IMPLEMENTASI FILTERING FIREWALL UNTUK MENCEGAH SERANGAN HTTP DOS

(Studi Kasus: Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango)

Oleh :

MOH. RIZKI KAUNANG
T3117034

SKRIPSI

Untuk Memenuhi Salah Satu Syarat Ujian

Guna Memperoleh Gelar Sarjana

PROGRAM SARJANA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS ICHSAN GORONTALO
GORONTALO

2023

PENGESAHAN SKRIPSI

IMPLEMENTASI FILTERING FIREWALL UNTUK MENCEGAH SERANGAN HTTP DOS

(Studi Kasus: Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango)

Oleh :

MOH. RIZKI KAUNANG

T3117034

SKRIPSI

Untuk memenuhi salah satu syarat ujian Guna memperoleh gelar Sarjana dan telah disetujui oleh pembimbing pada bulan

Gorontalo, Mei 2023

Pembimbing Utama	Pembimbing Pendamping
Abd. Rahmat Karim Haba, M.Kom	**Sunarto Taliki, M.Kom**
NIDN. 0923118703	**NIDN. 0906058301**

PERSETUJUAN SKRIPSI

IMPLEMENTASI FILTERING FIREWALL UNTUK MENCEGAH SERANGAN HTTP DOS

(Studi Kasus: Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango)

Oleh :

MOH. RIZKI KAUNANG
T3117034

Diperiksa oleh Panitia Ujian Strata Satu (S1)
Universitas Ichsan Gorontalo
Gorontalo, Mei 2023

1. Ketua Penguji
   Rofiq Harun, M. Kom ……

2. Anggota
   Sudirman Melangi, M.Kom ……

3. Anggota
   Warid Yunus, M. Kom ……..

4. Anggota
   Abd. Rahmat Karim Haba, M.Kom ……..

5. Anggota
   Sunarto Taliki, M. Kom ……..

Mengetahui :

Dekan Fakultas Ilmu Komputer

Irvan A. Salihi, M.Kom
NIDN. 0928028101

Ketua Program Studi

Sudirman S. Panna, M.Kom
NIDN. 0924038205

PERNYATAAN SKRIPSI

Dengan ini saya menyetakan bahwa :

1. Karya tulis (Skripsi) saya ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Sarjana) baik di Universitas Ichsan Gorontalo maupun di perguruan tinggi lainnya.
2. Karya tulis (Skripsi) saya ini adalah murni gagasan, Rumusan, dan penelitian saya sendiri,tanpa bantuan pihak lain, kecuali arahan dari tim Pembimbing.
3. Dalam karya tulis (Skripsi) saya ini tidak terdapat karya atau pendapat yang telah di publikasikan orang lain, kecuali secara tertulis di cantumkan sebagai acuan/sitasi dalam naskah dan dicantumkan pula dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma-norma yang berlaku di Universitas Ichsan Gorontalo.

Gorontalo, Mei 2023

Yang membuat Pernyataan,

MOH. RIZKI KAUNANG

ABSTRAK

MOH. RIZKI KAUNANG. T3117034. IMPLEMENTASI FILTERING FIREWALL UNTUK MENCEGAH SERANGAN HTTP DOS

Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango sering terjadi masalah dalam lambatnya mengakses pada layanan internet serta penggunaan internet. Masalah ini diakibatkan oleh adanya waktu luang setelah kegiatan maupun saat kegiatan sering kali dimanfaatkan pegawai untuk melakukan browsing situs, membuka situs pemutar audio maupun video serta membuka situs media sosial untuk mengisi waktu luang. Dalam pencegahan terjadinya serangan DoS maka dilakukan pengamanan yang seharusnya pada router mikrotik, salah satu penerapanmikrotik dalam pengamanan jaringan yaitu bagaimana melakukan filtering firewall agar pegawai Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolangotidak dapat mengakses situs tertentu. Dari hasil analisis kinerja yang diperoleh padapenerapan filtering protocol yang di terapkan di firewall router mikrotik, Untuk serangan http dos pada Protocol TCP masih sulit dikenali trafic data yang masuk, dikarenakan protocol tcp digunakan bersamaan dengan akses browsing dan download oleh client. Sedangkan untuk protocol UDP dan ICMP Trafic lebih mudah dikenali sehingga rule filtering yang diterapkan pada firewall otomatis melakukan drop pada paket ddos tersebut.

Kata kunci: *Filtering Firewall*, serangan HTTP DOS

ABSTRAK

Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango sering terjadi masalah dalam lambatnya mengakses pada layanan internet serta penggunaan internet. Masalah ini diakibatkan oleh adanya waktu luang setelah kegiatan maupun saat kegiatan sering kali dimanfaatkan pegawai untuk melakukan browsing situs, membuka situs pemutar audio maupun video serta membuka situs media sosial untuk mengisi waktu luang. Dalam pencegahan terjadinya serangan DoS maka dilakukan pengamanan yang seharusnya pada router mikrotik, salah satu penerapan mikrotik dalam pengamanan jaringan yaitu bagaimana melakukan filtering firewall agar pegawai Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango tidak dapat mengakses situs tertentu.

Dari hasil analisis kinerja yang diperoleh pada penerapan filtering protocol yang di terapkan di firewall router mikrotik, Untuk serangan http dos pada Protocol TCP masih sulit dikenali trafic data yang masuk, dikarenakan protocol tcp digunakan bersamaan dengan akses browsing dan download oleh client. Sedangkan untuk protocol UDP dan ICMP Trafic lebih mudah dikenali sehingga rule filtering yang diterapkan pada firewall otomatis melakukan drop pada paket ddos tersebut.

Kata Kunci : Implementasi, *Filtering Firewall*, Serangan HTTP DOS

KATA PENGANTAR

Bismillahirrahmanirrahim

Puji Syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmat-Nya penulis dapat menyelesaikan skripsi ini dengan judul, "**Implementasi Filtering Firewall Untuk Mencegah Serangan HTTP DOS**". Untuk memenuhi salah satu syarat mendapat gelar sarjana Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo. skripsi ini dapat terlaksana dengan baik berkat dukungan dari banyak pihak, Oleh karena itu penulis menyampaikan terimakasih kepada:

1. Bapak Muhamad Ichsan Gaffar S.E M.AK, selaku Ketua Yayasan Pengembangan Ilmu Pengetahuan Dan Teknologi (YPIPT) Ichsan Gorontalo.
2. Bapak Dr. Abdul Gaffar La Tjokke, M.Si, selaku Rektor Universitas Ichsan Gorontalo.
3. Bapak Irvan Abraham Salihi, S.Kom., M.Kom, selaku Dekan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.
4. Bapak Sudirman Melangi, M.Kom, selaku Wakil Dekan I Bidang Akademik Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.
5. Ibu Irma Surya Kumala Idris, M.Kom, selaku Wakil Dekan II Bidang Administrasi Umum dan Keuangan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.
6. Bapak Sudirman S. Panna, M.Kom, selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.
7. Bapak *Abd*. *Rahmat* Karim *Haba*, M.Kom, sebagai Pembimbing Utama dalam penelitian ini yang telah membimbing penulis selama skripsi ini.
8. Bapak *Sunarto Taliki*, M.Kom, sebagai Pembimbing Pendamping dalam penelitian ini yang telah membimbing penulis selama menyusun skripsi ini.
9. Bapak dan Ibu Dosen yang telah mendidik dan membimbing dan mengajarkan berbagai disiplin ilmu kepada penulis.

10. Kepada bapak, Ibu, Kakak, Adik dan Keluaraga yang selalu memberikan dorongan moral maupun materil dari awal sampai akhir perkuliahan.
11. Teman-teman di jurusan Teknik Informatika dan semua pihak yang ikut membantu penulis dalam menyelesaikan Skripsi ini.

Walaupun demikian, penulis menyadari masih banyak kekurangan dalam penyusunan skripsi ini. Oleh karena itu, diharapkan saran dan kritik untuk penyempurnaan penulisan lebih lanjut. Semoga skripsi ini dapat bermanfaat bagi pihak yang berkepintingan terutama bagi penulis sendiri.

Gorontalo, Mei 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

PENDAHULUAN

1.1 Latar Belakang

Pada era Globalisasi sekarang ini, setiap orang harus bisa memanfaatkan dan menghemat teknologi pada bidang telekomunikasi, dan jaringan yang paliing dibutuhkan, karena dengan menggunakan jaringan bisa kita dapat memperoleh banyak manfaat, Banyak masyarakat, perusahaan dan instansi pemerintah yang menggunakan jaringan komputer yang biasa digunakan untuk memperluas dan melancarkan informasi serta meningkatkan kinerja pada perusahaan dan instasni tersebut. [1]

Penyediaan informasi dalam bentuk halaman web pada layanan saat ini sudah merupakan sebuah kebutuhan, karena akan mempermudah dan mempercepat penyebaran informasi. Namun dalam prosesnya ternyata ada saja masalah yang dialami baik itu berasal dari dalam misalnya koneksi maupun dari luar misalnya serangan terhadap layanan yang bersumber dari internet. Jenis serangan yang sering mematikan layanan adalah serangan DOS (Denial Of Service). Serangan DoS merupakan ancaman keamanan dimana penyerang menghabiskan sumber daya jaringan internet pada server, oleh sebab itu host target menolak akses dari pengguna yang berhak dimana layanan dari host menjadi tidak tersedia, maka dengan itu serangan mengganggu ketersediaan sistem. [2]

Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango merupakan salah satu dinas yang memiliki banyak pegawai negeri dan pegawai honorer, dalam keseharian pegawai Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango dalam menggunakan pelayanan kepada masyarakat menggunakan layanan web yang disediakan oleh pemerintah pusat dalam pelayanan berkas kependudukan sehingga membutuhkan layanan koneksi jaringan internet. Kebutuhan layanan jaringan internet pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango sudah berkerja sama dengan beberapa ISP Pememrintah dan swasta, bandwith yang di miliki di oleh oleh admin dalam sebuah konfigurasi mikrotik.

Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango sering terjadi masalah dalam lambatnya mengakses pada layanan internet serta penggunaan internet. Masalah ini diakibatkan oleh adanya waktu luang setelah kegiatan maupun saat kegiatan sering kali dimanfaatkan pegawai untuk melakukan browsing situs, membuka situs pemutar audio maupun video serta membuka situs media sosial untuk mengisi waktu luang. Tanpa disadari adanya kemungkinan sebuah serangan muncul yang dapat terjadinya kegagalan akses serta lambatnya internet, sehingga pekerjaan yang dilakukan oleh pegawai-pegawai mengalami terkendala yang mengakibatkan pelayanan kepada masyarakat terganggu. Pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango sistem keamanannya masih ada celah untuk masuknya sebuah serangan yang mungkin terjadi, untuk itu diperlukan adanya sistem keamanan yang dapat mengatasi masalah tersebut.

Berdasarkan masalah tersebut, Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango perlu melakukan firewall filter rule akses internet, serta melakukan pemblokiran situs. Melalui konfigurasi mikrotik dapat mengatasi masalah diatas. Mikrotik adalah sistem operasi yang berbasis perangkat lunak (software) dimana digunakan untuk membuat komputer sebagai router suatu jaringan. Router merupakan sebuah alat dimana bisa menyambungkan dua atau lebih jaringan komputer yang berbeda [3]. MikroTik RouterOS memiliki beberapa kelebihan dan mudah dalam konfigurasi pada operating system WinBox pada Windows. Sumber daya yang kecil juga menjadi sebuah kelebihan router tersebut. [4]

Dalam pencegahan terjadinya serangan DoS maka dilakukan pengamanan yang seharusnya pada router mikrotik, salah satu penerapan mikrotik dalam pengamanan jaringan yaitu bagaimana melakukan filtering firewall agar pegawai Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango tidak dapat mengakses situs tertentu serta hardening web server, selanjutnya pemanfaatan keamanan pada router mikrotik adalah implementasi fitur yang berada pada Firewall yang berfungsi sebagai filter rules dalam sebuah jaringan, Filter Rules tersebut dapat melakukan filtrasi penyaringan situs-situd yang digunakan.

Pengerasan sistem atau *system hardening* adalah proses mengamankan konfigurasi dan setelan *system* untuk mengurangi kerentanan IT dan kemungkinan disusupi (*crack*, *hack* dan lainnya). Teknik hardening bertujuan untuk menambah tingkat keamanan pada server dengan mengurangi tingkat kerawanan di dalamnya. Proses hardening diterapkan pada tiap fundamental server seperti firewall, ssh, dll. Prinsip itu juga yang digunakan untuk menerapkan hardening server yang berpengaruh terhadap keamanan server. [4]

Penelitian sebelumnya yang dilakukan oleh Rico Alfaris, 2020. Dengan judul Rancang Bangun Jaringan Lan Berbasis Mikrotik Router Pada Jurusan Teknik Komputer Politeknik Negeri Sriwijaya, Penelitian ini bertujuan untuk mengimplementasi Mikrotik router dan membangun sebuah jaringan baru dikarenakan Jurusan Teknik Komputer ingin membangun sebuah jaringan baru dan ruang server baru khusus di gedung Teknik Komputer. Disini Mikrotik router sebagai pengatur lalu lintas data dan jaringan lokal internet. Hasil pengujian menunjukkan bahwa penulis menggunakan IP Static dimana komputer client akan terhubung dengan internet. [5]

Berdasarkan latar belakang, maka penulis mengangkat judul **"Implementasi Filtering Firewall Untuk Mencegah Serangan HTTP DOS"**.

1.2 Identifikasi masalah

Berdasarkan uraian latar belakang masalah di atas, maka identifikasi masalahnya adalah Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango belum membangun sistem yang bias memblokir situs serta membangun system *internet* yang baik untuk *user*

1.3 Rumusan masalah

Berdasarkan identifikasi masalah diatas, maka permasalahannya dapat dirumuskan sebagai berikut:

1. Bagaimana Implementasi Filtering Firewall Untuk Mencegah Serangan HTTP DOS?
2. Bagaimana Kinerja dari Filtering Firewall dan Hardening Web server Untuk Mencegah Serangan HTTP DOS?

1.4 Tujuan Penelitian

Berdasarkan Rumusan permasalahan diatas, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui Implementasi Filtering Firewall Untuk Mencegah Serangan HTTP DOS.
2. Mengetahui Kinerja dari Filtering Firewall Untuk Mencegah Serangan HTTP DOS.

1.5 Manfaat Penelitian

Penelitian ini diharapkan mempunyai manfaat, yaitu

1. Secara Teoritis, Memberikan masukan bagi perkembangan ilmu pengetahuan dan teknologi, khususnya pada bidang ilmu computer, yaitu berupa pemuktahiran dalam pengolahan data.
2. Secara Praktis, Sumbangan pemikiran, karya, bahan pertimbangan agar dapat menghasilkan system yang berkualitas.

BAB II
LANDASAN TEORI

2.1. Tinjauan Studi

Berikut ini adalah penelitian terdahulu yang terkait dengan *Filtering Firewall*, yaitu :

Tabel 2. 1 Penelitian Terkait

No	Peneliti	Judul	Tahun	Hasil
1.	Rico Alfaris [5]	Rancang Bangun Jaringan Lan Berbasis Mikrotik Router Pada Jurusan Teknik Komputer Politeknik Negeri Sriwijaya	2020	Penelitian ini bertujuan untuk mengimplementasi Mikrotik router dan membangun sebuah jaringan baru dikarenakan Jurusan Teknik Komputer ingin membangun sebuah jaringan baru dan ruang server baru khusus di gedung Teknik Komputer. Disini Mikrotik router sebagai pengatur lalu lintas data dan jaringan lokal internet. Hasil pengujian menunjukkan bahwa penulis menggunakan IP Static dimana komputer client akan terhubung dengan internet.
2.	Riska, Hendri Alamsyah [6]	Penerapan Sistem Keamanan WEB Menggunakan Metode WEB Aplication Firewall	2020	Hasil penelitian ini menunjukkan bahwa firewall dengan menggunakan module dan rule modSecurity berbasis Web Aplication

				Firewall (WAF) pada sistem keamanan web dapat memblokir SQL Injection, Cross Site Scripting (XSS), dan Command Execution dengan menampilkan pesan error kepada user yang melakukan perintah tersebut
3.	Fitri Ramadhani H, Abdul Muzakkir Yahya Mt	Analisis Dan Implementasi Firewall Dengan Metode Port Address Translation Pada Mikrotik Os	2018	Pada tahap akhir pengembangan metode firewall, hal-hal apa yang telah dilakukan dan apa yang belum dilakukan pada pengembangan firewall ini akan diulas dan di evaluasi pada bagian akhir laporan ini.

2.2. Tinjauan Pustaka

2.2.1. Jaringan Komputer

Jaringan Komputer merupakan kumpulan dari beberapa komputer dengan terhubung pada perangkat jaringan lainnya yang saling bekerja sama untuk mencapai pertukaran informasi dan data melalui kabel atau tanpa kabel sehingga memungkinkan pengguna di jaringan komputer untuk saling bertukar dokumen atau data, serta bisa berbagi sumber daya seperti perangkat keras atau perangkat lunak yang terhubung ke jaringan. [7]

Jaringan Komputer mempunyai beberapa keunggulan dibandingkan dengan komputer yang berdiri sendiri (stand-alone) yaitu:

1. Jaringan memaksimalkan sumber daya manajemen yang lebih baik, seperti pengguna / user bisa saling berbagi layanan printer dengan kualitas tinggi, selain itu untuk penggunaan lisensi pada software jaringan lebih murah dari pada menggunakan lisensi tunggal dalam penggunaan jumlah yang sama.

2. Jaringan yang menggunakan internet membantu menjaga informasi agar tetap andal dan mutakhir, serta jika ada sistem penyimpanan terpusat yang dikelola dengan baik memungkinkan banyak pengguna yang bisa mengakses data dari banyak lokasi berbeda dan membatasi akses ke data saat sedang diproses.
3. Jaringan memudahkan dan mempercepat proses sharing data (berbagi file). Saat ini transfer data menggunakan jaringan dengan kecepatan tinggi lebih cepat dibanding dengan sarana tranfer data lainnya seperti menggunakan media flashdisk, disket, cd atau lainnya.
4. Jaringan membuat komunikasi antar kelompok dalam bekerja menjadi lebih efisien. Seperti pengiriman surat elektronik (email) merupakan kebutuhan dengan menggunakan sistem jaringan. Selain itu sebagian besar sistem jaringan digunakan untuk pemantauan proyek, meeting online, kerja group untuk membantu pekerja agar lebih produktif

Agar Sistem kerja jaringan komputer bisa mencapai tujuan, maka setiap bagian dari jaringan komputer akan melakukan permintaan (request) dan layanan (service). Adapun pihak yang melakukan permintaan disebut sebagai client dan pihak memberikan layanan disebut server. Pada jaringan komputer konsep ini disebut sebagai sistem Client-Server, dan digunakan pada hampir smua aplikasi jaringan komputer.

Berikut merupakan beberapa type jaringan berdasarkan skala areanya :.

1. PAN (Personal Area Network)

   PAN adalah jaringan komputer yang terdiri dari: Transmisi antara beberapa komputer atau antara komputer dan perangkat non-komputer seperti printer, mesin faks, telepon seluler, PDA, telepon seluler. Jangkauan PAN sangat terbatas, sekitar 9-10 meter. Semacam PAN dapat dibangun menggunakan teknologi kabel dan nirkabel Internet. Teknologi kawat PAN dapat terhubung melalui USB dan FireWire. Wireless PAN dapat dihubungkan melalui teknologi Bluetooth, WiFi dan inframerah.

2. LAN (Local Area Network)

   LAN adalah jaringan komputer yang hanya mencakup satu area kecil. seperti jaringan komputer kampus, gedung, kantor, rumah, sekolah atau

kurang. Saat ini, sebagian besar jaringan area lokal didasarkan pada Teknologi IEEE 802.3 Ethernet menggunakan perangkat switching yang Kecepatan transfer data adalah 10, 100 atau 1000 Mbps.

3. MAN (Metropolitan Area Network)

   MAN Merupakan Jaringan dengan skala jarak jangkau antar kota, dengan teknologi yang digunakan oleh MAN mirip dengan LAN. itu hanya daerah lebih besar dan lebih banyak komputer yang terhubung ke jaringan MAN dibandingkan dengan jaringan area lokal. MAN adalah jaringan komputer Mencakup area berukuran kota atau kombinasi dari beberapa LAN yang terhubung menjadi jaringan yang besar. Jaringan metro dapat digabungkan Jaringan komputer beberapa sekolah atau beberapa kampus. MAN bisa di Diimplementasikan pada jaringan kabel dan nirkabel.

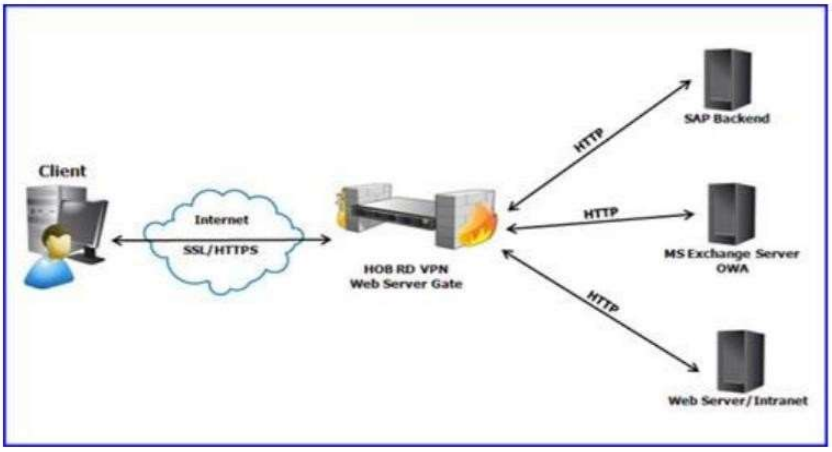
4. WAN (Wide Area Network)

   WAN adalah jaringan komputer yang mencakup area yang luas besar (lebar). Misalnya, jaringan komputer antar wilayah, kota atau kota bahkan sebuah negara, atau dapat didefinisikan sebagai jaringan komputer Diperlukan router dan saluran komunikasi umum. WAN digunakan untuk

   menghubungkan satu jaringan lokal ke jaringan lokal lainnya, sehingga pengguna atau komputer di lokasi yang sama dapat berkomunikasi dengan pengguna dan komputer di lokasi lain

2.2.2. Web Server

Definisi server web adalah program yang menyediakan layanan. Berdasarkan data dan fungsionalitas untuk menerima permintaan HTTP atau HTTPS di klien terkenal yang dikenal sebagai browser web (Mozilla Firefox dan Google Chrome) dan untuk mengirim hasil ke beberapa halaman web, umumnya sebagai dokumen HTML



Gambar 2. 1 Konsep Web Server

Fungsi utama server web adalah untuk mengeksekusi atau mentransfer file permintaan pengguna melalui protokol komunikasi yang ditentukan dengan cara ini. Halaman web yang diminta terdiri dari file teks, video, gambar, file, dan lainnya. Fungsi menggunakan server web untuk mentransfer semua aspek pendaftaran pada halaman web termasuk dalam bentuk teks, video, gambar, atau lebih

Prinsip server web adalah bahwa pengguna internet atau pengguna dapat dengan mudah membaca dari satu dokumen ke dokumen lain hanya dengan beberapa bagian dari beberapa halaman dokumen web. Proses yang mengklik dimulai dari klien web atau permintaan browser, akan diterima oleh server web, diproses, dan kemudian hasil proses oleh web kemudian dikembalikan server ke web lagi klien dan ini dilakukan dengan cepat dan transparan. Secara umum, server web hanya akan memproses semua permintaan yang diterimanya dari klien web.

2.2.3. Protokol OSI Layer

OSI (Open System Interonnections) adalah sistem terbuka yang merupakan seperangkat protokol yang memungkinkan koneksi dari dua sistem berbeda yang

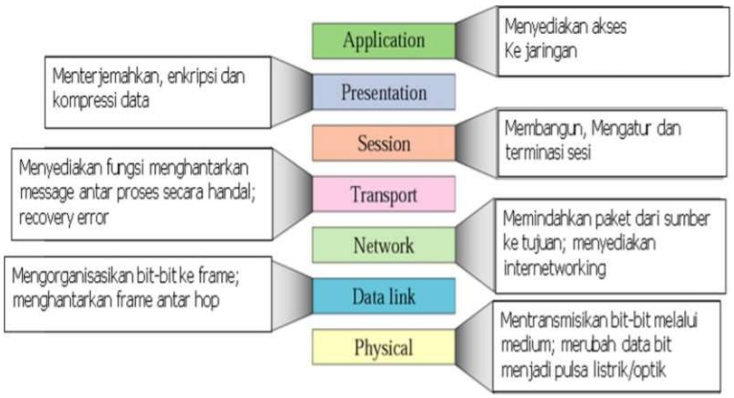
muncul dari struktur yang berbeda tetapi juga dapat diartikan sebagai seperangkat protokol yang membuat dua sistem komunikasi berbeda tanpa melihat desain sistem

di bawahnya. Dibuat oleh Organisasi Standar Internasional (ISO). OSI hanya model protokol, bukan protokol yang bisa digunakan.

Tujuan OSI adalah untuk memfasilitasi cara membangun koneksi darisistem yang berbeda tanpa perlu perubahan perangkat keras dan lunak di tingkat utama

Model OSI terdiri dari 7 layer: physical layer (Layer 1), data link layer (Layer 2), network layer (Layer 3), transport layer (Layer 4), session layer (Layer 5), width layer (Layer 6) dan lapisan aplikasi (Lapisan 7). Tiga lapisan pertama sering disebut sebagai "protokol tingkat atas", sedangkan empat lapisan terbawah disebut sebagai "protokol tingkat bawah". Setiap lapisan berdiri sendiri, tetapi fungsi setiap lapisan tergantung pada keberhasilan pemrosesan lapisan sebelumnya.

Layer yang mengirim hanya terikat pada layer penerima yang sama, seperti link layer atau data receive yang terkait pada layer link dengan data pengirim. Selain itu satu layer diatasnya atau dibawahnya memiliki lapisan layer yang terkait dengan transport layer pada lapisan atas atau bawah).



Gambar 2. 2 Ringkasan fungsi tiap layer pada osi layer

2.2.4. Keamanan Jaringan

Keamanan jaringan komputer adalah proses mencegah dan membatasi penggunaan jaringan komputer secara tidak sah. Langkah-langkah pencegahan membantu mencegah pengguna tidak sah yang disebut "peretas" mengakses bagian manapun dari sistem jaringan komputer. [8]

Tujuan dari keamanan jaringan komputer adalah untuk mengantisipasi risiko jaringan komputer dalam bentuk ancaman fisik dan logis, baik secara langsung maupun tidak langsung, yang mengganggu kegiatan yang sedang berlangsung di jaringan komputer.

Beberapa aspek keamanan dalam sebuah jaringan adalah sebagai berikut :

1. *Confidentiality*

Upaya untuk melindungi informasi dari orang yang tidak memiliki akses ke sana.

Privasi lebih mengarah pada data pribadi sementara kerahasiaan biasanya dikaitkan dengan data yang diberikan kepada pihak lain untuk tujuan tertentu (misalnya sebagai bagian dari pendaftaran layanan) dan hanya diizinkan untuk tujuan tertentu.

Contoh ancaman:
Email anggota tidak boleh dibaca oleh admin jaringan Data pelanggan sebuah ISP dijaga kerahasiaannya

· Solusi : Kriptografi (enkripsi dan dekripsi)

2. *Integrity*

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa izin dari pemilik informasi.

Contoh ancaman: Trojan, virus, dan seorang pria di tengah serangan mengubah konten email.

Solusi: enkripsi, tanda tangan digital

3. *Availabel*

Aspek available atau Ketersediaan berkaitan dengan ketersediaan informasi sesuai kebutuhan. Menyerang / mencabut sistem informasi dapat mengganggu / mencegah akses ke informasi.

Contoh hambatan: "penolakan serangan layanan" (serangan DoS), di mana permintaan dikirim ke server (biasanya palsu) yang mendesak atau permintaan tidak dapat diprediksi sehingga mereka tidak dapat membuat permintaan lain atau

bahkan downtime, downtime, atau downtime. Mailbomb, di mana pengguna

mengirim rentetan email (untuk mentransfer ribuan email) begitu besar sehingga pengguna tidak dapat membuka email mereka atau mengalami kesulitan mengakses email mereka.

· Solusi : Spam blocker, Connection limit.

4. *Non Repudiation*

Aspek ini mencegah seseorang untuk tidak dapat melakukan transaksi. Misalnya, orang yang mengirim email untuk meminta item tidak dapat menyangkal bahwa ia mengirim email. Aspek ini sangat penting dalam kasus e-commerce. Penggunaan tanda tangan digital dan teknologi enkripsi secara umum dapat melindungi aspek ini. Namun, undang-undang ini harus didukung agar mode tanda tangan digital menjadi jelas legal

5. Autentication

Aspek ini berkaitan dengan cara di mana informasi tersebut benar-benar diakui / bahwa orang yang mengakses / menyediakan informasi adalah orang yang dimaksud. Masalah pertama, yang membuktikan keaslian dokumen, dapat dilakukan dengan menggunakan teknologi tanda air dan tanda tangan digital. Tanda air juga dapat digunakan untuk memelihara "kekayaan intelektual", yaitu dengan menandai dokumen / karya dengan "tanda tangan" pabrikan. Masalah kedua biasanya berkaitan dengan kontrol akses, yang berkaitan dengan pembatasan siapa yang dapat mengakses informasi. Dalam hal ini, pengguna harus menunjukkan bukti bahwa ia sebenarnya adalah pengguna yang sah, misalnya dengan kata sandi, biometrik (properti orang), dan sejenisnya. Penggunaan teknologi kartu pintar sekarang tampaknya meningkatkan aspek keamanan ini.

6. Access control

Aspek ini berkaitan dengan bagaimana mengelola akses ke informasi. Ini biasanya terkait dengan masalah otentikasi dan privasi. Akses sering dikontrol

menggunakan kombinasi User ID / Password atau mekanisme lainnya

7. Accountability

Akuntabilitas berarti bahwa setiap aktivitas pengguna akan direkam di jaringan. Pengguna tidak akan berusaha melanggar kebijakan keamanan karena identitas dan aktivitas mereka dapat ditentukan sehingga mereka dapat dituntut sesuai. Akuntabilitas mencegah perilaku ilegal. Dalam sistem yang didasarkan pada akuntabilitas murni, tidak ada mekanisme kontrol akses yang diterapkan.

• Masalah dengan sistem akuntabilitas: Ini hanya berfungsi ketika identitas tidak dapat dipalsukan.

• Pengguna kehilangan kepercayaan diri. Tanpa kontrol akses, pengguna dapat menghancurkan seluruh sistem. Untuk alasan ini, sistem berbasis akuntabilitas biasanya dikombinasikan dengan sistem berbasis kontrol akses.

2.2.5. Jenis Serangan atau Ancaman Keamanan di Jaringan

1. DoS (Denial of Service)

Serangan Denial of Service (Serangan DoS) adalah jenis serangan pada komputer atau server di Internet yang menghabiskan semua sumber daya komputer, dan mencegah komputer menjalankan fungsinya dengan benar, dan memungkinkan pengguna lain untuk mengakses layanan tersbut akan terganggu. [9]

2. DDoS (Distributed Denial of Service)

DDoS adalah singkatan dari Distributed Denial of Service dan dalam bahasa Indonesia dapat diartikan sebagai Distributed Denial of Service. DDOS adalah jenis serangan yang dilakukan dengan membanjiri lalu lintas di Internet atau server [8]

3. UDP Flooding

UDP atau User Diagram Protocol adalah protokol jaringan tanpa sesi, yang membanjiri port server dari jarak jauh secara acak. Dengan demikian, server host harus melakukan pengecekat port ini dan melaporkan pengguna yang menggunakan paket ICMP agar Layanan pada host server lumpuh dan tidak bisa diakses. [9]

Jika sistem mengenali bahwa tidak ada aplikasi yang terkait dengan data, sistem akan mengirimkan paket "Destination Unreachable". Makan Semakin banyak paket UDP yang dikirim penyerang, semakin banyak paket yang dikirim sistem, membebani sistem dan menolak koneksi lain yang mencoba masuk atau keluar dari sistem.

4. SYN Flooding

Paket SYN adalah jenis paket protokol protokol kontrol transmisi yang dapat digunakan untuk membuat koneksi antara dua host dan dikirim oleh host yang ingin membuat koneksi sebagai langkah pertama dalam membangun koneksi pada "TCP three-way" Akan dilakukan. Handshake ". Proses. Dalam serangan banjir SYN, penyerang mengirimkan paket SYN ke port "pendengaran" host target. Biasanya, paket SYN yang dikirim berisi alamat sumber yang mewakili sistem yang sebenarnya, tetapi paket SYN untuk serangan ini dirancang untuk memiliki alamat sumber yang tidak mewakili sistem yang sebenarnya. [10]

5. ICMP Flood

ICMP Flood atau di kenal dengan Ping Flood Adalah Ping serangan DDOS yang membuat crash atau crash target. Ping flood dapat dikirim dalam jumlah yang sangat besar, dan target dapat gagal atau lumpuh. Sasaran dari ping flood biasanya adalah server hosting website yang dapat membuat website tidak dapat diakses, sehingga sangat merugikan, namun jika paket yang dikirim tidak sesuai dengan permintaan pelaku maka seramgan ping flood akan dihentikan [11]

6. IP Spoofing

Spoofing atau lebih sering dikenal dengan IP Spoofing merupakan suatu teknik atau cara yang digunakan untuk mendapatkan akses yang tidak berhak kepada komputer korban, dengan cara penyerang/penyusup mengirim pesan ke sebuah komputer dengan sebuah alamat IP yang menandakan pesan tersebut berasal dari host yang terpercaya. Dengan kata lain IP Spoofing adalah merubah/memodifikasi alamat sumber IP penyerang/penyusup pada IP Headers

menjadi sebuah alamat IP baru yang terpercaya. [12]

7. Sniffing

Packet Sniffing merupakan pencegatan data paket-paket yang mengalir pada jaringan. Dengan sebuah program Sniffer yang bekerja pada layer 2 serta kombinasi dari NIC yang berada pada mode promiscuous (mode mendengar) untuk men-capture semua traffic yang mengalir dari dan ke internet pada suatu jaringan. Dengan demikian, semua aktivitas yang dilakukan oleh komputer yang berada pada jaringan tersebut dapat diketahui. Sniffing merupakan ancaman keamanan yang bersifat pasif karena tidak melibatkan penyerangan secara langsung, hanya mendengarkan traffic yang ada di jaringan. [13]

8. Port Scanning

Port Scanning merupakan suatu usaha mengumpulkan informasi/ reconnaissance terhadap suatu komputer target (biasanya server), yang dimana informasi yang dicari berupa layanan-layanan apa saja yang disediakan, sistem operasi komputer target dan lain-lain. Sehingga dari informasi yang didapatkan, dapat menentukan langkah selanjutnya dalam melakukan penyerangan.

9. Hijacking

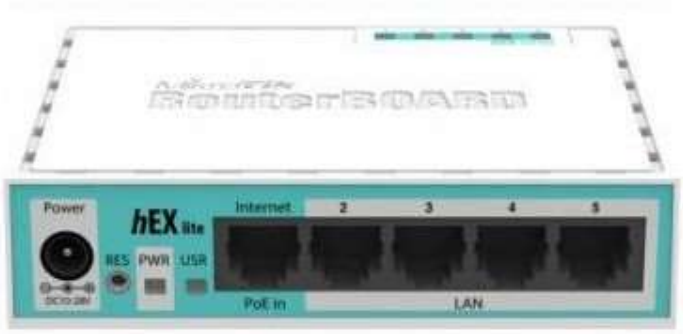
MITM merupakan sebuah teknik yang mengambil keuntungan dari kelemahan protocol stack TCP/IP, dan bagaimana cara header-header dibangun. MITM terjadi ketika ada seseorang diantara 2 titik yang dimana kedua titik itu saling berkomunikasi, tetapi seseorang tersebut secara aktif memonitor, mencapture, dan mengontrol komunikasi 2 titik tersebut secara transparan. Dan pada akhirnya kedua titik tersebut tidak sadar bahwa mereka tidak berkomunikasi satu sama lain, tetapi padahal berkomunikasi dengan seseorang tersebut.

10. Trojan

Trojan merupakan sebuah program berbahaya yang pada penampilannya hanya berupa sebuah software/paket biasa yang dimana software/paket tersebut berisi kode-kode berbahaya begitu diluncurkan dan masuk ke komputer korban. Kebanyakan program remote control spyware merupakan jenis ini.

2.3. Mikrotik

Mikrotik adalah perangkat router yang mengirimkan paket data melalui jaringan atau Internet ke tujuannya melalui proses yang disebut perutean. Router bertindak sebagai penghubung antara dua atau lebih jaringan, meneruskan data dari satu jaringan ke jaringan lain. Router Mikrotik adalah perangkat jaringan komputer yang menggunakan sistem operasi Mikrotik RouterOS dengan kernel Linux untuk router jaringan. Router mikrotik memiliki banyak utiliti seperti bandwidth management, firewall dengan access point untuk akses dan operasi, Winbox GUI administrator untuk remote dan routing.

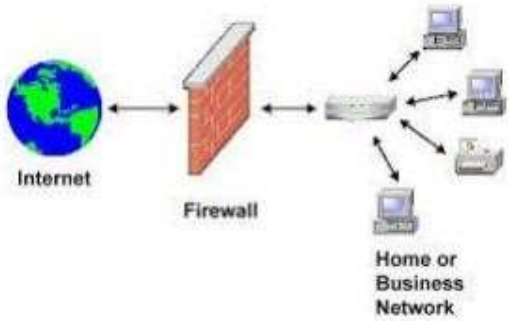


Gambar 2. 3 Router Mikrotik

2.4. Firewall

Firewall atau yang yang disebut tembok api merupakan sebuah sistem yang menjaga keamanan suatu jaringan dari pihak yang tidak bertanggung jawab yang berusaha merusak, mengubah, ataupun mendistribusikan data – data penting yang bersifat rahasia perusahaan atau mencegah seluruh ancaman yang masuk pada jaringan. Cara kerja firewall yaitu menggunakan *rule* khusus. Rule ini nantinya yang akan menentukan tindakan yang dilakukan oleh router terhadap Paket yang melintasi router. Pada setiap rule diatur dengan kondisi dan prosedur yang wajib diterapkan.

Pilihan strategi dan keterampilan administrator jaringan sebagian besar akan membedakan apakah jaringan mudah ditembus atau tidak. Firewall adalah alat untuk menerapkan kebijakan keamanan. Sedangkan kebijakan keamanan didasarkan pada keseimbangan antara fasilitas yang disediakan dan implikasi keamanan. Semakin ketat kebijakan keamanan, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan lebih banyak fasilitas yang tersedia atau dalam konfigurasi sederhana yang diterapkan, lebih mudah bagi orang usil dari luar untuk masuk ke sistem, karena akibat langsung dari kebijakan keamanan sistem yang lemah. Di dunia nyata, firewall adalah tembok yang bisa memisahkan ruangan, sehingga api di satu ruangan tidak menyebar ke ruangan lain. Tetapi kebenarannya adalah bahwa firewall internet lebih seperti pertahanan di sekitar benteng, bertahan terhadap serangan eksternal.



Gambar 2. 4 Konsep Firewal Pada Jaringan

Fungsi dari firewal yaitu Membatasi paket yang memasuki jaringan internal, Membatasi paket yang meninggalkan jaringan internal serta Mencegah penyerang mendekati sistem pertahanan

Firewall harus mengizinkan lalu lintas data keluar dan masuk dalam jaringan. Firewall dapat menjadi kombinasi yang tepat dari router, server, dan perangkat lunak pendamping. Firewall adalah suatu metode/sistem/mekanisme yang berlaku pada perangkat keras, perangkat lunak, atau sistem itu sendiri, melindungi beberapa atau semua hubungan/aktivitas segmen dalam jaringan

pribadi dengan jaringan eksternal, menyaring, membatasi, atau menyangkalnya. melakukan. Dalam jangkauan. Segmen dapat berupa workstation, server, router, atau jaringan area lokal (LAN).

2.4.1. Manfaat Firewall

Adapun Manfaat firewall pada jaringan komputer adalah sebagai berikut :

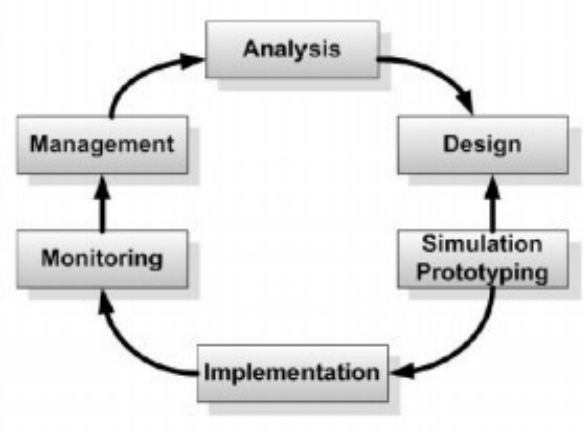
1. Perlindungan informasi sensitif dan berharga yang diabaikan. Misalnya, lalu lintas FTP (File Transfer Protocol) dari jaringan komputer dikendalikan oleh firewall. Ini dilakukan untuk mencegah pengguna di jaringan secara sengaja atau tidak sengaja mengirim file sensitif ke pengguna lain.
2. digunakan sebagai filter untuk mencegah lalu lintas tertentu mengalir ke subnet jarin/gan Anda. Ini mencegah pengguna berbagi file atau bermain game melalui jaringan..
3. Manfaat firewall lainnya adalah untuk memodifikasi paket data yang datang didi firewall. Proses ini disebut Network Address Translation (NAT).

Adapun cara kerja dari sistem keamanan firewall yaitu :

1. Mentutp port Kecuali untuk port tertentu yang harus tetap terbuka. Firewall komputer mencari port terbuka yang dapat diakses oleh peretas yang mencoba masuk ke jaringan komputer Anda, sehingga mereka bertindak sebagai pertahanan garis depan untuk mencegah segala macam peretasan ke jaringan Anda.
2. Firewall adalah perangkat keras atau perangkat lunak, tetapi firewall bekerja paling baik ketika kedua jenis perangkat ini digabungkan. Firewall tidak hanya membatasi akses ke jaringan komputer, tetapi juga memungkinkan akses jarak jauh ke jaringan pribadi melalui otentikasi dan sertifikat keamanan login.
3. Firewall merupaka perangkat keras dapat dibeli sebagai produk yang berdiri sendiri, tetapi biasanya ditemukan pada router broadband dan memerlukan pengaturan pada perangkat ini untuk mengakses jaringan komputer..
4. Cara kerja firewall lainnya adalah menyaring lalu lintas jaringan berdasarkan alamat IP, nomor port, dan protokol. Firewall dapat menyaring data dengan mengidentifikasi isi pesan itu sendiri.

2.5. Network Development Life Cycle (NDLC)

Network Development Life Cycle (NDLC) Sebuah model penting dari siklus hidup pengembangan jaringan (NDLC), proses desain jaringan komputer. NDLC sendiri merupakan siklus proses dari langkah-langkah mekanisme yang diperlukan untuk proses desain untuk mengembangkan atau mengembangkan sistem jaringan komputer.. [7]



Gambar 2. 5 Urutan Kerja NDLC

Berikut adalah urutan kerja dari metode Network Developement Life Cycle :

a. Analisis

Ini adalah langkah pertama dalam menganalisis yaitu kebutuhan yang dibutuhkan, masalah yang di hadapi, kebutuhan pengguna, dan topologi atau analisis jaringan yang ada.

b. Desain

Pada tahap ini dilakukan perancangan infrastruktur jaringan komputer dan semua lokasi di area produksi, gudang, dan ruang server yang menampung semua peralatan utama peralatan jaringan komputer telah terhubung. Pada fase ini dibuat gambar topologi untuk memperkirakan kebutuhan yang ada..

c. Simulasi

Pada tahap ini, simulator dipilih untuk digunakan. Ini adalah model elemen jaringan skala besar dengan berbagai fungsi jaringan yang ditentukan dalam konfigurasinya. Ada beberapa simulasi yang memang juga menggunakan cara

pengujian langsung..

d. Implementation

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi ini akan menerapkan semua yang telah direncanakan dan didesign sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya project yang akan dibangun dan ditahap inilah Team Work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis..

e. Monitoring

Setelah implementasi, fase pemantauan merupakan fase penting untuk memungkinkan komputer dan jaringan komunikasi berfungsi sesuai dengan kebutuhan dan tujuan desain awal.

f. Management

Pada tahap manajemen atau regulasi, salah satu perhatian khusus adalah masalah kebijakan. Kebijakan harus dibuat atau diatur oleh pihak-pihak terkait agar dapat menciptakan atau mengatur sistem yang dibangun dan dijalankan dengan baik oleh bisnis.

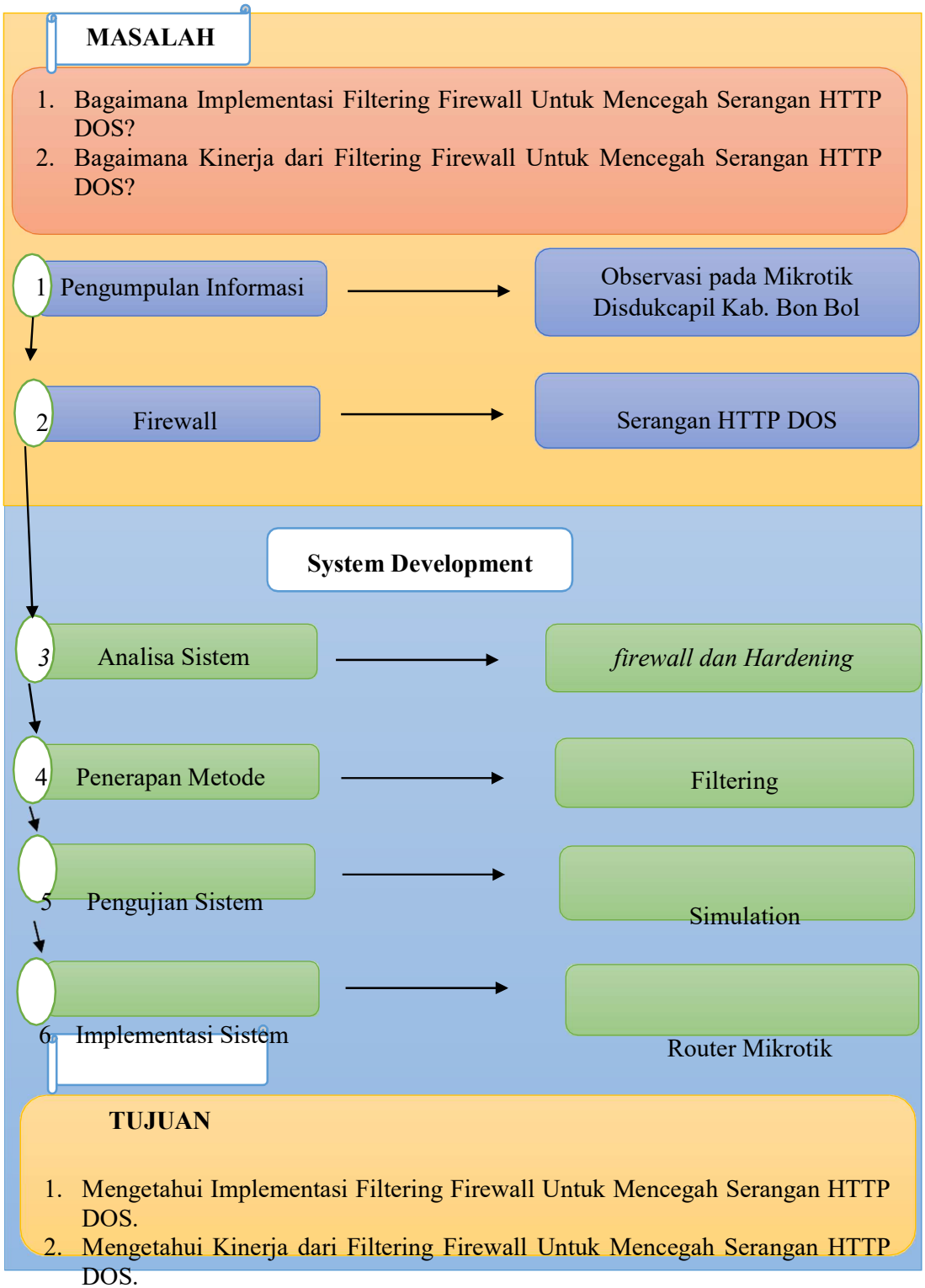
2.6. Pengujian Sistem

Pengujian sistem merupakan elemen penting dari jaminan kualitasperangkat lunak dan merupakan tinjauan komprehensif dari spesifikasi, desain, dan pengkodean. Tujuan dari tes ini adalah untuk menemukan berbagai potensi kesalahan dan konfigurasi jaringan komputer Anda dengan sedikit usaha dan waktu.

Pada Fase ini menguji sistem yang dibuat. Pengujian berfokus pada bagian dalam yang logis dan bagian luar yang fungsional dari perangkat lunak. Mengarahkan pengujian untuk menemukan bug dan memastikan bahwa input yang dibatasi menghasilkan hasil aktual yang sesuai dengan hasil yang diperlukan.

Pengujian operasional juga dilakukan selama fase ini, yang mengarah pada kematangan implementasi

2.7. Kerangka Pemikiran



Gambar 2. 6 Kerangka Pikir

BAB III
METODE PENELITIAN

1.1. Jenis, Metode, Subjek, Objek, Waktu, dan Lokasi Penelitian

Penelitian ini menggunakan metode penelitian studi kasus. Dengan demikian jenis penelitian ini adalah penelitian deskriptif.

Berdasarkan latar belakang dan kerangka pemikiran seperti yang telah diuraikan diatas maka yang menjadi objek penelitian adalah Penerapan Filtering Firewall Untuk Mencegah Serangan HTTP DOS. Penelitian ini dimulai dari 01 Agustus 2022 s/d Desember 2022 yang berlokasi di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango

1.2. Pengumpulan Data

1. Data primer

Data Primer Yaitu data yang diperoleh Dengan Metode Wawancara dengan staf admin dan Observasi Langsung Pada Router Mikrotik Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango.

2. Data Sekunder

Data Sekunder yaitu Data diperoleh dengan cara mengumpulkan data atau keterangan melalui berbagai macam referensi seperti hasil penelitian terdahulu, buku teks, jurnal yang terkait dari internet yang berhubungan dengan metode port knocking.

1.3. Pengembangan Sistem

Prosedur atau langkah-langkah pokok dalam menerapkan sistem keamanan menggunakan Filtering Firewall dan Hardening Web server, kemudian menggunakan sistem operasi kali linux dalam hal uji coba serangan HTTP DOS pada mikrotik dan dilakukan simulasi untuk menguji kinerja sistemnya.

1.4. Desain Sistem

Desain sistem menggunakan pendekatan topologi dalam hal menentukan rule pada firewall.
Architecture Design, dalam bentuk :

- Topologi Jaringan
- Spesifikasi *hardwere* dan *software* yang direkomendasikan adalah:

1. Sistem Operasi : Windows 10
2. Prosesor Dengan Kecepatan Minimal 1,6GHz

3. Memori :1 GB
4. Harddisk free space 3GB
5. RAM: 2 GB

1.5. Rancangan Sistem

Gambar 3.1. Rancangan Sistem

1.6. Konstruksi Sistem

Pada tahap ini dilakukan perancangan sistem keamanan menggunakan Filtering Firewall dan Hardening Web server di router mikrotik. Dan untuk menguji kinerja sistem menggunakan simulasi langsung dengan menyerang langsung pada router mikrotik. Pada tahap ini penulis melakukan tahap perancangan sistem dan desain sistem sebelumnya..

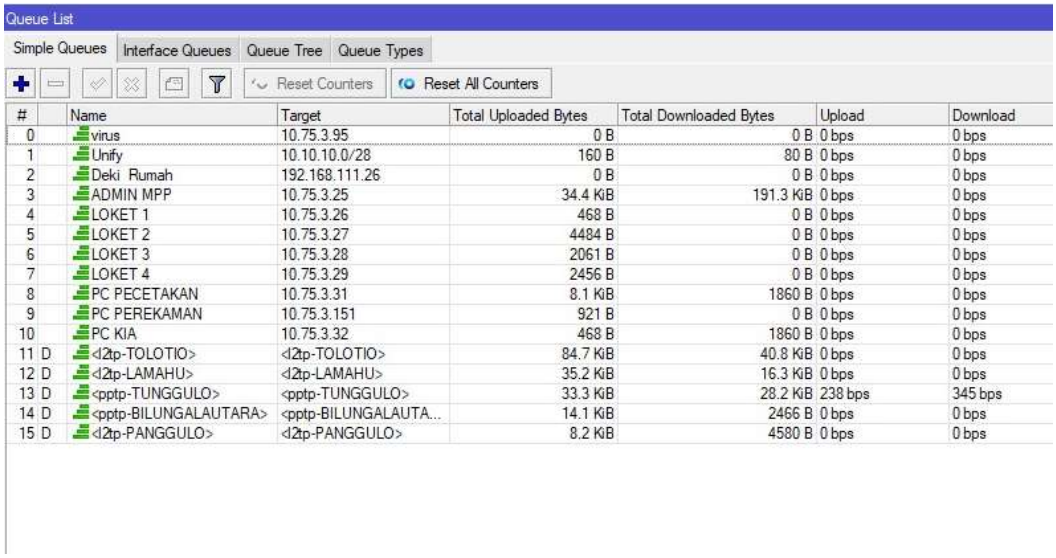
1.7. Pengujian Sistem

Pada pengujian ini penulis menggunakan konsep hacking yaitu melakukan simulasi beberapa jenis serangan HTTP DOS seperti Scanning dan exploit pada router mikrotik dengan bantuan tool hacking seperti UDP-Unicorn tools untuk mengetahui kinerja dan keberhasilan sistem keamanan Filtering Firewall Mikrotik

BAB IV
HASIL PENELITIAN

4. 1 Hasil Pengumpulan Data

Pada tahap ini dilakukan pengumpulan data yang akan digunakan dalam melakukan penelitian ini yaitu adapun terdapat beberapa data penggunaan bandwith harian pada dinas kependudukan dan catatan sipil, dari hasil monitoring pada manajemen bandwith mikrotik pada tabel dibawah ini :



#		Name	Target	Total Uploaded Bytes	Total Downloaded Bytes	Upload	Download
0		virus	10.75.3.95	0 B	0 B	0 bps	0 bps
1		Unify	10.10.10.0/28	160 B	80 B	0 bps	0 bps
2		Deki Rumah	192.168.111.26	0 B	0 B	0 bps	0 bps
3		ADMIN MPP	10.75.3.25	34.4 KiB	191.3 KiB	0 bps	0 bps
4		LOKET 1	10.75.3.26	468 B	0 B	0 bps	0 bps
5		LOKET 2	10.75.3.27	4484 B	0 B	0 bps	0 bps
6		LOKET 3	10.75.3.28	2061 B	0 B	0 bps	0 bps
7		LOKET 4	10.75.3.29	2456 B	0 B	0 bps	0 bps
8		PC PECETAKAN	10.75.3.31	8.1 KiB	1860 B	0 bps	0 bps
9		PC PEREKAMAN	10.75.3.151	921 B	0 B	0 bps	0 bps
10		PC KIA	10.75.3.32	468 B	1860 B	0 bps	0 bps
11	D	<l2tp-TOLOTIO>	<l2tp-TOLOTIO>	84.7 KiB	40.8 KiB	0 bps	0 bps
12	D	<l2tp-LAMAHU>	<l2tp-LAMAHU>	35.2 KiB	16.3 KiB	0 bps	0 bps
13	D	<pptp-TUNGGULO>	<pptp-TUNGGULO>	33.3 KiB	28.2 KiB	238 bps	345 bps
14	D	<pptp-BILUNGALAUTARA>	<pptp-BILUNGALAUTA...	14.1 KiB	2466 B	0 bps	0 bps
15	D	<l2tp-PANGGULO>	<l2tp-PANGGULO>	8.2 KiB	4580 B	0 bps	0 bps

Gambar 4. 1 Penggunaan Bandwitdh

4. 2 Analisa dan Perancangan Sistem

4.2.1 Analisa Kebutuhan Sistem

Pada tahap ini sebelum dilakukan konfigurasi dan implementasi filtering firewall untuk pencegahan serangan ddos dengan protocol http, udp dan icmp penulis lebih dulu melakukan analisa terhadap kebutuhan perangkat keras (hardware) dan perangkat lunak (software) yang digunakan dalam uji coba serangan pada penelitian ini :

Tabel 4. 1 Kebutuhan Hardware dan Software

Hardware	Keterangan	Software	Keterangan
Laptop	Acer	Port Scanner	V.2.5
Router Mikrotik	RB 951	Unicorn DDOS	V.3.7

4.2.2 Analisa Serangan HTTP DOS

Berdasarkan tools exploit yang penulis dapatkan dan digunakan pada penelitian ini, ada beberapa fitur yang bisa digunakan seperti bypass dengan ip router, bypass dengan mac router jika ip router tidak ditemukan dan fitur mac discover yang berfungsi untuk mencari MAC address yang terhubung.

Serangan HTTP DoS (Denial of Service) adalah jenis serangan di mana serangan mencoba membanjiri

situs web / ataupun server dengan permintaan HTTP palsu untuk mengganggu akses pengguna yang sah. Serangan ini bertujuan untuk membuat situs web menjadi tidak responsif atau bahkan menonaktifkan server dengan membanjiri server dengan lalu lintas yang sangat tinggi.

Saat terjadi serangan HTTP DoS, pada mikrotik akan terlihat peningkatan lalu lintas yang tidak biasanya sperti terjadi penumpukan request traffic dan kenaikan resource dari mikrotik. Jika jumlah permintaan yang diterima oleh mikrotik secara tiba-tiba meningkat secara signifikan dalam waktu yang singkat, maka ini dapat menjadi tanda adanya serangan.

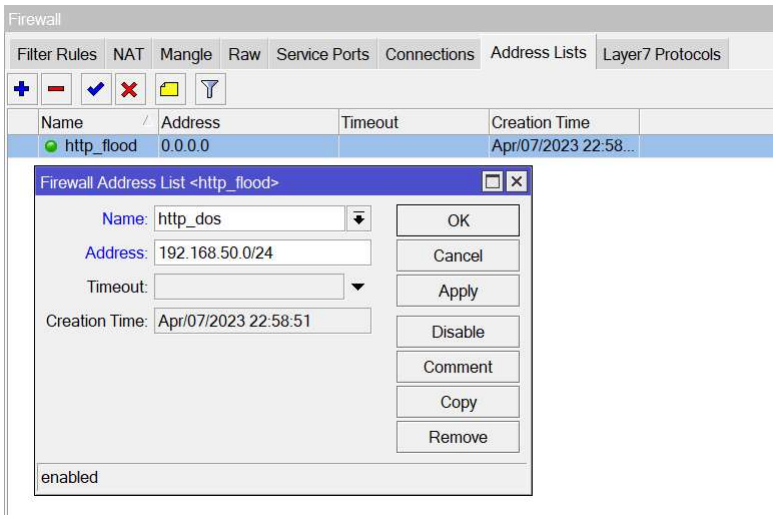
4.2.3 Analisa Perancangan Sistem

Perancangan sistem keamanan serangan DOS harus dilakukan secara mendalam, dengan melakukan analisa dan identifikasi jenis serangan DDoS yang sering terjadi dan berpotensi mengancam jaringan, menentukan kebijakan akses jaringan, termasuk pembatasan akses dan jenis protokol yang di izinkan, serta menentukan jumlah koneksi atau paket yang dapat di tangani oleh server.

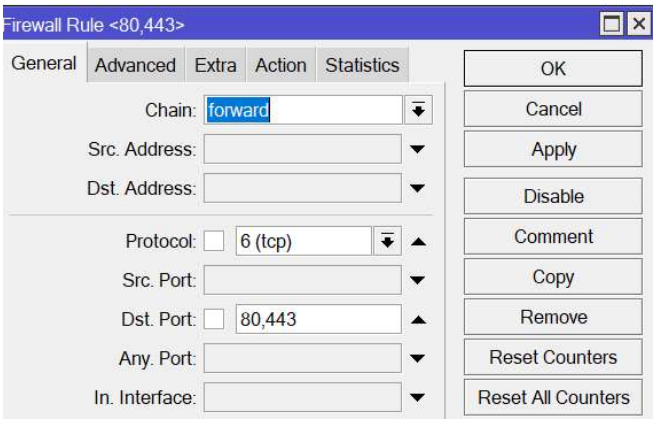
4.2.4 Perancangan Sistem Keamanan Serangan HTTP DOS

untuk melakukan perancangan sistem keamanan HTTP DOS dengan Firewall Filtering, diperlukan pembuatan address list untuk menandai ip local yang di ijinkan pada mikrotik. Yang bisa dilihat pada gambar dibawah.

Langkah selanjutnya adalah menambahkan alamat IP baru ke dalam daftar alamat http_dos yang telah

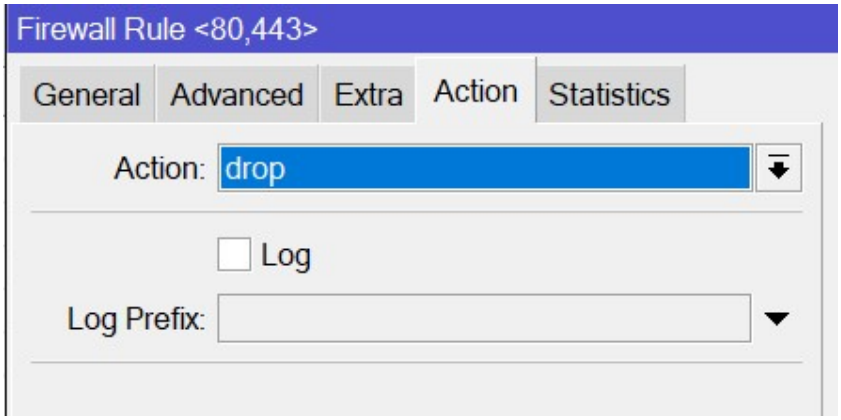


dibuat sebelumnya dengan pengaturan jumlah koneksi dari alamat IP tersebut melebihi batas tertentu dalam waktu yang ditentukan. Dalam contoh ini, jumlah koneksi maksimum adalah 50 per 32 detik dan setelah 1 jam alamat IP akan dihapus dari daftar alamat http_flood.



Gambar 4. 3 Konfigurasi Port

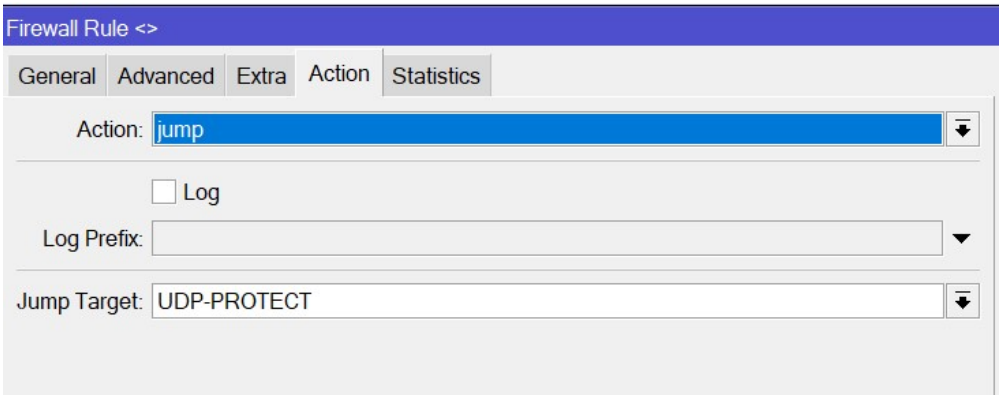
Selanjutnya melakukan konfigurasi untuk menolak semua paket jika terjadi serangan HTTP DOS dari alamat IP yang ada di dalam daftar alamat http_dos.



Gambar 4. 4 Konfigurasi Drop Action

4.2.5 Perancangan Sistem Keamanan Serangan UDP Flood

Pada tahap perancangan sistem keamanan serangan UDP Flood ada 2 langkah yang dilakukan yaitu : membuat request protocol udp yang masuk dengan parameter jump-target yang bertujuan untuk menentukan pembacaan rule agar lebih efisien seperti pada gambar dibawah :



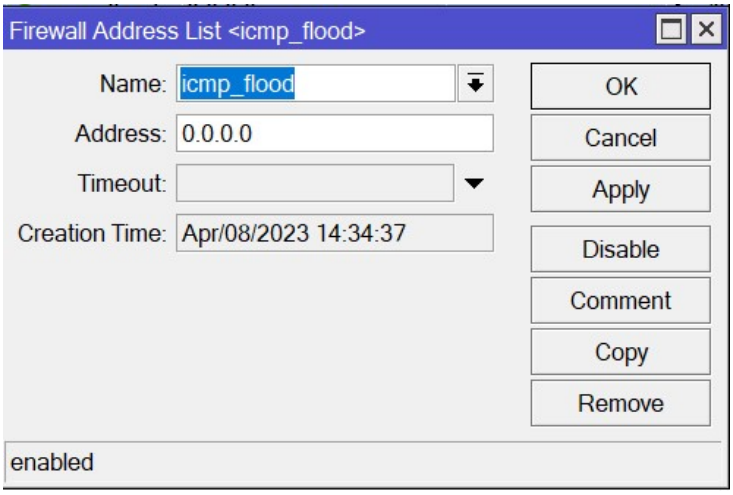
Gambar 4. 5 Konfigurasi Jump target

Selanjutnya menentukan jumlah batas koneksi paket udp yang bias diterima oleh mikrotik/server dengan rate 1000 packet per detik dengan burst time 5 detik seperti pada gambar dibawah :

Gambar 4. 6 Konfigurasi Limit Paket

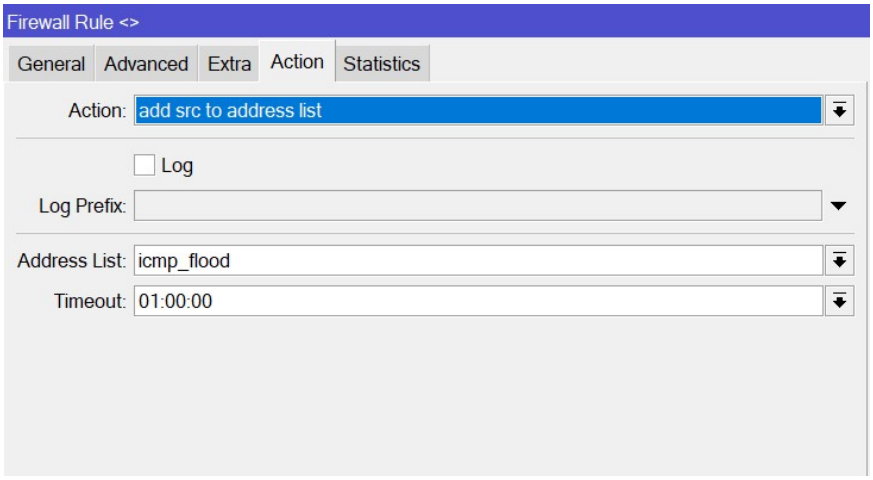
4.2.6 Perancangan Sistem Keamanan Serangan ICMP DOS

Pada tahap perancangan sistem keamanan serangan ICMP DoS langkah yang dilakukan adalah membuat list address yang melakukan serangan seperti pada gambar dibawah :



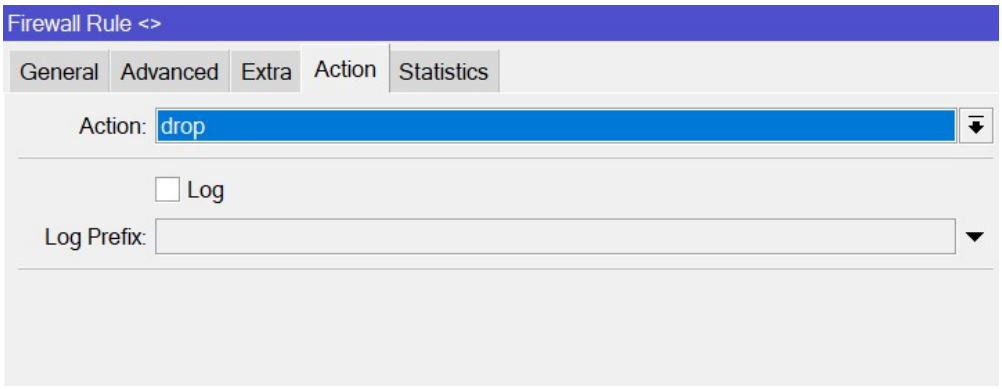
Gambar 4. 7 Konfigurasi Address List ICMP

Selanjutnya melakukan konfigurasi untuk menambahkan alamat IP yang melakukan serangan ICMP Flood ke daftar address list yang telah dibuat sebelumnya dengan aturan membatasi jumlah koneksi dengan melebihi batas tertentu. Pada penelitian ini penulis menerapkan untuk koneksi maksimum adalah 10 per 32 detik dan setelah waktu 1 jam alamat ip akan dihapus dari daftar alamat icmp_flood sperti pada gambar dibawah.



Gambar 4. 8 Konfigurasi Penandaan IP List

Selanjutnya pada tahap terakhir yaitu mengkonfigurasi agar semua paket icmp yang masuk melalui IP yang sudah terdaftar di address list akan di tolak / drop oleh mikrotik seperti pada gambar berikut.



Gambar 4. 9 Konfigurasi Drop Paket ICMP

4.2.7 Pengujian Keamanan Serangan DDOS

4.2.8 Pengujian Serangan Sebelum Menerapkan Firewall Filtering

Pada tahap ini dilakukan pengujian terhadap metode keamanan dengan Firewall Filtering terhadap menggunakan http dos. Adapun tahapan yang dilakukan adalah melakukan proses serangan dengan menggunakan tool ddos unicorn.

Pengujian sistem firewall terhadap ddos dilakukan menggunakan tools udp unicorn. Tools udp unicorn dipilih karena terbukti bisa membanjiri atau mampu mengirimkan paket udp dan tcp sebanyak mungkin terhadap router yang dituju. Pengujian pertama dilakukan tanpa mengaktifkan fungsi filtering di firewall dengan parameter

yang digunakan sebagai berikut :

Target = IP address Lokal Mikrotik 192.168.50.1

Protocol = Random

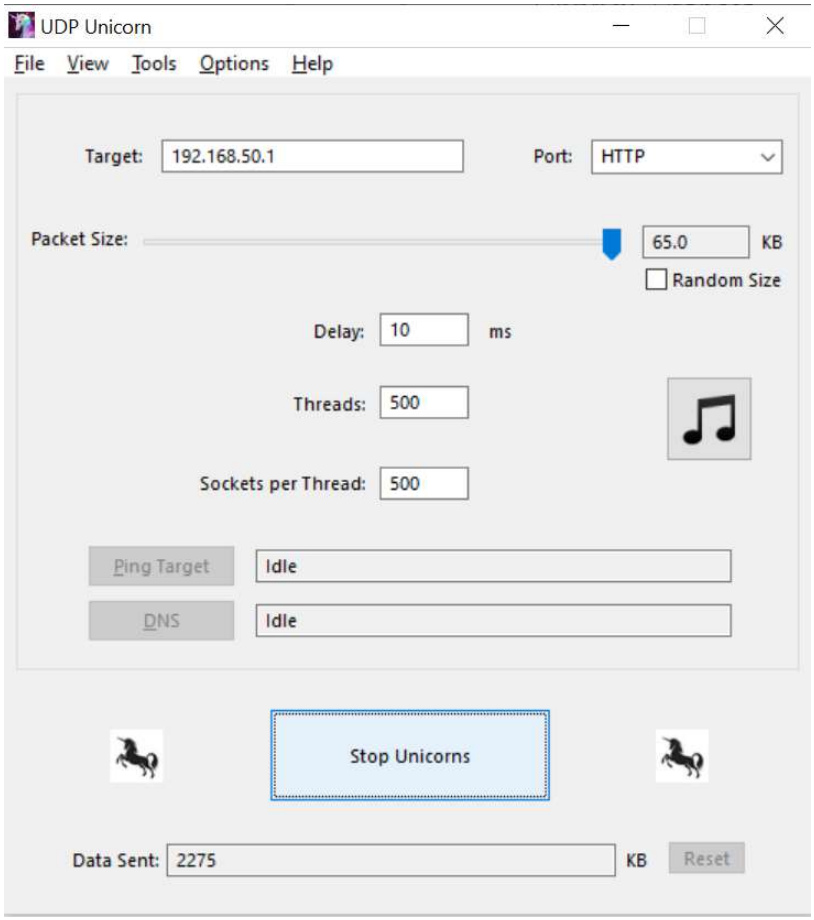
Port = DNS (53)

Packet Size = 65kb

Delay = 10 ms

Threads : 500

Socket Per Threads : 500



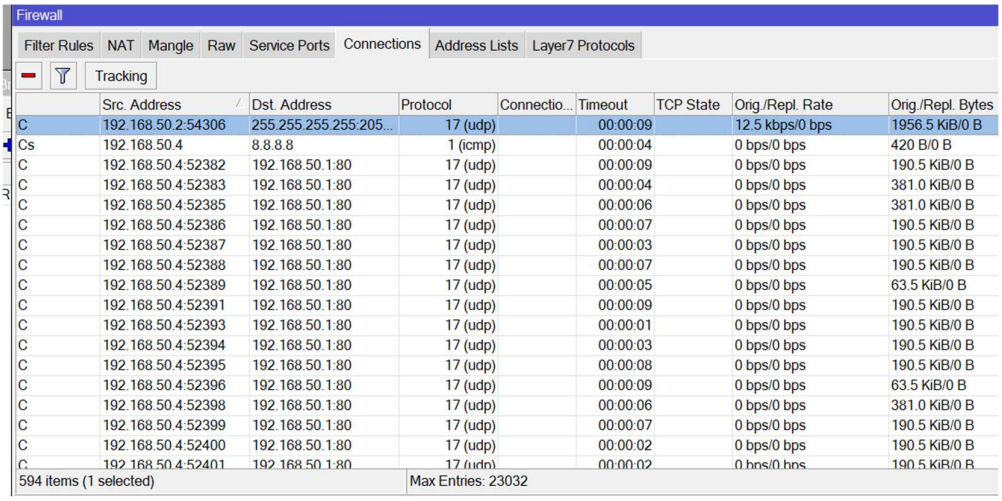
Gambar 4. 10 Uji Coba Serangan HTTP DOS

Dari hasil pengujian serangan flood tehadap mikrotik terlihat bahwa trafik jaringan meningkat melebihi batas normal berdasarkan besaran data yang terkirim dari tool udp unicorn.

Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
17 (udp)		00:00:09		16.7 Mbps/0 bps	1056.9 MiB/0 B
6 (tcp)		16:12:06	established	0 bps/0 bps	1226 B/4990 B
6 (tcp)		23:59:33	established	0 bps/0 bps	21.5 KiB/30.1 KiB
6 (tcp)		23:59:03	established	0 bps/0 bps	27.2 KiB/26.8 KiB
6 (tcp)		23:59:59	established	7.4 kbps/215.3 kbps	892.0 KiB/24.8 MiB

Gambar 4. 11 Hasil Monitoring Trafik Meningkat

Pengujian serangan juga dilihat dari firewall connection mikrotik yang meningkat pesat sampai jumlah client yang aktif mencapai 500 – 700 user sekaligus dan mengakibatkan fungsi dari mikrotik lambat bekerja dan akses internet menjadi lambat (delay) seperti pada gambar dibawah :



Gambar 4. 12 Proses Request Conectiom Serangan DOS

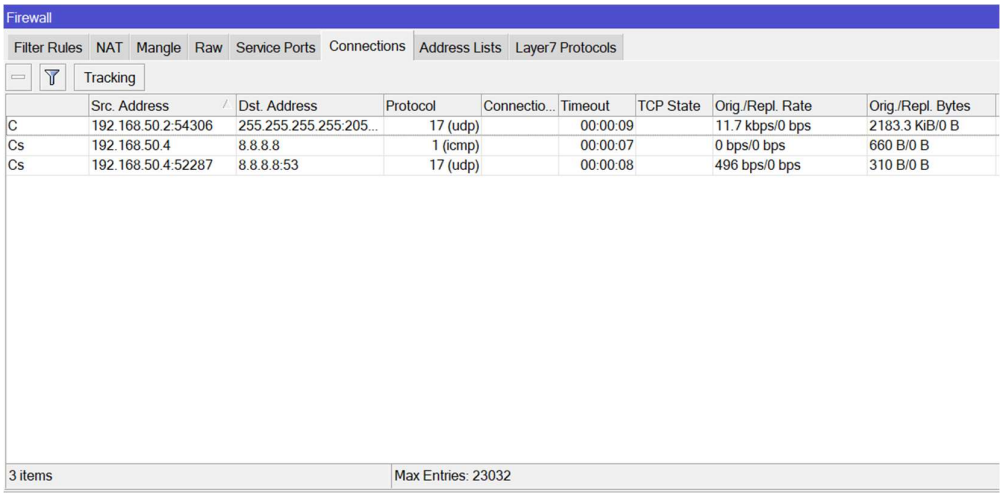
4.2.9 Pengujian Serangan DOS Sesudah Menerapkan Firewall Filtering

Selanjutnya pengujian menggunakan teknik filtering dengan melakukan percobaan serangan yang sama dan hasil trafik yang di terima mikrotik terlihat normal, bahkan flood udp tidak masuk pada router.

Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
6 (tcp)		16:08:20	established	0 bps/0 bps	1226 B/4990 B
6 (tcp)		23:59:45	established	0 bps/0 bps	21.9 KiB/30.5 KiB
6 (tcp)		23:59:18	established	0 bps/0 bps	27.9 KiB/27.5 KiB
6 (tcp)		23:59:59	established	11.6 kbps/397.0 kbps	1067.8 KiB/30.2 ...

Gambar 4. 13 Monitoring Serangan Setelah penerapan filtering firewall

Selanjutnya melakukan monitoring juga pada firewall connection mikrotik untuk mengetahui apakah ada beban trafik berlebih yang masuk pada mikrotik dengan memantau request conection yang masuk sesuai dengan jumlah komputer yang terhubung dengan mikrotik.



Gambar 4. 14 Proses Request Conection Normal

BAB V
PEMBAHASAN PENELITIAN

5. 1 Pembahasan Sistem

5.1.1 Hasil Tampilan Rule Firewall

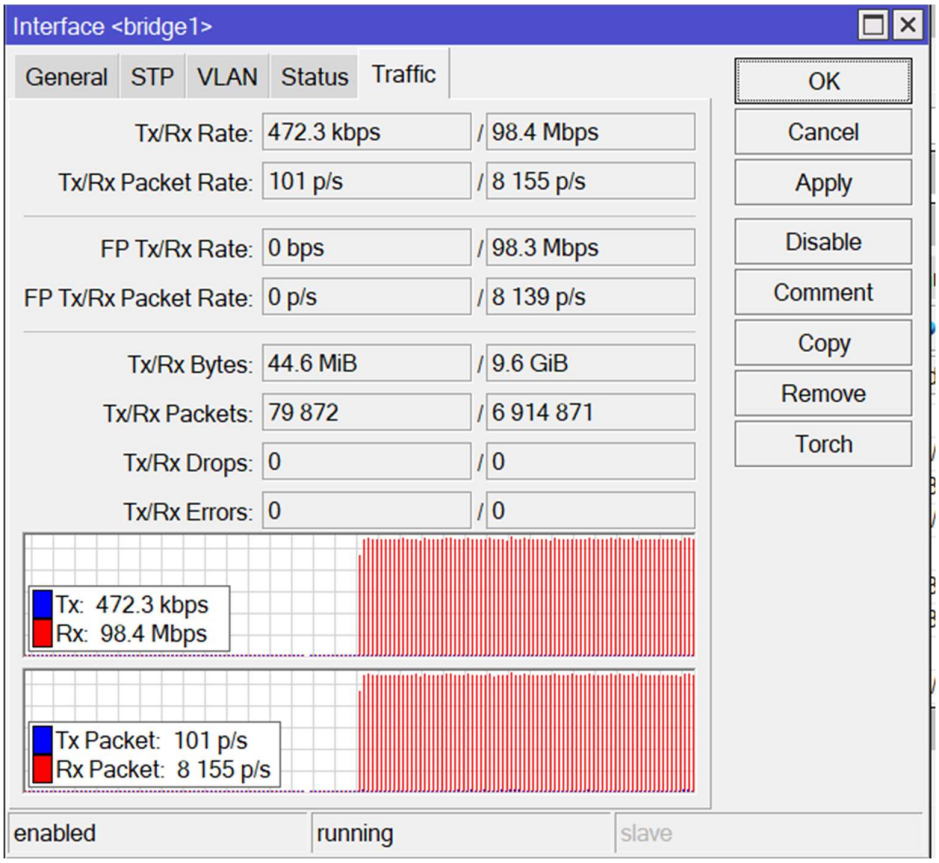
Berikut adalah hasil tampilan sistem keamanan dengan metode Firewall Filtering yang digunakan dalam penelitian ini dan dirancang pada firewall mikrotik:

;;; Allow Hp Dudi												
12		acce...	forward	10.75.3.5	0.0.0.0/0							
13		acce...	forward	10.75.3.31	0.0.0.0/0							
14		acce...	forward	10.75.3.100	0.0.0.0/0							
;;; Drop All												
15		drop	forward	10.75.3.95	0.0.0.0/24							
16		drop	forward	10.75.3.95	10.75.3.0/24							
17		drop	forward	10.75.3.0/24	0.0.0.0/0							
;;; Allow Desa												
18		acce...	forward	192.168.22...	10.75.3.2							
19		acce...	forward	192.168.22...	10.75.3.24							
;;; Drop Desa												
20		drop	forward	192.168.22...	0.0.0.0/0							
;;; HTTP DOS Filtering												
21		drop	input			6 (tcp)			ether2			
22		drop	forward			1 (icmp)						
;;; UDP Flood Protection												
23		jump	input			17 (udp)						
;;; Add attacker to UDP-ATTACK list												
24		add ...	UDP-PRO...			17 (udp)			ether2			
;;; Drop UDP attack from attacker list												
25		drop	UDP-PRO...			17 (udp)			ether2			UDP-A...
;;; Add to HTTP DOS list												
26		add ...	forward			6 (tcp)		80,443	ether2			
;;; Drop HTTP flood												
27		drop	forward			6 (tcp)		80,443	ether2			http_dos
;;; Add to ICMP flood list												
28		add ...	forward			1 (icmp)						
;;; Drop ICMP flood												
29		drop	forward			1 (icmp)						

Gambar 5. 1 Tampilan Rule Sistem Keamanan Firewall Filtering

Pada gambar diatas adalah merupakan rule dari sistem keamanan serangan DoS dimana urutan rule harus sesuai dengan proses identifikasi dari serangan agar fungsi dari filtering paket berjalan dengan baik.

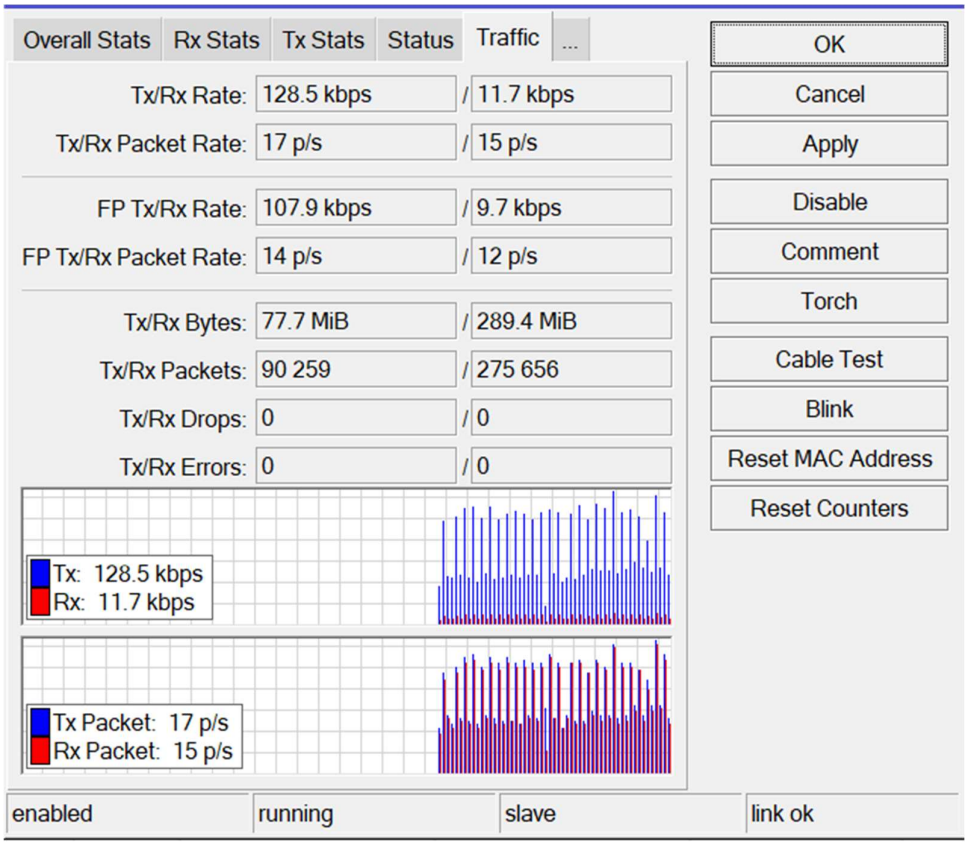
5.1.2 Hasil Tampilan Trafik Tanpa Filtering Firewall



Gambar 5. 2 Hasil Monitoring Trafic Serangan DDOS

Pada gambar diatas merupakan tampilan dari monitoring traffic data yang yang di request oleh komputer yang melakukan serangan ddos, dimana terlihat penggunaan data mencapai 98Mbps sehingga koneksi internet menjadi lambat.

5.1.3 Hasil Tampilan Traffic Menggunakan Firewall Filtering



Gambar 5. 3 Hasil Monitoring Traffic Normal Serangan DDOS

Pada gambar diatas merupakan hasil monitoring traffic pada interface ether 2 yang menjadi pusat interconnection hotspot dimana terlihat traffic berjalan normal dengan tetap melakukan percobaan serangan ddos.

5. 2 Hasil Pengujian Model Serangan

5.2.1 Tabel Hasil serangan ddos Mikrotik Tanpa Filtering

Tabel 5. 1 Hasil Pengujian Serangan HTTP Tanpa Filtering Firewall

IP Address	Jumlah Serangan Packet Rand	Status Traffic		Status Resource Mikrotik
		Tx Rate	Rx Rate	CPu Load
192.168.50.2	65 Kb	0 mbps	-+30mbps	60 %
192.168.50.3	50 Kb	0 mbps	-+20mbps	45 %
192.168.50.4	30 Kb	0 mbps	-+20mbps	34 %

5.2.2 Http dos Protocol Mikrotik Dengan Filtering

Tabel 5. 2 Hasil Pengujian Serangan HTTP DOS Setelah Diterapkan Firewall Filtering

IP Address	Jumlah Packet Rand	Status Traffic		Status Resource Mikrotik
		Tx Rate	Rx Rate	CPu Load
192.168.50.2	65 kb	0 mbps	-+30mbps	3 %
192.168.50.3	50 kb	0 mbps	-+50mbps	10 %
192.168.50.4	30 kb	0 mbps	-+75mbps	18 %

Berdasarkan hasil eksperiment pada penelitian ini dengan melakukan ujicoba serangan menggunakan 3 client dengan menggunakan parameter packet size pada tool unicorn di dapat hasil dari resource mikrotik secara bervariasi seperti pada table 5.1 diatas.

BAB VI
PENUTUP

6. 1 Kesimpulan

Berdasarkan Hasil Penelitian yang dilakukan pada router mikrotik dinas kependudukan dan catatan sipil dan pembahasan yang telah diuraikan sebelumnya, maka dapat ditarik kesimpulan bahwa :

1. Secara umum sistem firewall berbasis filtering terhadap serangan http dos pada protocol tcp yang diterapkan sudah berhasil mencegah serangan ddos.
2. Dari hasil analisa penerapan filtering firewall yang diterapkan, protocol http masih sulit di identfikasi karenan packet http bersamaan masuk dengan akses browsing dan download, sehingga ada rule yang belum bisa melakukan drop packet otomatis terhadap protocol http karena bisa mengakibatkan gagal koneksi dibandingkan drop packet ICMP dan UDP.

6. 2 Saran

Setelah melakukan penelitian dan perancangan sistem filtering pada firewall mikrotik dinas kependudukan dan catatan sipil, ada beberapa saran yang perlu diperhatikan untuk mencapai tujuan yang diharapkan, yaitu sebagai berikut :

1. Sistem Filtering ini dapat dikembangkan dengan melakukan filtering pada protocol yang bisa menimbulkan serangan ddos selain TCP, UDP, Dan ICMP
2. Untuk Meningkatkan sistem keamanan yang lebih baik, diharapkan bisa dilakukan monitoring serangan secara realtime

\

DAFTAR PUSTAKA

[1] Imam Riadi. 2011 ,Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Miktorik.

[2] S. Hidayatulloh, "Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol Ipsec," *J. Inform.*, vol. 1, no. 2, pp. 93–104, 2018.

[3] I. G. Komang and O. Mardiyana, "Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali," *Stmik Stikom*, vol. 1, no. 86, pp. 9–10, 2015.

[4] D. Aprilianto, T. Fadila, and M. A. Muslim, "Sistem Pencegahan UDP DNS Flood Dengan Filter Firewall Pada Router Mikrotik," *Techno.Com*, vol. 16, no. 2, pp. 114–119, 2017.

[5] R. ALFARIS, "RANCANG BANGUN JARINGAN LAN BERBASIS MIKROTIK ROUTER PADA JURUSAN TEKNIK KOMPUTER POLITEKNIK NEGERI SRIWIJAYA," *Molecules*, vol. 2, no. 1, pp. 1–12, 2020

[6] R. Riska and H. Alamsyah, "Penerapan Sistem Keamanan Web Menggunakan Metode Web Aplication Firewall," *J. Amplif. J. Ilm. Bid. Tek. Elektro Dan Komput.*, vol. 11, no. 1, pp. 37–42, 2021

[7] FITRI RAMADHANI H, "ANALISIS DAN IMPLEMENTASI FIREWALL DENGAN METODE PORT ADDRESS TRANSLATION PADA MIKROTIK OS FIT," *Photosynthetica*, vol. 2, no. 1, pp. 1–13, 2018

[8] Y. Mardiana and J. Sahputra, "Analisa Performansi Protokol TCP , UDP dan SCTP," *J. Media Infotama*, vol. 13, no. 2, pp. 73–84, 2017.

[9] A. Hidayat and I. P. Saputra, "Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia.Net, Tanjung Harapan Lampung Timur)," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 1, no. 2, pp. 118–124, 2018.

[10] H. Kurniawan and S. Kosasi, "Penerapan Network Development Life Cycle Dalam Perancangan Intranet," *Penerapan Netw. Dev. Life Cycle Dalam Peranc. Intranet Untuk Mendukung Proses Pembelajaran*, vol. 5, no. 2, pp. 178–188, 2015.

[11] L. Menggunakan and S. Kerja, "Perancangan dan implementasi monitoring jaringan lokal menggunakan sistem kerja," 2011.

[12] N. E. I. N. U. Tara, "PENGEMBANGAN SISTEM KEAMANAN JARINGAN KOMPUTER BERBASIS MIKROTIK PADA SMK NEGERI 1 INDRALAYA UTARA C OMPUTER N ETWORK S ECURITY S YSTEM D EVELOPMENT B ASED ON M IKROTIK AT SMK Imam Solikin , 2 Suryayusra , 3 Maria Ulfa Pendahuluan Perkembangan Jaringan in," pp. 61–70.

[13] "Pendeteksian Serangan Ddos (Distributed Denial of Service) Menggunakan Ids (Intrusion Detection System) Universitas Pasundan November 2016," no. November, 2016.

[14] R. TOWIDJOJO, *MIKROTIK KUNGFU*, KITAB 1. JASAKOM.

[15] Y. Kristianto and M. Salman, "Implementasi dan Analisa Unjuk Kerja Keamanan Jaringan pada Infrastuktur Berbasis IDPS (Intrusion Detection and Prevention System)," p. 10, 2010.and Prevention System)," p. 10, 2010.

Lampiran Script :

```
# Block all incoming packets that are not part of established or related connections
/ip firewall filter
add action=drop chain=input connection-state=!established,related

# Block all incoming TCP SYN packets that exceed a certain limit
/ip firewall filter
add action=add-src-to-address-list address-list=SYN_limit address-list-timeout=1m chain=input connection-state=new protocol=tcp tcp-flags=syn limit=10,minute

# Drop all incoming packets from the SYN limit address list
/ip firewall filter
add action=drop chain=input src-address-list=SYN_limit

# Block all incoming UDP packets that exceed a certain limit
/ip firewall filter
add action=add-src-to-address-list address-list=UDP_limit address-list-timeout=1m chain=input protocol=udp limit=10,minute

# Drop all incoming packets from the UDP limit address list
/ip firewall filter
add action=drop chain=input src-address-list=UDP_limit

# Block all incoming packets that are part of known DDoS attack signatures
/ip firewall filter
add action=drop chain=input comment="Drop known DDoS attack signatures" protocol=tcp dst-port=80,443 src-address-list=ddos_signature

# Block all incoming packets with a TTL value of 1
/ip firewall filter
add action=drop chain=input comment="Drop packets with TTL=1" ttl=1
```

```
# Log all dropped packets for debugging and analysis purposes
/ip firewall filter
add action=log chain=input log-prefix="DDoS packet dropped: "

# Create address list for HTTP flooding IPs
/ip firewall address-list
add list=http_flood

# Add new HTTP flooding IP to the list
/ip firewall filter
add action=add-src-to-address-list address-list=http_flood address-list-timeout=1h chain=forward
comment="Add to HTTP flood list" dst-port=80,443 protocol=tcp connection-limit=50,32

# Drop all HTTP requests from IPs on the HTTP flooding list
/ip firewall filter
add action=drop chain=forward comment="Drop HTTP flood" dst-port=80,443 protocol=tcp src-address-
list=http_flood

# Create address list for ICMP flooding IPs
/ip firewall address-list
add list=icmp_flood

# Add new ICMP flooding IP to the list
/ip firewall filter
add action=add-src-to-address-list address-list=icmp_flood address-list-timeout=1h chain=forward
comment="Add to ICMP flood list" protocol=icmp icmp-options=8:0-65535 connection-limit=10,32

# Drop all ICMP requests from IPs on the ICMP flooding list
/ip firewall filter
add action=drop chain=forward comment="Drop ICMP flood" protocol=icmp address-list=icmp_flood
/ip firewall filter
add chain=input connection-state=new protocol=tcp tcp-flags=syn action=jump jump-target=SYN-PROTECT
comment="SYN Flood Protection"
```

add chain=SYN-PROTECT protocol=tcp tcp-flags=syn limit=1000,5 action=add-src-to-address-list address-list=SYN-ATTACK address-list-timeout=1m comment="Add attacker to SYN-ATTACK list"

add chain=SYN-PROTECT protocol=tcp tcp-flags=syn src-address-list=SYN-ATTACK action=drop comment="Drop SYN attack from attacker list"

add chain=input protocol=icmp action=jump jump-target=ICMP-PROTECT comment="ICMP Flood Protection"

add chain=ICMP-PROTECT protocol=icmp limit=50/5s action=add-src-to-address-list address-list=ICMP-ATTACK address-list-timeout=1m comment="Add attacker to ICMP-ATTACK list"

add chain=ICMP-PROTECT protocol=icmp src-address-list=ICMP-ATTACK action=drop comment="Drop ICMP attack from attacker list"

DAFTAR RIWAYAT HIDUP

Nama	: Moh. Rizki Kaunang
Tempat, Tgl Lahir	: Gorontalo, 11 Maret 1997
Alamat	: Toto Utara, Tilongkabila, Bone Bolango
Email	: dekikaunang575@gmail.com

Riwayat Pendidikan :

1. Tahun 2009 Menyelesaikan Pendidikan di SDN 1 Toto.
2. Tahun 2012, Menyelesaikan Pendidikan di SMP N 1 Kabila.
3. Tahun 2016, Menyelesaikan Pendidikan di SMK Negeri 1 Suwawa.
4. Tahun 2017, Mendaftar dan Diterima Menjadi Mahasiswa di Universitas Ichsan Gorontalo

Riwayat Pekerjaan :

1. Tahun 2018 Bekerja Sebagai Administrator Database Pada Dinas Kependudukan Dan Pencatatan Sipil (DUKCAPIL) Sampai dengan saat ini.

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
LEMBAGA PENELITIAN

Kampus Unisan Gorontalo Lt.3 - Jln. Achmad Nadjamuddin No. 17 Kota Gorontalo
Telp: (0435) 8724466, 829975 E-Mail: lembagapenelitian@unisan.ac.id

Nomor : 4490/PIP/LEMLIT-UNISAN/GTO/I/2023
Lampiran : -
Hal : Permohonan Izin Penelitian

Kepada Yth,
Kepala Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango
di,-
Tempat

Yang bertanda tangan di bawah ini :

Nama	:	Dr. Rahmisyari, ST.,SE.,MM
NIDN	:	0929117202
Jabatan	:	Ketua Lembaga Penelitian

Meminta kesediannya untuk memberikan izin pengambilan data dalam rangka penyusunan **Proposal / Skripsi**, kepada :

Nama Mahasiswa	:	Moh. Rizki Kaunang
NIM	:	T3117034
Fakultas	:	Fakultas Ilmu Komputer
Program Studi	:	Teknik Informatika
Lokasi Penelitian	:	DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KABUPATEN BONE BOLANGO
Judul Penelitian	:	IMPLEMENTASI FILTERING FIREWALL UNTUK MENCEGAH SERANGAN HTTP DOS (STUDI KASUS DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KABUPATEN BONE BOLANGO)

Atas kebijakan dan kerja samanya diucapkan banyak terima kasih.

Gorontalo, 09 Januari 2023
Ketua,

Dr. Rahmisyari, ST.,SE.,MM
NIDN 0929117202

PEMERINTAH KABUPATEN BONE BOLANGO

DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL

Jalan Prof. Dr.Ing.BJ. Habibie, Desa Moutong Kecamatan Tilongkabila

SURAT KETERANGAN

Nomor : 400.7.22.1/DKPS/BB/7/V/2023

Yang bertanda tangan di bawah ini :

Nama : Oktavianus S.W. Rahman, M.Pd. M.Si

NIP. : 197110161998011001

Pangkat/Gol : Pembina Utama Muda, IV/C

Menerangkan bahwa :

Nama : Moh. Rizki Kaunang

TTL : Gorontalo, 11 Maret 1997

NIM : T3117034

Fakultas : Fakultas Ilmu Komputer

Program Studi : Teknik Informatika

Judul penelitian : Implementasi filtering firewall untuk mencegah serangan HTTP DOS

Adalah benar telah melakukan pengambilan data penelitian dalam rangka penyusunan Proposal/ Skripsi pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bone Bolango.

Suwawa, 3 Mei 2023

KEPALA DINAS

OKTAVIANUS S.W RAHMAN, M.Pd, M.Si
Pembina Utama Muda
NIP.197110161998011001

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI

UNIVERSITAS ICHSAN GORONTALO

FAKULTAS ILMU KOMPUTER

SURAT KEPUTUSAN MENDIKNAS RI NOMOR 84/D/O/2001

Jl. Achmad Najamuddin No. 17 Telp. (0435) 829975 Fax (0435) 829976 Gorontalo

SURAT REKOMENDASI BEBAS PLAGIASI

No. 149/FIKOM-UIG/R/V/2023

Yang bertanda tangan di bawah ini :

Nama	: Irvan Abraham Salihi, M.Kom
NIDN	: 0928028101
Jabatan	: Dekan Fakultas Ilmu Komputer

Dengan ini menerangkan bahwa :

Nama Mahasiswa	:	Moh. Rizki Kaunang
NIM	:	T3117034
Program Studi	:	Teknik Informatika (S1)
Fakultas	:	Fakultas Ilmu Komputer
Judul Skripsi	:	Implementasi Filtering Firewall Untuk Mencegah Serangan HTTP DOS

Sesuai hasil pengecekan tingkat kemiripan skripsi melalui aplikasi **Turnitin** untuk judul skripsi di atas diperoleh hasil *Similarity* sebesar **16%**, berdasarkan Peraturan Rektor No. 32 Tahun 2019 tentang Pendeteksian Plagiat pada Setiap Karya Ilmiah di Lingkungan Universitas Ichsan Gorontalo dan persyaratan pemberian surat rekomendasi verifikasi calon wisudawan dari LLDIKTI Wil. XVI, bahwa batas kemiripan skripsi maksimal 30%, untuk itu skripsi tersebut di atas dinyatakan **BEBAS PLAGIASI** dan layak untuk diujiankan.

Demikian surat rekomendasi ini dibuat untuk digunakan sebagaimana mestinya.

Gorontalo, 12 Mei 2023

Mengetahui
Dekan,

Irvan Abraham Salihi, M.Kom
NIDN. 0928028101

Tim Verifikasi,

Zulfrianto Y. Lamasigi, M.Kom
NIDN. 0914089101

Terlampir :
Hasil Pengecekan Turnitin

16% Overall Similarity

Top sources found in the following databases:

- 16% Internet database
- Crossref database
- 0% Submitted Works database
- 1% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	ilyasparid98.blogspot.com Internet	3%
2	eprints.mercubuana-yogya.ac.id Internet	2%
3	seminar.bsi.ac.id Internet	2%
4	docplayer.info Internet	1%
5	ijadis.org Internet	<1%
6	eprints.polsri.ac.id Internet	<1%
7	jurnal.pancabudi.ac.id Internet	<1%
8	kingsmpls.com Internet	<1%

9	idmetafora.com Internet	<1%
10	ejournal.unib.ac.id Internet	<1%
11	jurnal.univrab.ac.id Internet	<1%
12	goens89.blogspot.com Internet	<1%
13	ejurnal.itats.ac.id Internet	<1%
14	jtera.polteksmi.ac.id Internet	<1%
15	id.wikipedia.org Internet	<1%
16	id.123dok.com Internet	<1%
17	repository.bsi.ac.id Internet	

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
FAKULTAS ILMU KOMPUTER
UPT. PERPUSTAKAAN FAKULTAS
SK. MENDIKNAS RI NO. 84/D/0/2001
Jl. Achmad Nadjamuddin No.17 Telp(0435) 829975 Fax. (0435) 829976 Gorontalo

SURAT KETERANGAN BEBAS PUSTAKA

No : 016/Perpustakaan-Fikom/V/2023

Perpustakaan Fakultas Ilmu Komputer (FIKOM) Universitas Ichsan Gorontalo dengan ini menerangkan bahwa :

Nama Anggota	:	Moh. Rizki Kaunang
No. Induk	:	T3117034
No. Anggota	:	M202343

Terhitung mulai hari, tanggal : Jumat, 12 Mei 2023, dinyatakan telah bebas pinjam buku dan koleksi perpustakaan lainnya.

Demikian keterangan ini di buat untuk di pergunakan sebagaimana mestinya.

Gorontalo, 12 Mei 2023
Mengetahui,
Kepala Perpustakaan

Apriyanto Alhamad, M.Kom
NIDN : 0924048601