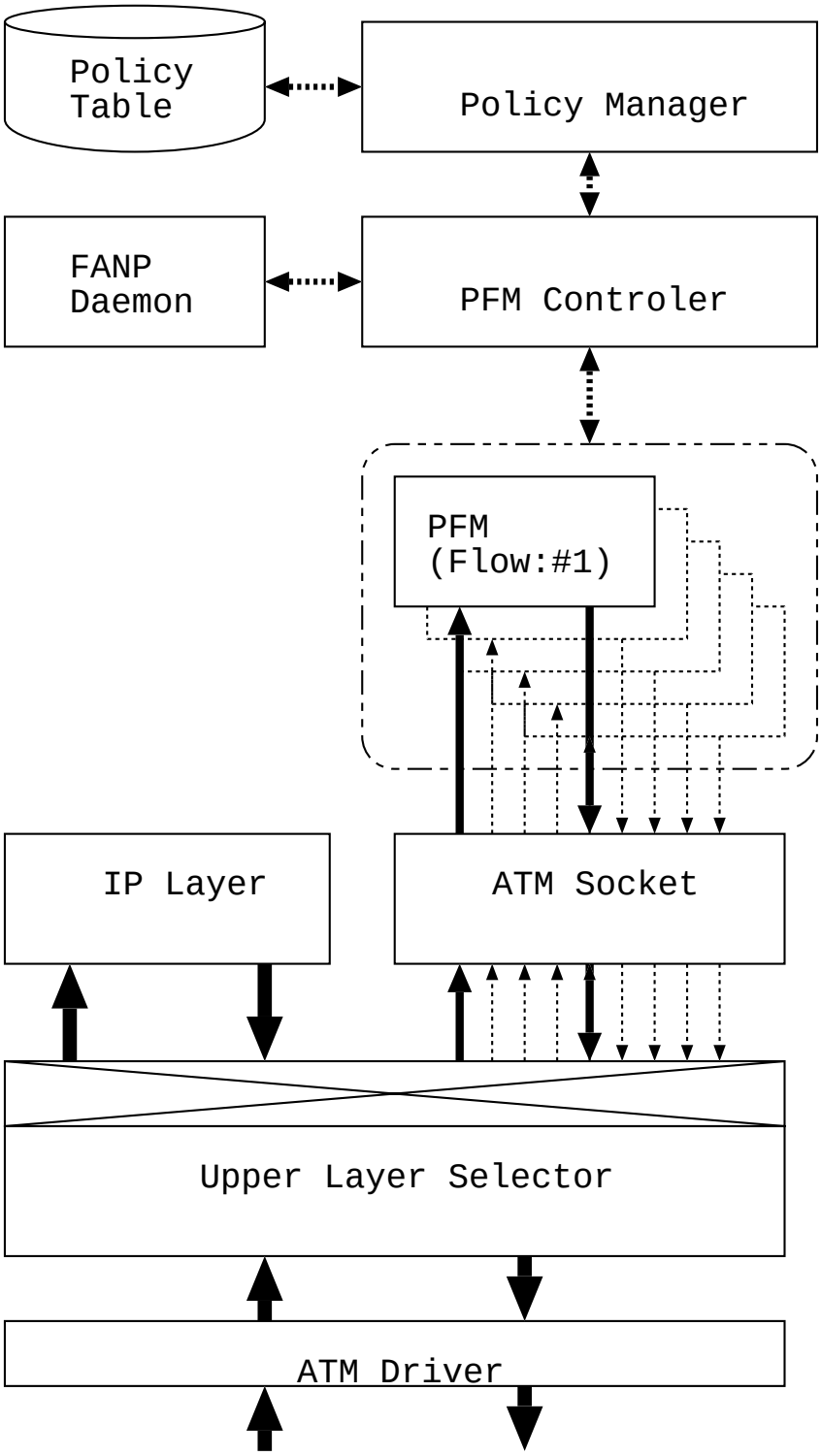

図 7.1: プロトタイプのモジュール構成

第 8 章

考察

本研究では、

- PFM を用いでコア・ルータにおいてフィルタリングを行う方式。
- フィルタリング処理を委託し、エッジルータでフィルタリング処理を行う方式。

を提案した。

本章では、これらの方式に関する考察を行う。

8.1 PFM 方式と処理委託方式の融合

エッジ・ルータへフィルタリング機能を委託する事によりパケット・フィルタリング機能を実現する方式は、完全なカット・スルーが可能であるために、最も魅力的な方式である。しかし、この方式のみでの実現は、多くのラベルスイッチルータのセキュリティーを一定以上に保つ必要があり困難である。

そのため、PFM 方式とエッジ委託方式を組み合わせてのフィルタリング機能の実現が現実的である。あらかじめ、一定以上のセキュリティーが確保されているエリアを定めておき、そのエリア内で終端するカット・スルー経路については終端点のルータへフィルタリング処理を委託し、それ以外のカット・スルー経路については PFM を用いて処理する。

このように、PFM 方式とエッジ委託方式を組み合わせる事により、ラベルスイッチング・ネットワークの特徴を最大限に生かした、パケット・フィルタリング、ひいてはファイヤウォールの構築が実現できる。

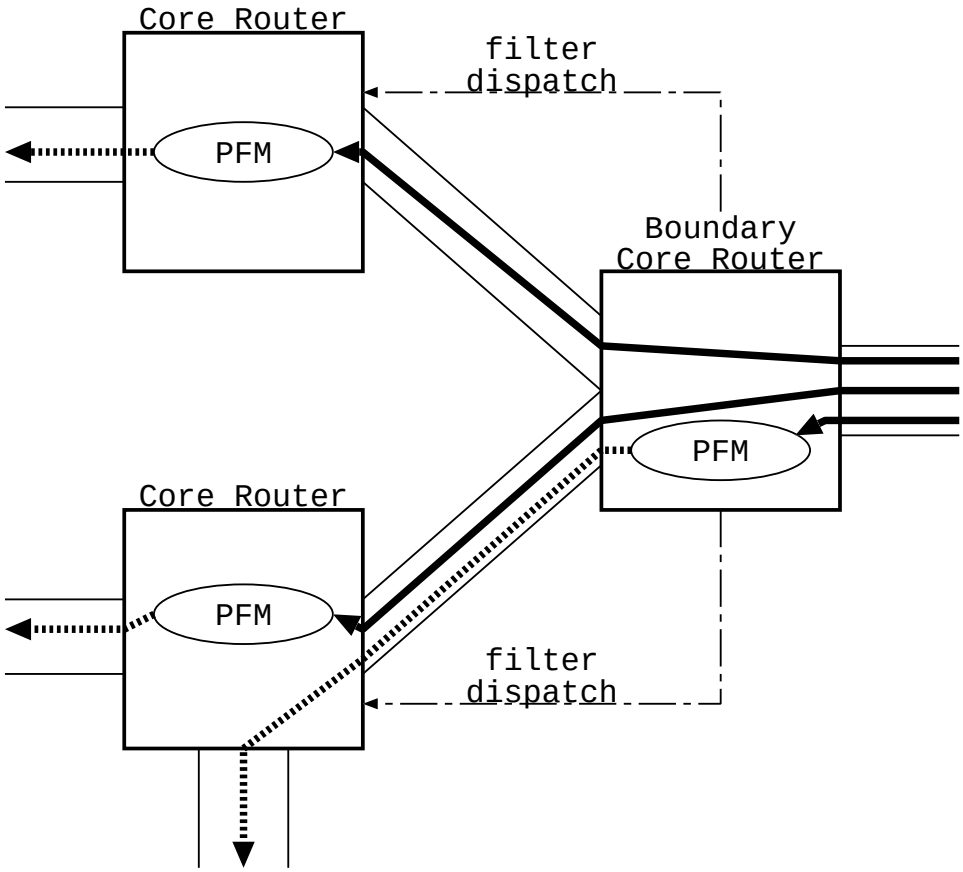

図 8.1: 複数のコア・ルータでの協調動作

8.2 性能向上に関する考察

8.2.1 次段/前段コア・ルータへ PFM を委託する

フィルタリング処理の委託では、エッジ・ルータに処理を委託することを中心に検討を行った。本節では、コア・ルータへのフィルタリング処理の委託について検討する。

フィルタリング処理を行う境界ルータは、トラフィックが集中する箇所である。集中するトラフィックを処理する方法として、第 5章ではコンピュータ・クラスタを用いる方法を提案した。

別の解決方式として図 8.1のように複数のコア・ルータにおいて PFM を用いてフィルタリングを行う事が可能である。ここで、フィルタリング処理の委託のための手順は、第 6章において提案した、次段/前段ルータへのフィルタリング処理の委託方式を用いる事に

よって実現できる。

先に述べたコンピュータ・クラスタを用いる方式と、ここで提案した複数のコア・ルータへフィルタリング処理を委託する方式は相反するものではない。これらを組み合わせる事によりさらなる性能改善が可能となる。

8.2.2 セルの先だし

ATM を用いたラベルスイッチング・ネットワークにおいては、パケットは AAL5 フレームにカプセル化され、さらにセルに分割されて伝送される。

AAL5 フレームの再構成は、AAL5 フレームを構成する全てのセルが揃わない限り行われない。フレームを構成する一部のセルが失われた場合、該当フレームは破棄される。

プロトタイプ実装においては、PFM は AAL5 フレーム単位で転送を行ったが、セル単位で行う事も可能である。セル単位で転送を行った場合、フレームを構成する最後のセル以外は、フィルタリング・ルールの評価前に先出しする事が可能である。フィルタリング・ルールの評価結果により、パケットの破棄が求められる場合は、最悪でも、フレームを構成する最後のセルのみを破棄すればよい。この性質より、セルの転送とフィルタリング・ルールの評価を並列して処理することも可能であると言える。

8.3 応用に関する考察

本研究では、ラベルスイッチルータでパケット・フィルタリング機能を実現する手法を提案した。この手法を、パケット・フィルタリング以外の機能へ応用する事が可能である。

8.3.1 Network Address Translator (NAT) 機能への応用

IPv4 アドレス空間の枯渇問題などから、近年では、ルータにおける NAT 機能が多く用いられている。NAT 機能では、通過するパケットの情報の抽出と書き換えが行われる。ラベルスイッチルータを通過する各パケットの情報の抽出は、パケット・フィルタリング機能で必要とされたものにほかならない。

各パケットの情報の抽出は、本研究で提案したフィルタリング手法を用いる事により可能である。また、その拡張により、パケット情報の書き換えも容易である。

NAT におけるパケットの情報の書き換えでは、パケットの前後依存関係を用いている。このため、PFM を用いて特定ルータのみで実現する事は容易であるが、エッジ・ルータへの委託を用いて複数箇所で実現する手法を用いるためには、さらなる検討が必要である。

8.3.2 フロー・アグリゲーションにおけるラベルの付け替えへの応用

ラベルスイッチ・ネットワークでは、各ラベルスイッチルータで扱う事のできる最大ラベル数は有限値である。最大ラベル数は、LAN 環境でラベルスイッチング・ネットワークを用いる上で問題になる程度の値ではないが、バックボーン環境でラベルスイッチング・ネットワークを用いる上で充分に大きな値とは言えない。

フロー・ドリブン方式のラベルスイッチング・ネットワークでは、必要ラベル数は、フロー数により決まる。バックボーン環境では、フロー数が非常に多くなるため、必要なラベル数も非常に多くなる。そこで、同じような特徴を持つ複数のフローに対し同じラベルを割り当てる事により必要ラベル数を低減させる事が提案されている。

外部ネットワーク (バックボーン) でフロー・アグリゲーションが行われると、内部ネットワークで用いるラベルの割り当て方針と、外部ネットワークで用いるラベルの割り当て方針が異なる場合がある。このような場合、境界ルータでは、ラベルの付け替えを行う必要が生じる。

内部から外部に向かうパケットに付いては、内部ネットワークにおけるラベルのみの評価で、外部ネットワークにおけるラベルを特定できるので問題はない。一方、外部から内部に向かうパケットでは、外部ネットワークにおけるラベルのみの評価では、内部ネットワークにおけるラベルを特定できない。このため、パケットの情報を抽出し、それを元に内部ネットワークにおけるラベルを特定しなければならない。

ラベルスイッチルータを通過する各パケットの情報の抽出は、パケット・フィルタリング機能で必要とされたものにほかならない。本研究で提案した、PFM を用いる事によりこの実現が可能となる。

第 9 章

今後の課題

本章では、本研究で課題として残った点について述べる。

9.1 PFM 方式の有効性の実証

本研究におけるプロトタイプでは、PFM を用いた方式の実装を行った。しかし、この実装では、PFM を用いたパケット転送が、広帯域・低遅延というラベルスイッチング・ネットワークの特性が維持できているか疑問の余地がある。

そこで、PFM 方式の有効性の実証を行うために動作速度の検証を行う必要がある。今回の実装の PFM 部分をカーネルに実装し動作させる事により、動作速度の検証を行いたい。

9.2 PFM クラスタにおける適切な負荷分散手法

PFM によるパケット転送の高速化手法として、コンピュータ・クラスタを用いる方法を提案した。各 PFM は独立して動作が可能であるため、PFM を複数のコンピュータに分散配置するというものである。

この実現において、効率良く負荷の分散を行うために、如何に PFM を分散配置すべきかという問題がある。各カット・スルー経路のトラフィックは同一ではない。さらにつねに一定とは限らない。このため、PFM の負荷は PFM 毎にまちまちとなる。よって、PFM の配置アルゴリズムについての検討が必要である。

9.3 フィルタリング処理の委託に関する議論

本研究では、フィルタリング処理の方式として大きく分けて 2 種類のものを提案したが、今回は特に PFM を用いる方式について詳しく検討を行った。

フィルタリング処理を外部ルータ、特に、第 6.2節で提案した管理ドメイン外の信頼できるルータに処理を委託し、カット・スルー経路を用いて VPN を生成する方式についての議論は、充分になされたとは言えない。よって、この方式に付いては、今後、より詳細な議論を行う必要がある。

9.4 本研究の応用に関する詳細な議論

本研究ではパケット・フィルタリングの実現のための手法を提案したわけであるが、考察において述べた通り、この手法は別の機能を提供するためにも利用可能である。

そこで、第 8.3節で述べた、

- NAT への応用
- ラベルの付け替えへの応用

についても、詳しく検討したい。

9.5 一般化

最後になるが、本研究では、ラベルスイッチング・ネットワークを用いる事を大前提として各種議論を行った。この垣根を取り払い、本研究での提案をもとに、分散型ファイヤウォール構築手法に関する議論への拡張が可能ではないかと思われる。

第 10 章

まとめ

本論文では、ラベルスイッチング・ネットワークにおいて、その特性を生かしたパケットフィルタリングの実現方法について提案し、議論を行った。

ラベルスイッチング・ルータにおいては、その特性から、パケット・フィルタリング機能を効果的に提供する事が困難であった。そこで、本研究では、これを実現するための手法として、

- PFM を用いて実現する方式
- 他ルータ委託を用いて実現する方式

を提案した。

また、これらの提案をもとに、効果的なフィルタリング処理の手法、高速化のための提案、他の用途への応用方法などについて議論した。

謝辞

本研究を進めるにあたり指導教官である篠田陽一助教授には、様々な助言、指導を頂いた。そして、所属研究室の方々からも様々な意見を頂いた。また、WIDE Project のメンバーの方々には、本研究に対して有意義な議論をして頂いた。さらに、(株) 東芝には、本研究を進める上で必要な機器やソースコードを提供して頂いた。記して、ここに感謝の意を示す。

参考文献

[1] P. Newman, T. Lyan, G. Minshall, "Flow labelled: Connectionless ATM Under IP", Engineer Conference, Networld+Interop '96 Las Vegas, April, 1996.

[2] H. Esaki, "A High Speed IP Packet Forwarding Architecture over Internet using ATM Technology", 博士論文, 東京大学, May, 1997.

[3] S. Lin, N. Mckeown, "A Simulation sutudy of IP Switching", ACM SIGCOMM, 1997.

[4] K. Nagami, Y, Katsube, H. Esaki, O. Nakamura, "Effect of flow aggregation in label switching network", SPIE Proceedings Vol.3529, November, 1998.

[5] 永見 健一, 江崎 浩, 勝部 泰弘, 中村 修, "ラベルスイッチルータにおける必要ラベル数の評価とフローアグリゲーションの効果", インターネットコンファレンス '98 論文集 pp.97–105, 日本ソフトウェア科学会, December, 1998.

[6] P. Newman, W. Edwards, R. Hinden, E. Hoffman, F. Ching Liaw, T. Lyon, G. Minshall, "Ipsilon Flow Management Protocol Specification for IPv4 Version 1.0", IETF RFC1953, May, 1996.

[7] Y. Katsube, K. Nagami, H. Esaki, "Toshiba's Router Architecture Extensions for ATM : Overview", IETF RFC2098, February, 1997.

[8] Y. Rekhter, B. Davie, D. Kats, E. Rosen, G. Swallow, "Cisco Systems's Tag Switching Architecture Overview", IETF RFC2105, February, 1997.

[9] K. Nagami, Y. Katsube, Y. Shobatake, A. Mogi, S. Matsuzawa, T. Jinmei, H. Esaki, "Toshiba's Flow Attribute Notification Protocol (FANP) Specification", IETF RFC2129, April, 1997.

[10] P. Doolan, B. Davie, D. Katz, Y. Rekhter, E. Rosen, "Tag Distribution Protocol", IETF Internet-Draft, May, 1997.

[11] A. Viswanthan, N. Feldman, R. Boivie, R. Woundy, "ARIS: Aggregate route-based IP switching", IETF Internet-Draft, March, 1997.

[12] N. Feldman, A. Viswanthan, "ARIS Spacification", IETF Internet-Draft, March, 1997.

[13] E. Rosen, A. Viswanthan, R. Callon, "Multi protocol Label Switching Architecture", IETF Internet-Draft, March, 1998.

[14] L. Andersson, P. Doolan, N. Feldman, A. Fredette, R. Thomas, "Label Distribution Protocol", IETF Internet-Draft, March, 1998.