1ZA-03

SRv6による組織内ネットワークにおける攻撃由来通信の隔離ネットワーク誘導

坂尾優斗† 嶋田創‡

名古屋大学情報学研究科† 名古屋大学情報基盤センター‡

1. まえがき

近年，企業などを狙った標的型攻撃による被害が深刻となっている．攻撃を受け，組織内の端末が感染していることが発覚した場合，感染拡大を抑えるために早急に組織ネットワークから隔離することが重要である．しかし，単純に物理ネットワークから切り離すだけでは，それがどのような攻撃なのかを知ることができず，対策を立てることが難しくなる．また，そうした封じ込めを攻撃者やマルウェアが検知した場合，再攻撃や，データの上書きや暗号化などといった証拠隠滅行動を起こす可能性がある．逆に，あえて封じ込めを遅らせて攻撃者の行動を監視するという手段もあるが，こちらは自組織のネットワークを踏み台にされ，第三者への攻撃に利用される可能性もあり，非常にリスクのある手法であると言える．そこで，仮想環境を用いて攻撃を仮想環境に誘導し，安全に挙動を観察するという手法が考案されている．これにより，実環境を保護しつつ，攻撃者や感染端末の行動を観察することができる．

こうした悪性通信の隔離ネットワーク誘導と観察の手法に関する研究は既に行われており，その実現手法は OpenFlow などの SDN(Software Defined Network)技術の利用[1]や仮想環境での実環境の模倣[2]など，様々である．

OpenFlow などの従来の SDN は自由度が高い代わりにコスト性能比が悪いため，近年では送信元のネットワークスイッチ等で通信経路が指定できる Segment Routing の技術が，より軽量な SDN として活用され始めている．特に，Segment Routing を IPv6 ネットワーク上で行う SRv6(Segment Routing over IPv6)は，IPv6 トンネリングなどの技術と併用することで，現在まで主として利用されている IPv4 通信に対しても Segment Routing を提供することができる．

本実験では，マルウェア感染端末の通信を仮想マシンに誘導するネットワーク制御を，SRv6 を利用したサブネット単位での経路変更で実現する．

2. 提案システム

本稿では，文献[1]で提案されている組織内のネットワークに接続している端末がマルウェア等に感染していることが判明した後の処置として感染端末による通信を隔離ネットワークへ誘導する手法に対して，SRv6 を導入することによるコスト低減と経路設定能力向上の実現を提案する．この手法では，攻撃を受けていない平常時の通信は実環境で通常通り行い，攻撃を受けて感染した端末が確認され次第，ルータに SRv6 の設定を追加し，感染端末からの通信を全て隔離ネットワークへ誘導する．もしマルウェアを完全に除去し，感染端末が安全になれば，ルータから SRv6 の設定を消去し，感染端末と実環境の通信を再開する．

提案構成の得失を表 1 に示す．OpenFlow は IP アドレス単位での細かな制御の点で優れるが，コストの点で不利である．隔離ネットワークをクラウドに設置する場合，SRv6 はネットワークスイッチの機能のみで実現できるに優れる．

表 1: 隔離ネットワーク誘導手法と得失

	IPv4 のみ	SRv6	OpenFlow
IP アドレス単位の制御	×	×	○
外部 NW（クラウド）との連携	△ (VPN)	○	△
コスト	○	○	△

3. 実装

本研究は，ネットワークシミュレータである

Diverting Attack Traffics on Internal Network to Isolated Network using SRv6

† Sakao Yuto・Graduate School of Information Science, Nagoya University

‡ Simada Hajime・Information Technology Center, Nagoya University

GNS3 上で行い，ルータとして VyOS，クライアントおよびサーバとして VPCS を用いて図 1 のような検証ネットワークを構成した．このネットワークは，端末とルータ間のネットワークが IPv4，ルータとルータ間のネットワークが IPv6 となっており，それぞれのルーティングは全て静的に行った．また，端末間の通信には，IPv6 トンネリング技術を用いた．ここでは，PC1 がマルウェア等に感染したと想定し，PC1 から PC2，および PC1 から Server への通信を，SRv6 を利用して攻撃観察用の環境に誘導した．なお，攻撃観察用の環境から PC1 への返信は SRv6 を用いず，IPv6 トンネリングを用いた静的ルーティングを採用した．平常時の通信では，PC1 からの PC2 への通信や Server への通信は実環境内で正しく行われる．一方，攻撃観察時の通信では，PC1 からは PC2 や Server へ通信を行っているように見えるが，実際はルータ（VyOS-1 および VyOS-4）によって通信が捻じ曲げられており，攻撃観察用環境の偽の端末と通信を行っている．

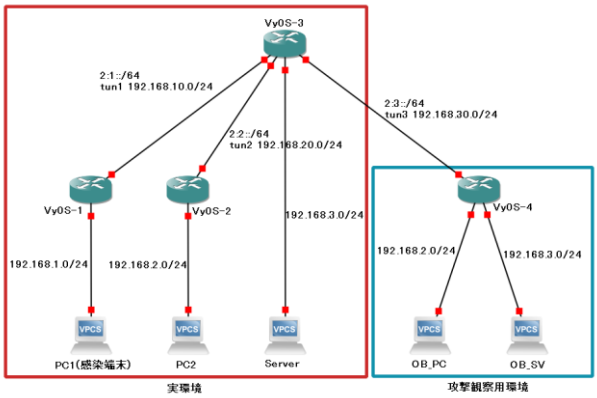

図 1：検証ネットワーク

まず，図 1 の通りにネットワークを設定した．
続いて，VyOS-1，VyOS-4 に対して次の手順で SRv6 の設定を行った．

1. VyOS-1，VyOS-4 の通信に関する設定ファイル"/etc/sysctl.conf"に以下の設定を加え，SRv6 機能を有効化する．

```
net.ipv6.conf.all.seg6_enabled = 1
net.ipv6.conf.default.seg6_enabled = 1
net.ipv6.conf.eth0.seg6_enabled = 1
```

2. VyOS-1 で以下の 2 つのコマンドを実行し，IPv4 パケットのカプセル化，および拡張ヘッダの追加のための設定を加える．

```
vyos@vyos:~$ sudo ip route add
192.168.2.0/24 encap seg6 mode encap segs
2:3::1,2:10::2 dev eth0
vyos@vyos:~$ sudo ip route add
192.168.3.0/24 encap seg6 mode encap segs
2:3::1,2:10::3 dev eth0
```

3. VyOS-4 で以下の 2 つのコマンドを実行し，カプセル化されたパケットを IPv4 パケットに戻して攻撃観察用の端末へ転送するための設定を行った．

```
vyos@vyos:~$ sudo ip -6 route add 2:10::2
encap seg6local action End.DX4 nh4
192.168.2.1 dev eth1
vyos@vyos:~$ sudo ip -6 route add 2:10::3
encap seg6local action End.DX4 nh4
192.168.3.1 dev eth2
```

4. 検証実験

1. PC1 からの PC2，および Server への通信が攻撃観察用環境へ誘導されていることを確認するため，PC1 からそれぞれの端末へ ping を送信した．なお，このとき，実環境の PC2 と Server は起動せずに行った．
2. 続いて，隔離されていない端末同士が実環境内で正常に疎通できることを確認するため，PC2 と Server を起動し，PC2 から Server へ ping を送信した．

これらの通信は正常に行われた．また，感染端末から実環境内への通信と，感染端末から観察環境への通信では速度に大きな差が見られなかった．

5. あとがき

SRv6 を用いて感染端末からのパケットを仮想環境に誘導し，通信を観察する手法を提案した．この手法により，感染端末が属するサブネット以外に影響を与えず，安全に攻撃を観察することができる．ただし，文献[1]と比較して同一サブネットの端末への水平移動の防止やヘッダ打ち替えによる攻撃者への隠匿はできないため，使い分けが必要である．

参考文献

[1] 大橋宗治ら，"組織内部での攻撃行動を仮想環境へ誘導する挙動分析システム，" 信学技報，Vol. 119，No. 228，pp. 31-36，2019 年 11 月．
[2] 津田侑ら，"サイバー攻撃誘引基盤 STARDUST，" CSS2017 論文集，pp. 472-479，2017 年 10 月．