DNS と OpenFlow スイッチとの連携による動的ファイアウォール

岡山聖彦[†1]　山井成良[†1]　ガーダ[†1]　大塚友和[†1]

本稿では 通信の殆どが事前に DNS による名前解決を行う点に着目し，DNS にクライアントの アドレスを通知する機構を組み込むことにより，問合せ元のクライアントに応じて動的に検査内容を変更することのできるファイアウォールを提案する．これにより，クライアントの IP アドレスに基づいて信頼できる通信と疑わしい通信を分離し，信頼できる通信についてはファイアウォールを迂回した高速通信を許可する一方で，疑わしい通信については遮断したり帯域を制限したりするなど，スループットの向上を図ることができる．

Proposal of proactive firewall system in cooporation with DNS and OpenFlow switches

KIYOHIKO OKAYAMA[†1]　NARIYOSHI YAMAI[†1]
GADA[†1]　TOMOKAZU OHTSUKA[†1]

In this paper, we propose a proactive firewall system which introduces client's IP address notification function into DNS and dynamically controls communications going through the firewall system, since almost all TCP/IP communication perform name resolution by DNS in advance. With such a function, this system can identify whether each communication flow is trusted or not. Consequently, the proposal firewall system allows trusted flows to go through bypass route of higher bandwidth without packet inspection and otherwise makes untrusted flows blocked or restricted by packet inspection, so that the firewall system totally performs higher throughput.

1. はじめに

近年，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，その対策が急務である．不正アクセスへの一般的な対策として，組織の対外接続点に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表す）を導入し，組織内外を跨る通信を検査する方法がよく用いられている．

しかし，多くのファイアウォールでは負荷の高い処理を行うとスループットの低下を招くため，これを回避するには監視対象となる通信を限定したり，負荷な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．さらに，このような設定の多くは管理者が手動で行う必要があるため，管理者の負担も増加するという問題もあった．

そこで，本稿では，アプリケーションレベルで通信相手を IP アドレスで直接指定するような場合を除き，TCP/IP 通信では原則として事前に DNS（Domain Name System）[1,2]による名前解決を行う点に着目し，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（以下，送信元・送信先情報）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する．本システムでは，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バイパスしたり，負荷の高い検査を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，不正アクセスと見なして遮断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．

2. ネットワーク環境と問題点

2.1 対象となるネットワーク環境

本稿では，図 1に示すような構成でインターネットと組織ネットワークとの間を接続しているようなネットワーク環境を想定している．この図において，レイヤ3スイッチ（L3SW）/負荷分散装置（LB）は送信元や送信先のIPアドレスやポート番号等のレイヤ3,4の情報に基づいて特定の条件を満たすフローをファイアウォール（FW）やアプリケーションレベルゲートウェイ（ALG）に振り分けるあるいはこれらを迂回させる機能を持つ．FWは主にレイヤ4より上位レイヤの情報に基づいて検査を行う．ALGはHTTPやSMTPなど特定のアプリケーションに関して，たとえば電子メールにおけるウイルス検査などFWで実施するのが困難あるいは適切でないような検査を行う．SSL-VPN装置なども便宜上ALGに含めるものとする．FWやALGはそれぞれ複数台あってもよく，また検査内容や処理能力が異なる場合もありうる．また，1台の装置で仮想的に複数のFWやALGの役割を果たしても構わない．

†1 岡山大学
Okayama University

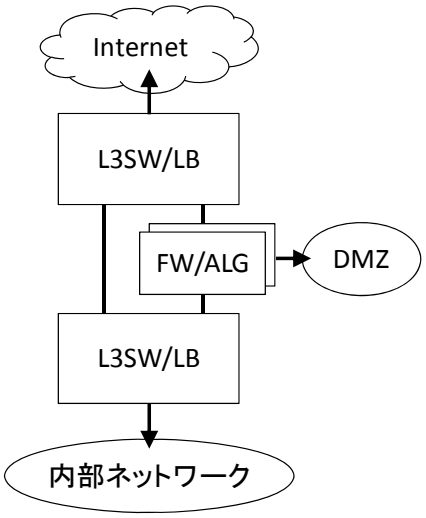

図 1　想定するネットワーク環境

Figure 1　Assumed network environemnt.

このようなネットワーク環境は多くの組織で見られるものであり，またそれ以外の組織でも比較的容易にこのようなネットワーク環境を構成可能であると思われる．

2.2 従来のファイアウォールシステムの問題点

一般にファイアウォールでは，スループットは検査内容によって大きく異なり，SPI（Stateful Packet Inspection）[3]やウイルス検査などの負荷の大きな処理を行うとスループットが低下する．また，最大同時接続セッション数や最大新規接続セッション数にも制限があり，組織ネットワークの規模とファイアウォールの性能によっては一部の通信が行えなかったり遅延が発生したりするという問題がある．

この問題に対して，たとえばブラックリストやホワイトリストのように，安全性の高い一部の通信についてはファイアウォールを迂回させるようにレイヤ 3 スイッチ/負荷分散装置を設定したり，負荷の高い検査を省略したりするようにファイアウォールを設定したりする一方，危険性が高い一部の通信についてはレイヤ 3,4 の情報に基づいてレイヤ 3 スイッチ/負荷分散装置で遮断する方法がある．但し，この方法では管理者が手動で設定を行う必要があるため，管理者の負担が増加するなどの問題がある．

3. DNS との連携による動的ファイアウォールシステム

本章では，前節で述べた問題点を軽減する手法として，DNS を送信元（クライアント）のアドレスを通知するように機能拡張し，送信元・送信先情報に基づいてレイヤ 3 スイッチ/負荷分散装置やファイアウォールの設定を動的に変更するようなファイアウォールシステムを提案する．

3.1 基本方針

TCP/IP では送信元・送信先の識別子として IP アドレスを用いるが，利用者が直接指定することは稀であり，通常は可読性に優れるホスト名（ドメイン名）を用いる．その際，名前解決（ホスト名から IP アドレスへの変換）に用いられるのが DNS である．

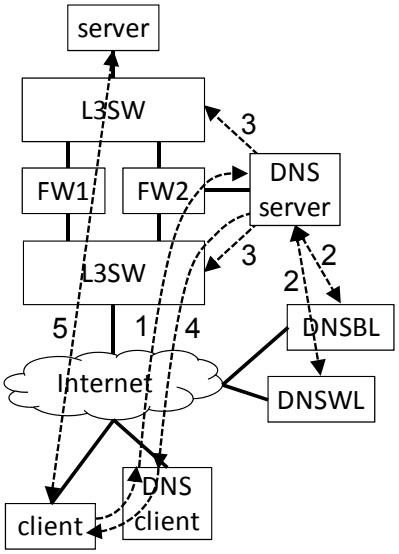

図 2　システム全体の構成例

Figure 2　An example of system structure

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（以下，問合せ元）の情報は問合せメッセージには含まれておらず，またキャッシュサーバの存在により通信を行おうとする度に必ず問合せを行うとは限らない．しかし，アプリケーションプロトコルによる通信を行う前に問合せが発生するという性質は他には見られない重要な特徴である．そこで，本稿ではこの性質に着目し，問合せ先（ファイアウォール側）が送信元・送信先情報を事前に把握することにより，ファイアウォールシステムの設定を動的に変更できるようにする．

3.2 システムの動作例

例として，外部で提供されている DNS ベースのホワイトリスト（DNSWL）およびブラックリスト（DNSBL）に基づいて動的に検査内容を変更する場合のシステム全体の典型的な構成を図 2 に示す．この図において，FW1 はホワイトリストに含まれる相手との通信用で，負荷の高い検査を省略したファイアウォール，FW2 はそれ以外の相手との通信に用いるファイアウォールを表す．また，初期状態では全ての通信は FW2 を経由するようにレイヤ 3 スイッチ（L3SW）で設定されているものとする．

この構成例において，インターネット上のクライアントが組織内ネットワーク上のサーバにアクセスする場合の動作手順を以下に示す．なお，手順中の番号は図中の番号と対応している．

(1) クライアントはクライアント側 DNS サーバ（DNS client）にサーバの名前解決を依頼する．クライアント側 DNS サーバはクライアントの IP アドレスを含めた問合せパケットをサーバ側 DNS サーバ（DNS server）送信する．

(2) サーバ側 DNS サーバは問合せメッセージにクライアントの IP アドレスが含まれていればこれを取り出し，DNSBL，DNSWL に登録されているかどうか確認する．クライアン

トの IP アドレスが含まれていなければ(4)に進む.
(3) サーバ側 DNS サーバは DNSBL, DNSWL への登録の有無によりレイヤ 3 スイッチの設定を変更する．すなわち，DNSWL に登録されている場合にはクライアントとサーバとの通信を FW1 経由で行うように制御する．DNSWL に登録がなく，かつ，DNSBL に登録されている場合には，クライアントの IP アドレスを送信元あるいは送信先として含むパケットを廃棄するようにレイヤ 3 スイッチの設定を変更する．クライアントの IP アドレスが DNSBL，DNSWL のいずれにも登録されていない場合，あるいは問合せメッセージにクライアントの IP アドレスが含まれていない場合には，レイヤ 3 スイッチの設定は特に変更しない.
(4) サーバ側 DNS サーバはクライアント側 DNS サーバにサーバの IP アドレスを含む応答メッセージを送信する．クライアントの IP アドレスが DNSBL に登録されている場合には，(3)でレイヤ 3 スイッチの設定を変更せず，サーバの IP アドレスの代わりに他の IP アドレス（たとえばハニーポットやレイヤ 3 スイッチで予め設定しておいたパケット廃棄用 IP アドレスなど）を返してもよい．クライアント側 DNS サーバはサーバの IP アドレスを得てこれをクライアントに通知する.
(5) クライアントはサーバとの通信を開始する．これまでの手順により，途中のレイヤ 3 スイッチによってクライアントからのパケットが廃棄されるかどうか，そうでない場合には FW1, FW2 のどちらを経由するかが設定済みである.

以上の動作により，管理者がブラックリストやホワイトリストに基づいて予めレイヤ 3 スイッチを設定しておく必要がなくなり，管理者の負担を軽減しながらファイアウォールのスループットを維持することができる.

3.3 実現方法の検討

上記のファイアウォールを実現するには，DNS を用いて問合せ元 IP アドレスを問合せ先に通知する機能が必要になる. また, 通信開始時に確実に問合せを行わせるために，クライアント側の DNS サーバにおいてキャッシュ機能を一部無効化する機能が必要になる.

以下では，これらの機能の実現方法について検討する.

3.3.1 問合せ元 IP アドレスの通知

提案システムでは, 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 アドレスをサーバ側 DNS サーバに通知する機能が必要になる．文献[4]では，EDNS0[5]を活用するなどして，DNS の問合せメッセージに問合せ元（クライアント）の IP アドレスを含める方法などが検討されているが，最近ではクライアントのサブネットアドレスを通知する方法[6]が提案されている.

この方法は，前述した 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メッセージに埋め込むものである．基本的にはネットワーク単位での通知を想定していると考えられるが, ネットマスクを 32 ビットとすることによりクライアントの IP アドレスを通知することも可能であるため，今後はこの方法を組み込むことを検討する.

3.3.2 キャッシュ機能の一部無効化

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（TTL: Time to Live）の間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ある．すなわち, 同一 DNS サーバを利用するクライアントのうちの 1 つがサーバにアクセスしようとして名前解決を行うと，この（クライアント側）DNS サーバではサーバの IP アドレスがキャッシュされるため, キャッシュの有効期限内に他のクライアントが同一サーバにアクセスしそのクライアントの IP アドレスがサーバ側に通知されない.

この問題を解決するためには，キャッシュ機能の一部無効化が必要となる．すなわち，異なるクライアントから問合せを受けた場合, クライアント側 DNS サーバは以前の問合せ結果（サーバのアドレス）を含む資源レコード（A レコード，AAAA レコード）のキャッシュを無視し，再度同じ名前解決を行うようにする．ただし，クライアント IP アドレスの通知はサーバ側 DNS サーバに対して 1 度だけでよいため，NS レコード，MX レコードなど，サーバの IP アドレスを含まない資源レコードについてはキャッシュを無効化する必要はない．また，HTTP など，同一クライアント・サーバ間で多数のフローが発生するプロトコルが存在することから，同一のクライアントからの問合せに対してはキャッシュ機能を有効にすべきである．その際，サーバ側では A レコード，AAAA レコードの有効期限を長めに設定し, この値に基づいてレイヤ 3 スイッチ/負荷分散装置の設定を維持するようにすれば設定変更回数を削減できる.

3.3.3 NAT 機能との併用

本システムはクライアント側，サーバ側とも NAT（Network Address Translation）[7]機能を併用することが可能である．ただし，いずれの側でも多少の工夫が必要となる．クライアント側，サーバ側とも NAT ルータを用いた場合の構成例を図 3 に示し，この図を用いて必要となる工夫を説明する.

まず, クライアント側では NAT ルータあるいはクライアント側 DNS サーバで問合せ元 IP アドレスを NAT ルータで変換されるものに変更する必要がある．変換後の（グローバル）IP アドレスが 1 種類しかない場合にはクライアント側 DNS サーバでそのアドレスを付加する方法が容易に実現可能である．しかし，変換後の IP アドレスが 2 種類以上ある場合には，NAT ルータ自身が予め変換後の IP アドレスを決定して問合せメッセージにそれを付加し，その後クライアント・サーバ間の通信（図中の 5）でも同じ IP アドレスを用いるように変換する必要がある.

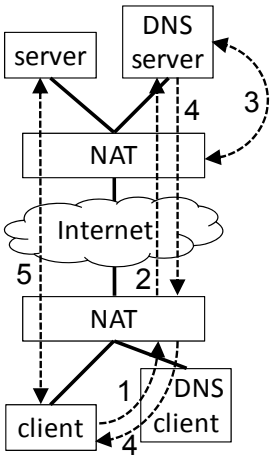

図 3　NAT ルータを用いた場合の構成例

Figure 3 An example of system structure with NAT routers.

一方，サーバ側では，DNS サーバが問合せメッセージを受信すると, その中に含まれる問合せ元 IP アドレスと解決したいホスト名を取り出し，NAT ルータの外部側（グローバル）IP アドレスと問合せ対象のホストの内部用（プライベート）IP アドレスを相互変換するように NAT ルータを設定する．その後，NAT ルータの IP アドレスを問合せに対する応答として送信するようにする．これにより，事前に DNS 問合せがない通信を全て遮断しながら，組織内の複数のサーバが存在する場合でも 1 つのグローバル IP アドレスで対応できる．

3.3.4 OpenFlow **スイッチの導入**

3.2 節で述べたように，本システムでは，検査内容の異なる複数のファイアウォール装置をあらかじめ設置し，問合せ元の IP アドレスをブラックリストやホワイトリストと照合した結果に応じて，通過するファイアウォールを動的に振り分ける．これを実現するための方法として，レイヤ 3 スイッチのポリシルーティング機能などを利用して，IP アドレスごとに転送先を指定することが考えられるが，レイヤ 3 スイッチの設定を外部から動的に変更する統一的な仕組みは提供されていない．これに対し，代表的な SDN（Software Defined Networking）技術として知られている OpenFlow[8]では，外部（OpenFlow コントローラ）からネットワーク（OpenFlow スイッチ）を制御するためのインタフェースが提供されており，高速かつ柔軟なフロー制御が可能である．

そこで本研究では，図 1 のレイヤ 3 スイッチの代わりに OpenFlow スイッチを導入し, DNS サーバと OpenFlow コントローラの連携により動的に転送先のファイアウォールを切り替える仕組みを検討する．また，OpenFlow は IP アドレスやポート番号の書き換えもサポートしているため，3.3.3 節で述べたような NAT ルータの動作が OpenFlow スイッチで実現できるかどうかも検討する．

3.4 アドレス通知機能を用いない動作

本システムは問合せ元 IP アドレスの通知機能を前提としている部分が多いが, クライアント側 DNS サーバが未対応などの理由でこの機能を用いない場合でもある程度有効である．たとえば電子メールにおける SPF（Sender Policy Framework）と同様に，クライアント側 DNS サーバが問合せを受け付ける IP アドレスの範囲を公開するような仕組みを導入すれば, 問合せ元 IP アドレスそのものは特定できないが, 代わりに問合せ元 IP アドレスの範囲を絞り込むことが可能になり，その結果に応じてファイアウォールの動作を変更できる. また, そのような仕組みがない場合でも，たとえばポートスキャンなど，事前に名前解決を行わないような通信を排除したり検査を強化したりすることが可能である．なお，このような動作は組織外から組織内への通信だけでなく組織内から組織外への通信にも適用可能である．これにより，たとえば組織内ホストからの不審なアクセスを検出して遮断することが可能になる．

4. おわりに

本稿は，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，事前に送信元・送信先情報を得て動作を動的に変更可能なファイアウォールシステムを提案した．現在のところ検討段階であるが，今後は詳細設計および実装を行い，有効性を検証したい．

謝辞　本研究の一部は平成 25～27 年度科学研究費補助金（基盤研究（C），課題番号 25330105）の補助を受けている．ここに記して感謝の意を表する．

参考文献

1)　P.V. Mockapetris:　Domain Names - Concepts and Facilities, RFC1034, IETF, 1987.
2)　P.V. Mockapetris: Domain Names - Implementation and Specification, RFC1035, IETF, 1987.
3)　Seungyong Yoon, Byoungkoo Kim, Jintae Oh and Jongsoo Jang: High Performance Session State Management Scheme for Stateful Packet Inspection, Managing Next Generation Networks and Services, Lecture Notes in Computer Science, Vol. 4773, pp.591-594, 2007.
4)　山井成良，金勇，岡山聖彦，河野圭太，中村素典: DNS との連携による動的ファイアウォールシステムの提案，情報処理学会コンピュータセキュリティ研究会コンピュータセキュリティシンポジウム 2010(CSS2010)論文集，Vol.II，pp.729-734，2010.
5)　P. Vixie: Extension Mechanisms for DNS (EDNS0), RFC2671, IETF, 1999.
6)　C. Contavalli, W. van der Gaast, S. Leach and E. Lewis: Client Subnet in DNS Requests, draft-vandergaast-edns-client-subnet-02, Internet Draft, Work in progress, IETF, 2013.
7)　P. Srisuresh and K. Egevang: Traditional IP Network Address Translator (Traditional NAT), RFC3022, IETF, 2001.
8)　N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner: Openflow: Enabling Innovation in Campus Networks, In Proceedings of SIGCOMM 2008, pp.69-74, 2008.