DAMPAK SERANGAN DDOS PADA SOFTWARE BASED OPENFOW SWITCH DI PERANGKAT HG553

Alimuddin Yasin[1)], Ismail Mohidin[2)]
[1,2] Program Studi Teknik Informatika, Politeknik Gorontalo
email: alimuddiny@poligon.ac.id [1)]

ABSTRAK

Software Defined Network (SDN) adalah salah satu evolusi terbesar dalam dunia jaringan komputer. Dengan adanya SDN kemudahan dalam mengontrol jaringan lebih mudah dibandingkan dengan jaringan komputer biasa. Dimana dengan SDN konfigurasi jaringan lebih terpusat dikarenakan adanya pemisahan antara data plane dengan control plane. Data Plane berada pada sisi perangkat switch sedangkan control plane berada pada sisi server. Ada dua jenis switch Openflow yakni software based Switch Opeflow dan Hardware Based Switch Opeflow. Dalam penelitian ini jenis switch yang di pakai adalah Software Based Openflow Switch yang di pasang pada perangkkat HG553. Isu keamanan adalah isu yang masih terbuka luas untuk diteliti dalam Software Defined Network. Salah satunya adalah DDoS. DDoS adalah kegiatan untuk membanjiri jaringan dengan data sehingga lalulintas jaringan menjadi penuh dan jaringan tidak dapat diakses oleh orang yang tidak berhak. Jenis DDoS UDP Flooding adalah jenis DDoS Conectionless. Dalam penelitian menunjukan DDoS UDP Flooding yang terjadi dalam jaringan SDN menyebabkan jaringan SDN sulit untuk di akses dikarenakan Switch Opeflow terlepas dari kontroller dan menyebabkan penggunaan reource tinggi pada Switch Openflow.

Kata kunci : DDoS, Software Based Switch Openflow, HG553.

ABSTRACT

Software Defined Network (SDN) is one of the biggest touches in the world of computer networks. With the availability of SDN convenience in the network that is easier than ordinary computer networks. Where the SDN network configuration is more centralized between receiving data between planes and control aircraft. Plane data is on the side of the switch device while the control plane is on the server side. There are two types of OpenFlow switches, namely OpenFlow Switch based software and OpenFlow Hardware Based Switch. In this study, the type of switch used is the Software-Based OpenFlow Switch which is installed on the HG553 device. Social issues are issues that are still widely open to research in the Software Defined Network. One of them is DDoS. DDoS is an activity to flood networks with data networks becoming networks and not accessible to unauthorized people. UDP Flooding DDoS type is a DDoS Connectionless type. In the study, the UDP Flooding DDoS that occurs in the SDN network causes the SDN network to be difficult to access because of the Switch Opect flow from the controller and high rejection on the OpenFlow Switch.

Keywords: DDoS, OpenFlow Based Switch Software, HG553.

1. PENDAHULUAN

Software Defined Network (SDN) merupakan salah satu evolusi yang terjadi dalam perkembangan jaringan komputer. SDN memberikan kemudahan dalam membangun aplikasi untuk mengontrol perangkat jaringan secara terpusat. Dalam SDN fungsi dataplane dan control plane terpisah sehingga paket yang berjalan didalam jaringan dapat langsung di kontrol dengan perantara protokol openflow. Hal ini sangat berbeda dengan jaringan biasa yang menempatkan kedua fungsi tersebut dalam satu perangkat jaringan (Mininet Team, n.d.).

Openflow merupakan protokol yang ditujukan untuk mengontrol data plane switch yang dipisahkan dari control plane secara fisik. Data plane pada switch dapat dikontrol dengan memakai perangkat lunak (controller) yang dipasang pada server dengan perantara protokol openflow (Appelman, Boer, & Pol, 2012).

Switch Openflow merupakan perangkat switch yang mendukung protokol openflow di dalamnya. Terdapat dua jenis switch openflow. Yang pertama ada hardware based switch openflow yaitu switch yang dikeluarkan oleh beberapa vendor yang didalamnya sudah menerapkan TCAM dan Firmware khusus dalam mengimplementasikan flow tabel dan openflow protokol. Sedangkan software based switch openflow adalah perangkat jaringan yang firmwarenya menggunakan kernel Linux untuk menerapkan protokol openflow dan flow tabel (Kartadie & Suryanto, 2015).

Isu kemanan merupakan isu yang masih terbuka lebar dalam jaringan SDN. Salah satunya adalah dampak serangan DDoS di jaringan SDN. DDoS adalah aktifitas pengiriman paket dalam jaringan dalam jumlah besar yang ditujukan untuk membanjiri jaringan dengan data sehingga suatu host menjadi tidak dapat diakses oleh pengguna yang berhak.

Serangan ini memanfaatkan protocol UDP yang bersifat connectionless untuk menyerang target. Oleh karena itu UDP flood sangat mudah dilakukan. Paket-paket besar dan banyak dikirimkan begitu saja kepada korban sehingga paket tersebut membanjiri komputer

korban. pada beberapa kasus computer tersebut akan hang karena besarnya paket data yang dikirimkan (Hermawan, 2015).

HG553 adalah perangkat modem yang dikeluarkan oleh huawey yang firmware di dalamnya bisa di modifikasi dengan firmware linux. Sehingga dapat dimodifikasi menjadi software base switch openflow. Sehingga dalam penelitian ini akan dilakukan ujicoba Serangan DDoS dalam Jaringan SDN dan melihat dampak DDoS terhadap Software Based Switch Openflow di Perangkat HG553.

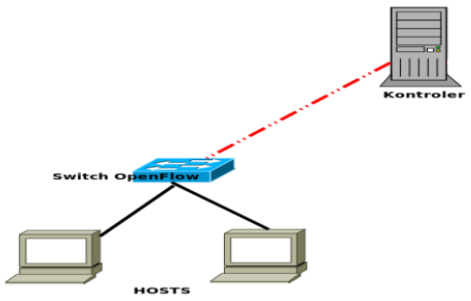
Dalam penelitian sebelumnya tentang pengujian serangan Distributed Denial Of Service di Jaringan Software Defined Network pada GNS3 hasil penelitian menunjukan bahwa serangan DDoS dapat mengakibatkan peningkatan penggunaan resource ram dan prosessor. (Alimuddin) Dalam penelitian tersebut ujicoba dilakukan dengan menggunakan Software Simulator GNS3. Sehingga menimbulkan pertanyaan apakah serangan DDoS yang dilakukan di jaringan SDN dalam simulator GNS3 akan berdampak sama pada jaringan nyata SDN dengan perangkat Software Based Switch Openflow.

2. METODE PENELITIAN

Langkah-langkah yang digunakan dalam penelitian ini Langkah langkah yang digunakan dalam penelitian ini: (1) Perancangan Topologi, (2) Implementasi Software Based Openflow Switch di perangkat HG553, (3) Simulasi serangan DDoS, (4) Pengamatan Resource pada Perangkat Software Based Openflow Switch

2.1. Perancangan Topologi

Topologi yang digunakan dalam penelitian ini adalah topologi star yang menghubungkan Huawei HG553 sebagai Software based Switch Openflow dengan controller dan 2 buah host computer seperti gambar berikut



Gambar 1. Topologi yang Digunakan dalam Penelitian

Keterangan Topologi yang digunakan pada Gambar 1 sebagai berikut:

Kontroller : Sebagai server yang mengontrol Switch Openflow
Switch Openflow : Menunjukan Posisi Perangkat HG553 sebagai Software Based Switch Openflow
Host : Host yang terhubung pada Switch Openflow
_____ : Link yang menghubungkan Kontroller dengan Switch Openflow
---------- : Link yang menghubungkan Host dengan Switch Openflow

2.2. Implementasi Software Based Openflow Switch

Langkah-langkah mengimplementasi Software Based Openflow Switch di perangakat HG553 sebagai berikut:

- Menganti firmware HG553 dengan firmware yang dibangun dengan kernel linux. Dalam penelitian ini digunakan firmware Lede yang merupakan turunan dari firmware OpenWRT
- Instalasi paket OpenVSwitch. OpenVSwitch adalah paket aplikasi pada sistem operasi linux yang dapat mengubah Komputer atau Perangkat jaringan yang bersistem kernel linux menjadi software based switch openflow
- Konfigurasi Perangkat agar terhubung dengan Kontroller.

2.3. Konfigurasi Kontroller

Kontroller berfungsi untuk mengontrol arus data dalam jaringan yang berada pada switch openflow. Dalam penelitian ini kontroller yang digunakan adalah kontroller Ryu. Ryu kontroller dipasang pada ubuntu server.

2.4. Simulasi Serangan DDoS dan Pengamatan Resource pada Perangkat Software Based Openflow Switch.

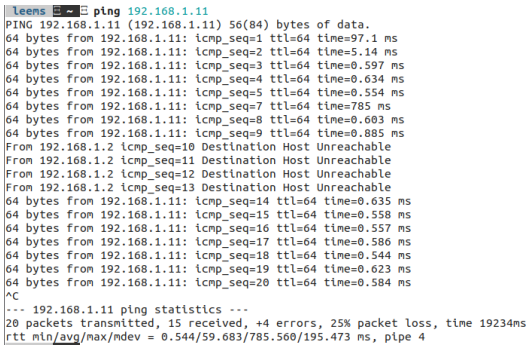
Jenis serangan DDoS yang digunakan dalam penelitian ini UDP Flooding attack. Yakni jaringan SDN yang berjalan dengan perangkat HG553 akan dibanjiri paket UDP dengan pengiriman paket mulai dari 20000 paket sampai 100000 paket. Saat terjadi serangan di jaringan SDN, resource Ram dan Prosessor pada Perangkat Software Based Openflow Switch yaitu perangkat HG553 dilakukan pengamatan apakah serangan yang terjadi pengaruh pada penggunaan ram dan prosessor.

3. HASIL DAN PEMBAHASAN

Dari hasil pengamatan dari serangan DDoS yang dilakukan di jaringan SDN dengan perangkat Switch Openflow mengakibatkan koneksi antara kontroller dan Switch Openflow ikut menjadi penuh dengan banyaknya dataflow yang masuk ke kontroller sehingga menyebabkan terputusnya koneksi dari kontroller ke switch openflow. Sehingga layanan jaringan yang ada dalam jaringan SDN menjadi lumpuh selama adanya serangan. Setelah itu akan pulih kembali setelah tidak ada serangan. Seperti yang telihat pada Gambar 2.

Pada gambar 2 terlihat jaringan SDN tidak dapat bekerja pada seq 10 sampai 13 hal ini dikarenakan serangan flood attack bertipe UDP dengan besar 60000 paket UDP selama 1 detik sedang berlangsung. Dan ketika

sudah tidak terdapat serangan maka jaringan akan pulih dengan sendirinya seperti terlihat pada seq 14.



Gambar 2. Kondisi jaringan Saat terjadi Serangan DDoS

Selain dapat menyebabkan jaringan lumpuh, serangan DDoS juga dapat mempengaruhi penggunaan resource prosessor dari perangkat software based switch openflow menjadi naik. Berikut hasil tabel penggunaan resource ram dan processor pada Switch Openflow.

Tabel 1. Dampak Serangan DDoS terhadap Resource Switch Openflow.

Jumlah Paket UDP (dlm 1 Detik)	RAM (64MB)	CPU %
Tanpa Serangan	29 MB	13%
20000	41 MB	43%
40000	42 MB	50%
60000	42 MB	69%
80000	42 MB	75%
100000	45 MB	80%
Flooding Selama 1 Menit	61 MB	98%

Dari Tabel 1 terlihat bahwa serangan yang terjadi dalam jaringan SDN mengakibatkan penggunaan resource dari ram dan cpu pada perangkat switch openflow ikut meningkat. Sehingga mempengaruhi kinerja dari switch. Dari beberapa serangan yang dilakukan mulai dari jumlah paket 20000 sampai 80000 dampak serangan terhadap switch openflow menyebabkan penggunaan RAM rata-rata sekitar 42MB. Akan tetapi penggunaan processor pada switch openflow mengalami peningkatan secara bertahap mulai dari 43% sampai 80% sesuai dengan besaran paket UDP Flood yang di lepaskan di dalam jaringan. Ketika dilakukan serangan flooding paket UDP secara terus terusan selama 1 menit dalam jaringan, penggunaan ram 61MB dari 64MB ram dan penggunaan processor mencapai 98%. Sehingga menyebakan switch tidak dapat bekerja sama sekali dan sulit untuk di akses selama serangan UDP Flood berlangsung.

4. KESIMPULAN DAN SARAN

Dari hasil yang di dapat dapat disimpulkan bahwa serangan DDoS UDP Flooding Attack yang berada dalam jaringan SDN di perangkat HG553 menyebabkan jaringan SDN tidak dapat bekerja. Hal ini dikarenakan switch openflow tidak dapat berkomunikasi dengan kontroller. Selain itu serangan yang terjadi mengakibatkan penggunaan prosessor menjadi tinggi sehingga ikut mempengaruhi perangkat HG553 secara keseluruhan.

DAFTAR PUSTAKA

Appelman, M., Boer, M.DE., & Pol, R.VAN DER. (2012). Performance Analysis of OpenFlow Hardware, 28. Diambil dari delaat.net/rp/2011-2012/p18/report.pdf%0A%0A

Hermawan, R. (2015). Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDOS). *Faktor Exacta*, *5*(1), 1–14. https://doi.org/10.1016/j.bbrc.2010.02.152

Kartadie, R., & Suryanto, T. (2015). Uji Performa Software-Based Openflow Switch Berbasis Openwrt. *Sisfotenika*, *5*(2). Diambil dari http://www.sisfotenika.stmikpontianak.ac.id/index.php/ST/article/view/83/93

Mininet Team. (n.d.). Mininet: An Instant Virtual Network on your Laptop (or other PC) - Mininet. Diambil 22 Oktober 2018, dari http://mininet.org/

Yasin, A. (2016). Pengujian Serangan Distributed Denial of Service (Ddos) Di Jaringan Software-Defined Pada Gns3. *Jurnal Teknologi Informasi*, *XI*(32).