不正パケット遮断システムにおけるポリシ機能の実装と評価

05T263 松木崇（最所研究室）

不正パケットが検出されると L2 スイッチあるいは Firewall で自動遮断し、問題が解決されれば自動解除するシステムの開発を行っている。本研究では、遮断や解除の制御を自動的に行うポリシ機能の実装と評価を行う。

1 はじめに

ネットワーク社会における情報保護は個人、および組織にとっての最重要課題のひとつとなっている。特に、企業・大学といった組織からの個人情報・機密情報の流出は、組織の運営に関わる問題である。また、その問題について対策を行わなければならないネットワーク管理者の負担が増大しており、それを解消することも重要な課題となっている。

この問題に対処するために、侵入検知システム(IDS)を利用して特定したホストのパケットをレイヤ 2 スイッチ(L2 スイッチ)、Firewall を用いて遮断する不正パケット遮断システム機構の設計･開発を行ってきた。昨年度までに、不正パケット遮断システムの制御ツールの実装、インタフェース、運用ポリシの設計と試作が行われた[1][2][3]。本研究では、不正パケット遮断システムのポリシ機能について再検討し、実装および性能評価を行う。

2 概要

不正パケット遮断システムの概要を図 1 に示す。

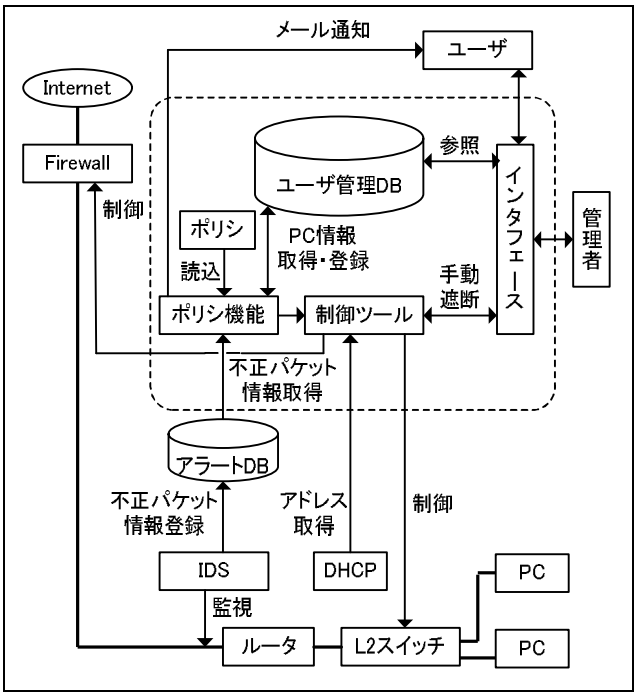

図 1 不正パケット遮断システム

IDS が不正パケットを検知し、情報をアラートデータベースに登録する。ポリシ機能がその情報を参照し、制御ツールを用いることによって Firewall あるいは L2 スイッチを制御し、内部からの情報流出を阻止する。その後、管理者と利用者に通知する。その際に利用者には対策すべきことを示すことで復帰を早めることを助ける。PC を特定する際は、DHCP が持つ IP アドレスと MAC アドレスの情報や、ユーザ管理データベースの情報を用いる。また、IDS として Snort を用いる。

3 ポリシ機能の設計・実装

3.1 概要

ポリシ機能に必要な機能は次の 3 つに分類できる。本研究では自動遮断機能の問題点を修正し、昨年度までに未実装であった自動解除機能、メール通知機能を実装する。言語は PHP を使用し、データベースは MySQL を用いる。

- 自動遮断機能
  IDS が検知した不正パケットの情報を取得し、不正パケットを発するホストの特定、遮断手法の決定、遮断までの一連の流れを自動的に行う。

- 自動解除機能
  遮断中のホストを問題が解決した場合にネットワークに復帰させる。

- メール通知機能
  不正パケットを発したユーザに対して、検知したパケットの種類や処理内容、情報閲覧ページの URL 等を記載したメールを送信する。

3.2 自動遮断機能

- アラート情報取得機能の修正
  昨年度までの実装では、重複する IP アドレスからの情報はパケットの危険度を無視してひとつにまとめられ、その後で遮断レベルを決定していた。このため、一つのホストから危険度の高いパケットと危険度の低いパケットが同時に検知されたとき、場合によっては危険度の高いパケットが無視され、危険度の低いパケットにあわせて処理が実

行されてしまう問題があった。この問題を解決するために、新たに遮断対象をまとめるためのデータベースを作成し、危険度の高いパケットに合わせて処理を実行するように修正する。

- ポートの差し換えへの対策
  L2 スイッチで遮断を行った場合に、遮断されたホストが別のポートに差し換えられると再び通信が可能になり、差し換え前のポートは他のユーザであっても通信できない。この問題を解決するために、ポートの差し換えが行われるときに、差し換えた後のポートを遮断し、差し換え前のポートの遮断を解除するよう修正する。

- 遮断の実行修正
  昨年度までは全ての処理が順番に実行されていた。このため複数のホストから同時に不正パケットが検知された場合、処理が完了するまでに時間がかかってしまう。この問題を解決するために、遮断処理をバックグラウンドで実行するように修正し、複数の処理を並行して実行できるようにする。

3.3 自動解除機能

自動解除機能は次の 2 つの機能に分けて実装する。

- パケットの観測による解除機能
  不正パケットが最後に観測された時刻と現在時刻とを比較して自動的に解除を行う。

- ユーザ通知による解除機能
  遮断中のユーザがセキュリティ対策を完了した場合にシステムにメール通知が行われると、メールアドレスからホストを特定し、過去の遮断回数や警告回数、現在の遮断手法を考慮した解除を行う。解除後すぐに不正パケットを発した場合は悪質なユーザとして自動解除の対象から除外する。

3.4 メール通知機能

不正者に対してメールの通知を行う機能。ユーザ管理データベースから不正ホストの連絡先を取得し、遮断箇所に応じて送信先を選択する。

4 評価

ポリシ機能の各機能が正しく動作するかを確認するために動作実験を行った。ホストから ping で通信を確認しつつ不正パケットを送信し、自動的に遮断が行われるかを確認する。結果を図 2 に示す。このとき図 3 に示すメールがユーザに送信された。次に、不正パケットを検知して遮断を完了するまでにかかる時間を測定した。同時に遮断するホストが 1 台増えるごとに、L2 スイッチ遮断では約 4.4 秒ずつ、Firewall 遮断では約 0.9 秒ずつ増加した。ネットワーク管理者

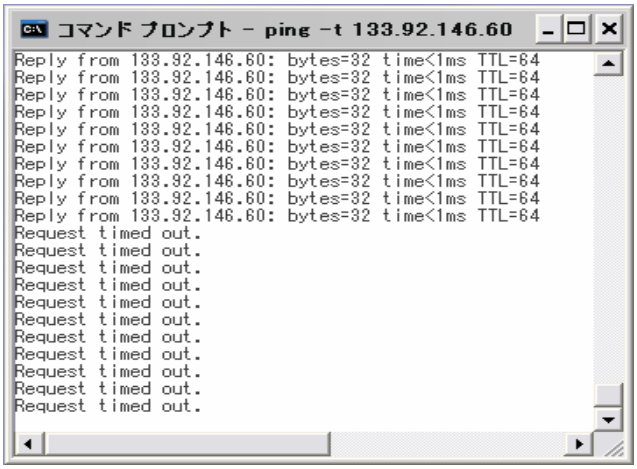

図 2 遮断確認

図 3 通知メール

が手動で制御する手間を考えると十分な処理速度だといえる。

5 まとめ

ポリシ機能で必要な機能である自動遮断機能、自動解除機能、メール通知機能を実現できた。また、これらの機能によって不正パケットを発するホストを自動的に遮断できることが確認できた。今後は本システムを実環境で使用してユーザに評価してもらい、システム全体の調整をして行くことが必要である。

参考文献

[1] 原田知拡，“不正パケット遮断システムにおける自動制御ツールの開発”，香川大学工学部卒業論文,2007 年.
[2] 岡原聖，“不正パケット遮断システムのユーザインタフェース開発”，香川大学工学部信頼性情報システム工学科，卒業論文，2007.
[3] 高橋巧，“組織内における不正パケット遮断システムの運用ポリシ設計および実装”，香川大学大学院工学研究科，修士論文，2007.