DECODE: Jurnal Pendidikan Teknologi Informasi
ISSN Cetak : 2775-2984 | ISSN Online : 2775-1813
Vol. 2, No. 1, Maret 2022, Hal: 1-7, Doi: http://dx.doi.org/10.51454/decode.v2i1.29
http://journal.umkendari.ac.id/index.php/decode

PENERAPAN KEAMANAN JARINGAN MENGGUNAKAN METODE FIREWALL SECURITY PORT

Rahmat Novrianda Dasmen[1)*], M. Hendra Firmansyah[1)], M. Khadafi[1)], Tri Yolanda[1)]
[1]Universitas Bina Darma, Palembang, Indonesia
Email: rahmat.novrianda.d@gmail.com

Abstrak

Penerapan keamanan jaringan dalam menggunakan *security port* berguna untuk memblok akses jaringan, memantau dan mencegah terjadinya pencurian data oleh pihak yang tidak bertanggung jawab atau bukan dari pihak yang berwenang dalam pengguna hak akses. Tujuan dari penelitian ini adalah untuk mengantisipasi dan mengamankan jaringan lokal terhadap ancaman maupun serangan dalam jaringan. Penerapan *port security* terbilang cukup mempuni dalam keamanan serta biaya yang perlu dikeluarkan cukup minim. Metode yang digunakan dalam penelitian ini adalah metode *action research* dimana metode ini akan memberikan tahapan untuk mengklasifikasikan proses penelitian. Berdasarkan hasil penerapan yang dilakukan, dapat diambil suatu kesimpulan bahwa dengan menerapkan metode *firewall security port* setidaknya dapat mengantisipasi suatu permasalahan dalam sistem jaringan komputer dan lebih meningkatkan kualitas keamanan jaringan itu sendiri. Demi menjaga kemanan jaringan yang lebih handal, perlu kegiatan memperbaharui sistem keamanan jaringan dan selalu memantau jika adanya titik lemah yang terdapat pada sistem keamanan jaringan, sehingga dapat bertindak cepat dalam memperbaiki keamanan jaringan tersebut.

Kata kunci: firewall; keamanan; jaringan; security port.

NETWORK SECURITY IMPLEMENTATION USING FIREWALL SECURITY PORT METHOD

Abstract

The application of network security in using security ports is useful to block network access, monitor and prevent the theft of data by irresponsible parties or not from the authorities in the user's access rights. The purpose of the study was to anticipate and secure local networks against threats and attacks within the network. The application of port security is quite successful in security and the costs that need to be incurred are quite minimal. The method used in this research is an action research method where this method will provide a stage to classify the research process. Based on the results of the application carried out, it can be concluded that by applying the firewall method security port can at least anticipate a problem in the computer network system and further improve the quality of network security itself. In order to maintain more reliable network security, it is necessary to update the network security system and always monitor if there are weak points contained in the network security system, so that it can act quickly in improving the security of the network.

Keywords*: firewall; security; network; security port.*

Submitted:	Reviewed:	Accepted:	Published:
22 Januari 2022	19 Februari 2022	19 Maret 2022	19 Maret 2022

PENDAHULUAN

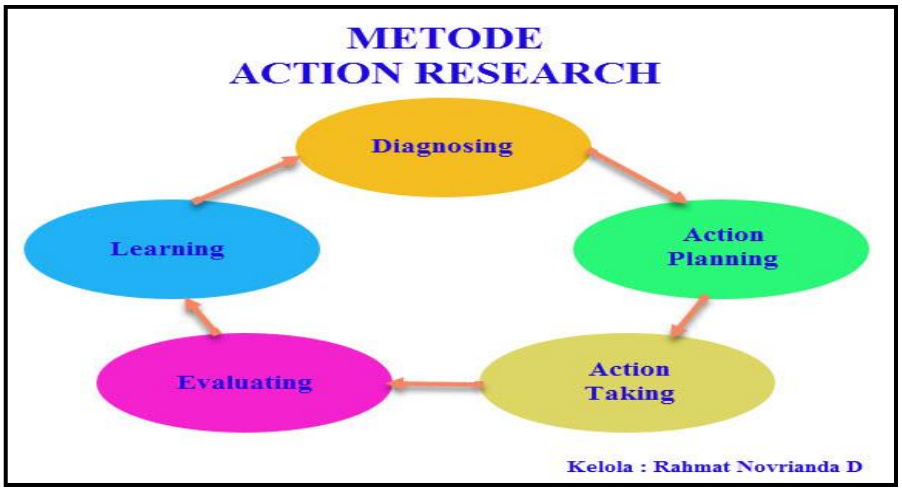
Peningkatan akses jaringan komputer tentunya bermanfaat bagi para pendidik, perusahaan dan perkantoran untuk mempermudah pekerjaan. Namun ada satu hal yang penting dalam mengelola sebuah jaringan komputer yaitu keamanan jaringan itu sendiri. Banyaknya jumlah pengguna yang mengakses jaringan, maka potensi pelaku kejahatan *cyber* akan meningkat, mulai dari pencurian data hingga peretas yang dapat memasuki akses jaringan (Sutiman & Gunawan, 2021). Ada banyak teknik yang dapat digunakan untuk mengurangi kejahatan pada jaringan ini. Salah satu teknik yang paling populer untuk mengamankan jaringan lokal adalah penggunaan *port security*, teknik yang memungkinkan siapa saja yang berhak memiliki akses untuk mengakses jaringan melalui *port* yang terhubung di *switch* (Sulaiman, 2016). *Port security* berfungsi sebagai sistem keamanan jaringan untuk menghindari koneksi jaringan dari akses yang tidak berkepentingan (Ocanitra & Ryansyah, 2019).

Pada setiap perusahaan maupun perkantoran, sering terjadi perubahan lokasi ruang kerja, serta kehadiran karyawan baru. Adanya perubahan ini membuat perusahaan atau perkantoran harus melakukan registrasi ulang pekerjaan karyawannya, sehingga sangat perlu mengamankan jaringan pada setiap *port Local Area Network* (LAN) dengan menggunakan *secure standard* atau *static port security sticky* pada tiap *port* yang terhubung ke ruang kerja. Metode ini berguna untuk memblokir akses jaringan bagi karyawan yang tidak melaporkan relokasi ruang kerja atau tidak memiliki akses ke fasilitas baru. Hal ini tentu saja dapat mencegah pelanggaran data oleh orang asing atau karyawan perusahaan (Sudaryanto, 2018).

Demi membangun keamanan suatu jaringan sistem komputer tidak cukup dengan penggunaan keamanan yang disediakan oleh vendor yang biasanya ada pada system operasi windows server, dimana pihak microsoft menyediakan (*windows firewall with advanced security*) (Zakir, 2015). Penulis menyarankan agar setiap pengguna jaringan lokal menambahkan keamanan jaringan komputer. Salah satunya dengan memberikan *security port* standar/statis (kemampuan untuk mendaftarkan dan membatasi perangkat yang dapat terhubung ke *port switch*), dan kemampuan *switch* yang dapat mengenali *Mac Address* (konversi alamat MAC) untuk mengenali setiap perangkat yang terhubung dan memblokir alamat *Mac* yang tidak terdaftar di setiap *port* (Fikri & Djuniadi, 2021). Dalam menerapkan jenis *security port*, tentunya penulis juga mencari dari berbagai sumber yang terkait agar nantinya dalam penerapan ini akan menghasilkan suatu permasalahan yang bisa diatasi dengan tepat dan signifikan.

METODE

Pada manajemen jaringan penulis menerapkan keamanan jaringan komputer dengan memberikan keamanan *port security* (kemampuan untuk mendaftar dan beralih untuk membatasi perangkat yang terhubung ke *port*). Disini kami menggunakan metode *Action Research* dengan *Flowchart* sebagai berikut:



Gambar 1. Flowchart Action Research (Dasmen & Khudri, 2021)

Metode ini akan memaparkan kronologi penelitian, termasuk desain penelitian, prosedur penelitian (Algoritma, Pseudocode atau lainnya), eksperimen, dan pengumpulan data. Untuk dapat dikatakan ilmiah, definisi program peneliti harus didukung dari beberapa referensi (Rasmila & Amalia, 2019).

Tahapan *diagnosing* merupakan tahapan awal dalam penelitian ini untuk mendiagnosa manajemen keamanan jaringan yang akan digunakan. Hasil diagnosa menunjukkan manajemen keamanan jaringan yang akan diterapkan ialah jenis *security port* yang merupakan suatu teknik yang berfungsi untuk mengamankan jaringan dan memungkinkan akses melalui *port* yang ada pada *switch* dengan pengawasan dari pihak IT (*Information Technology*). Hal ini memastikan bahwa semua karyawan di perusahaan akan memberitahu ketika ada perubahan di ruang kerja atau ketika ada karyawan baru yang ingin menggunakan akses jaringan, karena akses yang mereka gunakan akan otomatis terblokir jika tidak adanya laporan. Perangkat baru yang menghubungkan ke *switchport* diblokir oleh *port security* dan Pihak IT (*Information Technology*) dapat mengontrol dan menyatakan bahwa jaringan yang digunakan untuk kepentingan perusahaan saja. Penulis menyarankan untuk tetap menggunakan semua infrastruktur yang ada menggunakan VLAN (*Virtual Local Area Networks*) (Kurniati & Dasmen, 2019). VLAN dapat membagi jaringan menjadi banyak *subnet*, dan setiap partisi memiliki beberapa keunggulan VLAN seperti keamanan data, penghematan *bandwidth*, dan VLAN memudahkan untuk mengelola jaringan yang ada (Nitra & Ryansyah, 2019).

Tahapan kedua adalah *Action Planning*, Dalam tindakan ini, penulis mencoba menggambarkan pada aplikasi perangkat lunak emulator dalam bentuk simulasi aplikasi jaringan. *Software* yang kami gunakan adalah *Cisco Packet Tracer* yang mana software ini yang akan memudahkan dalam implementasi suatu jaringan (Dasmen & Rasmila, 2019).

Tahapan ketiga adalah *Action Taking*, dimana pada tahapan ini pengujian keamanan jaringan awal dilakukan dengan menguji konektivitas jaringan antara klien dan perangkat yang digunakan oleh komputer dengan VLAN yang berbeda. Pada pengujian pertama, perangkat yang digunakan sudah dikonfigurasi dan pada *switch* dikonfigurasi tanpa menggunakan *port security* (Dewanto, 2015).

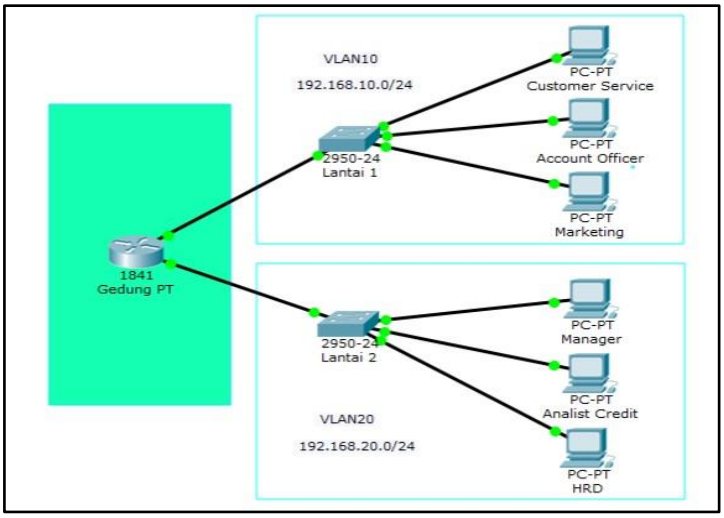
Tahapan keempat adalah Evaluating. Saat mengamankan jaringan dengan *port security* yang digunakan, dalam hal ini penggunaannya sangat penting, karena setiap perangkat pengguna sudah diketahui tentang *MAC-Address* nya dan dijelaskan di *port* yang digunakan. Ini akan lebih aman ketika mengakses jaringan yang ada. *MAC-Address* inilah yang nanti berfungsi pada *port switch* jika tidak terdaftar maka secara otomatis akan terblok oleh *port security* (Sulaiman, 2016).

Tahapan kelima adalah *Learning*, dimana *switch* yang digunakan dikonfigurasi *port security* kemudian dilakukan proses pengujian, menggunakan satu *switch* per lantai dan terhubung beberapa perangkat *client* dibeberapa ruang kerja setiap lantai. Semua *switch* dikonfigurasi dengan *security port*. Pengoperasian dilakukan dengan mengkonfigurasi *switch* yang digunakan, dan tiap *port* yang telah dikonfigurasi akan memblok ketika adanya perangkat baru maupun tidak dikenal yang akan mengakses jaringan tersebut. Maka permasalahan ini akan bisa diatasi oleh pihak yang mengelola dan bertanggung jawab atas akses jaringan.

HASIL DAN PEMBAHASAN

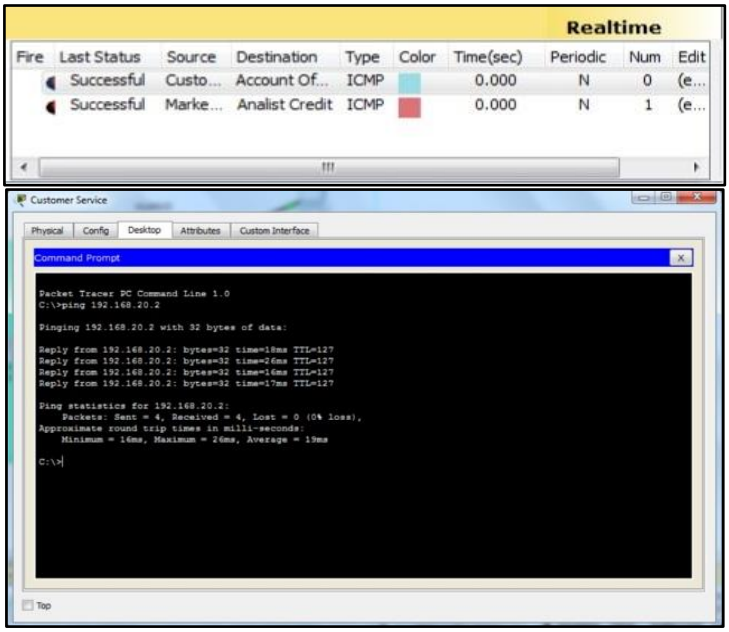
Penerapan keamanan yang akan kami implementasikan ialah dengan menggunakan metode *firewall security port*. Dimana metode ini akan memberikan keamanan pada akses jaringan sekaligus teknik yang akan mengizinkan hak akses melalui *port* yang tersedia pada tiap *switch* dan bisa dipantau oleh orang yang bertanggung jawab atas pengelolaan jaringan tersebut. Hal inilah yang akan membuat semua pengguna yang berada pada jaringan lokal dapat memberikan informasi jika terjadi perpindahan ruang kerja atau ada karyawan baru yang akan mengakses jaringan tersebut, karena secara otomatis hak akses pada perangkat baru yang akan dihubungkan ke *port switch* akan di *block* oleh *port security*. Jadi pihak IT dapat mengontrol dan memastikan bahwa akses jaringan pada gedung hanya digunakan untuk kepentingan perusahaan.

Topologi jaringan pada implementasi ini, kami menggambarkan simulasi jaringan dengan menggunakan jaringan pada dua lantai, dimana pada tiap *switch* terhubung dengan beberapa PC *client* yang berbeda ruangan. Disini kami menggambarkan dalam bentuk simulasi jaringan tersebut menggunakan *software Cisco Packet Tracer*.



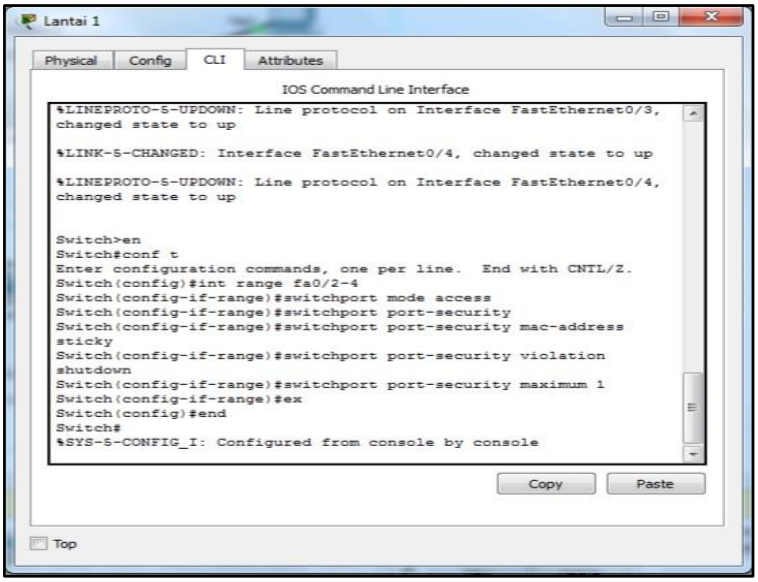
Gambar 2. Topologi Jaringan Dua Lantai

Simulasi jaringan awal sebelumnya penulis sudah mengkonfigurasi (*routing*, *switching*) seluruh perangkat agar jaringan tersebut bisa terhubung dan juga menerapkan VLAN pada tiap *switch*. Akan tetapi *switch* yang dikonfigurasi belum menerapkan/ mengunakan *security port*. Untuk pengujian tes nya kita coba menggunakan pengiriman Pesan/Data pada tiap-tiap PC yang terhubung ke *router* dan juga test ping dr PC CS Lantai 1 Ke PC Manager Lantai 2, untuk memastikan proses jaringan telah terhubung.



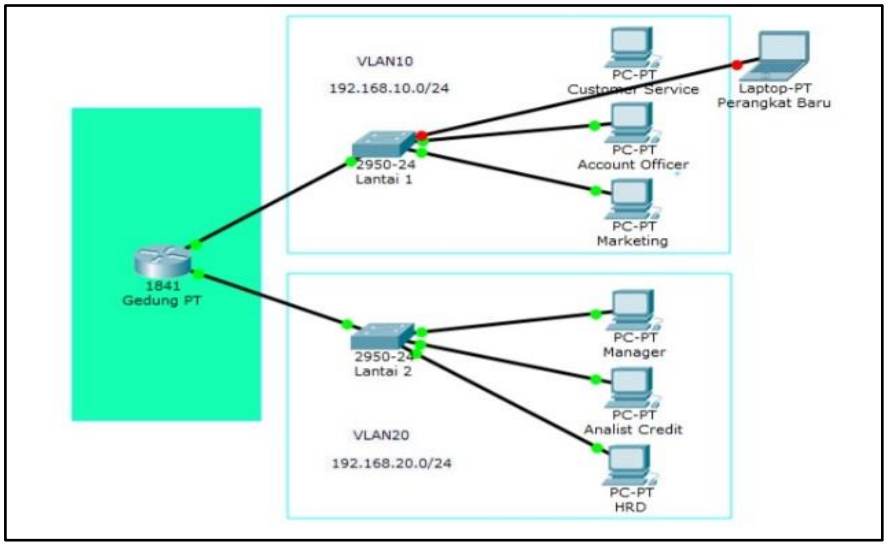
Gamabar 3. Test Jaringan

Jika semua perangkat sudah terhubung selanjutnya penulis akan menerapkan Port Security, penerapan keamanan jaringan mengunakan *Security port* pada setiap *switch* cara konfigurasinya sama. Hanya memberikan perintah *mac-address port security sticky*. Berikut tahapan konfigurasinya pada gambar 4.



Gambar 4. Konfigurasi *Port Security*

Untuk tes nya, kita meletakkan satu Laptop (perangkat baru) anggap saja laptop dari karyawan baru ataupun seseorang yang ingin memasuki akses jaringan (pengguna tidak dikenal). Kemudian ia mencabut salah satu kabel koneksi dari *PC* yang terhubung ke *switch* dan meletakkan ke perangkat baru nya serta mengkonfigurasi atau memasukkan alamat IP yang sama.



Gambar 5. Koneksi Perangkat Baru

Pada gambar 5, tepatnya pada lantai 1 kita dapat melihat *port* yang tersambung ke perangkat baru berwarna merah yang artinya, akses jaringan pada perangkat tersebut tidak terkoneksi walaupun mengkonfigurasi alamat IP yang sama, karena *port* pada *switch* akan otomatis *shutdown* jika ada perangkat yang tidak dikenal terkoneksi tidak sesuai dengan *mac-address* nya.

KESIMPULAN DAN SARAN

Penentuan jenis *firewall* sangat berpengaruh pada sistem keamanan jaringan, oleh karena itu penulis memilih terhadap jenis *port security* karena jenis ini mudah dalam konfigurasi dan pihak yang mengelola bisa mendapatkan informasi terhadap jaringan lokal. Pemanfaatan *security port*, maka sistem keamanan jaringan yang dikelola lebih efisien sekaligus menghindari koneksi jaringan dari akses yang tidak berkepentingan, serta menjaga data-data menjadi lebih aman. Penerapan metode *security port* dapat mengatur lalu lintas jaringan yang dizinkan, maka pihak yang bertanggung jawab atas jaringan (IT) dapat memanajemen setiap pengguna jaringan atas hak akses yang terkena *block*. *Firewall* dapat mengoptimalisasikan jaringan sehingga dapat membentengi ancaman-ancaman maupun serangan yang terjadi di dunia internet.

Saran yang dapat penulis sampaikan adalah dalam artikel ini membahas mengenai *firewall* yang digunakan sebagai system kemanan pada akses jaringan komputer dengan metode *security port* serta penerapan *firewall* mengenai konfigurasi *firewall* pada jaringan komputer, yang kemudian nanti diharapkan dapat menjadi bahan referensi mengenai *firewall* terutama jenis *security port*.

DAFTAR PUSTAKA

Dasmen, R. N., & Khudri, A. (2021). Optimasi Jaringan Wireless PT. TASPEN dengan RADIUS Server dan Firewall Filter Rules. *Techno.COM*, *20*(1), 134-146.

Dasmen, R. N., & Rasmila. (2019). Rancang Bangun VLAN pada Jaringan Komputer RRI Palembang dengan Simulasi Cisco Packet Tracer. *Jurnal Teknologi*, *11*(1), 47-56.

Dewanto, Y. (2015). Konfigurasi VLAN pada Cisco Switch di Gedung Indosat dengan Menggunakan Program Simulasi. *Jurnal TICom*, *3*(3), 1-5.

Fikri, K. Al, & Djuniadi. (2021). Keamanan Jaringan Menggunakan Switch Port Security. *InfoTekJar: Jurnal Nasional Informatika Dan Teknologi Jaringan*, *5*(2), 302-307.

Kurniati, & Dasmen, R. N. (2019). The Simulation of Access Control List (ACLs) Network Security for Frame Relay Network at PT. KAI Palembang. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, *10*(1), 49-61.

Nitra, R. O., & Ryansyah, M. (2019). Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *7*(1), 52. https://doi.org/10.26418/justin.v7i1.29979

Rasmila, & Amalia, R. (2019). Sistem Informasi Penentuan Persiapan Stok Obat menggunakan Weight Moving Average. *SISTEMASI: Jurnal Sistem Informasi*, *8*(3), 465-478.

Sudaryanto. (2018). Implementation Port Security for Security Systems Network at the Computing Laboratory of Adisutjipto College of Technology. *Conference SENATIK ITDA*, 257-265.

Sulaiman, O. K. (2016). Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. *CESS (Journal Of Computer Engineering, System And Science)*, *1*(1), 9-14.

Sutiman, & Gunawan, A. (2021). Firewall Port Security Switch untuk Keamanan Jaringan Komputer menggunakan Cisco Router. *CONTEN: Computer and Network Technology*, *1*(1), 13–22.

Zakir, S. (2015). *Optimalisasi Windows Firewall With Advanced Security Dalam Membangun Keamanan Jaringan* (Skripsi). Retrieved from http://repo.iainbukittinggi.ac.id/150/

How to cite:
Dasmen., R. N., Firmansyah, M. H., Khadafi. M., & Yolanda. T. (2022). Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port. *DECODE: Jurnal Pendidikan Teknologi Informasi, 2(1),* 1-7. DOI: http://dx.doi.org/10.51454/decode.v2i1.29