BAB 1
PENDAHULUAN

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi sangat berkembang pesat dalam beberapa tahun terakhir, seiring perkembangan tersebut muncul teknologi yang bernama VPN (*Virtual Private Network*) yaitu sebuah jaringan pribadi virtual yang bisa digunakan untuk berkomunikasi, mengirim file antar satu dengan yang lain. VPN menggunakan perantara internet atau jaringan publik untuk menghubungkan *remote-site* dengan server ataupun dengan *remote-site* lainnya [1].

Dengan adanya VPN banyak client yang berada di luar jaringan LAN yang berbeda dengan VPN Server ataupun di tempat lain yang berjauhan dapat mengakses jaringan LAN VPN Server tersebut dari kejauhan dengan menggunakan teknologi VPN ini. Sehingga di era sekarang banyak perusahaan hingga instansi pemerintah pun memiliki sebuah VPN Server pribadi untuk keperluan komunikasi internal mereka [1].

Akan tetapi meskipun dikatakan sebuah jaringan pribadi virtual, VPN Server tetap memiliki celah (bug) didalam nya sehingga dapat mengakibatkan oknum-oknum yang tidak bertanggung jawab melakukan serangan ke VPN Server tersebut. Serangan yang biasa dilakukan ialah DDoS Attack (*Distributed Denial of Service*) yaitu serangan dengan cara mengirimkan sebanyak-banyaknya traffic ke jaringan server vpn agar server tersebut down. Jika server tersebut down berakibat komunikasi internal di perusahaan tersebut akan mengalami loss koneksi sehingga pengiriman data, dll akan terputus. Hal buruk yang bisa semakin terjadi selain server tersebut down ialah proses bisnis di perusahaan akan berhenti.

Dengan latar belakang permasalahan tersebut, maka penulis bermaksud untuk membuat penelitian dengan tema Analisis penanggulangan terhadap serangan DDoS Attack agar VPN Server tetap berjalan normal.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan diatas maka dapat dirumuskan beberapa masalah, yaitu:

1. Bagaimana traffic jaringan dari VPN Server dengan Protokol PPTP di Netdata sebelum di DDoS Attack?
2. Bagaimana traffic jaringan dari VPN Server dengan Protokol PPTP di Netdata ketika di DDoS Attack?
3. Bagaimana traffic jaringan dari VPN Server di Netdata sesudah di DDoS Attack?
4. Bagaimana perancangan sebuah Firewall di VPN Server agar dapat mengidentifikasi dan menyaring paket-paket yang keluar masuk di jaringan VPN Server serta bagaimana mengaktifkan SYN Cookies di tingkat kernel?

1.3 Tujuan

Maksud dari tujuan dilakukannya penelitian ini adalah

1. Memahami kondisi traffic jaringan dari VPN Server di Netdata sebelum di DDoS Attack
2. Memahami kondisi traffic jaringan dari VPN Server di Netdata ketika di DDoS Attack
3. Mengetahui hasil traffic jaringan dari VPN Server di Netdata sesudah di DDoS Attack
4. Dapat mengetahui dan memahami solusi untuk menanggulangi serangan DDoS Attack pada VPN Server dengan perancangan Firewall dan pengaktifan SYN Cookies di tingkat kernel

1.4 Batasan Masalah

Agar penelitian tidak meluas, maka penulis memberikan batasan-batasan permasalahan sebagai berikut:

1. VPN Server menggunakan OS Linux Ubuntu Server sedangkan DDoS Attack menggunakan OS Kali Linux Dekstop.
2. Pengujian Serangan DDoS Attack dilakukan dengan *Virtual Machine* (VirtualBox), dikarenakan terbatasnya media perangkat yang ada.
3. VPN Server menggunakan Protokol PPTP sedangkan DDoS Attack menggunakan Protokol HPing3.
4. Pemantauan hasil traffic sebelum, sedang, dan sesudah di DDoS Attack pada VPN Server menggunakan software Netdata di Linux Ubuntu Server.
5. Solusi untuk menanggulangi serangan DDoS Attack pada VPN Server adalah perancangan sebuah Firewall di VPN Server agar dapat mengidentifikasi dan menyaring paket-paket yang keluar masuk di jaringan VPN Server. Selain itu juga mengaktifkan SYN Cookies di tingkat kernel.

1.5 Kontribusi

Dengan adanya penelitian ini, diharapkan dapat mengetahui serta memahami upaya penanggulangan terhadap serangan DDoS Attack pada VPN Server sehingga dapat menjadi tolak ukur dalam penanganan dalam menangani serangan DDoS Attack.

1.6 Metode Penelitian

Dalam menganalisis penyusunan penelitian penanggulangan serangan *distributed denial-of-service* (DDoS) pada VPN Server ini, terdapat beberapa langkah-langkah penelitian yang dilakukan yaitu:

1. Studi Literatur

   Pada tahap ini, penelitian yang dilakukan mengumpulkan dan mencari referensi dari beberapa jurnal, buku, dan artikel dari internet yang berhubungan dengan Serangan DDoS serta upaya untuk penanggulangannya.
2. Perancangan & Implementasi Sistem

   Tahap ini melakukan perancangan yang dimulai dari pembuatan VPN Server, VPN Client, serta pembuatan Firewall untuk upaya menanggulangi serangan DDoS pada VPN Server dan pengaktifan SYN Cookies di tingkat kernel.

   Perancangan di implementasikan melalui VPS & software VirtualBox sebagai simulasi penelitian.
3. Pengujian Keberhasilan Firewall & SYN Cookies Dalam Percobaan Serangan DDoS

   Pada tahap ini, dilakukan uji coba terhadap perancangan firewall yang telah dibuat dan SYN Cookies yang telah diaktifkan, yaitu dengan melakukan Serangan DDoS di kali linux terhadap VPN Server, kemudian akan dilakukan pemantauan traffic jaringan pada VPN Server seperti apa hasilnya.
4. Analisis Data

   Tahap ini, akan dilakukan analisis data dari hasil percobaan Serangan DDoS terhadap VPN Server. Kriteria analisis data yang diambil yaitu seberapa berhasilkah penerapan Firewall & pengaktifan SYN Cookies sebagai upaya penanggulangan terhadap Serangan DDoS.
5. Penulisan Laporan

   Tahap yang terakhir, akan dilakukan penulisan laporan sebagai hasil fisik penelitian yang telah dilakukan.

1.7 Jadwal Penelitian

Pelaksanaan penelitian tugas akhir ini berdasarkan perencanaan jadwal yang dilampirkan sebagai berikut:

Tabel 1.1 Jadwal Pelaksanaan Penelitian

No.	Jenis Kegiatan	Tahun 2022/2023																			
		Maret				April				Mei				Juni				Juli			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Instalasi OS Ubuntu Server & Kali Linux	■																			
2.	Instalasi & Konfigurasi PPTP VPN Server		■	■	■																
3.	Instalasi & Konfigurasi Netdata					■															
4.	Perancangan Firewall & Aktif SYN Cookies						■	■	■	■	■	■	■								
5.	Pengujian & Analisis keberhasilan Firewall & SYN Cookies						■	■	■	■	■	■	■								
6.	Penyusunan buku Tugas Akhir													■	■	■	■	■	■		
7.	Sidang Tugas Akhir																		■		
8.	Revisi buku Tugas Akhir																			■	■