BINA DARMA CONFERENCE ON Computer Science

Volume 2, Number 1, 2020

Diterbitkan Oleh:
Direktorat Riset dan Pengabdian kepada Masyarakat
Universitas Bina Darma

Diselenggarakan Oleh:
Fakultas Ilmu Komputer Universitas Bina Darma

pISSN: 2685-2675 eISSN: 2685-2683

HRIS-Universitas Bina Darma | SimlitabmasNG - Login | (23) WhatsApp | Vol 2 No 1 (2020): Bina Darma
conference.binadarma.ac.id/index.php/BDCCS/issue/view/16

Muhammad Surahman, Leon Andretti Abdillah, Ferdiansyah Ferdianyah 196-206

Download PDF

PENERAPAN ALGORITMA NAÏVE BAYES UNTUK MENENTUKAN NASABAH POTENSIAL KLAIM PADA PT PENJAMINAN JAMKRINDO SYARIAH

Aji Army, Baibul Tujni 207-217

Download PDF

PERBANDINGAN MONITORINGTOOL CACTI, MRTG DAN NAGIOS DALAM MONITORING JARINGAN DI UNIVERSITAS BINA DARMA PALEMBANG

Harris Eka Syaputra, Yesi Novaria Kunang, Eka Puji Agustini 218-228

Download PDF

PENERAPAN SISTEM KEAMANAN FIREWALL PADA ROUTER CISCO 1841 DAN MONOWALL PADA SISTEM OPERASI BSD (BERKELEY SOFTWARE DISTRIBUTION)

Rinto Erlando, Diana Diana, Maria Ulfa 236-243

Download PDF

IMPLEMENTASI KEAMANAN BASIS DATA PADA DATA PEGAWAI DI PT. TIRTA MUSI MENGGUNAKAN METODE RC4

Muhammad Ridho, Jemakmun Jemakmun 244-253

Download PDF

Simulasi UN SMP Berbasis Web Menggunakan Metode Linear Congruential Generator (LCG)

Syafari Syafari, Siti Sauda 254-264

ENG 10:00 29/10/2020

PENERAPAN SISTEM KEAMANAN *FIREWALL* PADA *ROUTER CISCO* 1841 DAN *MONOWALL* PADA SISTEM OPERASI BSD *(BERKELEY SOFTWARE DISTRIBUTION)*

Rinto Erlando[1], Diana[2], Maria Ulfa[3]
Fakultas Ilmu Komputer, Universitas Bina Darma
Email: **rintoerlando96@gmail.com[1], diana@binadarma.ac.id[2], maria.ulfa@binadarma.ac.id[3]**

ABSTRAK

Salah satu bentuk dari sistem keamanan jaringan, seperti firewall dan monowall, yang merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware dan software ataupun sistem sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan luar, yang bukan merupakan ruang lingkupnya. Salah satu bentuk dari sistem keamanan jaringan, seperti firewall dan monowall, yang merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware dan software ataupun sistem sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan luar, yang bukan merupakan ruang lingkupnya.Adapun langkah-langkahnya sebagai berikut : menentukan topologi, melakukan simulasi pada topologi, menentukan topologi jaringan monowall, konfigurasi sistem operasi, konfigurasi NAT firewall mikrotik, konfigurasi ip adddress dengan mengikuti langkah-langkah tersebut dan menggunakan router cisco 1841 pengguna dapat memblokir situs yang diinginkan.

Kata kunci: **:** Keamanan jaringan, *Firewall*, *Monowall*, DdoS (*Denial of Service*), *Router Cisco*

ABSTRACT

One form of network security systems, such as firewalls and monowalls, which is a method or mechanism that is applied both to hardware and software or the system itself with the aim to protect, either by filtering, limiting or even rejecting one or all of the relationships / activities of a segment on the outside network, which is not the scope. One form of network security systems, such as firewalls and monowalls, which is a method or mechanism that is applied both to hardware and software or the system itself with the aim to protect, either by filtering, limiting or even rejecting one or all of the relationships / activities of a segment on external networks, which are not the scope. As for the steps as follows: determine the topology, simulate topology, determine the monowall network topology, operating system configuration, configuration of the NAT proxy firewall, ip configuration configuration by following these steps and using cisco 1841 router users can block the desired site.

Key Word : *Network Security, Firewall, Monowall, Denial of Service*

1. PENDAHULUAN

Menurut [1] bahwa perkembangan teknologi informasi dan internet di Indonesia setiap tahun menunjukkan kemajuan yang sangat pesat dari segi infrastruktur, pengguna, perangkat keras (*hardware*), perangkat lunak (*software*) dan sistem informasi yang handal.Penggunaan teknologi komputer dan internet menjadi acuan yang dapat memaksimalkan hasil dan kualitas dari sebuah system”.“ [2] Kebutuhan akan teknologi informasi diaera modern ini sangat besar serta dapat diaplikasikan dalam berbagai bidang, sebab itu juga banyak pihak-pihak yang saat ini jadi bergantung pada sistem komputer sehingga sistem komputer dituntut untuk berjalan sepanjang waktu pada jaringan internet”.[3] Jaringan komputer yang terhubung ke *internet* harus direncanakan dan dikoordinasikan dengan baik, agar dapat melindungi sumber daya dan investasi di dalamnya.Sistem keamanan jaringan komputer merupakan komponen yang sangat luas, dan memiliki manfaat yang banyak”.“ Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunanya”.“ [4] Sistem harus dilindungi dari segala macam serangan, dan usaha-usaha penyusupan oleh pihak yang tidak berhak”.“[5] Dikarenakan masih terlalu banyak kekurangan dari metode ini, sehingga dikembangkan berbagai bentuk, konfigurasi dan jenis *firewall* dengan berbagai *policy* (aturan) di dalamnya”. “[6]*Firewall* secara umum diperuntukkan melayani mesin komputer, setiap mesin komputer yang terhubung langsung ke jaringan luar atau *b* terdapat pada komputernya terlindungi”. “ [7] Jaringan-jaringan komputer yang terdiri lebih dari satu buah komputer, dan berbagai jenis *topologi* jaringan yang digunakan, baik yang dimiliki oleh perusahaan”.

Keamanan jaringan merupakan suatu cara atau suatusystem yang digunakan untuk memberikan proteksi atauperlindungan pada suatu jaringan agar terhindar dari berbagaiancaman luar yang mampu merusak jaringan dan pencuriandata perusahaan. “[8]Menurut Ri2M (2010) Keamanan jaringan dapat digambarkan secara umum yaitu apabila komputer yang terhubung dengan jaringan yang lebih banyak mempunyai ancaman keamanan dari pada komputer yang tidak terhubung ke mana – mana. Namun dengan adanya pengendalian maka resiko yang tidak diinginkan dapat dikurangi. Adanya keamanan jaringan maka para pemakai berharap bahwa pesan yang dikirim dapat sampai dengan baik ke tempat yang dituju tanpa mengalami adanya keacatan yang diterima oleh si penerima, misalnya saja adanya perubahan pesan. Biasanya jaringan yang aksesnya semakin mudah, maka keamanan jaringanya semakin rawan, namun apabila keamanan jaringan semakin baik maka pengaksesan jaringan juga semakin tidak nyaman”.

Firewall merupakan suatu cara/sistem/mekanisme yang diterapkan baik terhadap *hardware* dan *software* ataupun sistem itu sendiri, dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi, dengan jaringan luar yang bukan merupakan sebuah *workstation, server, router,* atau *Local Area Network* (LAN) Anda. “[9]*Firewall*adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang tidak aman. Umumnya sebuah jaringan lokal dan jaringan lainnya.*Firewall* umumnya juga digunakan untuk mengontrol dan mengakses terhadap jaringan pribadi dari pihak luar parameter proteksi”. Sedangkan, [10] *Monowall* merupakan *embedded firewall* berbasiskan *free BSD* yang ringan dan mudah penggunaannya. *Monowall* adalah proyek yang ditujukan untuk menciptakan *firewall*, lengkap paket perangkat lunak, bila digunakan bersama dengan PC, menyediakan semua fitur penting dari kotak *firewall* komersial (termasuk kemudahan penggunaan) di sebagian kecil dari harga (*software* gratis). *Monowall* didasarkan pada

versi awal dari *Free* BSD, bersama dengan *web server*". *M0n0wall* adalah sebuah *embedded firewall software* bebasiskan Sistem *Operasi Free* BSD. File. Berbeda dengan *Linux liveCD router*, *m0n0wall* memiliki tampilan antar muka yang lebih baik dengan menggunakan *web* GUI (*Graphical User Interface*) sehingga bagi beberapa orang yang menginginkan kemudahan, *m0n0wall* adalah jawabannya karena pada *m0n0wall* seluruh konfigurasi berbasiskan *web* sehingga jauh lebih lebih menarik dan mudah jika dibandingkan dengan *Linux live CD router*.Sebelum melakukan konfigurasi pengguna lebih baik terlebih dahulu melihat dan mencatat konfigurasi alamat IP yang diberikan oleh pihak ISP (*Internet Service Provider*), *subnet mask*, DNS *server*, DHCP *server*, *Gateway*, dengan cara mengetikkan *ipconfig*/all atau *ifconfig* (*Linux*). Ini dimaksudkan supaya pada saat hendak melakukan konfigurasi *router*, tidak ada kesalahan dalam melakukan konfigurasi.

2. METODOLOGI PENELITIAN

2.1. Langkah Penelitian

Pada penelitian ini dilakukan 2 uji coba yaitu menggunakan firewall dan monowal. Langkah yang dilakukan untuk menguji firewall adalah

1) Menentukan Topologi Jaringan Firewall
   Topologi jaringan yang digunakan yaitu topologi jaringan tersebut menggunakan perangkat *Router Cisco* 1841, dalam penelitian ini adalah komputer core i3 dengan sistem operasi *windows* 10, pada laboratorium *cisco* memiliki 24 PC (Personal Computer) *client*, yang terhubung melalui peralatan *switch* dan menggunakan *router cisco.*

Tabel 1. IP *Address* LAN Pada Lboratorium *Cisco*

No	Nama	*IP Address*	*Subnetwork*
1	Internet Modem	192.168.100.1/24	255.255.255.0
2	Router 1841	192.168.10.1/24	255.255.255.0
3	Server	192.168.10.1/24	255.255.255.0
4	PC1 – PC24	192.168.10.3/24 s/d192.168.10.26/24	255.255.255.0

2) Melakukan simulasi pada topologi jaringan *Router Cisco* 1841 dan menjalankanya selama 60 menit.Langkah yang dilakukan untuk menguji monowall adalah :
   a) Konfigurasi *Operating System*
   b) Untuk mengkonfigurasi *mikrotik* pada awal pemakaian di PC *router*, digunakan terminal login CLI (*command line interface*). Kemudian set nama *interface ethernet* dan alamat IP *Mikrotik*.
   c) Melakukan pendefinisian dan menentukan kartu jaringan untuk dijadikan *interface*.
   d) Konfigurasi NAT *Firewall Mikrotik*
   e) *Network Address Translation* atau yang lebih biasa disebut dengan NAT adalah salah satu fasilitas router untuk meneruskan paket dari IP asal ke IP tujuan.
   f) Konfigurasi IP *Address*
   g) *M0n0wall* sangat sederhana, untuk menggunakan konfigurasi. Masukkan alamat IP *m0n0wall* ke dalam kotak Alamat pada *webbrowsers m0nowall* yaitu 192.168.2.1 dan akan diminta untuk user dan *Password*.

2.2. Metode Pengumpulan Data

Metode Pengumpulan Data yaitu Data Primeryang dikumpulkan secara langsung dari objek yang diteliti. Adapun cara yang digunakan untuk mengumpulkan data primer adalah dengan melakukan percobaan dengan uji coba. Pada metode ini, peneliti mengamati secara langsung permasalahan, serta melakukan penelitian mandiri guna mendapatkan informasi yang dibutuhkan dan Data SekunderYaitu suatu data yang diperoleh melalui daftar pustaka, buku-buku, dan literatur-literatur yang berhubungan dengan masalah yang sedang peneliti buat, dan diambil dalam bentuk yang sudah jadi, serta data yang peneliti dapatkan dari pengetahuan teoritis, dan melalui materi perkuliahan.

2.3. Alat dan Bahan

Kebutuhan alat dan bahan komponen yang terdapat pada sistem ini meliputi kebutuhan *hardware* dan *software*, yang akan digunakan untuk saling mendukung satu sama lainnya.

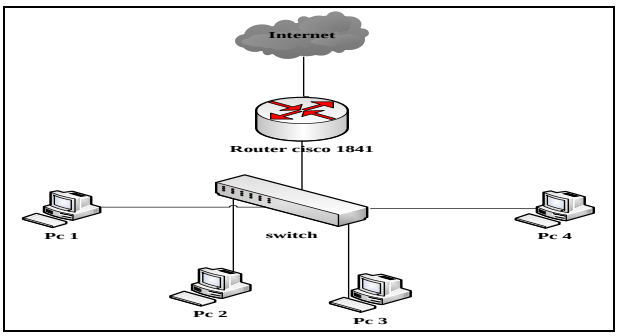
1) Kebutuhan *Hardware*
   1. *Router* 1841
   2. PC Komputer
   3. Laptop E5-471-36 WV
   4. *Memory* 4GB DDR3L
   5. *Harddisk* 500GB
   6. *Keyboard* dan *mouse*
   7. Kabel *cross*
   8. Kabel *strac*
   9. *Printer*
2) Kebutuhan *Software*
   1. *Wireshark*
   2. *Firewall*
   3. *System Operasi Windows 7, 32 bit*
   4. *System Operasi Windows 10,64 bit*
   5. *Microsoft Office Word 2007*
   6. *Monowall*
   7. *OS Free BSD*

2.4 Data Penelitian

Data yang digunakan pada penelitian ini adalah data hasil 10 uji coba untuk firewall dan 10 kali uji coba untuk monowall. Data diperoleh melalui metode eksperimen yaitu penelitian yang dilakukan dengan mengadakan manipulasi terhadap objek penelitian serta adanya kontrol.

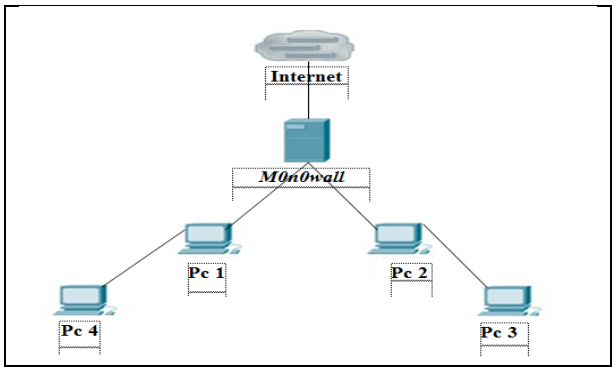
3. HASIL DAN PEMBAHASAN

Topologi jaringan yang digunakan yaitu topologi jaringan tersebut menggunakan perangkat Router Cisco 1841, dalam penelitian ini adalah komputer core i3 dengan sistem operasi windows 10, pada laboratorium cisco memiliki 24 PC (Personal Computer) client, yang terhubung melalui peralatan switch dan menggunakan router cisco.



Gambar 1. Topologi jaringanMenggunakan *Router Cisco 1841*

3.2. Topologi M0n0wall



Gambar 2 Topologi M0n0wall

.

PC router diinstall melalui CD instalasi m0n0wall melalui booting CD-ROM, ukuran filenya hanya sekitar 15 MB. Kemudian m0n0wall akan memulai memformat seluruh isi harddisk dan memulai instalasi. Setelah instalasi selesai, sistem akan melakukan reboot, dan PC router dengan sistem operasi mikrotik siap digunakan

3.3. Hasil Uji Coba

Hasil uji coba serangan DDoS menggunakan sistem keamanan *Firewall* pada *router CISCO* 1841 dengan 10 kali percobaan mendapatkan hasil 6 kali percobaan gagal masuk dan 4 kali percobaan berhasil masuk menggunakan system keamanan *Firewall*.

Tabel 2. Uji Coba Firewall

Uji Coba	Proses Berhasil	Proses Gagal	Keterangan
1	√		Masih ada celah di *Firewall* yang menyebabkan masih bias masuk kejaringan.
2	√		Terbentuknya *Port* di IP menyebabkan penyerang bias masuk ke jaringan.
3	√		Koneksi secara simultan dalam jumlah yang banyak akan membebani resource memori
4	√		pemrosesan data dimana data yang pertama masuk akan terlebih dahulu di proses sampai selesai kecuali request tersebut mengalami keadaan time out dimana request tidak dapat dilayani sampai waktu yang ditentukan
5		√	Adanya *router* yang mengatur seluruh jaringan
6		√	Adanya pembagian *bandwith* upload dan *Download* yang teratur dan menggunakan *transparent proxy mikrotik*.
7		√	Menggunakan *firewall* dan *security router* yang handal.
8		√	Gagal masuk karena dinding penghambat yang tidak mengizinkan pengguna yang tidak punya hak mengakses jaringan.
9		√	Gagal Masuk karena kejadian-kejadian yang berhubungan dengan sistem keamanan
10		√	Gagal masuk merekam/mencatat *event-event* mencurigakan, serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan *security*.

Tabel 3. Hasil Uji *M0n0wall*

Uji Coba	Proses Berhasil	Proses Gagal	Keterangan
1	√		Karena sistem keamanan yang tinggi membuat youtube tidak bias di blok
2	√		Karena sistem keamanan yang tinggi membuat Facebook tidak bias di blok
3		√	Karena sistem keamanan yang lemah membuat blog mudah untuk di blok
4	√		Tidak adanya pengaturan jaringan keseluruhan
5	√		Tidak dapat membagi *bandwith* yang teratur.
6		√	Menggunakan *firewall* dan security *router* yang handal.
7	√		M0n0wall adalah sistem operasi yang dirancang untuk menjadi router.
8	√		Karena Sistem Monowall Update firewall dengan manual
9	√		Karena pengaturan m0n0wall lebih rumit
10	√		Tidak dapat membagi *bandwith* yang teratur.

Firewall bekerja dengan cara menganalisis paket data yang keluar dan masuk ke dalam lingkungan yang dilindungi oleh sistem *firewall*. Paket data yang mengandung kejanggalan akan ditolak untuk masuk ataupun keluar jaringan komputer yang dilindungi.

4. KESIMPULAN

Berdasarkan data yang diperoleh dari hasil pengujian sistem keamanan jaringan awal, *firewall* dapat melindungi data yang diberikan ke pihak lain untuk keperluan tertentu sering diketahui oleh pihak lain dimulai dari proses serangan dan pendeteksian serta penanganan serangan. Tampilan dari data yang dianalisis, kondisi sebelum dan sesudah penyerangan. Setelah melakukan berbagai proses dalam penerapan *firewall*, terdapat kemudahan dalam penerapannya. Dari hasil proses pengujian yang telah dilakukan adalah kondisi berjalan dengan baik pada saat sebelum terjadi penyerangan, kemudian terjadi gangguan saat serangan dilakukan, yang membuat pendeteksian menampilkan informasi dan rincian data dari penyerang, kemudian berhasil dilakukan penanganan dengan kondisi yang diperlukan sehingga semua serangan berhasil diblokir dengan baik. Untuk mengetahui seberapa aman tingkat keamanan yang telah diterapkan dalam sebuah jaringan *wireless*/nirkabel maupun kabel.Seperti yang diketahui tingkat keamanan bukan hanya berasal dari *hardware* dan *software* yang sudah ada namun peran penting dari pengguna yang melakukan konfigurasi dan dari perancangan jaringan itu sendiri.

DAFTAR PUSTAKA

[1] Realize and H. Uni, “PENGARUH PENGGUNAAN IPTABLES FIREWALL DAN ACID Jurnal EdikInformatika,” *J. EdikInformatika*, vol. 3, no. 2, pp. 157–164, 2017.

[2] Munawar, “PERANCANGAN ALGORITMA SISTEM KEAMANAN DATA MENFI GGUNAKAN METODE KRIPTOGRAFI ASIMETRIS,” *J. Komput. dan Inform.*, vol. 1, no. 1, pp. 11–17, 2012.

[3] Sugiyono, “Sistem keamanan jaringan komputer menggunakan metode watchguard firebox pada pt guna karya indonesia,” *J. CKI*, vol. 9, no. 1, pp. 1–8, 2016.

[4] J. Y. Babys, Kusrini, and Sudarmawan, “Analisis Aspek Keamanan Informasi Jaringan Komputer (Studi Kasus : STIMIK Kupang),” *Semin. Nas. Inform. 2013*, vol. 7, no. semnasIF, pp. 7–14, 2013.

[5] A. Hikmaturokhman, A. Purwanto, and R. Munadi, “Analisis Perancangan Dan Implementasi Firewall Dan Traffic Filtering Menggunakan Cisco Router,” *Semin. Nas. Inform.*, vol. 1, no. 3, pp. 1–8, 2010.

[6] H. Februariyanti, “Internert Murah dengan Membangun Jaringan RT-RW Net,” *J. Teknol. Inf. Din.*, vol. 13, no. 2, pp. 98–114, 2008.

[7] S. R. I. Mardiyati, “Mengoptimalkan Suatu Sistem Firewall Pada,” vol. 7, no. 1, pp. 72–83, 2014.

[8] M. U. S. Saleh Opim Salim; Sinaga, Hendra H, “Implementasi dan Perbandingan Firewall Security Menggunakan Mikrotik dan M0n0wall Pada Local Area Network,” *Alkhawarizmi*, no. Vol 1, No 1 (2012): Jurnal Alkhawarizimi, pp. 1–8, 2012.

[9] Dista Amalia Arifah, “KASUS CYBERCRIME DI INDONESIA Indonesia’s Cybercrime Case,” *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.

[10] S. Rheno Widianto and I. Abdullah Azzam, “Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server,” *Elektra*, vol. 3, no. 2, pp. 19–28, 2018.