CONTEN : Computer and Network Technology
Vol. 1, No. 1, Juni 2021, hlm. 13-22
ISSN: 2797-5274

FIREWALL PORT SECURITY SWITCH UNTUK KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN *CISCO ROUTER* 1600S PADA PT. TIRTA KENCANA TATA WARNA SUKABUMI

Sutiman[1] A.Gunawan[2]

[1]Program Studi Ilmu Komputer, Universitas Bina Sarana Informatika
[2]Program Studi Ilmu Komputer, Universitas Bina Sarana Informatika
Email: [1]tirman212@gmail.com [2]a.gunawan.agn@bsi.ac.id

Abstrak

Perkembangan teknologi informasi saat ini sangat cepat akses kirim mengirim data tidak terhalang jarak dan waktu, aset kekayaan insfratuktur tidak berupa jalanan fisik tetapi berupa sebuah jaringan yang saling terhubung satu sama lain yang dibuat teknologi itu sendiri untuk saling memudahkan akses data, komunikasi, saling bertukar informasi, sehingga jaringan menjadi sebuah kebutuhan sehari-hari untuk beraktivitas menjalankan kegiatan sehari-hari. Pada peradaban saat ini para ilmuan berupaya untuk terus melakukan pengembangan revolusi dari teknologi itu sendiri yang aksesnya adalah menggunakan jaringan, sudah terbukti seperti perusahaan amazone, alibaba, ebay, facebook, google dan lain-lain. Yang berperan aktiv memakai teknologi jaringan komputer menjadikan mereka sebuah perusahaan raksasa yang memiliki kekayaan luar biasa, di Indonesia pun ada beberapa perusahaan yang sukses seperti kaskus, gojek dan yang lainnya. Pada studi kasus penulis melakukan sebuah penelitian yang meliputi banyak teknik untuk analisa sebuah jaringan di perusahaan PT. Tirta Kencana Tata Warna yang berlokasi di sukabumi, perusahaan tersebut memakai jaringan MAN (*Metropolitan Area Network*) untuk akses informasi pertukaran data, sehingga penulis melakukan sebuah analisis untuk melakukan perbaikan sebagai keamanan jaringan dari perusahaan tersebut. Tujuannya adalah meningkatkan kualitas dari jaringan PT. Tirta Kencana Tata Warna Sukabumi untuk keamanan jaringannya.

Kata Kunci : *Firewall*, *Port Security Switc, Router 1600S*

Abstract

The development of information technology at this time is very fast access to send send data unhindered distance and time, infrastructure assets are not in the form of physical roads but in the form of a network that is connected to each other made the technology itself to facilitate data access, communication, information exchange , so that the network becomes a daily necessity for activities to carry out daily activities. In the current civilization, scientists are trying to continue to develop a revolution of the technology itself whose access is to use the network, it has been proven as an Amazon company, Alibaba, eBay, Facebook, Google and others. The active role of using computer network technology makes them a giant company that has extraordinary wealth, in Indonesia there are also some successful companies such as kaskus, gojek and others. In the case study the authors conducted a study which included many techniques for analyzing a network in the company PT. Tirta Kencana Tata Warna, which is located in Sukabumi, the company uses a MAN (Metropolitan Area Network) network to access data exchange information, so the authors conducted an analysis to make improvements to the network security of the company. The aim is to improve the quality of PT. Tirta Kencana Tata Warna Sukabumi for network security.

Keywords*: Firewall, and Port Security Switch, Router 1600S*

1. PENDAHULUAN

Jaringan komputer dapat dikatakan sebagai sebuah sistem yang terdiri dari berbagai komputer beserta *resource*-nya yang didesain agar dapat menggunakan sumber daya yang ada, sehingga dapat mengakses informasi yang diperlukan (Afrianto & Setiawan, 2015). Jaringan komputer memiliki peran penting karena di jaman sekarang jaringan sangat dibutuhkan untuk kegiatan konektivitas antar manusia.

Peran jaringan di berbagai aspek konektivitas sangat membantu untuk proses berjalannya hubungan komunikasi antara satu sama lain, sehingga banyak perusahaan yang manual beralih menggunakan jaringan komputer untuk kepentingan bisnis.

Tetapi pada jaringan komputer tentunya dibutuhkan beberapa *management* untuk merawat dan melindungi data perusahaan agar data perusahaan tidak bocor keluar, dalam hal ini perusahaan harus benar-benar serius agar jaringan komputer di perusahaan tersebut tidak mudah di retas dari dalam maupun dari luar.

Selain melindungi dari ancaman *Cyber Crime* Menurut Krianto Sulaiman (2016), Salah satu faktor yang mempengaruhi kualitas dalam jaringan adalah *network security* atau keamanan jaringan, banyak teknik yang dapat dilakukan dalam meningkatkan keamanan jaringan, baik dengan membangun sistem *firewall*, dengan menggunakan *layer 7 protocol* maupun dengan *port security*, *port security* memanfaatkan *port-port* yang ada untuk mengizinkan akses ke jaringan.

Seperti perusahaan yang saat ini menjadi tempat penulis riset yaitu PT. TIRTA KENCANA TATA WARNA sukabumi perusahaan ini telah menggunakan sistem jaringan komputer yang sudah terintegrasi dengan internet dan di tempat perusahaan dibangun topologi jaringan MAN (*Metropolitan Area Network*) untuk akses data yang terintegrasi dengan server komputer setiap cabang perusahaan sehingga memudahkan para pekerja untuk kepentingan data.

Setelah dilakukan analisa terkait keamanan jaringan, arsitektur jaringan dan desain jaringan ditempat riset penulis mendapatkan beberapa permasalahan diantaranya jaringan tersebut masih tidak ada kemanan jaringan *firewall* sehingga siapapun pengguna masih bisa keluar masuk dengan akses yang sama, dalam arsitektur jaringan tersebut yang meliputi pengalamatan *ip address* belum dilakukannya *subneting* hal ini berpengaruh pada pembatasan jumlah *host*, desain server perangkat setiap cabang masih belum terealisasi dengan maksimal sehingga mengakibatkan pemborosan biaya pembelian perangkat keras *server* di setiap cabang perusahaan dan *security port* untuk keamanan pada setiap switch agar tidak sembarang pc lain mengakses pada port yang telah ditetapkan.

2. METODE PENELITIAN

Dalam pelaksanaan proses pengumpulan data yang lengkap dan akurat dilakukan beberapa metode yaitu :

a. Observasi
   Melakukan pengamatan langsung atau peninjauan secara cermat di lokasi tempat penelitian penulis riset.
b. Wawancara
   Melakukan tanya jawab mengenai keluhan dan kebutuhan secara langsung kepada *admistrator* dan *user* untuk mengetahui kebutuhan apa saja yang harus di perbaiki pada jaringan komputer di perusahaan tersebut.
c. Studi Pustaka
   Melakukan pencarian terhadap teori terkini yang merujuk dan menunjang penelitian yang penulis buat.

2.1. Analisa Penelitian

a. Analisa Kebutuhan
   Dari analisa kebutuhan yang sudah ada dilakukan dengan metode pengumpulan data penulis membuat catatan untuk di carikan sebuah solusi yaitu dengan penerapan sistem *firewall* pada beberapa *router cisco* yang terhubung di jaringan komputer perusahaan tersebut, melakukan *seting ip address* terkait arsitektur jaringan, melakukan desain *server* agar penggunaan perangkat keras maksimal dalam penggunaannya dan *security port* pada *switch* untuk keamanan *port* pada setiap cabang.
b. Desain Jaringan
   Setelah melakukan analisa kebutuhan dari *administrator* dan *user* selanjutnya penulis melakukan tahap desain jaringan untuk membuat sebuah jaringan MAN (*Metropolitan Area Network*) yang sesuai dengan kebutuhan yang perusahaan minta dan dilengkapi sistem keamanan jaringannya. Adapun usulan yang diberikan berupa desain mengenai perangkat, topologi, skema, metode dan konsep yang akan digunakan (Rahman, 2018).
c. *Testing*

 ISSN: 2797-5274

Setelah desain skema jaringan baru selesai dibuat lalu melakukan tahap *testing* dengan menggunakan *virtual* jaringan seperti *Paket Tracer* untuk menguji sebelum tahapan implementasi, di *mode* bagian ini dilakukan uji *testing* jaringan menggunakan perintah (*ping, traceroute*, atau program lainnya).

d. Implementasi
Pada tahapan ini adalah bagian dari proses penggabungan topologi fisiknya yang bila sebelumnya hanya simulasi pada *virtual* jaringan untuk melakukan tahap *testing* tetapi bagian implementasi ini adalah penggabungan antara fisik yang sudah ada dengan yang baru yang telah lolos dalam tahap pengujian pada saat *testing*, dari *seting ip, pembatasan ip address, konfigurasi routing switching, desain perubahan server* dan sistem keamanannya meliputi *firewall* dan *security port* nya.

2.2.Ruang Lingkup

Kegiatan penelitan keamanan jaringan komputer milik perusahaan PT. TIRTA KENCANA TATA WARNA ini adalah kegiatan yang dilakukan penulis untuk mempelajari dan analisa sistem keamanan jaringan pokok agar tidak menyimpang dari pokok pembahasan, dari itu pada bagian ini penulis membatasi pembahasan skripsi ini dengan melakukan beberapa pembahasan yang lebih spesifik yaitu meliputi seting *ip address*, pembatasan *ip address*, *konfigurasi routing switching static,* desain perubahan *server* dan sistem keamanan jaringan yaitu *firewall* dan *security port* pada *switch.*

2.3.Keamanan Jaringan

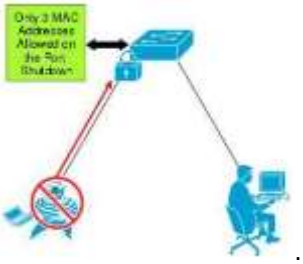
1. FIREWALL

Firewall Adalah suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal. firewall bekerja dengan cara melacak dan mengendalikan (Mohd, 2017).

Gambar 1. *Firewall*

2. Switch Port Security

Sebuah kemampuan *switch manageable* untuk meningkatkan keamanan jaringan dengan menggunakan *port-port* yang tersedia pada *switch* tersebut (Oris, 2016).



Gambar 2. Contoh Gambar *Port Security*

Dari analisa permasalahan jaringan diatas penulis membuat solusi untuk permasalahan jaringan di PT Tirta Kencana Tata Warna yaitu sebagai berikut:

1. Melakukan *subneting* atau pengalamatan sesuai kebutuhan jaringan yang akan diterapkan untuk berapa pengguna *client server* agar tersetruktur rapi dalam pengalamatannya.
2. Menerapkan sistem *firewall* untuk keamanan pada jaringan PT Tirta Kencana Tata Warna.
3. Melakukan perancangan desain perubahan server untuk meminimalisir biaya pembelian perangkat keras server .
4. Menerapkan *security port* pada masing-masing *switch*.

3. HASIL DAN PEMBAHASAN

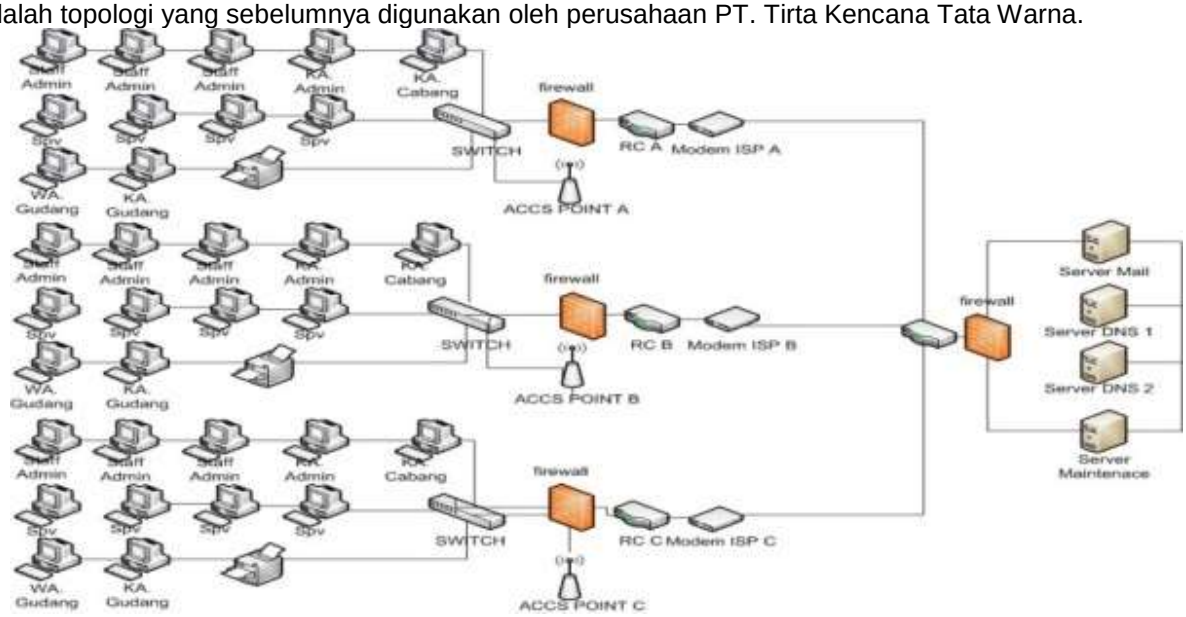
Dari permasalahan yang di uraikan penulis membuat beberapa usulan dan perubahan pada jaringan komputer PT. Tirta Kencana Tata Warna yang meliputi beberapa perubahan yang meliputi subneting *ip*

 ISSN: 2797-5274

address, perubahan desain *server*, implementasi *firewall* dengan cara memanfaatkan fitur *access-list* pada *router cisco* 1600s dan *security port* pada *switch.*

3.1. Topologi Jaringan

Berdasarkan dari hasil analisa dan penelitian penulis terkait kebutuhan akan sumber pemanfaatan jaringan di PT. Tirta Kencana Tata Warna penulis tidak merubah topologi jaringan sebelumnya karena dianggap sudah memenuhi kebutuhan dan efisien untuk keperluan jaringan tersebut. Topologi jaringan star adalah topologi yang sebelumnya digunakan oleh perusahaan PT. Tirta Kencana Tata Warna.



Gambar 3. Topologi Jaringan

3.2. *IP Address*

Pada pengalamatan *ip address* dilakukan beberapa *subneting* atau perubahan pengalamatan untuk membatasi *client* setiap cabang hal ini dilakukan bertujuan untuk membatasi *ip addres* dan penataan alamat *ip address* agar terhindar dari kemacetan lalu lintas dalam jaringan berikut ini adalah data table *subneting ip address* usulan PT. Tirta Kencana Tata Warna :

Table 1. *IP Address* jaringan MAN server

Device	Interface	IP Address	Subnet Mask	Default Gateway
RS	GE 0/0	192.168.10.254	255.255.255.0	N/A
	GE 0/1	10.10.10.1	255.255.255.252	
	GE 0/2	10.10.10.6	255.255.255.252	
	GE 0/3	10.10.10.10	255.255.255.252	
DNS 1	NIC	192.168.10.1	255.255.255.0	192.168.10.254
DNS 2	NIC	192.168.10.2	255.255.255.0	192.168.10.254
SERVER MAIN	NIC	192.168.10.3	255.255.255.0	192.168.10.254
SERVER MAIL	NIC	192.168.10.4	255.255.255.0	192.168.10.254

 ISSN: 2797-5274

Table 2. IP *Address* jaringan MAN cabang A

Device	Interface	IP Address	Subnet Mask	Default Gateway
RC1	GE 0/0	192.168.20.14	255.255.255.240	**N/A**
	GE 0/1	10.10.10.2	255.255.255.252	
ACC POINT	INT	192.168.20.12	255.255.255.240	192.168.20.14
KA. CABANG	NIC	192.168.20.1	255.255.255.240	192.168.20.14
KA. ADMIN	NIC	192.168.20.2	255.255.255.240	192.168.20.14
STAFF ADM 1	NIC	192.168.20.3	255.255.255.240	192.168.20.14
STAFF ADM 2	NIC	192.168.20.4	255.255.255.240	192.168.20.14
STAFF ADM 3	NIC	192.168.20.5	255.255.255.240	192.168.20.14
SPV 1	NIC	192.168.20.6	255.255.255.240	192.168.20.14
SPV 2	NIC	192.168.20.7	255.255.255.240	192.168.20.14
SPV 3	NIC	192.168.20.8	255.255.255.240	192.168.20.14
SPV 4	NIC	192.168.20.9	255.255.255.240	192.168.20.14
KA. GUDANG	NIC	192.168.20.10	255.255.255.240	192.168.20.14
WA. GUDANG	NIC	192.168.20.11	255.255.255.240	192.168.20.14
PRINTER	NIC	192.168.20.13	255.255.255.240	192.168.20.14

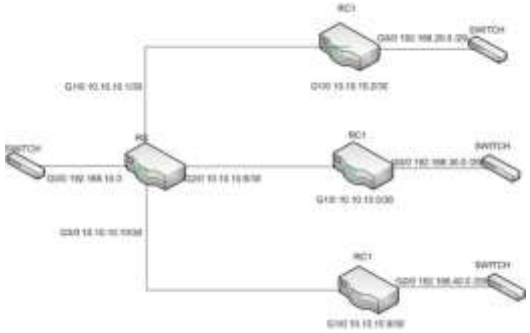
Table 3. *IP Address* jaringan MAN cabang B

Device	Interface	IP Address	Subnet Mask	Default Gateway
RC2	GE 0/0	192.168.30.14	255.255.255.240	N/A
	GE 0/1	10.10.10.5	255.255.255.252	
ACC POINT	INT	192.168.30.12	255.255.255.240	192.168.30.14
KA. CABANG	NIC	192.168.30.1	255.255.255.240	192.168.30.14
KA. ADMIN	NIC	192.168.30.2	255.255.255.240	192.168.30.14
STAFF ADM 1	NIC	192.168.30.3	255.255.255.240	192.168.30.14
STAFF ADM 2	NIC	192.168.30.4	255.255.255.240	192.168.30.14
STAFF ADM 3	NIC	192.168.30.5	255.255.255.240	192.168.30.14
SPV 1	NIC	192.168.30.6	255.255.255.240	192.168.30.14
SPV 2	NIC	192.168.30.7	255.255.255.240	192.168.30.14
SPV 3	NIC	192.168.30.8	255.255.255.240	192.168.30.14
SPV 4	NIC	192.168.30.9	255.255.255.240	192.168.30.14
KA. GUDANG	NIC	192.168.30.10	255.255.255.240	192.168.30.14
WA. GUDANG	NIC	192.168.30.11	255.255.255.240	192.168.30.14
PRINTER	NIC	192.168.30.13	255.255.255.240	192.168.30.14

3.3. *Routing and Switching*

Pada umumnya jaringan bisa saling terkoneksi dikarenakan ip network satu sama lain saling mengenal dengan ip network lainnya proses ini dinamakan *routing and switching* adalah membagikan dari kiriman paket yang dikirim dari komputer dalam jaringan yang sama atau tidak, ada dua cara dalam menentukan *route* (jalur) yaitu dengan *static* dan *dynamic,* masing-masing memiliki perbedaan dalam implementasinya tetapi untuk kegunaan sama yaitu berpungsi untuk penghubung ip network satu dengan yang lain sehingga jaringann bisa saling terhubung.

 ISSN: 2797-5274



Gambar 4. *Routing and switching*

1. *Router Server* (RS)
   RS#show ip route
   10.0.0.0/30 is *subnetted, 3 subnets*
   C 10.10.10.0 is *directly connected, GigabitEthernet1*/0
   C 10.10.10.4 is *directly connected, GigabitEthernet*2/0
   C 10.10.10.8 is *directly connected, GigabitEthernet*3/0
   C 192.168.10.0/24 *is directly connected, GigabitEthernet*0/0
   S 192.168.20.0/24 [1/0] *via* 10.10.10.2
   S 192.168.30.0/24 [1/0] *via* 10.10.10.5
   S 192.168.40.0/24 [1/0] *via* 10.10.10.9

2. *Router* Cabang (RC1)
   RC1#*show ip route*
   10.0.0.0/30 *is subnetted, 3 subnets*
   C 10.10.10.0 *is directly connected, GigabitEthernet*1/0
   S 10.10.10.4 [1/0] *via* 10.10.10.1
   S 10.10.10.8 [1/0] *via* 10.10.10.1
   S 192.168.10.0/24 [1/0] *via* 10.10.10.1
   192.168.20.0/28 *is subnetted,* 1 *subnets*
   C 192.168.20.0 *is directly connected, GigabitEthernet*0/0
   192.168.30.0/28 *is subnetted*, 1 *subnets*
   S 192.168.30.0 [1/0] *via* 10.10.10.5
   192.168.40.0/28 is *subnetted*, 1 *subnets*
   S 192.168.40.0 [1/0] *via* 10.10.10.9

3.4.Kemanan Jaringan

3.4.1.Penerapan *Access List (firewall)*

Ketika *access list (firewall)* diterapkan dalam *router* ataupun sebuah PC *server* dan *client* maka *access list* tersebut berpungsi untuk melakukan *filter* terhadap paket yang dikirim oleh *client* maka *acces list* tersebut hanya memperbolehkan beberapa *network* yang terdaftar saja.

1. RC1 (*Router* Cabang 1)
   RC1#*show access-lists*
   Standard IP access list 3
   10 *deny* 192.168.30.0 0.0.0.15
   20 *deny* 192.168.40.0 0.0.0.15
   30 *permit any*
2. RC2 (*Router* Cabang 2)
   RC2#*show access-lists*
   Standard IP access list 3
   10 *deny* 192.168.20.0 0.0.0.15
   20 *deny* 192.168.40.0 0.0.0.15
   30 *permit any*

 ISSN: 2797-5274

3. RC3 (*Router* Cabang 3)
   RC3#*show access-lists*
   Standard IP access list 3
   10 *deny* 192.168.20.0 0.0.0.15
   20 *deny* 192.168.30.0 0.0.0.15
   30 *permit any*

3.4.2. Penerapan Switch Port Security

Pada saat *mac-address security* diaktivkan pada sebuah *port switch*, maka *switch* tidak akan meneruskan paket data karena *mac-address* tersebut tidak terdaptar dalam tabel data *switch port security*, sistem keamanan *port security* ini dibuat agar *port* tidak sembarang di akses oleh perangkat keras yang belum terdaftar.

Gambar 5. *PORT SECURITY*

SWRC1(*config*)#*int* fa0/2
SWRC1(*config-if*)#*switch mode access*
SWRC1(*config-if*)#*switch port-security*
SWRC1(*config-if*)#*switch port-security mac-address* 0002.169B.E012
SWRC1(*config-if*)#*switch port-security violation restrict*
SWRC1(*config-if*)#*exit*
SWRC1(*config*)#*exit*
Artinya adalah *MAC-ADDRESS* 0002.169B.E012 adalah *mac-address* yang bisa mengakses *switch port interface fastehernet* 0/2 SWRC1.

3.5.Pengujian Jaringan

Pada bagian pengujian jaringan ini penulis mencoba untuk menguji pada bagian awal sebelum dilakukan perubahan oleh penulis dan setelah dilakukan perubahan jaringan.

3.5.1.Pengujian Jaringan Awal

Pada pengujian jaringan awal ini penulis akan melakukan uji coba dengan cara melakukan perintah *ping* dan *tracert* untuk mengetahui jaringan sebelumnya pada saat melakukan penelitian.

1. Pengujian dengan perintah *PING*
   Dari jaringan cabang A dengan ip 192.168.1.2 ke alamat ip 192.168.2.2 cabang B dan ke alamat ip 192.168.3.2 cabang C.

Gambar 6. Pengujian perintah *PING*

Keterangan pada gambar 10 bahwa cabang A bisa melakukan ping ke cabang B dan cabang C pada jaringan sebelumnya tidak ada filter jaringan sehingga akses pada jaringan lain sangat mudah diakses.

2. Pengujian dengan perintah *TRACERT*
   Perintah ini berpungsi untuk mengetahui jalur mana saja paket dikirim hingga sampai ke tujuan missal saya ambil paket cabang A dengan Ip Address 192.168.1.2 mengirim pesan ke cabang B dengan IP Adress 192.168.1.2 atau ke *server* cabang C yang memiliki *ip address* 192.168.3.2

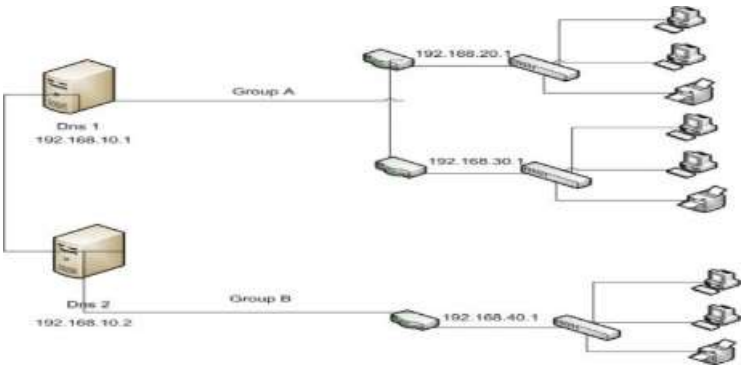
 ISSN: 2797-5274

Gambar 7. Pengujian perintah *tracert*

Pengiriman paket dari *ip address* 192.168.1.2 yang ditunjukan ke *ip address* 192.168.2.2 melewati jalur *ip address* 10.20.0.1 begitupun dengan paket yang dikirim dari cabang ke cabang 3 melewati *ip address* 10.20.0.1 dengan demikian jalur pengiriman paket melewati jaringan kelas A untuk akses penghubung jaringan antar cabang.

3.5.2.Pengujian Jaringan Akhir

Dalam tahap pengujian akhir ini dilakukan setelah dilakukan beberapa perubahan yang telah di jelaskan pada bagian perancangan usulan jaringan yang telah di grup dan terkoneksi pada masing-masing server dns.

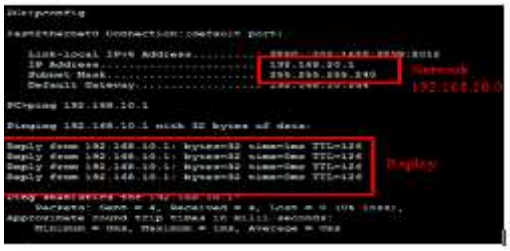


Gambar 8. Skema Grup Jaringan Usulan

Table 4. Grup jaringan PT. Tirta Kencana Tata Warna

Device	Network	Nama Server	IP SERVER
Grup A	192.168.20.0	DNS 1	192.168.10.1
	192.168.30.0	DNS 1	192.168.10.1
Grup B	192.168.40.0	DNS 2	192.168.10.2

1. Pengujian dengan perintah *PING* dari cabang ke grup *server*
   Dalam pengujian ini pengiriman paket data *ping* harus *replay* karena masih berada dalam grup *server* jaringannya.



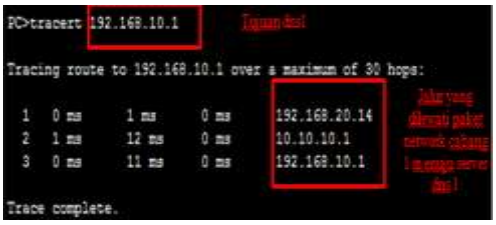
Gambar 9. *ping* cab 1 *group server* dns1

 ISSN: 2797-5274

2. Pengujian dengan perintah *PING* dari cabang ke luar grup atau cabang lain.
   Pengujiannya harus *request time out* atau *destination host unreachable* dikarenakan telah diterapkan *access list (Firewall)* di *server* dan di *router cisco*, untuk melintasi jaringan tersebut tidak diperbolehkan untuk melindungi privasi dari masing-masing cabang grup jaringan.

Gambar 10. ping cab 1 ke luar grup dan luar cabang

3. Pengujian perintah *tracert*
   Perintah ini adalah sebuah perintah yang bertujuan untuk melacak jalur paket hingga sampai ke tujuan dengan mengirimkan pesan *Internet Control Masage Protocol* (ICMP) *echo request* ke tujuan berdasarkan alamat ip tujuan.



Gambar 11. *ping* cab 1 ke grup *server dns1*

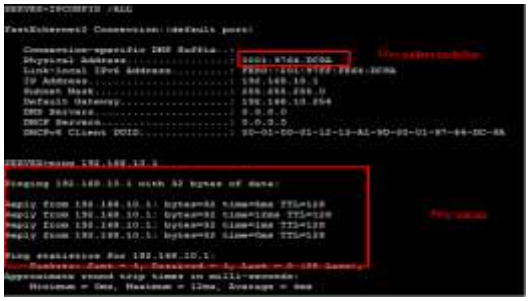
4. Pengujian *access-list (firewall)*
   Pengujian ini akan dilakukan dengan cara melakukan perintah *ping* kepada jaringan yang bukan grup dari jaringan tersebut.

Gambar 12. *access list* cabang 1

Gambar 13. *access list* cabang 3

5. Pengujian *Port-Security* pada *switch*
   Tujuan dari keamanan *port security* ini adalah agar *port* tidak sembarang diakses oleh komputer lain, sehingga cara kemanannya adalah memanfaatkan fitur dalam *switch* itu sendiri yang bernama *port security*, hal yang harus dilakukan adalah mendaftarkan *mac-address* pada masing-masing *port* tersebut.

 ISSN: 2797-5274



Gambar 14. pengujian *port security mac address* terdaftar

4. KESIMPULAN

Berdasarkan uji coba pada saat pengujian akhir dilakukan dengan *packet tracer* 7.0 dan pengujian dengan menggunakan *Virtual Box* maka dapat di simpulkan pengujian *PING,*Pengujian ini bertujuan untuk melakukan sebuah koneksi apakah dalam perangkat saling terhubung dengan baik. Pengujian *Tracert* berfungsi untuk melakukan pelacakan paket melewati jalur *ip address* mana saja proses tracert akan berhenti apabila packet telah sampai ke *ip address* tujuan. Penerapan *ACCESS LIST (FIREWALL)* Penerapan fitur ini bertujuan untuk memfilter paket, membatasi akses keluar masuk paket untuk keamanan jaringan tersebut. Penerapan *SECURITY PORT* Ini penting untuk keamanan *port* pada sebuah *switch* bertujuan agar tidak sembarang masuknya perangkat lain yang belum terdaftar pada *port.*

REFERENSI

Afrianto, I., & Setiawan, E. B. (2015). Kajian virtual private network (vpn) sebagai sistem pengamanan data pada jaringan komputer (studi kasus jaringan komputer unikom). *Majalah Ilmiah UNIKOM*, *12*(1), 43–52. https://doi.org/10.34010/miu.v12i1.34

Aji, S., Fadlil, A., & Riadi, I. (2018). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 11. https://doi.org/10.26555/jiteki.v3i1.5665

Arta, Y., Syukur, A., & Kharisma, R. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *It Journal Research and Development*, *3*(1), 104. https://doi.org/10.25299/itjrd.2018.vol3(1).1346

Al Gojali, 2017. Pengertian Topologi Tree Serta Kelebihan Dan Kekurangannya. Diambil dari https://www.utopicomputers.com/pengertian-topologi-tree-serta-kelebihan-dan-kekurangannya/.

Bayu, Yamin, A. (2017). *Analisa keamanan jaringan wlan dengan metode*. *3*(2), 69–78.

Chandra, Y. I., & Kosdiana. (2018). Rancang Bangun Jaringan Komputer Nirkabel Dan Hotspot Menggunakan Router Mikrotik Rb850gx2 (Studi Kasus Di STMIK Jakarta STI&K). *Konferensi Nasional Sistem Informasi 2018*, *2*, 8–9.

Dian, 2016. Pengertian Topologi Star dan Gambarnya, Ciri-Ciri, Cara Kerja, serta Kelebihan dan Kekurangannya.Diambil dari https://www.maxmanroe.com/vid/teknologi/komputer/ pengertian-topologi-star.html.

Jul Al Gray, 2017. Jenis-Jenis Jaringan Komputer: PAN, LAN, MAN, dan WAN. diambil dari www.jejakwaktu.com/jenis-jaringan-komputer/

Lukman, A. M., & Bachtia, Y. (2016). Analisis sistem keamanan jaringan dengan. *Computer Engineering, System And Science*, *1*(1), 9–14.

Pi, R. (2019). *Implementasi IPTables untuk Packet Filtering Firewall*. *6*(1), 61–66.

Rudolf Huizen, R. (2016). Manajemen Jaringan Internet Sekolah Menggunakan Router Mikrotik Dan Proxy Server. *XI Nomor Jurnal Teknologi* Informasi, *32*, 1907–2430.

Sulaiman, K. (2016). Analisis Jaringan Dengan Menggunakan Switch Port Security *Computer Engineering, System and science, I*(1), 1-16.

VARIANTO, E., & MOHAMMAD BADRUL. (2015). Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada Pt.Valdo International. *Jurnal Teknik Komputer Amik Bsi*, *1*(1), 55–56.