様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 ２７ 日現在

機関番号：１５３０１
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０１０５

研究課題名（和文）ＤＮＳとの連携による動的ファイアウォールシステム

研究課題名（英文）Proactive Firewall System in Cooperation with DNS

研究代表者
岡山　聖彦（Kiyohiko, Okayama）

岡山大学・その他部局等・准教授

研究者番号：２０２５２５８８

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：ネットワークのセキュリティ対策の一つとして、ファイアウォール製品が広く用いられいるが、厳密な検査を行うと負荷が高くなり、性能低下を招く。この問題を解決するため、本研究課題では、DNSと連携する動的ファイアウォールシステムに関する研究開発を行った。本システムでは、クライアントがサーバとの通信前にDNS問合せを行う点に注目し、問合せ時にクライアントIPアドレスをサーバ側に伝達する。サーバ側では、これに基づいてファイアウォールの検査レベルを動的に変更することにより、信頼できるクライアントは検査を簡略化して高速に通信させる一方で、疑わしいクライアントに対しては厳重な検査を行うことができるようにした。

研究成果の概要（英文）：With the popularity of the Internet services, network security becomes critical issue in the Internet world. Especially, the threats of malicious accesses make the firewall systems have to low down performance due to strict inspections. In this study, we propose an adaptive firewall system in collaboration with DNS (Domain Name System) which introduces querier's IP address notification feature. With such a feature, the proposal system can identify whether each communication flow can be trusted or not by checking the querier's IP address and the DNS query target domain name. Then based on the result of checking, the firewall system adaptively decides specific operation for specific connection. Consequently, the trusted flows go through bypass route of higher bandwidth without heavy packet inspection while untrusted flows will be blocked or restricted by strict packet inspection. Thus, the firewall system totally accomplishes higher throughput.

研究分野：情報ネットワーク

キーワード：DNS　ファイアウォール

１．研究開始当初の背景

最近，組織外から組織内の計算機に対する不正アクセスや不正侵入（以下、単に不正アクセスと表す）が後を絶たず、その対策は急務である。従来の不正アクセスへの対策では，ファイアウォール装置や UTM（Unified Threat Management）製品（以下、単にファイアウォールという）がよく用いられてきた。しかし、多くのファイアウォールは負荷の高い処理を行うとスループットの低下を招き、逆に十分なスループットを得るためには監視対象となる通信を限定したり、あるいは負荷の高い検査を行わないようにしたりするなどの設定を行う必要があった。また、このような設定に伴い、管理者の負担が増加するという問題もあった。

２．研究の目的

前項の問題を解決するため、我々の研究チームでは、DNS に送信元（クライアント）の IP アドレスを通知する機構を組み込むことにより、ファイアウォールが送信元 IP アドレスと問合せ対象のホスト名を事前に把握して動的に検査内容を決定するようなシステムを提案している。このシステムでは、たとえば送信元が信頼できる場合にはファイアウォールを経由しないようにしたり、負荷の高い検査は行わないようにしたりして高速通信を許可する一方、通信相手が信頼できない場合には帯域を制限したり、負荷の高い検査を行ったりすることが可能になる。また、ボットを発信源とする通信の多くに見られるような、名前解決を行わない通信については、不正アクセスとみなして遮断したり、ハニーポットなどの特別なサーバに誘導したりすることも可能である。これにより、信頼できる通信と疑わしい通信を分離し、信頼できる通信の高速化を図るとともに、管理の省力化を目指す。

３．研究の方法

上述したシステムを実現するため、本研究課題では、以下のサブテーマについて研究開発を実施した。

(1) DNS へのクライアント IP アドレス通知機能の設計と実装

現在の DNS のプロトコルでは、名前解決を行いたいクライアントの IP アドレスは問合せメッセージには含まれていない。そこで、既存の DNS プロトコルと互換性を保ちながら問合せ元の IP アドレスを問合せ先の DNS サーバに通知する機能を設計し、DNS クライアントおよび DNS サーバに実装する。

(2) DNS サーバにおけるキャッシュの一部無効化機能の実現

DNS では問合せ回数を削減するためにキャッシュ機能が設けられており、各資源レコードに対して指定された有効期限までは同一資源レコードの問合せは行わないようになっている。しかし、提案方式ではこの機能により問合せ元 IP アドレスの通知が行えない場合が生じるため、クライアント側 DNS サーバに対して、異なるクライアントから問合せを受けた場合にはキャッシュを無視して名前解決を行う機能を組み込む。

(3) DNS サーバへの OpenFlow スイッチ制御機能の設計・実装

ファイアウォールにおける検査内容を動的に決定するために、提案手法では、ファイアウォールの前後にあるスイッチ（またはルータ）で転送先を動的に制御する方法を想定している。たとえば、信頼できるネットワークに属するクライアントからの問合せは、ファイアウォールを迂回させることにより高速化を図ることができる。このような制御を行うため、本研究ではスイッチの部分に OpenFlow という技術を適用する。OpenFlow はスイッチとコントローラから構成され、OpenFlow スイッチが保持する転送ルールを OpenFlow コントローラが動的に変更することが可能である。本研究では、サーバ側 DNS サーバと OpenFlow コントローラが連携することにより、クライアントとサーバの情報に基づいて OpenFlow スイッチの転送先を動的に決定することができる機能を設計・実装する。

(4) NAT ルータ対策

クライアント側において、NAT ルータの内側に DNS サーバとクライアントが配置されている場合、DNS サーバはクライアントのプライベート IP アドレスをサーバ側 DNS サーバに通知することになる。このため、クライアント DNS サーバに対して、NAT ルータが IP アドレス変換に用いるグローバル IP アドレスを通知するような機能を実現する必要がある。さらに、NAT ルータが複数のグローバル IP アドレスを変換に使用している場合に対応するために、NAT ルータが DNS サーバの送信した問合せメッセージを監視して、メッセージに埋め込まれたクライアントのプライベート IP アドレスを予め決められたグローバル IP アドレスに書き換えるような機能についても検討する。

４．研究成果

前項で示したサブテーマ(1)～(4)それぞれについて、研究の成果を以下に示す。

(1) DNS へのクライアント IP アドレス通知機能、および、(2) DNS サーバにおけるキャッシュの一部無効化機能

(1)および(2)の機能を同時に実現するた

め、既存の DNS サーバの実装を変更するのではなく、クライアントと従来のクライアント側 DNS サーバの間に独自のキャッシュサーバを挟み込む方法を採った。DNS の問合せメッセージにクライアントの IP アドレスおよびネットマスクの情報を追加する方法としては、DNS の拡張プロトコルである EDNS0 を利用して、クライアント側 DNS サーバがクライアントのサブネットアドレスとネットマスクの組を問合せ DNS メッセージに埋め込む方法を採用した。

一方、クライアント側 DNS サーバにおけるキャッシュの一部無効化機能を実現するため、上述した独自キャッシュサーバが問合せ元のクライアント IP アドレスを一定時間記憶するようにして、異なるクライアント IP アドレスから同じ FQDN の問合せがあった場合には、キャッシュを無視して FQDN を問い合わせるようにした。独自キャッシュサーバは Perl 言語により作成し、実際のインターネット環境で動作確認実験を実施した結果、意図した通りに動作していることを確認している。

(3) DNS サーバへの OpenFlow スイッチ制御機能

ネットワーク環境として、検査ポリシの異なる複数のファイアウォール装置が接続された OpenFlow スイッチを想定し、クライアントからの DNS 問合せを受けた DNS サーバが、クライアントからの通信をどのファイアウォール装置に転送するかを動的に OpenFlow スイッチに設定する仕組みを設計した。具体的には、DNSWL や DNSBL の仕組みを用いて送信元 IP アドレスに基づくホワイトリストあるいはブラックリストを登録できるようにしておき、DNS 問合せに含まれるクライアント IP アドレスを照合することにより、その結果に応じて通過させるファイアウォール装置を動的に変更する。

本機能の実装には、OpenFlow フレームワークの一つである Trema を使用して、OpenFlow スイッチを制御するプログラム（OpenFlow コントローラ）を作成した。OpenFlow コントローラはホワイトリストのデータベースを持ち、データベースは DNS サーバによって更新され、その内容に応じて OpenFlow コントローラが OpenFlow スイッチの動作を動的に変更するようにした。

(4) NAT ルータ対策

クライアント側でプライベート IP アドレスが割り当てられ、外部との通信に NAT ルータが使用される環境において、クライアント側 DNS サーバから通知されるプライベート IP アドレスを、NAT ルータがグローバル IP アドレスに書き換える機能を FreeBSD の natd に実装した。

最後に、(1)～(4)の各機能を組み合わせたプロトタイプシステムを構成し、実験ネットワークで性能評価実験を行った。1 台のサーバに対して複数台のクライアントを用意して、1 台のクライアントからは通常の通信（ホワイトリストに登録して OpenFlow スイッチを通過させる）、残りのクライアントからは DoS 攻撃に相当する通信（ホワイトリストに登録せず、OpenFlow スイッチで遮断される）を発生させ、通常の通信がどれだけ DoS 攻撃の影響を受けるかを測定した。その結果、通常の通信は DoS 攻撃の影響をほとんど受けず、提案方式が実用上問題ないことが確認できた。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

① Tomokazu Otsuka, Nariyoshi Yamai, Kiyhiko Okayama, Yong Jin, Hiroya Ikarashi, Naoya Kitagawa, Design and Implementation of Proactive Firewall System in Cooperation with DNS and SDN, Proc. of The 31st International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2016), 印刷中, 査読有, 2016-07.

② Tomokazu Otsuka, Gada, Nariyoshi Yamai, Kiyhiko Okayama, Yong Jin, Design and Implementation of Client IP Notification Feature on DNS for Proactive Firewall System, Proc. of The 39th Annual International Computer Software & Applications Conference (COMPSAC2015/ADMNET WS), Vol.1, pp.127-132, 査読有, 2015-07.

③ 大塚友和, ガーダ, 山井成良, 岡山聖彦, 動的ファイアウォールシステムのための DNS によるクライアント IP アドレス通知機能, マルチメディア・分散・協調とモバイル(DICOMO2014)シンポジウム論文集, 1 巻, pp.184-189 査読無, 2014-07.

④ 岡山聖彦, 山井成良, ガーダ, 大塚友和, DNS と OpenFlow スイッチとの連携による動的ファイアウォール, 情報処理学会第 6 回インターネットと運用技術シンポジウム(IOTS2013)論文集, 1 巻, pp.95-98 査読無, 2013-12.

〔学会発表〕（計 4 件）

① 藤巻伶緒, 大塚友和, 山井成良, 北川直哉, 岡山聖彦, NAT 環境に対応した DNS・SDN 連携型動的ファイアウォールシステム, 情報処理学会インターネットと運用技術研究会, 2016 年 3 月 4 日, 虹の松原ホテル(佐賀県唐津市).

② 大塚友和, 山井成良, 岡山聖彦, DNS と OpenFlow との連携による動的ファイアウォールシステムの構築, 第 17 回 IEEE 広島支

部学生シンポジウム, 2015年11月21～22日, 岡山大学津島キャンパス(岡山県岡山市).
③ 大塚友和, ガーダ, 山井成良, 岡山聖彦, 動的ファイアウォールシステムのためのDNSによるクライアントIPアドレス通知機能, マルチメディア,分散,協調とモバイルシンポジウム, 2014年7月9日, 月岡温泉・ホテル泉慶(新潟県新発田市).
④ 岡山聖彦, 山井成良, ガーダ, 大塚友和, DNSとOpenFlowスイッチとの連携による動的ファイアウォール, 情報処理学会第6回インターネットと運用技術シンポジウム, 2013年12月13日, 広島大学東広島キャンパス(広島県東広島市).

〔図書〕（計0件）

〔産業財産権〕
○出願状況（計0件）

○取得状況（計0件）

〔その他〕
特になし

６．研究組織
(1)研究代表者
岡山 聖彦（OKAYAMA, Kiyohiko）
岡山大学・情報統括センター・准教授
研究者番号：20252588

(2)研究分担者
山井 成良（YAMAI, Nariyoshi）
東京農工大学・工学（系）研究科（研究院）・教授
研究者番号：90210319

(3)連携研究者
なし