IMPLEMENTASI *BACKBONE NETWORK SECURITY SYSTEM* MENGGUNAKAN *FIREWALL* PADA KOMUNIKASI *HYBRID*

Muhamad Yusuf Imani[1)] , Nur Rachman [2)] Prisca Chorina [3)]
Politeknik Angkatan Darat, Jl. Raya Anggrek, Pendem, Junrejo Batu
[1)]Jurusan Telekomunikasi Prodi D4 Teknik Telkommil Poltekad Kodiklatad
[2)]Kepala Kelompok Dosen Poltekad,[3)]Universitas Islam Raden Rahmat Malang
E - mail : xea0796@gmail.com[1)], nurrudal@gmail.com [2)],
priska_choirina@uniramalang.ac.id[3)]

IMPLEMENTATION OF BACKBONE NETWORK SECURITY SYSTEM USING FIREWALL IN HYBRID COMMUNICATION

Abstract: *Security systems in communication are very important. Confidentiality of information has become a fixed price. Researchers create a security system on the existing backbone network in hybrid communication using a firewall. This system aims to secure the network from people who are not responsible. This backbone network security uses UFW with parameters IP, Port, UDP, and SSH for limiting access rights. These parameters will be placed on the server for monitoring. The research method used in this research is the mixing method. The results of this study are expected to be able to provide a security system when carrying out communication. Users who can communicate are only users who have registered on the server, so that not just anyone can use this communication. Then this security system also supports sending notifications to server operators if the server experiences excess access rights or overload.*

Keywords: Firewall, Security, Monitoring, Zabbix, Backbone Network.

Abstrak: *Sistem keamanan pada komunikasi sangatlah penting. Kerahasiaan suatu informasi sudah menjadi harga mati. Peneliti membuat sistem keamanan pada jaringan backbone yang ada pada komunikasi hybrid dengan menggunakan firewall. Pengembangan sistem ini bertujuan untuk mengamankan jaringan tersebut dari orang-orang yang tidak bertanggung jawab. Pengamanan jaringan backbone ini menggunakan UFW dengan parameter IP, Port, UDP, dan SSH untuk pembatasan hak akses. Parameter tersebut akan diletakkan pada server untuk monitoring. Metode penelitian yang digunakan dalam penelitian ini adalah metode mixing. Hasil dari penelitian ini diharapkan mampu memberikan system keamanan saat melaksanakan komunikasi. Pengguna yang bisa berkomunikasi hanya pengguna yang sudah melaksanakan registrasi pada server, sehingga tidak sembarang orang bisa menggunakan komunikasi ini. Kemudian system keamanaan ini juga mendukung pengiriman notifikasi kepada operator server apabila server mengalami kelebihan hak akses atau overload.*

Kata kunci: Firewall, Pengamanan, Monitoring, Zabbix, Jaringan Backbone.

PENDAHULUAN

Perkembangan era teknologi 4.0 saat ini berjalan seiring dengan kemajuan dalam *analisis* data, *otomasi*, dan *internet of things*. Di masa depan, sistem komunikasi utama militer akan lebih canggih. Komunikasi akan bisa dilakukan oleh semua pasukan militer maupun organisasi sipil. Pengembangan teknologi komunikasi saat ini lebih fokus ke arah optimalisasi perangkat komunikasi yang digunakan untuk melaksanakan tugas di masa perang maupun di masa selain perang. Perkembangan teknologi komunikasi yang digunakan saat ini masih belum menggunakan system keamanan yang mumpuni. Kebocoran suatu data tentu saja bukan hal yang kita inginkan. Apabila hal tersebut terjadi, maka akan sangat membahayakan baik personil maupun materil. Oleh karena itu dibutuhkan suatu sistem komunikasi dengan system keamanan dan *monitoring* yang canggih, sehingga mampu mencegah terjadinya kebocoran informasi oleh pihak yang tidak bertanggung jawab.

Sistem keamanan jaringan backbone merupakan suatu system keamanan jaringan komunikasi yang digunakan untuk mengamankan informasi mulai dari pengirim sampai dengan penerima. Pengamanan jaringan backbone ini menggunakan firewall dan *Zabbix system*. *Firewall* adalah sistem keamanan untuk mengelola dan memantau trafik masuk dan keluar berdasarkan aturan keamanan (*security rules*) yang sudah ditentukan. *Firewall* berfungsi mencegah akses yang tidak diinginkan dari atau ke dalam jaringan atau server. Selain firewall perlu juga adanya monitoring jaringan atau network services yang digunakan untuk komunikasi. Hal ini perlu dilakukan karena untuk memonitor jaringan, dan status dari berbagai *network service*, *bandwidth*, *delay*, *jitter* dan *throughput*

Berdasarkan permasalahan diatas maka akan dibuat sebuah sistem keamanan jaringan *backbone* menggunakan *Firewall*. Pembuatan meliputi pemberian akses kepada *user* tertentu dan sistem *monitoring* serta memberikan informasi kepada operator server apabila terjadi gangguan pada *system* komunikasi. Sistem keamanan ini diharapkan bisa menjamin keamanan serta memberikan layanan komunikasi yang baik sehingga komunikasi dapat berjalan dengan aman dan lancar.

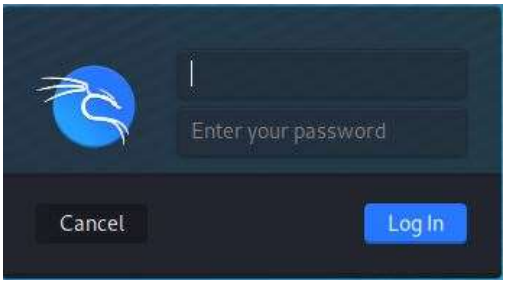
Dari latarbelakang diatas dapat diambil pokok rumusan masalah, yaitu :

1. Bagaimana program yang dibuat mampu mengatur user berdasarkan *IP*, *PORT*, *UDP*, dan *SSH* ?

2. Bagaimana program yang dibuat mampu mengirimkan notifikasi kepada operator apabila terjadi gangguan ?

Tujuan dari penelitian ini adalah Untuk membuktikan parameter yang ada pada *firewall* dan pengaruhnya pada pada user yang berbeda serta untuk membuktikan system yang dibuat dapat mengirimkan notification ke operator apabila server mengalami *overload*.

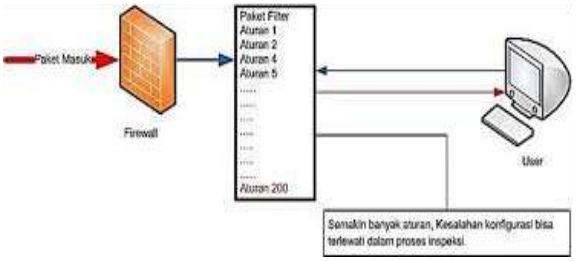
1. Linux.



Gambar 1. Linux

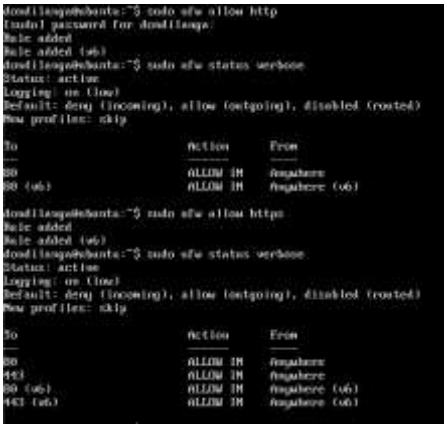
Linux merupakan sebuah *operating system* yang sifatnya *open source*. *Linux* sendiri memiliki lisensi *GNU*. Fitur-fitur yang ada pada linux tidak berbayar alias gratis. Hal inilah yang banyak diminati oleh banyak orang untuk menggunakan *linux*. Selain itu *OS linux* ini sangat ringan untuk digunakan, tidak memerlukan spesifikasi *computer* yang tinggi untuk menjalankan *OS* ini. Dengan menggunakan *linux*, para pengguna akan dengan mudah mendapatkan aplikasi beserta dengan kodingnya. Semua itu bukan illegal, karena sudah memiliki lisensi dari *GNU*.

2. Firewall



Gambar 2. Firewall

Firewall merupakan suatu *system* keamanan yang ada pada jaringan *computer*. Tujuannya yaitu untuk melindungi jaringan komputer dari berbagai macam gangguan atau serangan dari komputer yang tidak dikenal. *Firewall* dapat melihat aktifitas keluar masuk jaringan yang kita lakukan. Jadi definisi firewall secara umum adalah suatu program *software* yang dapat mencegah atau membatasi akses ke server atau jaringan kita. Hal ini sangatlah dibutuhkan untuk mengamankan sebuah server atau jaringan.



3. *Uncomplicated Firewall* (*UFW*)

Gambar 3. *UFW*

Uncomplicated Firewall atau sering disingkat dengan *UFW* merupakan salah satu fitur atau *interface open source* yang ada pada *OS linux*. Fitur ini digunakan untuk membuat *system* keamanan *firewall*. Sebelum menggunakan *UFW*, pembuatan system keamanan yang dulu menggunakan *IPTables*. *IPTables* adalah alat yang biasa digunakan untuk konfigurasi *firewall*. Dikarenakan *IPTables* dirasa oleh banyak orang memiliki tingkat yang rumit untuk dipahami, maka dikeluarkanlah *uncomplicated firewall* sebagai pengganti *IPTables*. Dengan demikian pengguna menjadi lebih mudah untuk melakukan konfigurasi *firewall* karena perintah-perintah yang ada pada *UFW* sudah disederhanakan menjadi lebih ringkas.

4. Zabbix

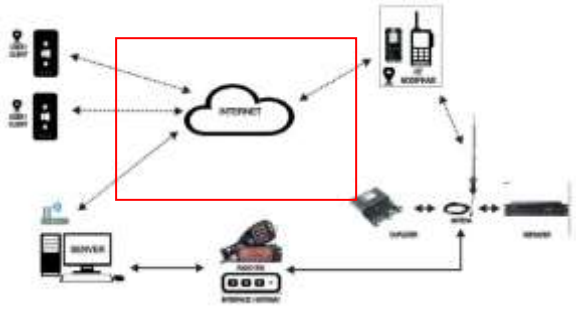
Gambar 4. Zabbix

Zabbix merupakan sebuah aplikasi *open source* yang ada pada *operating*

system linux yang menyediakan layanan untuk monitoring kinerja server. Server dapat dilihat seberapa banyak aktifitas yang dilakukan oleh server, bisa data masuk maupun data keluar. *Zabbix* sendiri sudah menggunakan *GUI* yaitu tampilan berupa map dan grafik sangat membantu operator server untuk membaca data. Pada kondisi warna hijau, itu menandakan kondisi normal. Sedangkan warna merah, itu menandakan bahwa server dalam kondisi tidak normal.

METODE PENELITIAN

Implementasi *backbone network security system* menggunakan *firewall* pada komunikasi *hybrid*, menggunakan *hardware* dan *software* untuk mendukung dan memperoleh hasil yang maksimal, sehimgga dapat digunakan sesuai dengan keinginan. Penelitian ini menggunakan metode penelitian mixing.



Gambar 5. Diagram alat

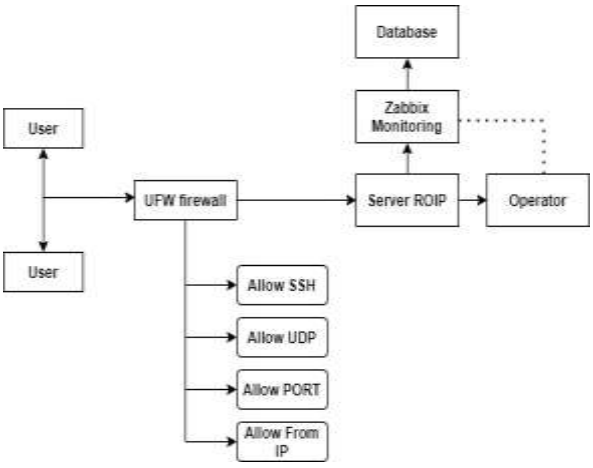
Pembahasan pada penelitian ini akan membahas blok per blok agar mudah untuk dipahami. Blok diagram akan dibagi menjadi dua bagian, yaitu pembuatan *firewall* menggunakan uncomplicated *firewall* atau *UFW* dan pembuatan system monitoring *Zabbix*. Dimana kedua bagian tersebut sangat penting karena akan mendukung kelancaran dan keamanaan saat berkomunikasi.

Penelitian ini dibuat melalui beberapa tahapan. Dimulai dari pengumpulan permasalahan yang ada saat ini, survei ke instansi-instansi terkait, sampai ke perencanaan sistem keamanaan dan pembuatan sistem keamanan jaringan *backbone*.

Pada penelitian implementasi *backbone network security system* pada komunikasi *hybrid* dilaksanakan di laboratorium politeknik Angkatan darat mulai dari bulan November 2020 sampai dengan bulan mei 2021.

Adapun alat dan bahan yang digunakan pada penelitian ini diantaranya adalah *personal computer* (*PC*), *operating system linux*, *Domain*, *Hosting*, dan aplikasi-aplikasi pendukung yang tersedia pada operating system *linux*.

Diagram alir pada penelitian *system* keamanan ini digambarkan mulai dari pengguna mengakses server melalui *firewall*, apabila pengguna memenuhi parameter-parameter yang telah di konfigurasi maka pengguna akan bisa mengakses ke server.



Gambar 6. Diagram alir

Setelah masuk ke server maka *zabbix* akan memonitor kinerja server. Apabila server mencapai batas akses pengguna maka *Zabbix* akan mengirimkan notifikasi berupa pesan kepada operator agar segera mengecek server. Monitoring ini dilakukan untuk mencegah terjadinya gangguan saat dilakukan komunikasi,

4

sehingga memberikan kenyamanan dan keamanan kepada pengguna.

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini dibagi menjadi dua yaitu hasil pada *firewall* dan hasil pada *monitoring Zabbix*.

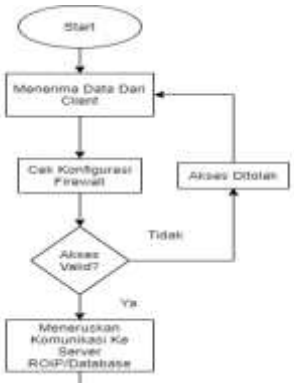
Gambar 7. Konfigurasi address

Tahapan awal konfigurasi *IP* sebagai parameter pembatasan hak akses menggunakan *OS linux*. Hal ini bertujuan untuk menentukan *IP* mana saja yang di ijinkan untuk mengakses server. Pendataan *IP* dilakukan sesuai dengan data yang telah ditentukan. Banyaknya pengguna *IP* tergantung dari kebutuhan di lapangan sehingga operator tidak membatasi jumlahnya.

Gambar 8. *Konfigurasi Secure Shell*

Konfigurasi *secure shell* atau *SSH* dilakukan untuk memastikan bahwa *IP* yang akan masuk benar-benar aman dan layak untuk mengakses server. *SSH* juga bisa digunakan untuk meremot aktifitas dari server.

Semua pengguna akan melewati firewall terlebuh dahulu sebelum masuk ke dalam server. Terbukti pengguna yang sudah diregistrasi dan terdaftar di server, bisa mengakses masuk ke dalam server. Sedangkan user yang belum diregistrasi tidak bisa masuk ke dalam server.



Gambar 9. Akses *firewall*

Setelah dinyatakan layak dan memenuhi parameter-parameter pada *firewall* yang sudah di konfigurasi selanjutnya pengguna sudah bisa mengakses server.

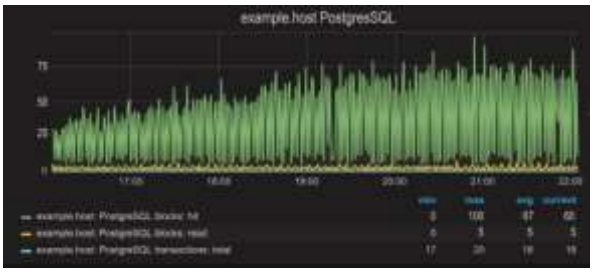
Gambar 10. Akses zabbix

Sistem *monitoring* ini sangat penting pada komunikasi *hybrid* dihadapkan dengan jumlah pengguna yang cukup banyak. Operator akan menerima notifikasi ketika

server kelebihan hak akses. Dengan demikian komunikasi menjadi lancar karena apabila terjadi gangguan operator akan selalu menerima notifikasi dari *zabbix*.

Gambar 11. *Zabbix overload*

Pada grafik pertama menunjukkan jumlah pengguna yang sedang mengakses server mencapai lebih dari 100 pengguna. Grafik menunjukkan warna merah yang berarti server kelebihan pengguna, sehingga mengakibatkan sistem ini mengirimkan notifikasi ke operator tentang keadaan server saat ini agar segera dilakukan perbaikan. Jika tidak segera dilakukan perbaikan oleh operator maka komunikasi tidak akan berjalan dengan lancar.



Gambar 12. *Zabbix* normal

Pada grafik kedua menunjukkan jumlah pengguna yang sedang mengakses server kurang dari 100 pengguna. Grafik menunjukkan warna hijau yang berarti server dalam keadaan normal, sehingga komunikasi dalam keadaan seperti ini aman untuk dalakukan. Sistem tidak akan mengirimkan notifikasi ke operator karena server sedang dalam keadaan yang normal.

PENUTUP

Berdasarkan pengimplementasian alat ini maka peneliti dapat mengambil kesimpulan yaitu system yang telah dibuat mampu untuk membatasi hak akses dan bekerja dengan baik, begitu juga dengan *system monitoring Zabbix* mampu memonitor keadaan server dimana jika server kelebihan pengguna maka server akan mengirimkan notifikasi kepada operator. Saran dari peneliti untuk penelitian selanjutnya adalah perlu dilakukan pembaharuan fitur pada konfigurasi *firewall* agar *system* keamanan bisa mengikuti perkembangan teknologi dan pemakaian *bandwith* agar di perbesar guna memperbanyak pengguna dan meningkatkan kinerja server agar lebih optimal.

DAFTAR PUSTAKA

Sulaiman, Oris Krianto., (2016). Analisis sistem keamanan jaringan dengan menggunakan *switch port security*.

Hananti, Uni., Realize., (2017). Pengaruh penggunaan *IPTables firewall* dan acid terhadap keamanan jaringan.

Siagian, Hary Purmanta., Akbar, M., & Andri., (2018). *Vulnerability assesment* pada web server www.binadarma.ac.id.

Kuswanto, Herman., (2018). Sistem *monitoring* perangkat jaringan menggunakan protocol SNMP dengan notifikasi *email*.

Ocanitra, Ridatu., & Ryansyah, Muhamad. (2019). Implementasi *system* keamanan jaringan menggunakan *firewall security port* pada vitaa multi *oxygen*.