ANALISIS DAN IMPLEMENTASI SISTEM REDUNDANT FIREWALL MENGGUNAKAN METODE INTRUSION PREVENTION SYSTEMS (IPS)

Frastuzi Affan[1], Yudha Purwanto[2], Agus Virgono[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Sistem Redundant Firewall adalah system firewall yang terdiri dari dua firewall atau lebih yang jikasalah satu firewall berhenti bekerja karena suatu hal (contoh: malicious attack), maka akan langsung digantikan oleh firewall lainnya. Penggunaan firewall tunggal sangat rentan bagi sebuah jaringan karena mempunyai banyak kelemahan, diantaranya adalah rawan terhadap para hacker yang dapat memanfaatkan kelemahan dari hardware maupun konfigurasi firewall yang dapat mengakibatkan firewall tidak berfungsi secara semestinya.

Hadirnya firewall telah banyak membantu dalam pengamanan, akan tetapi seiring berkembangnya teknologi sekarang ini, jika hanya dengan firewall keamanan tersebut belum dapat dijamin sepenuhnya. Oleh karena itulah dikembangkan teknologi pengamanan jaringan yang bernama IDS dan IPS, yaitu sebagai pembantu pengamanan data pada suatu jaringan komputer.

Pada implementasi sistem Redundant Firewall, sudah diujicobakan pada macam-macam tipe serangan, seperti serangan DDoS (Distributed Denial of Service) yang merupakan salah satu tipe serangan yang mengeksploitasi system dimana system akan dikirimkan request dalam jumlah sangat besar, sistem yang tidak mampu menangani request tersebut akan habis sumber daya sistemnya sehingga kinerja system secara utuh akan terganggu. Maka dari itu digunakanlah Redundant Firewall disertai dengan Intrusion Prevention System yang dapat membuat jaringan lebih tahan terhadap serangan semacam DDoS.

Kata Kunci : Firewall, Redundant, IDS, IPS, DDoS

Abstract

Redundant System Firewall is a firewall system that consists of two or more firewalls that if one firewall to stop working for some reason (eg, malicious attack), it will be immediately replaced by another firewall. The use of a single firewall is vulnerable to a network because it has many shortcomings, among them are vulnerable to hackers who can exploit the weaknesses of the hardware or firewall configuration may lead to the firewall is not functioning properly.

The presence of a firewall has a lot of help in security, but as the development of technology nowadays, if only with security firewalls are yet to be fully guaranteed. Hence, network security technology developed by the name of IDS and IPS, which is as an auxiliary securing data on a computer network.

Redundant Firewall on system implementation, has been tested on arange of different types of attacks such as DdoS attacks (Distributed Denial of Service) which is one type of attacks that exploit the system where the system will be sent in a number of very large requests, the system is not capable of handling such requests will the system runs out of resources so that performance of the system as a whole will be disrupted. Thus it is used along with Redundant Firewalls Intrusion Prevention System that can make the network more resilient to such attacks DDoS.

Keywords : Firewall, Redundant, IDS, IPS, DDoS

BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam beberapa tahun belakangan ini, sistem keamanan komputer telah menjadi fokus utama dalam dunia Jaringan Komputer. Keamanan komputer merupakan salah satu kunci yang dapat mempengaruhi tingkat *Reliability* yang di dalamnya termasuk *Performance* dan *Availibility* suatu Internetwork.

Saat ini telah banyak perusahaan yang mengeluarkan banyak biaya demi mengamankan sistemnya agar terhindar dari serangan *malware* jahat, *virus*, *hacker*, dan hal yang tidak diinginkan lainnya yang dapat berdampak pada terganggunya kinerja perusahaan mereka. Hal ini diperburuk dengan masih dipergunakannya *firewall* tunggal untuk mengamankan jaringan sebesar perusahaan, padahal untuk mengamankan jaringan di era ini sudah sangat diperlukan *multi firewall* yang bekerja secara *redundant* serta ditambahkan *dengan Intrusion Prevention System (IPS).*

IPS sendiri merupakan teknologi terbaru hasil dari pengembangan dari *Intrusion Detection System* (*IDS*). *IPS* merupakan jenis metode pengamanan jaringan yang dapat memonitor aktivitas yang tidak diinginkan atau *intrusion* dan dapat langsung bereaksi untuk mencegah aktivitas tersebut. Sebagai pengembangan dari teknologi *firewall*, IPS melakukan pengendali dari suatu system berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan *ports* atau *IP address* seperti *firewall* umumnya.

Selain itu *IPS* dapat menghasilkan *packet loss* yang bernilai 0% walau server dalam keadaan diserang, dan ketika server *IPS down* karena diserang sejumlah *client* penyerang dengan besaran paket tertentu, dengan bantuan *redundant firewall* akan berpindah secara otomatis dari *server master* ke *server slave* agar kerusakan dapat diminimalisir dengan segera.

1.2. Rumusan Masalah

Secara garis besar pokok permasalahan yang dibahas dalam tugas akhir ini meliputi:

- Pemodelan sistem *Failover Firewall* yang digunakan pada sistem *Redundant Firewall IPS*.
- Pemodelan sistem *Security* yang digunakan untuk menyerang sistem *Redundant Firewall IPS*.
- Menganalisa hasil implementasi yang telah dilakukan dengan pengukuran parameter performansi: f*ailover time* dan parameter *security* yang diujikan terhadap sistem *Redundant Firewall* tersebut.
- Menganalisa performansi jaringan pada saat sistem dilakukan pengujian
- Bagaimana mekanisme penyerangan terhadap sistem *redundant firewall IPS* untuk menguji karakteristik sistem.
- Bagaimana mekanisme pemblokiran serangan terhadap sistem *redundant firewall IPS* untuk menguji karakteristik sistem.
- Jumlah maksimal user yang bisa dilayani oleh sebuah single *firewall* dibandingkan dengan sistem *redundant firewall IPS*.

1.3. Batasan Masalah

Pembuatan sistem clustering yang diteliti pada tugas akhir ini dibatasi oleh beberapa hal sebagai berikut:

1. Sistem *Redundant Firewall* hanya menggunakan sistem *Failover Firewall*.
2. Server yang digunakan *operating system Ubuntu.*
3. Sistem yang dibangun menggunakan IPS (*Intrusion Prevention System*) sebagai sistem pemblokiran serangan.
4. Sistem diuji kemampuannya untuk mencegah serangan *DDoS* menggunakan program *TFN* serta digunakan pula *IPS* untuk memblok paket yang tidak diinginkan.

1.4. Tujuan dan Kegunaan

Hasil yang diharapkan dari penelitian ini antara lain sebagai berikut:

1. Memahami prinsip kerja suatu sistem *redundant firewall* menggunakan metode *failover firewall* , mulai saat sistem bekerja secara normal hingga sistem mengalami *failover* disebabkan karena kelemahan sistem.
2. Mengimplementasikan sistem *redundant firewall* dengan menggunakan metode *IPS*.
3. Mengetahui karakteristik dari metode IPS.

1.5. Metode Penelitian

Untuk melakukan kajian perancangan dalam permasalahan tersebut, metodologi penelitian yang diambil meliputi :

1. Studi literatur dan kepustakaan, yaitu mempelajari teori pendukung tentang sistem *redundant firewall,* dan metode keamanan jaringan.
2. Implementasi, yaitu mengimplementasikan rancangan yang telah dibuat dengan parameter yang telah ditentukan.
3. Analisa kinerja sistem dengan mengamati dan mengevaluasi data hasil tes performansi.

1.6. Sistematika Penulisan

Adapun sistematika penulisan pada Tugas Akhir ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi latar belakang, perumusan masalah, batasan masalah, tujuan, metodologi penelitian serta sistematika penulisan.

BAB II Dasar Sistem *Redundant Firewall*

Bab ini berisi deskripsi teori dasar mengenai sistem *redundant firewall dan Intrusion Prevention System*.

BAB III Implementasi Sistem *Redundant Firewall*

Bab ini akan dibahas proses perancangan dan implementasi sistem *redundant firewall IPS*, serta skenario pengujian terhadap sistem *redundant firewall IPS.*

BAB IV Analisa Implementasi Sistem *Redundant Firewall*

Bab ini akan membahas analisis dan evaluasi dari kinerja sistem *redundant firewall IPS* tersebut terhadap skenario parameter pengujian yang diberikan.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan dan saran dari Tugas Akhir terhadap untuk pengembangan lebih lanjut.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil implementasi serta pengambilan data dan analisis mengenai sistem *Redundant Firewall* yang diujikan menggunakan beberapa skenario, maka dapat diambil kesimpulan sebagai berikut:

1. Waktu perpindahan yang dibutuhkan oleh Sistem Redundant Firewall dari Server Master ke Server Slave ketika server down, membutuhkan waktu antara 10 sampai 35 detik (sesuai dengan spesifikasi komputer dan cara instalasi yang penulis gunakan).
2. Pada serangan DDoS ICMP Flood dalam uji coba untuk mengetahui ketahanan server IPS, batasan server masih dapat menahan serangan bersamaan serta beruntun adalah di angka 3000 paket kebawah (sesuai dengan spesifikasi komputer yang penulis gunakan), setelah itu server akan mulai mengalami failover. Batasan paket yang masih mungkin diterima pada satu waktu adalah berada di angka 9,887,574 paket.
3. Pada serangan DDoS UDP Flood dalam uji coba untuk mengetahui ketahanan server IPS, batas server masih dapat menerima serangan serentak serta terus menerus adalah di kisaran 2000 paket kebawah (sesuai dengan spesifikasi komputer yang penulis gunakan), setelah itu server akan mulai kewalahan yang pada akhirnya akan menyebabkan down/failover. Untuk batasan paket yang masih mungkin diterima pada satu waktu adalah berada di angka 9,582,120 paket.
4. Untuk kasus DDoS TCP/SYN Flood dalam uji coba untuk mengetahui ketahanan server IPS sedikit berbeda dari ICMP dan UDP Flood, pada kasus ini tidak terpaku pada berapa jumlah besar paket serangan serentak dan beruntun, namun lebih kepada jumlah Client yang menyerang, terlihat bahwa pada jumlah 2 client server masih sanggup menghadapi serangan yang datang bertubi-tubi, namun begitu client ditambah jumlahnya mejadi 3, server sudah kewalahan dan akhirnya down, sama halnya jika ditambah jumlahnya menjadi 4 (sesuai dengan spesifikasi komputer yang penulis gunakan). Terlihat pula perbedaan yang mencolok antara batas

maksimal paket yang dapat diterima dalam satu waktu dengan batas minimal paket yang menyebabkan server fail, yaitu 8,674,912 paket untuk paket maksimal dapat diterima, dan 30,376,823 paket untuk minimal paket yang mengakibatkan server fail.

5. Salah satu kakarakteristik yang terlihat mencolok yang dimiliki oleh IPS adalah *Packet Loss* yang Nampak pada semua tipe serangan yang tidak menyebabkan *failover* terlihat 0%, hal ini menunjukkan kelebihan dari karakteristik IPS yang tetap akan menyalurkan paket baik secara normal walaupun sedang dalam kondisi diserang, terkecuali jika server down, maka paket benar-benar *loss* semua.

5.2 Saran

Beberapa saran yang dapat diberikan guna pengembangan lebih lanjut antara lain:

1. Perlu dilakukan penelitian lebih lanjut tentang konfigurasi jaringan sistem *redundant firewall* agar diperoleh downtime mendekati 0 detik.
2. Untuk lebih mengoptimalkan kinerja sistem, perlu adanya penelitian lebih mendalam mengenai konfigurasi *firewall* yang digunakan.
3. Perlu dilakukan penelitian lebih lanjut tentang aplikasi multiple *firewall cluster*.
4. Perlu dilakukan penelitian lebih lanjut penggunaan tipe-tipe IPS *(Intrusion Prevention System)* agar dapat mengamankan jaringan dengan berbagai topologi.

DAFTAR PUSTAKA

[1]. Sourour.M, et al, "Collaboration between Security Devices toward improving Network Defense", sevent IEEE/ACIS International Conference on Komputer and Information Science, 2008.

[2]. Kjetil Haslum, et al," Real-time Intrusion Prevention and Security of Network using HMMs", Local Komputer Networks, 2008.

[3]. Xinyau Zhang, et al, "Intrusion Prevention System Design", Komputer and Information Technology, 2004

[4]. Martuza Ahmed, et al," NIDS : A Network based approach to intrusion prevention and prevention",International Association of Komputer Science and Information Technology - Spring Conference, 2009.

[5]. C. Pattinson, et al,"Trojan Prevention using MIB-based IDS/IPS system", Information, Communication and Automation Technologies, 2009.

[6]. Yaping Jiang, et al ,"A Model of Intrusion Prevention Base on Immune", Fifth International Conference on Information Assurance and Security, 2009.

[7]. E. Guillen, et al " Weakness and Strength Analysis over Network-Based Intrusion Prevention and Prevention Systems" Communications, 2009.

[8]. C.M. Akujuobi, et al "Application of Wavelets and Self-similarity to Enterprise Network Intrusion Prevention and Prevention Systems", Consumer Electronics, 2007.

[9]. Rainer Bye, et al, "Design and Modeling of Collaboration Architecture for Security", International Symposium Collaborative Technologies and Systems, 2009.

[10]. Robert Richardson, "CSI Komputer Crime & Security Survey 2008", 2008.

[11]. Anh Le, et al," On Optimizing Load Balancing of Intrusion Prevention and Prevention Systems", IEEE, INFOCOM Workshops, 2008

[12]. E. Carter, et al, "Intrusion Prevention Fundamentals : an introduction to network attack mitigation with IPS", Cisco press, 2006.

[13]. Kamei, S, et al," Practicable network design for handling growth in the volume of peer-to-peer traffic", Communications, Komputers and signal Processing, 2003.

[14]. Deris S, A. Hanan, M. Yazid, "The Measurement Internet Services", International Conferences, ICGC-RCICT, 2010.

[15]. Taras Dutkevych, et al, " Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks, IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007.

[16]. Zhijie Liu, et al, " Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling", International Conference on Information Security and Assurance, 2008.

[17]. Frias-Martinez.V, et al, "Behavior-Profile Clustering for False Alert Reduction in Anomaly Prevention Sensors " Komputer Security Applications Conference, 2008.

[18].Nur Ikhwan, Ariza, "Analisis Dan Implementasi Metode Failover Pada Sistem Redundant Firewall", 2009.

[19]. Deris Stiawan, "Intrusion Prevention System (IPS) dan Tantangan dalam pengembangannya", 2010.

[20]. IP Failover - Cloud Servers Wiki www.wikipedia.com. 27 Februari 2011.

[21]. TFN: Tribal Flood Network www.javvin.com. 10 Maret 2011.