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

04T260 原田 知拡 （最所研究室）

本研究では、不正なパケットを送信したホストを侵入検知システムを用いて特定し、そのホストの通信を Firewall またはインテリジェントレイヤ 2 スイッチを用いて遮断する不正パケット遮断システムにおける自動制御ツールの設計・開発を行った。

1 はじめに

ネットワークインフラの充実は、インターネットの利用の大衆化を促進してきた。そのような背景の中、充分な知識のないユーザの利用も増え、自覚のないままコンピュータウィルスに感染し、コンピュータ内の情報を流出させる事例が頻発している。このような問題に対して、Firewall とポート単位での制御を行うことができるインテリジェント L2 スイッチを用いたパケット制御を組み合わせた不正パケット制御システムを提案している。本システムは、侵入検知システムを用いてそのパケットを検知した後、不正パケットを送信したホストを特定し、対処内容を決定し、自動的に執行するシステムである。本システムは、

1. 侵入検知システムが検知した情報をもとに、どのように不正ホストに対処を行うかを決定し、検知した情報を制御ツールに提供するポリシ機能
2. 自動で不正ホストを特定し、Firewall または L2 スイッチで制御する機能
3. 管理者の判断で手動制御を行うユーザインタフェース

の 3 つから構成される。本研究では、2 番目の機能を持つ自動制御ツールの開発を行う。なお、システム全体の設計とポリシ機能の開発に関しては共同研究者である高橋氏 [2] が、ユーザインタフェースの開発に関しては岡原氏 [3] が担当している。

2 自動制御ツールの設計

2.1 概要

本システムにおける制御ツールの役割は、2 点ある。

- ホストを遮断するために必要な情報の取得
- Firewall や L2 スイッチの設定の自動的な変更

である。制御ツールに必要な機能は以下の 3 つに分類できる。

1. 情報の取得機能

   この機能で L2 スイッチを用いた制御に必要な情報である不正ホストの MAC アドレス、接続している L2 スイッチ及び、L2 スイッチの接続ポート番号を得る。

2. 通信の遮断機能

   ポリシ機能から取得した IP アドレス、使用したプロトコルとそのポート番号を元に、Firewall の設定を行う。あるいは、情報の取得機能で取得したの情報を元に、L2 スイッチの制御を行う。

3. 遮断の解除機能

   通信の遮断を行った後に、対象のホストの遮断解除を行う機能である。

今回、Firewall は、Linux マシン上で動作するパケットフィルタリング機能を用いた。L2 スイッチとしてアライドテレシス社のギガビット・インテリジェント・スイッチ『CentreCOM GS908M』を用いた。

2.2 情報の取得機能

情報の取得機能では、SNMP を利用し、L2 スイッチで制御するために必要な MAC アドレスや、不正ホストが接続している L2 スイッチの情報を取得する。この機能は、MAC アドレスの取得機能と不正ホストが接続している L2 スイッチの取得機能の 2 つで構成される。

MAC アドレスは、ルータの ARP テーブルを参照することにより取得する。

不正ホストが接続している L2 スイッチは、L2 スイッチの FDB を参照し、不正ホストがどの L2 スイッチに接続しているかを調べることで特定できる。FDB とは、フォワーディングデータベースのことで、スイッチに接続しているホストの MAC アドレスと接続ポート番号が入っている。

2.3 通信の遮断機能

Firewall の設定変更もしくは、L2 スイッチの制御を行うことにより、不正ホストの通信を遮断する。

Firewall を用いた遮断　ポリシ機能から遮断に必要な IP アドレス、ポート番号とそのプロトコルを受け取る。それらを元に Firewall の設定を記述したチェインを作成し、適応する。チェインには、パケットの IP アドレス、使用しているプロトコル、ポート番号、許可/破棄という制御情報が記述されている。そして、作成したチェインをシェルスクリプトとして書き込む。

シェルスクリプトは、本システム内にあるインタフェースを用いた手動での変更と矛盾がないようにするために用いる。さらに、何らかの障害で、登録しているチェインが変更されてしまったとしても復旧できるようにするために使用する。

L2 スイッチを用いた遮断　情報の取得機能を用いて、MAC アドレス、対象の L2 スイッチの IP アドレス、L2 スイッチの接続ポートを得る。通常 FDB はポートに接続すると自動的に MAC アドレスが登録される。このような状態を Dynamic モードという。この設定を Static モードに変更することにより、FDB に自動的に MAC アドレスを登録できないようにする。次に、FDB から対象となる MAC アドレスを削除する。これで、対象となるホストは遮断されたことになる。この作業は Telnet を用いて L2 スイッチにログインして行う。

2.4　遮断の解除機能

Firewall を用いた遮断の解除　基本的に Firewall を用いた遮断と同様の流れをとる。異なる点は、チェインの追加が削除に変更するという点と、遮断時に生成したチェインをシェルスクリプトから削除するという点である。

L2 スイッチを用いた遮断の解除　基本的に L2 スイッチを用いた遮断と同様の流れをとる。異なる点は、解除を行うポートを Dynamic モードに変更し、FDB の操作は行わない点である。しかし、カスケード接続により不正ホストが 2 台以上接続されていた場合、Static モードのままで、FDB に解除対象となる MAC アドレスを登録する。

3　実装

Firewall を用いてあるホストの tcp80 番ポートのパケット制御した後、そのホストのブラウザを用いてインターネットに接続した結果を図 1 に示す。Firewall を用いた遮断により、指定したパケットを遮断しているのが分かる。

あるホストに ping を送り続けながら、L2 スイッチを用いて遮断する前、遮断後、遮断解除後の結果を図 2 に示す。L2 スイッチを用いた遮断によりパケットが遮断され、解除後にパケットが通過しているのが分かる。

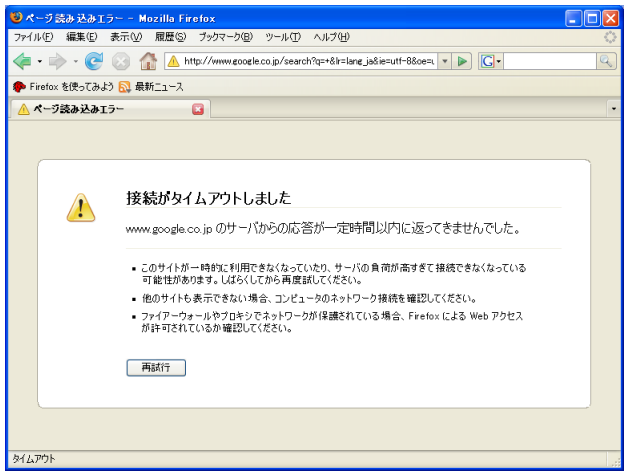

図 1: Firewall を用いて遮断を行った結果

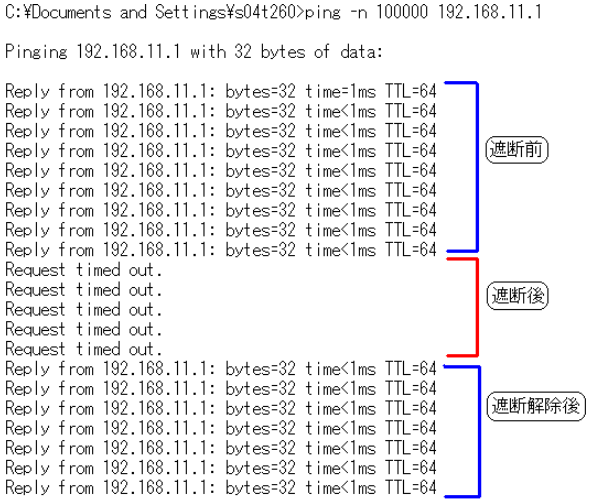

図 2: L2 スイッチで制御を行った結果

4　まとめ

自動制御ツールの機能である、情報の取得、通信の遮断、遮断の解除の機能を実現できた。今後の課題として、実環境での実験を行うことが挙げられる。

参考文献

[1] 串間竜治, “レイヤ 2 スイッチを用いた不正パケット遮断システムの研究”, 香川大学大学院 工学研究科, 修士論文, 2006.

[2] 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.

[3] 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.