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

06G470 高橋 巧 （最所研究室）

本稿では、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遮断する、不正パケット遮断システムの設計と開発について説明し、そのシステムの運用に際して重要な要素であるポリシについての検討・実装について記述している。

1 はじめに

現在、組織における個人情報・機密情報の保護は、組織の運営に関わる問題であるため、情報流出の防止は個人や組織にとっての最重要課題のひとつと言える。また、この問題が発生した場合、組織のネットワーク管理者（以下：管理者）に対して解決が求められるが、問題の性質から、管理者に対して素早い問題解決能力等が要求される。このため、管理者にとっての負担が大きく増大してしまう。

以上を解決するため、侵入検知システム（IDS）を利用して不正パケットを発行したホストを特定し、L2スイッチを用いて遮断する、不正パケット遮断システム機構の開発を行っている [1]。

本研究ではセキュリティの更なる強化と、ユーザに対してセキュリティ意識を高めさせることを目的とした、不正パケットを発する特定ホストの自動遮断・自動解除を行うシステムの開発を行う。本稿では、不正パケット遮断システムの概要と、システムを運用する際の重要な要素であるポリシについて述べる。

2 不正パケット遮断システムの概要

不正パケット遮断システムの概要を図1に示す。IDSが不正パケットを検知しポリシに通知を行い、それを合図にポリシが不正ホストを特定し、Firewall あるいは L2 スイッチのどちらで遮断を行うかを決定する。その後、制御ツールがポリシの決定に従い不正ホストを自動遮断することで、組織内部からの情報流出を阻止するものである。不正ホスト遮断後、ポリシが不正ホストの情報をユーザ管理 DB に登録する。最後に、ポリシが遮断を行ったホストを保持するユーザにメール通知を行うことで一連の処理を終了する。メール通知を行う際にユーザに対策法を示すことで復帰を助ける。PC を特定する際は、ルータの ARP テーブルが持つ IP アドレスと MAC アドレスの組み合わせ情報や、ユーザ管理 DB が保持する MAC アドレスとユーザ ID の組み合わせ情報を用いる。今回の実装では、IDS として Snort を用いる。インタフェースはユーザ情報の閲覧等を行うために利用する。

ホストの自動解除時も同様に、ポリシの決定を基にして制御ツールが Firewall あるいは L2 スイッチを制御することで実現する。

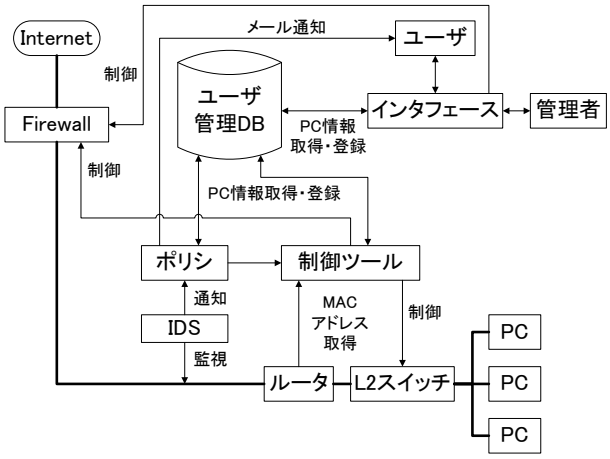

図 1: システム図

制御ツールは共同研究者の原田氏 [2] が、インタフェースは岡原氏 [3] がそれぞれ開発している。

「ユーザに対してセキュリティ意識を高めさせる」ためにシステムに盛り込む教育的要素として 2 つの機能を検討している。一つは、自動解除を行う際、ユーザの発した不正パケット情報を表示する画面の URL を添付したメールをユーザに送信する機能である。その際はユーザに確認ボタンをクリックさせ、その後自動解除を行う。もう一つは、不正パケットに対処できないユーザのために、不正パケットについての対処法を示す機能である。更に、第三者を参加させ悪意を持ったユーザに対する抑止力とすることも考える。

3 システム運用ポリシ

管理者がユーザ管理を行いやすくかつユーザに対する教育効果を期待できる運用ポリシを検討する。ポリシに基づき、それぞれの不正パケットに対してレベル付けを行い、それを基に該当ホストの自動遮断、自動解除手法を決定する。その流れの中で、遮断を行ったホストを保持するユーザへのメール通知や、不正ホスト情報の登録を行う。以下、各ポリシのレベル付けに関して述べる。

3.1 自動遮断ポリシ

自動遮断のレベルを検討する。セキュリティの強力な遮断手法順に並べると、L2 スイッチで即時遮断＞Firewall で即時遮断＞時間を置いて L2 スイッチで遮断＞時間を置いて Firewall で遮断＞ユーザに対する警告のみ、というレベル付けになる。

3.2 自動解除ポリシ

自動解除のレベルを検討する。「ユーザ通知の有無」、「遮断手法」、「遮断回数」によりレベルを決定する。信頼性の高い解除手法順に並べると、不正パケット観測を行った後 L2 スイッチレベルで解除＞不正パケット観測を行った後 Firewall レベルで解除＞前科のないユーザからの通知が来た後解除＞ Firewall レベルで遮断されていたユーザからの通知が来た後解除＞ L2 スイッチレベルで遮断されていたユーザからの通知が来た後解除、というレベル付けになる。

3.3 メール通知ポリシ

本システムにおける教育的要素の一つであるメール通知ポリシを検討する。「遮断回数」によりレベルを決定する。対象が少ない通知手法順に並べると、不正パケットを発したユーザのみに通知＞ユーザ、管理者に通知＞ユーザ、管理者、ユーザの上司に通知＞ユーザ、管理者、ユーザの上司、所属部署に通知＞インタフェースを使って悪質なユーザとして公開、というレベル付けになる。

4 自動遮断ポリシの設計・実装

4.1 必要機能

必要機能を以下に述べる。Snort が登録を行った不正パケット情報の取得を行うアラート情報取得機能、不正ホストを保持するユーザの特定を行うユーザ特定機能、不正ホストへの処理方法の決定を行う遮断レベル決定機能、制御の結果得られた情報をユーザ管理 DB に登録を行うユーザ管理 DB への情報登録機能、不正ユーザに対するメール通知機能、である。

4.2 ホストの遮断

遮断レベルの決定とホストの遮断について述べる。まず、新たなパケット情報が確認できた場合はその情報を取得する。取得する情報は、IP アドレス、タイムスタンプ、そして Snort が規定しているクラスタイプ（攻撃手法）である [4]。次に、IP アドレスを基にユーザ特定を行う。続けて、遮断レベルを決定する。遮断レベル決定の際は、ユーザの現在までの遮断・警告回数やクラスタイプを用いる。遮断レベル決定後に制御ツールの関数を呼び出し、ホストに対する遮断処理を行う。処理終了後、ユーザ管理 DB に決定事項の登録を行う。そして最後に、メール通知ポリシを基にユーザに対してメール通知を行う。

5 自動解除ポリシの設計・実装

5.1 必要機能

必要機能を以下に述べる。解除時に不正ホストに対してメール通知を行う解除メール通知機能、不正ホストへの解除処理法の決定を行う解除レベル決定機能、制御の結果得られた情報をユーザ管理 DB に登録を行うユーザ管理 DB への情報登録機能、である。

5.2 ホストの解除

解除レベルの決定とホスト遮断状態の解除について述べる。まず、解除時刻に到達した際に、不正ホストに対してメール通知を行う。その際に、ユーザ通知を受け付ける期限を設ける。その期限に達した後、ユーザ通知の有無、遮断手法、遮断回数を参照して解除レベルの決定を行った後、制御ツールの関数を呼び出し、ホストの解除を行う。解除処理が終了した後、ユーザ管理 DB に決定事項の登録を行う。

6 まとめ

本研究では、不正パケット遮断システムの概要について考案し、システムに盛り込む教育的要素やシステム運用ポリシの策定を行った。また、策定したポリシに基づいて、具体的なポリシの設計・実装を行った。そして、IDS とポリシの連携による、不正パケットの自動遮断を確認できた。同時に、遮断ホストの自動解除も確認できた。

今後の課題としては、IDS からの情報取得の効率化や、教育的要素の実装・充実化を行うことがある。また、ポリシを制御ツールやインタフェースと統合を行い、一つのシステムとすることも挙げられる。

参考文献

[1] 串間竜治・長野一樹・ 最所圭三, “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設計”, 平成 18 年度 電気関係学会四国支部連合大会論文集 16-8：p.250, 2006.

[2] 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, 2008.

[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”, 香川大学工学部卒業論文, 2008.

[4] Martin Roesch, “Snort ユーザズマニュアル Snort Release: 2.0.2”, Sourcefire, 2003.