[ポスター発表] 研究報告

OpenFlowを用いて適応的な通信制御を行うDNSサーバファイアウォールの実装と評価

井上 知英[1,a)]　桝田 秀夫[2]　森 真幸[2]　永井 孝幸[2]

Implementation and evaluation of DNS server firewall by adaptive control mechanism using OpenFlow

1. はじめに

インターネットを支える技術の 1 つである DNS は，インターネットを運用する上で重要な情報を扱っているため，DNS の情報や仕組みを悪用しようとする攻撃が数多く存在する．当研究室の瀬川らは，DNS サーバの前段に DNS クライアントからの通信を監視するシステムを配置し，攻撃者からのクエリに対してレスポンスを適応的に制御することで攻撃を抑える手法の提案に関する研究 [1] を行った．この研究では，DNS プロトコルには変更を加えずに，提案システムがパケットの中継や破棄，制限を行う方式を提案している．しかし，Python ベースの scapy を用いているため，性能が大きく劣化する問題がある．本研究では，DNS サーバへの攻撃性通信を Snort を用いて検知し，攻撃の特徴を考慮した柔軟な通信制御を Open vSwitch と Ryu コントローラ を用いて行うことで権威 DNS サーバを防御するシステムの実装及び評価を行う．

2. 要求

システムの構築にあたり，以下の要求を満たすように実装を行うものとする．

R1 既存の DNS サーバ及び DNS プロトコルに変更を加えないこと
R2 DNS サーバに関する通信に基づいた対応が行えること
R3 DNS サーバに関する通信を制御できること

3. 提案システム

本章では，2 章で述べた要求を満たすため，権威 DNS サーバの前段に通信を監視，制御するシステムを配置し，攻撃を抑制する手法について述べる．本システムを以下 DNS サーバファイアウォールと呼ぶ．

[1] 京都工芸繊維大学 大学院 工芸科学研究科 情報工学専攻
Department of Information Science, Kyoto Institute of Technology
[2] 京都工芸繊維大学 情報科学センター
Center for Information Science, Kyoto Institute of Technology
[a)] t-inue19@dsm.cis.kit.ac.jp

3.1 DNS サーバへの攻撃性通信の制御

庇護 DNS サーバの前段に，ブリッジ型で動作する機器を配置しパケット単位で通信を分別する設計とする．これにより，庇護 DNS サーバの IP アドレスを変更する必要がなく，DNS プロトコル自体に手を入れていないため，要求 R1 を満たすことができると考えられる．

3.2 DNS サーバに関する通信の監視及び攻撃性通信の検知

庇護 DNS サーバへの通信パケットを，そのまま攻撃性通信の検知にも利用する設計とする．これにより，要求 R2 を満たすことができると考えられる．

3.3 攻撃性通信の特徴に基づいた通信制御

DNS サーバへの攻撃の種類は数多く存在し，情報漏洩の危険性がある通信は破棄，DDoS 攻撃などの大量の通信に対しては制限するなど，攻撃性通信を単純に破棄するだけでなく攻撃の検知結果に基づいて柔軟な通信制御を適用することでより効果的な防御に繋がると考えられる．著者は，Snort の DNS に関する約 70 種のシグネチャに対して，どのような通信制御をすべきかを検討しており，「中継」「破棄」「制限」に分類を試みている [2]．

これを組み込むことにより，要求 R3 を満たすことができると考えらえる．

4. 実装

4.1 通信制御機能

DNS サーバファイアウォールは DNS サーバへの正規の通信に関しては中継する．攻撃性通信に関しては DNS サーバへの通信を抑止する．また，同一 IP アドレスからの大量の通信といった不審な通信の場合は帯域制限を行う．このような柔軟な通信制御によって DNS サーバの効果的な防御が可能になると考えられる．通信制御部は Open vSwitch と Ryu SDN Framework 上で開発した約 400 行のコードを記述し，攻撃検知部は不正侵入検知システムであ

ⓒ 2020 Information Processing Society of Japan

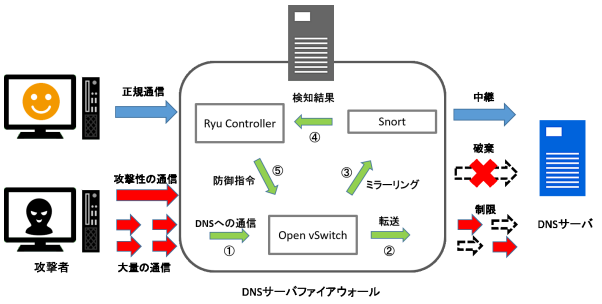

図 1　DNS サーバファイアウォールの概要

る Snort を使用した．本システムの構成図を図 1 に示す．

5.　実験と評価

5.1　実験環境

Cisco 社 UCS C210M2 で構築された KVM 環境上で，8 コア・メモリ 8GB のインスタンスとして，Open vSwitch 用，Ryu コントローラと Snort 稼働用，NSD 用の 3 つを稼働させた．また，resperf 及び tcpreplay を用い提案システムへ模擬トラフィックを送信するために Intel Celeron G540 2.5GHz，メモリ 4GB の物理 PC を用意した．

5.2　性能測定

resperf を用いてスループット (1 秒間の応答数) とレイテンシを測定する．性能測定の結果としてスループットは約 40,000qps，レイテンシは最大 0.1 秒だった．ただし現在の実装では，短時間に多くの未知 IP アドレスから通信を受けた場合，性能が低下するという特徴がある．今後この点を考慮した特定条件下での性能測定や性能向上を目的としたシステムの修正が必要であると考えられる．

5.3　効果推定

効果推定では，実際に運用されている DNS サーバへの観測トラフィックを実験環境において再現する．今回は観測トラフィックとして，本学情報科学センターのファイアウォール内部で観測されるトラフィックのうち，53 番ポート宛のものを対象とした．観測期間は 2020 年 6 月 8 日分とした．観測トラフィックの 1 時間当たり受信量と NSD が受信した 1 時間当たりの再現トラフィック受信量を比較したものを図 2 に示す．

元の観測トラフィックの総パケット数は 16,000,450 パケット，NSD の総受信パケット数は 7,868,673 パケットだった．このことから DNS サーバファイアウォールによって約 50.4 %の通信が抑止されたと考えられる．

次に，観測トラフィックと NSD が受信した再現トラフィックそれぞれについて，DNS に関するルールを適用した Snort によるアラート検知数を比較した．

観測トラフィックの総アラート数は 87,467 個，NSD が受信した再現トラフィックにおける総アラート数は 350 個

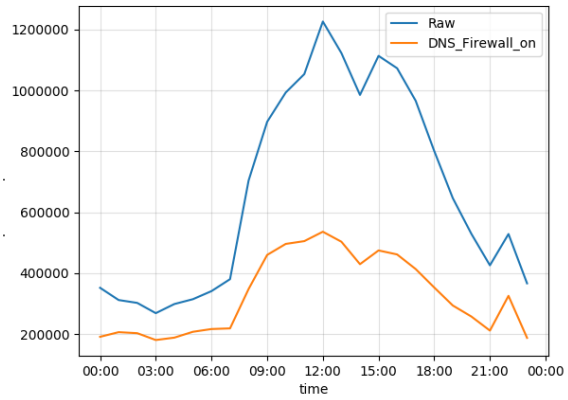

図 2　スループット比較

だった．この結果から，DNS サーバファイアウォールによって約 99.6 %の攻撃性通信が抑止されたことがわかった．一方で NSD の受信したトラフィックにおいて検知された攻撃性通信について，Snort による検知から Open vSwitch へのフローエントリの追加までの約 0.5 秒の遅延により，DNS サーバファイアウォールを通過してしまったと考えられる．また現段階では一度攻撃性通信とみなされた送信元 IP アドレスからの通信を正規のものであると修正する機能がなく，誤検知があった際に本来正規である通信をカットし続けてしまうという問題があるため，この点の修正も必要であると考えられる．

6.　おわりに

本研究では OpenFlow を用いた DNS サーバファイアウォールの実装，評価を行った．DNS サーバの防御機能をもつ製品も存在するがその多くは内部処理が非公開であるのに対して，本システムは OSS によって構成されているため不正なプログラムや脆弱性などを確認することが可能となる．さらに本システムでは IDS のルールごとに任意の通信制御を柔軟に設定でき，ハニーポットに誘導するなどの機能拡張により攻撃に対して詳細な調査が可能になると考えられる．また今後 DNS セキュリティにおいて DoT や DoH といった通信秘匿化の広がりが予想されるが，現時点では主にスタブリゾルバとフルサービスリゾルバ間の通信が対象であるため，権威 DNS サーバの防御には影響が少ないと考えられる．今後の課題としては，Snort ルールのチューニングや通信制御の種類の追加などが挙げられる．

参考文献

[1]　瀬川 駿他：柔軟な応答制御機構を持つ DNS サーバファイアウォールの提案と試作，研究報告インターネットと運用技術 (IOT) Vol.2018-IOT-40, No.3，pp. 1–6 (2018).
[2]　井上知英：DNS サーバファイアウォールの制御を目的としたトラフィック分析システムの検討，京都工芸繊維大学工芸科学部 情報工学課程 卒業研究報告，pp. 1–26 (2018).

ⓒ 2020 Information Processing Society of Japan