

Implementasi Keamanan Jaringan dan Filtering Web Server Menggunakan *pfSense* Pada PT. Televisi Transformasi Indonesia

Novita Ambarwati Sagala¹, M. Hanif Jusuf²

Jurusan Sistem Informasi, Universitas Indonesia Membangun

E-mail: [1Novitaambarwati61@gmail.com](mailto:Novitaambarwati61@gmail.com), [2hanif26@gmail.com](mailto:hanif26@gmail.com)

ABSTRACT

Network security design is a very important aspect in maintaining the confidentiality and availability of data in an organization. The company is one of the large organizations with many employees. Users can use internet facilities properly, but they can also misuse or accidentally open websites that contain malicious content, and if network security is not maintained, it will disrupt network traffic and company system services. One common method to design network security is to implement a firewall. Therefore, a system is needed to overcome and overcome the misuse of intentional or unintentional user carelessness in the form of network security threats. The system that detects this security intrusion is implemented using the pfSense application as the operating system. pfSense is an application that works as a firewall, pfSense is an open source firewall that has several network features in it. By using pfSense, it is hoped that it will be able to protect vulnerable systems and personal data on the network from unauthorized access, and can better protect the network layer at PT. Televisi Transformasi Indonesia.

Keywords: Firewall, pfSense, Internet.

ABSTRAK

Perancangan keamanan jaringan merupakan aspek yang sangat penting dalam menjaga kerahasiaan dan ketersediaan data dalam suatu organisasi. Perusahaan salah satu organisasi besar dengan karyawan yang terhitung banyak. Pengguna atau user dapat menggunakan fasilitas internet dengan baik, tetapi mereka juga dapat menyalahgunakan atau secara tidak sengaja membuka situs web yang berisi konten berbahaya, dan jika keamanan jaringan tidak dijaga, maka akan mengganggu traffic network dan layanan sistem perusahaan. Salah satu metode umum untuk mendesain keamanan jaringan adalah menerapkan firewall. Oleh karena itu, diperlukan suatu sistem untuk mengatasi dan menanggulangi penyalahgunaan kecerobohan user yang disengaja ataupun tidak sengaja dalam bentuk ancaman keamanan jaringan. Sistem yang mendeteksi gangguan keamanan ini diimplementasikan dengan menggunakan aplikasi pfSense sebagai sistem operasi. pfSense adalah aplikasi yang bekerja sebagai firewall, pfSense merupakan open source firewall yang memiliki beberapa fitur jaringan di dalamnya. Dengan menggunakan pfSense maka diharapkan akan dapat melindungi sistem yang rentan dan data pribadi dalam jaringan dari akses yang tidak sah, dan dapat lebih melindungi lapisan jaringan pada PT. Televisi Transformasi Indonesia.

Kata kunci: Firewall, pfSense, Internet.

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer saat ini menunjukkan bahwa sistem keamanan sangatlah penting bagi suatu sistem jaringan komputer yang terhubung dengan internet, karena internet merupakan suatu jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus ditanggung adalah bagaimana suatu jaminan keamanan bagi jaringan yang terhubung internet.

Akses jaringan internet pada PT.Televisi Transformasi Indonesia (Trans TV) masih sangat rentan dan belum diproteksi dengan baik sehingga user dapat dengan bebas mengakses apa saja di dalam internet dan digunakan secara terus menerus dalam jangka waktu yang lama. Dengan terbukanya akses internet tersebut banyak user atau karyawan yang mengakses konten yang berbau negative dan rentan untuk keamanan jaringan.

Di PT.Televisi Transformasi Indonesia (Trans TV) menggunakan internet dari beberapa ISP yaitu HSP, Iforte dan DIJ. Dan firewall yang digunakan sebelumnya yaitu hanya memfiltering port dan juga link website pada mikrotik di aplikasi winbox. Tetapi dikarenakan lapisan keamanannya hanya pada mikrotik saja maka masih banyak sering terjadi website yang dapat diakses dan mengakibatkan pc user terkena virus atau phising dikarenakan user juga sering kali asal mengklik iklan yang ada pada website tersebut.

Maka dari itu, dengan permasalahan tersebut kemudian dilakukanlah perancangan keamanan jaringan menggunakan pfSense, dengan mengkonfigurasi dan memasukkan daftar ISP yang digunakan agar bisa terpantau aktivitas apa saja yang terjadi dalam jaringan tersebut, lalu mengkonfigurasi DNSBL untuk filtering link dan ip website yang dapat di akses untuk semua network yang ada pada PT.Televisi Transformasi Indonesia (Trans TV) agar dapat melindungi jaringan internet baik dengan menyaring, membatasi atau bahkan menolak suatu hubungan dari luar kedalam ataupun dari dalam keluar.

1.1 Perumusan Masalah

Bagaimana merancang keamanan jaringan pada PT.Televisi Transformasi Indonesia (Trans TV) menggunakan pfSense ?

1.2 Tujuan Penelitian

Melakukan perancangan keamanan jaringan menggunakan firewall pfSense dengan cara memfiltering akses website dan memonitoring jaringan pada PT.Televisi Transformasi Indonesia (Trans TV)

2. METODE PENELITIAN

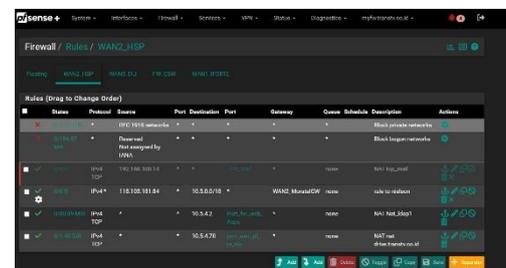
Metode penelitian merupakan kerangka pemikiran yang digunakan untuk melakukan riset. Penulis menggunakan metode pengumpulan data melalui migrasi data yang sudah ada pada mikrotik (winbox) sebelumnya, dan melakukan implementasi pada sistem pfSense

3. HASIL DAN PEMBAHASAN

Pada tahap pengujian pertama peneliti menginstall pfSense pada server, kemudian mengkonfigurasi IP Address, setting user dan password kemudian melakukan konfigurasi firewall pada menu rules untuk akses apa saja yang diizinkan pada jaringan internet dan melakukan filtering.

1. Konfigurasi Rules Wan_HSP

Berikut adalah tampilan konfigurasi WAN pada HSP:



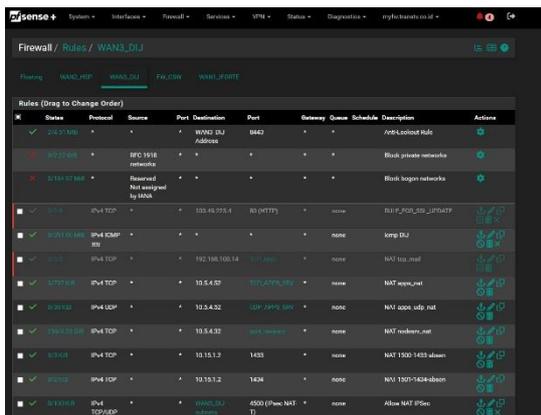
Gambar 1 Konfigurasi WAN_HSP

Berdasarkan gambar di atas, dapat terlihat bahwa ada beberapa akses yang diblok

seperti private network dan bogon network. Lalu ada juga akses yang diizinkan seperti contohnya adalah Nat_ldap1 yang artinya adalah mengizinkan akses untuk membuka email yang disimpan dalam server ldap1 dan memiliki ip 10.5.4.2.

2. Konfigurasi Rules Wan_DIJ

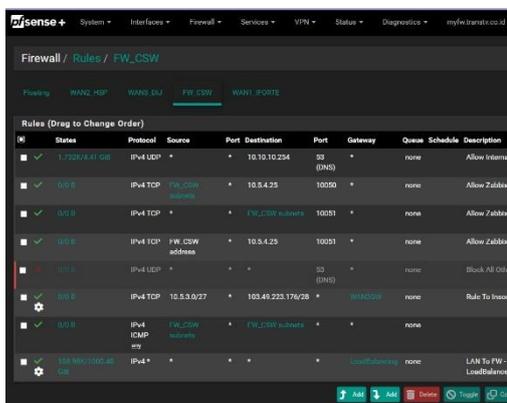
Berikut adalah tampilan konfigurasi WAN pada DIJ:



Gambar 2 Konfigurasi WAN_DIJ

Berdasarkan gambar di atas, rules pada ISP DIJ ini dikonfigurasi beberapa server yang ada pada PT.Televisi Transformasi Indonesia untuk mendapatkan akses untuk user yang menggunakan ISP DIJ. Contohnya seperti memberi akses pada server absensi yang ada pada PT.Trans TV.

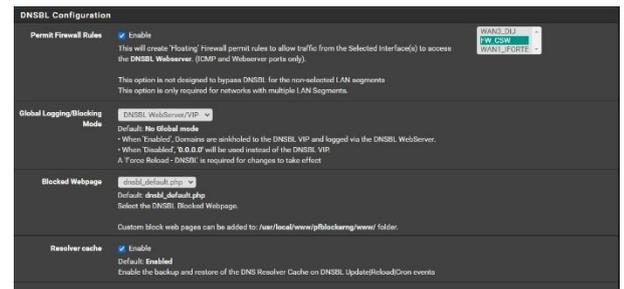
3. Konfigurasi Rules FW_CS



Gambar 3 Konfigurasi FW_CS

Berdasarkan gambar di atas, konfigurasi pada FW_CS selaku core switch pada PT.Televisi Transformasi Indonesia membuat blok kepada dns yang ada diluar jaringan, dan mengizinkan internal DNS, dan beberapa server yang memang tersambung pada jaringan core switch.

4. Konfigurasi DNSBL



Gambar 4 Konfigurasi DNSBL

Berdasarkan gambar diatas, saya memulai untuk melakukan filtering website apa saja yang dapat di akses oleh para user, pada DNSBL ini merupakan salah satu fitur yang ada pada pfSense yang mampu untuk membuat whitelist yang dimasukkan di dalamnya agar dapat diakses oleh user. Gambar diatas saya melakukan enable firewall terlebih dahulu pada jaringan FW_CS yaitu core switch.

5. Konfigurasi DNSBL Whitelist



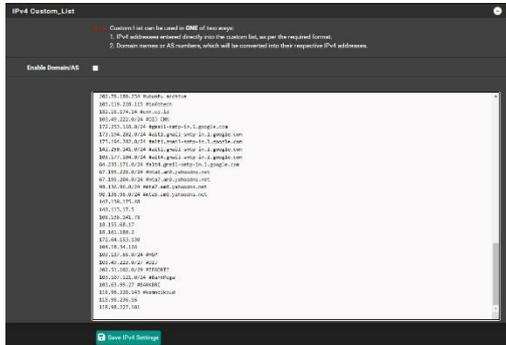
Gambar 5 Konfigurasi Whitelist

Berdasarkan gambar diatas, dibuatlah beberapa whitelist website yang dapat diakses oleh user. Dan saya membuat contoh yaitu saya memasukkan link website group

kemdikbud.go.id pada whitelist tersebut agar dapat diakses oleh seluruh user.

b. Website domain kemdikbud setelah dimasukkan kedalam whitelist

6. Konfigurasi IP Whitelist

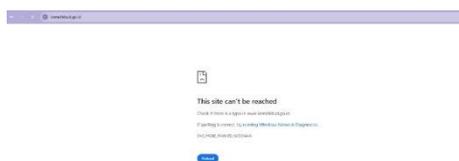


Gambar 6 Konfigurasi IP Whitelist

Berdasarkan gambar di atas, merupakan tampilan dari bagian IP beberapa website yang sudah dimasukkan kedalam DNSBL Whitelist sebelumnya. Agar dapat diakses tidak hanya link website nya saja yang dimasukkan, tetapi IP Address website tersebut pun harus dimasukkan. Contohnya saya memasukkan IP Address kemdikbud agar dapat diakses.

7. Tampilan Website

a. Website domain kemdikbud saat belum dimasukkan kedalam whitelist



Gambar 7 Website Can't Be Reached

Berdasarkan gambar di atas, menampilkan bahwa saat sebelum link domain kemdikbud.go.id belum dimasukkan kedalam whitelist DNSBL dan IP. Website tersebut tidak dapat diakses.



Gambar 8 Website Can Be Open

Berdasarkan gambar di atas, contoh tampilan pada saat alamat website dan IP sudah dimasukkan ke dalam whitelist DNSBL. Website tersebut sudah dapat diakses sesuai dengan yang telah di konfigurasi sebelumnya.

4. KESIMPULAN DAN SARAN
Kesimpulan

Keamanan Jaringan yang dilakukan oleh PT Televisi Transformasi Indonesia (Trans TV) masih belum efektif yaitu hanya menggunakan satu lapisan saja di mikrotik yang mengakibatkan masih banyak user yang masih dapat membuka website atau port yang negative ataupun membawa virus untuk pc user. Maka untuk memperkuat lapisan keamanan jaringan yang dimiliki oleh PT Televisi Transformasi Indonesia (Trans TV) yaitu menggunakan aplikasi open source yang bernama pfSense yang dimana didalam aplikasi tersebut banyak sekali fitur yang dapat digunakan seperti memonitoring jaringan, memblokir link atau pun port yang berbahaya bagi user maupun server, dan membuat whitelist untuk link dan port apa saja yang dapat diakses oleh semua user. Hal ini akan sangat membantu untuk melindungi keamanan jaringan pada perusahaan dan agar user pun tidak sembarangan membuka website yang menyebabkan pc user terkena virus ataupun phishing yang pastinya akan sangat bahaya untuk keamanan data yang dimiliki oleh perusahaan.

Saran

Agar implementasi ini dapat diterapkan dan supaya tujuan yang diharapkan dapat terwujud dengan baik maka ada beberapa hal yang harus diperhatikan :

1. Di perlukan adanya sosialisasi kepada user bahwa aka nada sistem dan kebijakan baru bahwa aka nada firewall yang akan membatasi hal yang mereka browsing.
2. Pada masa yang akan dating mungkin sistem ini akan dikembangkan lagi untuk keamanan jaringan lebih luas lagi.
3. Sehingga penerapan dalam penggunaan sistem dapat bermanfaat sesuai dengan yang diharapkan.

UCAPAN TERIMAKASIH

Saya Novita Ambarwati Sagala selaku penulis mengucapkan terimakasih kepada PT Televisi Transformasi Indonesia (Trans TV) karena saya diberi kesempatan untuk membuat implementasi ini pada ruang lingkup perusahaan sehingga saya dapat menuliskan dan menyelesaikan Tugas Akhir ini.

DAFTAR PUSTAKA

- [1] "Pengertian Firewall dalam Jaringan Komputer dan Jenis-Jenisnya." Accessed: Nov. 11, 2024. [Online]. Available: <https://it.telkomuniversity.ac.id/pengertian-firewall-dalam-jaringan-komputer-dan-jenis-jenisnya/>
- [2] "What is a Firewall? | Firewall Definition - Palo Alto Networks." Accessed: Nov. 11, 2024. [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall>
- [3] Sutarti, A. P. Pancaro, and F. I. Saputra, "Implementasi IDS (Intrusion Detection System) pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 2–3, 2018.
- [4] M. Arman and N. Rachmat, "Implementasi Sistem Keamanan Web Server Menggunakan Pfsense," *Jusikom J. Sist. Komput. Musirawas*, vol. 5, no. 1, pp. 13–23, 2020, doi: 10.32767/jusikom.v5i1.752.
- [5] A. W. N. Sholihan, A. R. Mukti, S. Suryayusra, and R. N. Dasmen, "Implementation of Network Security and Anticipating Attackers Using pfSense Firewall," *CESS (Journal Comput. Eng. Syst. Sci.)*, vol. 8, no. 1, p. 175, 2023, doi: 10.24114/cess.v8i1.42377.
- [6] K. Pada *et al.*, "BAB V," pp. 71–72.
- [7] M. Iqbal *et al.*, "Implementasi Pfsense-Snort Pada Sistem Pencegahan Intrusi," *J. Inform. Softw. dan ...*, vol. 4, no. 2, pp. 1–5, 2023, [Online]. Available: <https://www.jurnal.dccpringsewu.ac.id/index.php/ji/article/view/53>