G-16

Virtual Machine を用いたユーザ再配分を目的とした DDoS 対策システム
Distributed denial of service attack protection system using a user distribution mechanism based on virtual machine environment

○児玉賢祐[1]，　木原雅巳[2]
Kensuke Kodama[1]，　Masami Kihara[2]

Abstract: This paper proposes a security system ensures web access for regular users even if the web server is under Distributed Denial of Service attack. The method is based on a server distribution mechanism based on the Virtual Machine architecture consisting of multiple servers, software routers, and switches.

１．はじめに

本研究では，DDoS(Distributed Denial of Service attack)に対して，VM(Virtual Machine)を用いたトラフィックの振り分けシステムを用いることにより，Web サーバが DDoS を受けた場合であっても正規利用者からのアクセスを DDoS の影響を受けずに正常に処理，応答することを実現する．

２．研究内容

DDoS は，Web サービスに対して Bot ネットなどを用いて膨大なトラフィックを発生させる事により，対象 Web サービスの提供を困難にするものである．[1]

DDoS が有効に作用するためには，発生させたトラフィックが Web サービスの提供可能リソースを上回っている必要があるが，近年の DDoS はトラフィック量が 100Gbps を超える事も珍しく無い為[2]，リソースの増強で DDoS に対応するのはコストが際限なくかかってしまうため費用対効果の面で現実的ではない．

WAF(Web Application Firewall)などの専用のアプライアンスを組み込む手法も存在するが，これも同様にコストや利用環境の問題から全てのサービスに適用することは難しい．

本研究では，VM を用いて WAN 側の通信回線を複数用意し，メインの通信回線が DDoS などにより繋がりづらい状況になった場合には，CPU 使用率，メモリ使用率，ネットワーク帯域の使用率などの一定の判定基準を定め，それを用い，DDoS アクセスではないと思われる通信を，あらかじめ用意しておいた予備回線にリダイレクトする事により，一般ユーザのユーザビリティの確保を図るものである．

３．構築システム

VM の作成に用いるホストマシンは、ホスト OS を用いずにリソースを圧迫しないことからベアメタルハイパーバイザーのひとつである VMWareESXi[3]を選択した．仮想環境で使用するソフトウエアルータは VyOS を、スイッチには、VMWareEsxi の仮想スイッチ、サーバは、VM 上に CentOS7 を用いて構築する．

構成するシステムは Fig1. に示すように設計した．赤で示した NIC(Network Interface Card)は Global IP アドレスを付与したものであり，外部からのアクセスを受けるためのものである．青で示した NIC はサービス提供に用いるシステムを構築するものであるため Front End NIC とした．緑で示した NIC は各 VM を構成した機器の状態を管理するための NIC であるため，Back End NIC とした。Back End NIC は Global NIC 及び Front End NIC とは別のネットワークレンジを用いているため，システムの管理を行う際に，外部からのアクセスによるネットワーク帯域の圧迫に影響されない．

図 1 では同一な構成(系 1，2)が二つ存在するが，この構成は増やすことが可能であり，その数は Hypervisor を搭載するマシンのハードウェア性能に左右される．

４．システムの動作

外部からのアクセスは，図 1 左上に示した GlobalNIC に集約される．ルータを通過した後 GW Server(ゲートウェイサーバ)によって DDoS 攻撃であるか，一般ユーザからのアクセスであるかを判定される．判定結果は Back End NIC で構成されるバックエンドネットワークに存在する，Black List Server に一定期間保存される．その後，GW Server では

１：日大理工・学部・情報　２：日大理工・教員・情報

Black List Server に保存された判定結果を基にアクセスを振り分ける．DDoS と判定されたアクセスに対しては Black List HTTP Server へアクセスさせ，一般ユーザと判定されたアクセスに対しては HTTP Server へアクセスさせる．

認証サービスへのアクセスへは HTTP Server からのみ行える．各サーバの CPU，メモリ使用率，ネットワーク使用率などはバックエンドネットワークの Command Server を用いて監視される．

GW サーバの判定漏れによる，HTTP Server の負荷増加も考慮し，GW Server 及び HTTP Server の負荷，及びネットワーク使用率が増加した際には，一般ユーザを予め用意しておいた同一構成のサーバへリダイレクトする．これにより，一般ユーザは DDoS 攻撃によるサーバの負荷増加，ネットワーク使用率の増加に影響される事無く，Web アクセス及び認証サービスを利用することができる．

５．動作の検証方法

構築したシステムの動作を確認するために，VMWare ESXi 上に仮想的に WAN 環境を構築し，その中に配置した複数のマシンから構築システムに対して，DDoS 攻撃を行い，システムが正しく動作するかを確認する．

DDoS 攻撃を行うマシンは Linux を用いることとし，用いる負荷ツールは Apache Bench， httpef，Tsung など複数のツールを用いてデータを取得する．

Tsung は分散攻撃やマルチプロトコルに対応したツールであり，HTTP や SSL を始めとして WebDAV，MySQL などにも対応しているものである．[4]

６．まとめ

今回は，DDoS 対策システムの設計と検証方法について提案した．今後は，動作の検証を行い得られたデータを分析し，システムに最適なしきい値を検討するとともに，最適な構成を検討する．

７．参考文献

[1]警視庁技術対策課:「Dos/DDoS 対策について」，https://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf， 2003/06/03

[2] INTERNET Watch:「アーバーネットワークス、2016 年上半期のグローバル DDoS 攻撃データを公表」，http://internet.watch.impress.co.jp/docs/release/1011304.html，2016/07/21 06:00

[3]VMWare,inc:「vSphereHypervisor」， http://www.vmware.com/jp/products/vsphere-hypervisor.html， 2016

[4] Nicolas Niclausse:「Tsung」， http://tsung.erlang-projects.org， 2013

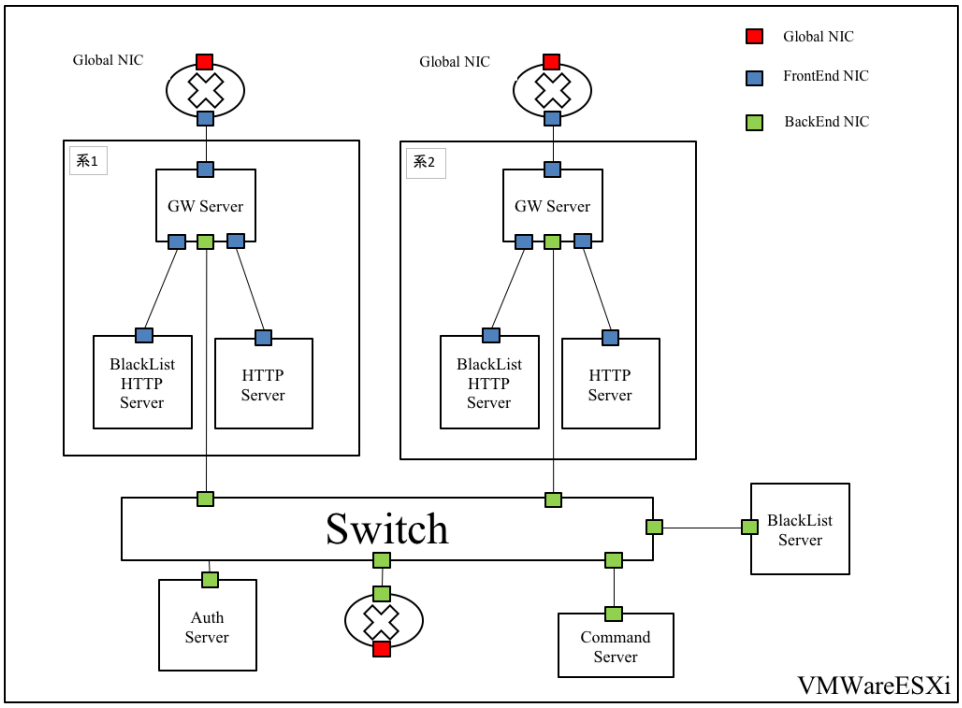

Fig1. System Configuration