Sistem Pencegahan *UDP DNS Flood* dengan *Filter Firewall* Pada Router Mikrotik

UDP DNS Flood Prevention System Using Filter Firewall On Mikrotik Router

Doni Aprilianto[1], Triyana Fadila[2], Much Aziz Muslim[3]
[1,2,3]Jurusan Ilmu komputer, FMIPA, Universitas Negeri Semarang
E-mail: [1]doniapr14@students.unnes.ac.id, [2]triyanafadila27@gmail.com
,[3]a212muslim@yahoo.com

Abstrak

Serangan terhadap server jaringan dapat terjadi kapan saja, jenis serangan yang dapat menyebabkan efek yang signifikan pada sebuah router adalah UDP-Flooding. UDP (User Datagram Protocol)-Flooding adalah jenis serangan yang memanfaatkan protokol UDP dengan mengurangi sambungan (connectionless) untuk menyerang target. Dalam analisis ini menggunakan metode penelitian deskriptif untuk memperoleh data secara langsung dengan melakukan teknik flooding serta teknik pencegahannya terhadap server yang telah dirancang. Dengan menggunakan Filter Rules yang telah dibuat, packet yang melalui port DNS selain IP Address yang telah di allow jika mencoba melakukan request atau flood DNS ke IP Public ISP pada router mikrotik, maka packet tersebut akan langsung di drop oleh pengaturan rules tersebut. kesimpulan yang dapat diambil yaitu penerapan filter firewall pada router mikrotik dapat mengurangi jumlah paket data UDP yang dikirimkan oleh attacker melalui port DNS sebanyak 60% dari jumlah paket yang masuk jika tanpa firewall.

Kata kunci: Flooding,UDP flooding, Firewall, keamanan jaringan

Abstract

Attacks on a network server can occur at any time, the type of attack that can cause a significant effect on a router is UDP-Flooding. UDP (User Datagram Protocol) -Flooding is a type of attack that utilizes UDP protocol by reducing connection (connectionless) to attack the target. In this analysis using descriptive research method to obtain data directly by flooding techniques and techniques of prevention against the server that has been designed. Using the Filter Rules that have been made, the DNS packet via a port besides IP Address that has been allow if trying to request or flood ISP Public DNS IP to the proxy router, then the packet will immediately drop by setting the rules. conclusions can be drawn that the implementation of filter proxy firewall on a router can reduce the amount of UDP data packets sent by attackers through DNS port as much as 60% of the number of incoming packets if no firewall.

Keywords*: Flooding, UDP flooding, firewall, network security*

1. PENDAHULUAN

Pada zaman sekarang ini, kebutuhan akan akses internet semakin besar. banyak pula instansi pendidikan yang menggunakan internet sebagai sarana untuk membantu dalam aktifitas belajar mengajar. Internet banyak digunakan karenadengan adanya internet akan didapatkan kemudahan dalam hal komunikasi dan transfer data. Internet juga sangat berguna bagi dosen maupun guru untuk melakukan proses belajar mengajar menggunakan *E-Learning.*

Selain memiliki banyak keuntungan, internet juga memiliki kekurangan. Salah satu kekurangan dari internet yaitu pada sisi keamanan jaringan. Serangan terhadap sistem keamanan jaringan sering terjadi belakangan ini. Jenis serangan yang kerap terjadi adalah DOS (*Denial of Services*).Serangan DOS bisa terjadi pada tipe jaringan apapun, sehingga perlu penelitian-penelitian untuk menemukan bagaimana mendeteksi serangan tersebut. Dampak dari serangan tersebut tidak bisa diremehkan lagi, karena dapat membuat sebuah jaringan dari skala jaringan kecil hingga besar berhenti bekerja (*Down*) [1].Namun dengan berkembangnya teknologi kemanan jaringan, kini serangan DOS berubah menjadi DDOS atau *Distributed Denial of services.*macam– macam serangan *DDOS* yang sering digunakan para *hacker* untuk menyerang yaitu *SYN-Flooding, SMURF Attack, UDP-Flooding, ICMP-Flooding, DNS-Flooding*[2].

Banyak dari kasus data flood disebabkan oleh adanya eksploitasi buffer overflow, yakni pengiriman data yang melebihi batas kapasitas. Data flood seperti yang telah disebutkan diatas dapt dicegah dengan metode validasi data, buffer non-excutable, array bounds checking, dan juga pemeriksaan indeks. Untuk melindungi serangan terhadap suatu sistem yang memanfaatkan jaringan komputer seperti sistem informasi pada perkembangannya diterapkan pula teknologi seperti Demilitarized Zone sebagai bentuk pengamanan data pada jaringan komputer. De-Militarised Zone (DMZ) merupakan mekanisme untuk melindungi sistem internal dari serangan hacker atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses, Untuk mengatasi ping attack atau ping of death pada server jaringan internal pada sebuah router Demilitarized Zone (DMZ) diperlukan konfigurasi aplikasi keamanan firewall filter , dimana mesin firewall akan melakukan filtering terhadap jaringan eksternal yang menuju jaringan internal yaitu dengan drop askes ip address tertentu sehingga user yang terdapat pada jaringan eksternal tidak dapat melakukan ping attack pada server jaringan internal dalam hal ini web server yang terletak dibelakang router mikrotik. Dari hasil pengujian serangan *flooding* dengan menggunakan tiga buah sampel pengujian diperoleh hasil dimana seluruh sampel serangan dapat dicegah dengan menggunakan system keamanan jaringan *Demilitarized Zone (DMZ)* berbasis *firewall filtering* dengan menggunakan sistem operasi mikrotik router os [3]**.**
Dari jenis-jenis serangan yang ada, serangan *UDP-Flooding* adalah jenis serangan yang dapat menyebabkan efek yang signifikan pada sebuah router. UDP (*User Datagram Protocol*)-*Flooding* adalah jenis serangan yang memanfaatkan protokol UDP dengan mengurangi sambungan (*connectionless*) untuk menyerang target. UDP adalah jenis serangan yang cukup mudah dilakukan dibandingkan dengan jenis serangan lain. *UDP-Flooding* dapat menyebabkan komputer server yang menjadi target mengalami *hang* akibat besarnya paket data yang diterima komputer server tersebut. Pengiriman data UDP yang berlebihan kedalamsuatu jaringan akanmembentuk suatu jalur hubungan dengan suatu servisUDP dari host tujuan dimana *UDP-Flood* ini akanmengirimkan karakter-karakter tertentu yang akan mengetesjaringan korban [4].
Jika menggunakan cara *spoofing,User datagram Protocol (UDP) flood attack* akan menempel pada layanan UDP *chargen* disalah satu perangkat yang digunakan untuk keperluan percobaan akan mengirimkan sekelompok karakter ke perangkat lain, yang diprogram untuk meng-*echo* setiap kiriman karakter yang doterima memalui *service chargen.* Karena peket UDP tersebut di *spoofing* diantara ke dua perangkat tersebut maka yang terjadi adalah banjir tanpa henti kiriman karakter yang tidak berguna diantara kedua perangkat. Untuk dapat menanggulangi *UDP flood* dengan mudah, dapat dengan mem*filter* pada *firewall* semua *service UDP* yang masuk [5].

Firewall melakukan *filter* dengan memeriksa data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diijinkan atau ditolak. *Firewall* dapat juga bertindak sebagai perantara dan permintaan *proxy host* yang dilindungi, sementara

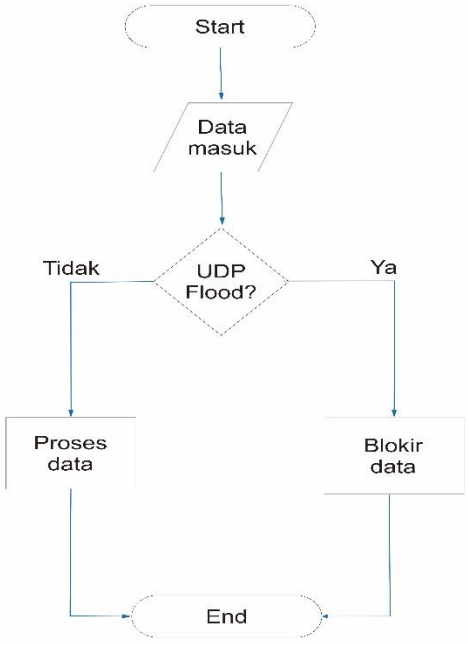
pada saat yang sama menyediakan sarana otentikasi akses untuk lebih memastikan bahwa hanya perangkat akses diberiakan. Meskipun *firewall* tidak dapat mencegah semua serangan firewall setidaknya lebih dapat membantu membuat data aman daripada tanpa *firewall* sama sekali [5].

2. METODE PENELITIAN

Dalam analisis ini menggunakan metode penelitian deskriptif untuk memperoleh data secara langsung dengan melakukan teknik *flooding* serta teknik pencegahannya terhadap server yang telah dirancang.

Langkah kerja yang diterapkan yaitu melakukan *flooding* secara langsung terhadap router tanpa adanya filter firewall. Setelah beberapa saat, trafik pada router naik. Kemudian diterapkan filter firewall, cara kerja filter firewall tersebut yaitu dengan menyaring data masuk kedalam *router* yang melalui port DNS. Firewall memeriksa data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diijinkan atau ditolak. Data yang akan ditolak adalah data yang dikirimkan oleh alamat ip yang tidak ada pada *list DNS*dan *firewall* akan memblokir alamat ip yang tidak dijinkan tersebut jika mencoba melakukan *request* atau *flood* DNS ke ip *public*. Data yang diijinkan masuk kedalam jaringan yaitu data yang dikirimkan oleh alamat ip yang ada pada *list DNS*.

Setelah itu, dilakukan upaya penyerangan *flooding* kembali untuk mengecek fungsi dari filter firewall.

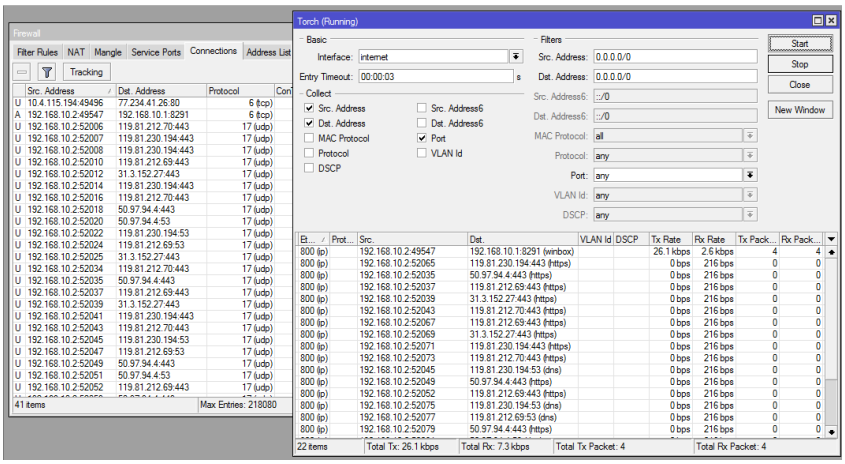


Gambar 1. *Flowchart* kerja filter firewall

3. HASIL DAN PEMBAHASAN

Setelah dilakukan *flooding*, trafik *upload*pada *monitoring router*naik cukup signifikan. Paket-paket data dikirim pada IP publik*router* melalui protokol UDP. Berdasarkan perubahan

trafik, dapat dikatakan bahwa percobaan *flooding*melalui protokol UDP tersebut cukup berhasil untuk membuat router menjadi sibuk dan akhirnya bisa *down*.



Gambar 2. trafik pada *router* setelah di *flooding* tanpa adanya *firewall*

Seperti yang ditujukkan pada gambar 1, trafik tersebut lumayan tinggi untuk client yang terhubung hanya 1 user dan tidak banyak melakukan aktifitas.

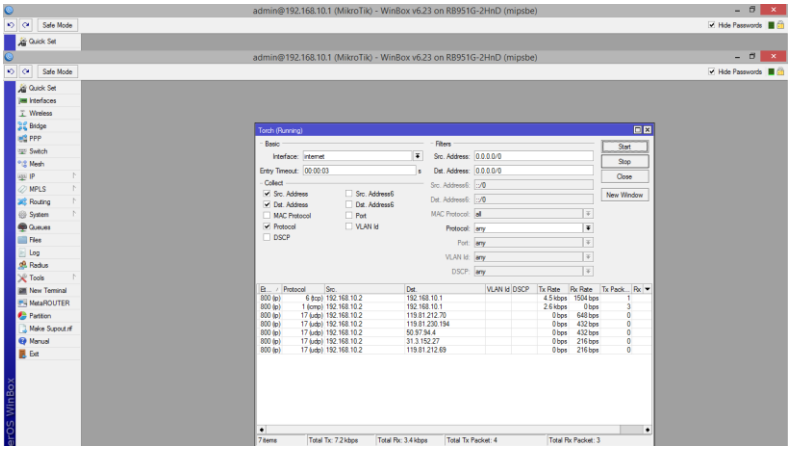
Agar UDP *flooding* tersebut tidak terjadi terus menerus adalah dengan mencegahnya melalui *filter* pada *firewall router*.*Filter* ini berfungsi untuk memblokir atau sebagai *drop* paket DNS yang tidak berasal dari DNS yang telah masuk *list Allow* DNS [6].

Untuk dapat membuat *filter* tersebut, dilakukan dengan membuat *input firewall* yang barupada *tab General* menggunakan *port* 53 dan *protocol* 17 (udp) dan atau *address list* yang dizinkan. *Address list* ini adalah *list* DNS *server*, fungsinya untuk mengisikan alamat IP yang diizinkan untuk menggunakan sistem jaringan tersebut. Dalam hal ini list DNS diisi dengan 2 DNS server dengan alamat 192.168.10.1 dan 192.168.20.1. DNS server dibuat 2 dengan tujuan agar DNS yang kedua berguna sebagai *backup* untuk mengatasi apabila sewaktu-waktu terjadi *downtime* atau gangguan teknis lainnya pada DNS 1 dan otomatis akan beralih menggunakana DNS ke 2.

Selanjutnya melakukan pemblokiran pada paket paket yang tidak diizinkan tersebut dengan mengatur *action* pada *filter firewall* menjadi *drop*.

Cara kerja *filter* ini yaitu setiap paket yang dikirimkan dengan protokol UDP dan melalui *port* DNS 53 jika tidak memenuhi syarat yang ada pada *list* DNS *server* maka paket tersebut akan di *drop*. Cara ini cukup efektif untuk mengatasi *flooding* pada jaringan skala menengah.

Setelah dibuat *filter* pada *firewall* tersebut, trafik paket data pada router menurun dan menjadi lebihstabil, seperti pada gambar berikut



gambar 3. trafik pada router setelah diterapkan firewall

setelah diterapkan *filter firewall*, trafik pada router menjadi lebih stabil dengan tidak banyak data yang masuk dibandingkan tanpa *firewall*. *Filter* tersebut mampu memblokir 60% paket yang mencoba masuk kedalam jaringan melalui port DNS yang awalnya 22 paket menjadi 7 paket.

Hal ini menunjukan bahwa pengaturan *filter* efektif mengatur penggunaan *bandwidth* secara wajar. IP *address* yang bukan merupakan DNS *server* yang diizinkan tidak dapat lagi melakukan request maupun *flood* DNS kepada IP publik *router* mikrotik.

4. KESIMPULAN

Berdasarkan pembahasan diatas, dapat disimpulkan bahwa penerapan *filter firewall* pada router mikrotik dapat mengurangi jumlah paket data UDP yang dikirimkan oleh *attacker* melalui port DNS sebanyak 60% dari jumlah paket yang masuk jika tanpa *firewall*. Sehingga router dapat berjalan secara normal kembali.

5. SARAN

Penelitiaan ini dapat dikembangkan dengan untuk mencegah serangan DDoS yang lain seperti *SYN-Flooding, SMURF Attack, UDP-Flooding, ICMP-Flooding* dan juga dapat dikembangkan dengan menggunakan algoritma lain untuk mencegah serangan DDoS.

DAFTAR PUSTAKA

[1] Ramadhani, kafi., Yusuf, M., Wahanani Henni E., 2015, *Pendeteksian Dini Serangan Udp Flood Berdasarkan Anomali Perubahan Traffic Jaringan Berbasis Cusum Algorithm*, Surabaya.

[2] Pratama, Johan A., Suadi, Wahyu., Dan Santoso, Bagus J., 2010, *Rancang Bangun Sistem Pencegahan Data Flooding Pada Jaringan Komputer*, Seminar Tugas Akhir Periode ITS Surabaya.

[3] Ria Pajri, Merry Agustina, Qoriani widayati, Rancang Bangun Model Sistem Keamanan Jaringan Berbasis De_Militarised Zone Di Poltek Kementerian Kesehatan Universitas Bina Darma, Palembang.

[4] Budi Triandi, 2015, Sistem Keamanan Jaringan Dalam Mencegah Flooding Data Dengan Metode Bloking IP Dan Port, *Seminar Nasional Teknologi Informasi dan Multimedia 2015*, Yogyakarta, 6-8 Februari.

[5] Kristanto, Y., 2010, Implementasi Dan Unjuk Kerja Keamanan Jaringan Pada Infrastruktur Berbasis IDPS (Insrusion Detection Prevention System), Skripsi, *Fakultas Teknik*, Universitas Indonesia, Depok.

[6] Nofriandi, 2016, Cara Drop UDP DNS Flooding pada Router Mikrotik, https://acenk90.com/2016/02/04/mengatasi-udp-dns-flooding-pada-router-mikrotik/#more-3086 diakses tanggal 8 Desember 2016.