Vol.2021-CSEC-93 No.10
Vol.2021-IOT-53 No.10
2021/5/13

IDS・SDN連携型ファイアウォールシステムにおけるSNMPトラップを用いたアラート通知

サリチ エルトゥール[1]　並木 涼[1]　山井 成良[1,a)]

概要：
ファイアウォールシステムの構成法としてIDS（Intrusion Detection System）とSDN（Software Defined Network）システムとを併用するIDS・SDN連携型ファイアウォールシステムが構成や機能の柔軟性の観点から注目されている．この構成法ではIDSからSDNコントローラへのアラートの通知方法が問題となる．本稿ではSNMPトラップによりアラートを通知する方法を提案する．これにより従来のsyslogに比べてSDNコントローラでの解析が容易になる効果が期待できる．

キーワード：
ファイアウォール，IPS，IDS，SDN，SNMP

Alert Notification using SNMP Trap in Firewall System Cooperating with IDS and SDN

Salic Ertugrul[1]　Ryo Namiki[1]　Nariyoshi Yamai[1,a)]

Abstract:
As one of the configuring methods of firewall systems, IDS/SDN-cooperating firewall systems that consist of IDS (Intrusion Detection Systems) and SDN (Software Defined Network) equipments are attracting attention from the viewpoint of flexibility in configuration and functions. In this configuration method, how to notify alerts from the IDS to the SDN controller is an important design issue. In this paper, we propose a method of alert notification using SNMP trap. In this paper, we propose a method using SNMP trap to notify alerts, which is expected to facilitate analysis by the SDN controller compared to conventional syslog function.

Keywords:
firewall, IPS, IDS, SDN, SNMP

1. はじめに

ファイアウォールは多くの場合組織内ネットワークと組織外ネットワークとの境界に設置され，主に組織外ネットワークからの攻撃や不正なアクセスを解析してこれらを遮断し，安全な通信のみを許可するシステムを指す[*1]．ネットワーク経由でのサイバー攻撃が年々増加している現代社会では，ファイアウォールは必要不可欠な存在であると言える．

ファイアウォールにはIPアドレスやポート番号などのレイヤ2-4情報に基づくフィルタリングを行うものや，DPI（Deep Packet Inspection）のようにペイロードの検査を行ってその結果に基づきフィルタリングを行うものなどが含まれており，様々な構成法がある．その1つとして，不正通信をIDS（Intrusion Detection System）により検出し，これをSDN（Software Defined Network）により遮断する構成法（以下，IDS・SDN連携型ファイアウォールシ

[1] 東京農工大学
Tokyo University of Agriculture and Technology
2-24-16, Nakacho, Koganei, Tokyo 184–8588, Japan
[a)] nyamai@cc.tuat.ac.jp

[*1] ファイアウォールの定義はまちまちであるが，本稿では不正通信を遮断するシステム全般を指し，IPS（Intrusion Protection System）の機能を含むものとする．

ステム）[1] が知られている．この構成法ではたとえば検査内容の異なる IDS を用いて不正通信の検出精度を高めたり，SDN で単に不正通信を遮断するだけでなくハニーポットに誘導したりすることも可能であり，従来の構成法より構成や機能の柔軟性が高い点で注目されている．

IDS・SDN 連携型ファイアウォールシステムでは IDS から SDN コントローラへの遮断内容の通知方法が設計上の問題として重要となる．桂らは IDS からのアラートメッセージをログファイルに記録し，ログ監視ツールを用いてこれを検出して REST（Representational State Transfer）[2] により SDN コントローラに通知する方法を用いた [3]．しかし，この方法ではログ監視のオーバヘッドが大きく，遮断動作が遅い点が問題となっていた．これに対して，我々は OpenFlow を用いた IDS・SDN 連携型ファイアウォールシステムにおいて IDS が syslog によりアラートメッセージを出力し，これを受け取った OpenFlow スイッチがそれを Packet-In により OpenFlow コントローラに中継し，これを OpenFlow コントローラが解析して OpenFlow スイッチに通信を遮断するようにフローエントリを追加する方法を提案した [4]．

本稿では SNMP（Simple Network Management Protocol）トラップ [5], [6] を用いて SDN コントローラにアラート通知を行う方法を提案する．米国国立標準技術研究所（NIST）による IDPS[*2] のガイド [7] では IDS が有するアラート通知方法の例として SNMP トラップが示されており，一般的なアラート通知方法である．syslog に加えて SNMP トラップをアラート通知に利用することで，利用可能な IDS の種類が増える効果が期待できる．また，SNMP トラップはメッセージのフォーマットが定まっているため，コントローラでの解析が比較的容易になる効果が期待できる．

2. syslog を用いたアラート通知

文献 [4] では IDS・SDN 連携型ファイアウォールシステムにおいて syslog によりアラート通知を行う方法を提案した．以下では**図 1** に示すように SDN として OpenFlow を用いる場合のシステム構成において IDS から OpenFlow コントローラにアラート通知を行う方法を説明する．

同図において IDS，OpenFlow スイッチ，OpenFlow コントローラは次のように動作する．

(1) OpenFlow スイッチはクライアント・サーバ間でやり取りされるパケットをミラーリングにより IDS に転送する．
(2) IDS は受信したパケットがアラート対象と判断した場合，アラートメッセージを syslog プロトコルにより UDP パケットとして OpenFlow スイッチに送信する．

[*2] IDS と IPS の総称．

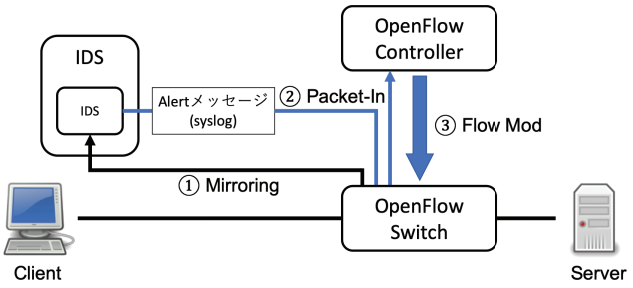

図 1 IDS から OpenFlow コントローラへの syslog を用いたアラート通知 [4]

(3) OpenFlow スイッチは受信したアラートメッセージを Packet-In により OpenFlow コントローラに転送する．
(4) OpenFlow コントローラは受信したアラートメッセージを解析し，制御対象となるトラフィックを特定する．
(5) OpenFlow コントローラは OpenFlow スイッチに対して制御対象となるトラフィックの遮断やハニーポットなどに転送するための設定（FlowMod）を行う．

なお，アラートメッセージの送信先 IP アドレスは実在する syslog サーバである必要はないが，syslog サーバが実在すれば OpenFlow スイッチでは OpenFlow コントローラへの Packet-In だけでなく syslog サーバへの転送も行うようにフローエントリを設定しておく必要がある．

上記の動作により，IDS は REST API を syslog メッセージを出力できる任意のものを使用することができ，ログ監視ツールを用いる必要がないことからオーバヘッドを削減する効果が期待できる．プロトタイプシステムで性能評価実験を行った結果，OpenFlow スイッチがパケットをミラーリングしてからアラートメッセージを中継するまでの時間が従来のログ監視ツールを用いる方法では 700ms であったのに対して syslog を用いた方法では 527ms となり，173ms のオーバヘッド削減効果が確認された．

3. SNMP トラップを用いたアラート通知

REST を用いずに IDS から SDN コントローラにアラート通知を行う方法は syslog に限られるものではない．しかし，TCP など複数のパケットをやり取りする必要がある通知方法はオーバヘッドが大きくアラート通知には適さない．そこで，syslog に加えて SNMP トラップを用いる方法を提案する．SNMP トラップは syslog と同様に UDP により送信されるため，1 パケットで通知することが可能である．

SNMP にはいくつかのバージョンが存在するが，そのうち試作システムで用いた Community-based SNMPv2（SNMPv2c）のパケットフォーマットを**図 2** に示す．各項目はタグ（データタイプ），長さ，データの 3 つのフィールから構成され，Variable Bindings を除く部分がヘッダである．SNMP トラップでは PDU Type のタグが 0xA7 と

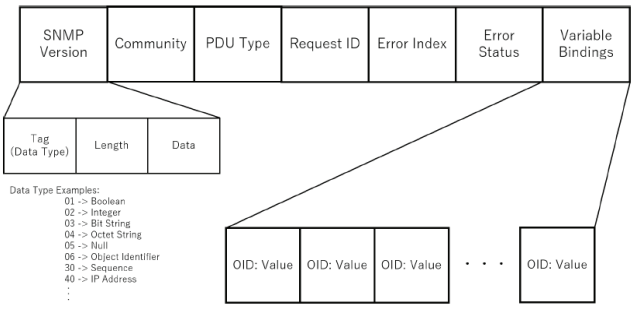

図 2 SNMPv2 のパケットフォーマット

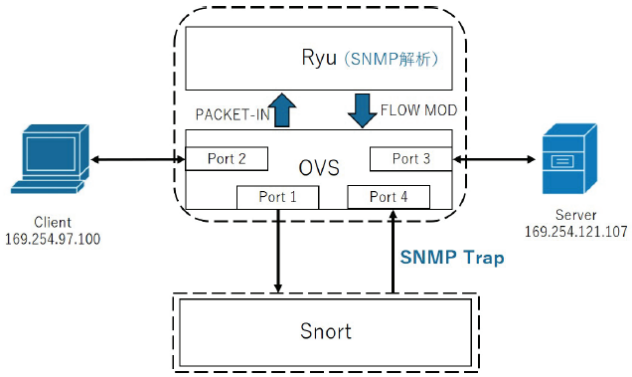

図 3 試作システムの構成

なっている．また，通知対象となるフロー情報は Variable Bindings の中に含まれる．syslog ではテキストフォーマットが用いられるため SDN コントローラで解析する際に正規表現などを用いた解析が必要となるが，SNMP トラップではこのようなフォーマットが用いられるため不要な部分は読み飛ばすことが可能で，SDN コントローラでの解析が比較的容易である．

3.1 試作システムの実装

我々は従来の IDS・SDN 連携型ファイアウォールシステムを改変し，syslog の代わりに SNMP トラップを用いたアラート通知を行う IDS・SDN 連携型ファイアウォールシステムを試作した．試作システムの構成を**図 3** に示す．この図において OpenFlow スイッチとして動作する Open vSwitch および OpenFlow コントローラとして動作する Ryu は 1 台の Raspberry Pi 4 に同居させ，IDS（Snort），クライアント，サーバはそれぞれ Raspberry Pi 3 を用いた．各ホストのスペックを**表 1** に示す．また，Open vSwitch，Ryu，Snort のバージョンを**表 2** に示す．なお，Snort で SNMP トラップを出力するためのプラグインである Snort-SNMP は Snort version 2.9.3.1 までしか対応しておらず，そのままでは試作システムで使用した Snort version 2.19.7 に対応していない．そこで，このプラグインを一部修正して Snort version 2.19.7 でも使用できるようにした．

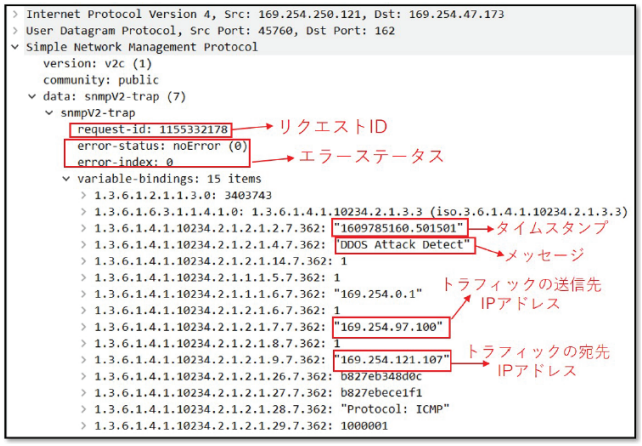

図 4 SNMP トラップによるアラートメッセージ

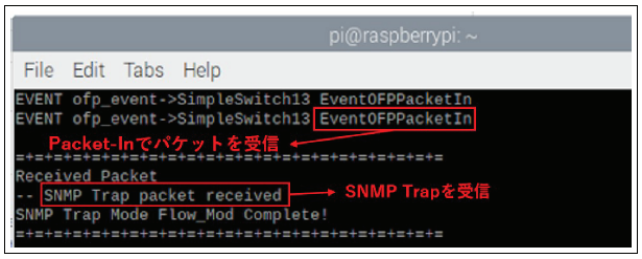

図 5 Ryu が SNMP トラップを受信した際のコンソール画面

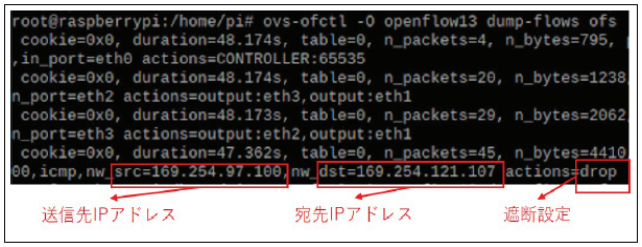

図 6 ICMP flood 攻撃後の Open vSwitch のフローテーブル

3.2 試作システムの動作検証

前節で説明した試作システムの動作を確認するため，図 3 の構成においてクライアントからサーバに疑似攻撃を行い，OpenFlow スイッチで遮断できるかどうかを検証した．疑似攻撃の方法としては hping3 による ICMP flood 攻撃を採用し，Snort にはこれを検出するルールを設定した．

検証の結果，Snort からは**図 4** に示すようなアラートメッセージが送信され，**図 5** に示すようにこのメッセージを Ryu が Packet-In により受信していることを確認した．また，Open vSwitch のフローテーブルを確認したところ，**図 6** に示すようにクライアントからサーバへの ICMP パケットを廃棄するエントリが追加されていることを確認した．なお，図 4 では図 2 における Variable Bindings の部分が OID（Object Identifier）の数字表記とその値の組合せのシーケンスとして示されているが，各 OID の意味については文献 [9] を参照されたい．

表 1　主な構成要素の諸元

役割	モデル名	プロセッサ	クロック周波数	メモリ容量	ネットワーク帯域
OpenFlow スイッチ，コントローラ	Raspberry Pi 4 Model B	BCM2711	1.5GHz	4GB	1Gbps
Snort	Raspberry Pi 3 Model B+	BCM2837B0	1.4GHz	1GB	300Mbps
クライアント	Raspberry Pi 3 Model B+	BCM2837B0	1.4GHz	1GB	300Mbps
サーバ	Raspberry Pi 3 Model B+	BCM2837B0	1.4GHz	1GB	300Mbps

表 2　主な構成要素で使用するソフトウェア

役割	ソフトウェア名，バージョン
OpenFlow スイッチ	Open vSwitch version 2.10.1
OpenFlow コントローラ	Ryu version 4.34
IDS	Snort version 2.9.17
SNMP	SnortSNMP[8]

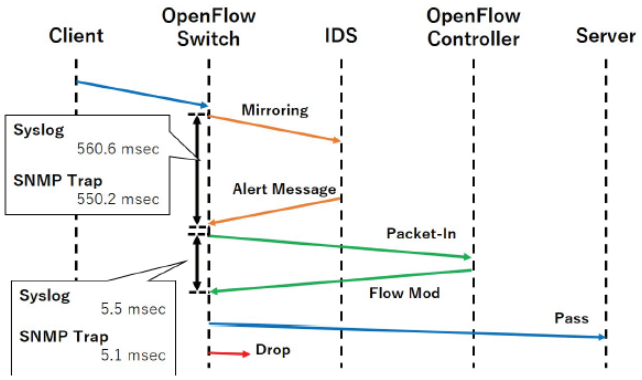

図 7　各アラート通知方法におけるアラート通知時間および遮断動作時間

3.3　試作システムの性能評価

次に，SNMP トラップによるアラート通知が十分高速に攻撃遮断動作を行えることを確認するため，試作システムの性能評価実験を行った．比較の対象として，図 3 と同じ構成において syslog によりアラート通知を行うシステムを実装した．疑似攻撃は動作検証と同様に hping3 コマンドによる ICMP flood 攻撃とし，1 回の実験では ICMP パケットをクライアントから 100 回送信し，Open vSwitch が最初の ICMP パケットをミラーリングしてからアラートメッセージを受け取るまでの時間ならびに Open vSwitch がアラートメッセージを Packet-In してから FlowMod メッセージを受け取るまでの時間を測定した．この実験を各通知方法について 5 回行い，その平均を求めた．

実験結果を**図 7** に示す．この図からわかるように，SNMP トラップによるアラート通知は syslog によるアラート通知よりも若干速く，十分高速であるといえる．

4.　まとめ

本稿では IDS・SDN 連携型ファイアウォールシステムにおいて，従来の syslog によるアラート通知に加えて新たに SNMP トラップによるアラート通知を提案した．また，IDS としてよく知られている snort に SNMP トラップによるアラート通知機能を組み込み，syslog によるアラート通知と比較して若干速く動作することを確認した．

今後の課題としては，IDS には双方向のパケットが全てミラーリングされることから，複数の IDS を用いて負荷を分散する方法が挙げられる．

参考文献

[1] Paul Zanna, Benjamin O'Neill, Pj Radcliffe, Sepehr Hosseini, MD. Salman Ul Hoque: "Adaptive Threat Management Through the Integration of IDS Into Software Defined Networks", *Proceedings of 2014 International Conference and Workshop on the Network of the Future (NOF2014)*, pp.13–17, December 2014.

[2] Roy Thomas Fielding: "Fielding Dissertation: CHAPTER 5: Representational State Transfer (REST)" (online), available from ⟨https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm⟩ (accessed 2021-04-07), 2000.

[3] 桂祐成，君山博之，堤智昭，米﨑直樹，丸山充: "ソフトウェアスイッチを使ったリアルタイム総当たり攻撃検出遮断システムの提案"，電子情報通信学会技術研究報告，NS2018-272, pp.461–464，2019 年 3 月．

[4] 桂祐成，児玉伊太郎，Pranpariya Sakarin，山井成良，君山博之，Vasaka Visoottiviseth : "IDS・SDN 連携型ファイアウォールシステムにおける遮断動作の高速化"，インターネットと運用技術シンポジウム 2019 論文集，Vol.2019，pp.116–117，2019 年 12 月．

[5] Case, J., Harrington, D., Presuhn, R. and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, IETF, December 2002.

[6] Presuhn, R., Ed., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMPv2)", STD 62, RFC 3416, December 2002.

[7] Karen Scarfone, Peter Mell: Guide to Intrusion Detection and Prevention Systems (IDPS) (online), Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-94, available from ⟨https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf⟩ (accessed 2021-04-07), February 2007.

[8] Cyber Solutions Inc.: SnortSNMP (online), available from ⟨https://www.cysol.co.jp/index.php/socialcontribution/snortsnmp⟩ (accessed 2021-04-07), March 2014.

[9] Glenn Mansfield Keeni: The SnortSnmpGuide (online), available from ⟨https://www.cysol.co.jp/contrib/snortsnmp/snortSnmpGuide.html⟩ (accessed 2021-04-07), May 2002.