1W-02

トラフィック監視による不正通信遮断システムの提案

田場　典智 †1　　長田　智和 †2　　谷口　祐治 †3

†1 琉球大学工学部情報工学科　　†2 琉球大学工学部工学科知能情報コース
†3 琉球大学総合情報処理センター

1　はじめに

2018 年現在，DoS 攻撃を始めとするサービス妨害攻撃は，世界的な問題として取り上げられている。実際に本学科にも，同様な攻撃系パケットがいくつも来ている。それにより，本学科と総合情報処理センターとの中間に位置する 1 台の UTM に多大な負荷がかかり，学科内外の通信が正常に行えない問題が度々生じた。その問題に対し，手動で本学科内のメインスイッチで不正アクセスを行う IP の通信にフィルタをかける対策を講じた。しかし，現在も外部からのグローバル IP アドレスに対する不正通信は頻繁に行われており，UTM がサービス不能に重くなってしまう問題は続いている。そこで本研究では，その問題を解決するため，Snort による DoS 攻撃の検知から, 上位メインスイッチにおいて，ブラックリストの更新に至る過程を自動化し，UTM の高負荷によるハングアップを防止する不正通信遮断システムを提案する。加えて，複数台のハニーポットを用いて，UTM の制御を超えて行われる認証を伴う不正アクセスを検知し攻撃元を特定することで，上記同様にブラックリストに自動で追加する機能を実装する。

2　関連研究と課題

Snort と低対話型ハニーポットの honeyd を用いた IP アドレスベースのフィルタリングを可能とする不正通信防止システムに関する研究として，比嘉らの研究 [1] がある。この研究では，snort と honeyd のログに現れる攻撃・不正アクセス元 IP アドレスを収集し，ブラックリストを作成しており，iptables を用いてフィルタリングを行っている。しかし，過去にフィルタ対象となり，現在ではアクセスがない IP アドレスがブラックリストに残り続けてしまう問題がある。

3　研究概要

3.1　Modern Honey Network

Modern Honey Network とは，ハニーポットが動作する sensor server，デプロイ及び sensor server で収集した情報の管理を行う mhn server の 2 つからなるシステムで構成されている。本研究では環境構築にかかるコストを抑え，実験環境を容易に実装することが可能な Modern Honey Network で複数のハニーポットを一元管理する。図 1 は，Modern Honey Network の構成要素を示している。

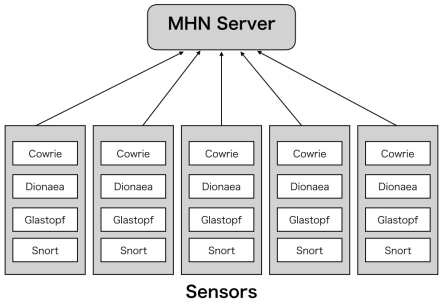

図 1: mhn の構成要素

3.2　提案システムの概要

本稿では，Snort を用いて DoS 系のトラフィックを検出するとともに，UTM を超えて行われる攻撃に対しては，ハニーポットで検知し，収集した IP アドレスを元にブラックリストを自動で更新するシステムを提案する。システムの環境概要を表 1 に示す。

提案システムでは，Snort とハニーポットを用いて，外部からの攻撃元アドレスを特定し，メインスイッチのブラックリストを Perl スクリプトを用いて自動で更新する。また，本システムではブラックリストに現在アクセスのない IP アドレスが残り続けてしまう問題を解

Network Monitoring and Topology Visualization Using OpenFlow
Noritomo Taba†1　Tomokazu NAGATA†2
Yuji TANIGUCHI†3
†1Faculty of Engineering and Information Engineering, University of the Ryukyus
†2Faculty of Engineering Computer Science and Intelligent Systems Program, University of the Ryukyus
†3Information Processing Center,

表 1: システムの環境概要

OS	CentOS 7.2
Snort	2.9.9.0
PostgreSQL	9.2.23
Perl	5.26.0
Modern Honey Network	2.1

消する目的で，攻撃元 IP アドレス及び特定した日時などの情報は，データベースを用いて管理を行う。また，Perl スクリプトは Snort が稼働しているサーバーで動作している。提案システムの運用構成を図 2 に示す。

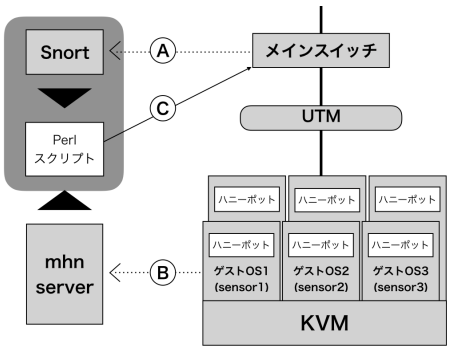

図 2: 運用構成

A) メインスイッチの全トラフィックを Snort で監視。(主に DoS 攻撃の検知)

B) 各 sensor server での不正アクセス検知，その情報を mhn server へ送信。(主に不正アクセスの検知)

C) メインスイッチのブラックリストに，特定した攻撃元の IP アドレスを追記し，更新する。

3.3 Snort による特定

Snort による DoS 攻撃を行なっている攻撃元 IP アドレスの特定は，alert が変更されたタイミングで，Perl スクリプトを用いて，外部のアドレスのみを抽出している。さらに，検知した攻撃元 IP アドレスをデータベースに格納し，検知日時を保存する。再度このアドレスが検知されると，レコードを更新する。レコードの最終更新日を，アドレス検知時に比較することで，過去にフィルタ対象となり，現在ではアクセスがない IP アドレスを削除し，ブラックリストに IP アドレスが残り続けてしまう問題を解消する。

3.4 ハニーポットによる特定

提案システムの目的では，UTM を越えて行われる認証を伴う不正アクセス元のアドレスを特定することにあるため，リスクの低い低対話型でも問題なく不正通信遮断システムを運用することが可能である。ハニーポットは，Modern Honey Network でデプロイ用のスクリプトが用意されている，複数のサービスをエミュレートできる dionaea，80 番ポートに対しての不正アクセスに有効な glastopf，ssh に特化した cowrie の 3 種類の低対話型ハニーポットを使用する。特定に関して，Modern Honey Network は REST API により，稼働しているハニーポットらが所有するアクセスログを収集し，攻撃元の IP アドレスや，日時，攻撃の種類などの情報を取得することができる。

4 開発状況

開発前段階において，実際に学科に攻撃系パケットが来ていることを確認した。現在は，Snort が検知した攻撃を Alert に出力するタイミングで，Perl スクリプトによりデータベースへ IP アドレスを格納し，Modern Honey Network から API を通して，ハニーポットへの攻撃情報の取得までを実装している。現在はメインスイッチに Perl スクリプトを用いてアクセスし，ACL の設定を更新する機能の追加がまだ未実装なため，その実装を進めている。

5 おわりに

調査の結果，現在も絶えず学科に攻撃系パケットが来ていることが分かった。Snort とハニーポットを活用し，Perl スクリプトに Alert ファイルの変更検知を行うことで，リアルタイムに攻撃元の IP アドレスを検知することが可能であり，DoS 攻撃に有用であると考えた。本稿では，Snort で UTM に流れる前のトラフィックを監視し，攻撃元を特定するとともに，UTM を超えて行われた攻撃に対しては，Modern Honey Network の REST API の機能を用いて設置したハニーポットらから攻撃元の特定を行う。さらにそれら攻撃元 IP アドレスをデータベースに集約し，メインスイッチのブラックリストへの更新処理を Perl スクリプトを用いて自動で行うシステムを提案した。今後は，現在開発中の提案システムを構築し，実際に学科システムに導入し，有効性を評価する予定である。

参考文献

[1] 比嘉哲也 他，“NIDS とハニーポットを組み合わせた不正侵入防止システムの開発”，電子情報通信学会信学技法研究会,vol 109，pp.1-4，2010