PENERAPAN STATIC VLAN DAN ACCESS LIST UNTUK MENINGKATKAN KEAMANAN JARINGAN

(STUDI KASUS PT. DIMENSI MANDIRI TEKNOLOGI)

AHMAD FITRIANSYAH[1]
Prodi Manajemen Informatika,
Universitas MH Thamrin
Jakarta, Indonesia
e-mail : hafaskom@gmail.com

ALARIK ANDREANSYAH[2]
Prodi Teknik Informatika
Universitas MH Thamrin
Jakarta, Indonesia
e-mail : alarikandre@gmail.com

ABU SOPIAN[3]
Prodi Teknik Informatika,
Universitas MH Thamrin
Jakarta, Indonesia
e-mail : ianprosia2@gmail.com

***Abstract*—On a network, one computer can share and exchange data with another computer in the form of images, text, or sound by passing through media that connects computers. Computer Networks having many advantages that can facilitate the work also has disadvantages for the organization. One threat that might occur is data theft. One way to protect against data transfer in a computer network is to use a Static VLAN and Access List. The purpose of this study is to analyze the current conditions and apply the concept of Static VLANs and Access Lists so that companies can provide data access rights from each computer user in each division, thereby minimizing the use of data protection by unauthorized parties.**

The method used in this study is a simulation method that uses Cisco Packet Tracer software and Sangfor firewall router devices. Data collection methods in this study were observation and interviews with company directors.

The results showed that the distribution of networks using static VLANs and data security using Access Lists can be implemented well in the company and making the network created can make companies do the job easier and transaction data for each division can be done safely.

Keywords-Static VLAN; Access List; Computer Network

I. PENDAHULUAN

Jaringan komputer merupakan kumpulan *hardware* dan *software* dalam suatu sistem dengan aturan tertentu untuk mengelola anggotanya dalam melakukan pertukaran data. Satu komputer yang terkoneksi ke jaringan menjadi satu node dari jaringan tersebut. Sedangkan *host* merupakan komputer pusat yang terkoneksi ke jaringan untuk dapat memberikan layanan jaringan [1]

Pada jaringan, antar komputer yang terhubung dapat saling berbagi dan bertukar informasi berupa gambar, teks, ataupun suara dengan media jaringan yang menghubungkan antar komputer. Jaringan komputer selain memiliki kelebihan yang dapat membantu mempermudah pekerjaan, juga memiliki ancaman yang dapat menjadi masalah besar bagi suatu organisasi jika tidak diantisipasi sejak dini.

Ancaman yang dapat terjadi pada jaringan komputer berasal dari internal maupun eksternal. Masalah internal dapat berupa pencurian data penting yang dilakukan karyawan sendiri, sedangkan masalah eksternal yang dapat menjadi ancaman dapat berupa faktor alam, manusia, hewan, dan sebagainya. Oleh karena itu, diperlukan perlindungan dan skema jaringan untuk melindungi data pada setiap divisi dan server agar tidak dicuri oleh pihak lain yang tidak berkepentingan.

VLAN merupakan teknologi yang memungkinkan kita membuat sebuah *subnet* jaringan secara logika tanpa harus memperthatikan lokasi fisik dari komputer yang terhubung[2]. Pesan yang disiarkan di VLAN terbatas pada subnet yang menyebabkan komunikasi dalam VLAN lebih efisien selama mayoritas lalu lintas jaringan (70 hingga 80 persen) berada di dalam VLAN yang sama[3]. VLAN didasarkan pada teknologi layer 2, yang menggunakan konfigurasi port atau alamat MAC untuk menentukan sistem anggota, harus memiliki port yang didedikasikan untuk koneksi router. Dalam jenis VLAN ini, administrator jaringan memilih port switch tertentu untuk menunjuk anggota VLAN atau membuat daftar alamat MAC workstation[3]. Dengan mekanisme subnet, maka anggota suatu VLAN tidak dapat mengakses anggota suatu VLAN yang berbeda sehingga keamanan data dalam jaringan menjadi lebih terjamin.

Salah satu cara untuk melindungi dari pencurian data dalam jaringan komputer yang ada dapat diatasi melalui penggunaan Static VLAN (*Virtual Local Area Network*) dan *Access List*. Dengan penggunaan Static VLAN dan Access List, perusahaan dapat mengatur hak akses suatu data dari setiap pengguna komputer yang berada di jaringan, sehingga meminimalisir ancaman terjadinya pencurian data oleh pihak yang tidak berkepentingan.

II. KAJIAN PUSTAKA

Penelitian sebelumnya yang membahas mengenai penerapan *Virtual Local Area Network* dan *Access List* telah banyak dilakukan. Penelitian pertama mengenai penerapan VLAN pada Rumah Sakit Mata Ramata. Penelitian ini membahas konfigurasi VLAN yang berperan penting dalam

mengoptimalkan komunikasi data. VLAN merupakan suatu model jaringan yang membagi jaringan secara logikal kedalam beberapa LAN yang berbeda. VLAN dapat dikonfigurasi secara virtual tanpa harus melihat kondisi fisik peralatan, sehingga VLAN memiliki fleksibilitas di dalam pengaturan jaringan dan memudahkan administrator jaringan dalam membagi jaringannya sesuai dengan fungsi dan kebutuhan keamanan jaringan tersebut. VLAN juga dapat menghemat biaya karena tidak perlu menggunakan banyak *switch* untuk keperluan jaringan pada rumah sakit ini [4].

Penelitian kedua melakukan konfigurasi jaringan menggunakan *access control list* sebagai *filter* lalu lintas jaringan, studi kasus PT. Usaha Entertainment Indonesia. Dengan *access control list*, lalu lintas data di jaringan *Wide Area Network* di PT. Usaha Entertainment Indonesia dapat lebih efisien. *Access control list* bisa menghindari adanya akses data yang tidak diperlukan dalam jaringan. Pengujian dilakukan dengan simulasi menggunakan software Cisco *Packet Tracer* [5].

Penelitian ketiga melakukan analisis dalam penggunaan *access control list* dalam jaringan komputer di Kawasan Batamindo Industrial Park Batam. Hasil penelitian menunjukan kesimpulan bahwa penggunaan *access control list* dalam jaringan komputer pada perusahaan di Kawasan Batamindo Industrial Park Batam adalah baik, karena lalu lintas jaringan sesuai kebutuhan perusahaan [6].

Dari beberapa penelitian terdahulu tersebut, maka dapat diuraikan beberapa perbedaan penelitian ini yaitu : (1) Lebih *user friendly* karena penulis menggunakan *Graphical User Interface*; (2) Lebih lengkap secara fitur dan lebih aman, karena menggunakan router firewall; (3) Satu *policy* bisa memuat banyak rule, sehingga lebih efisien; (4) Bisa melakukan filter jaringan berdasarkan aplikasi (DNS, HTTPS, dan sebagainya).

Keuntungan dari penggunaan VLAN : (1) Meningkatkan kinerja jaringan dengan membagi satu broadcast domain menjadi beberapa broadcast domain; (2) Meningkatkan keamanan jaringan, paket broadcast yang dikirim dari satu unit kerja tidak akan diterima oleh komputer pada unit kerja yang berbeda serta mengatur jaringan untuk mengijinkan atau tidak mengijinkan sebuah komputer terkoneksi dengan server atau komputer lain pada subnet yang berbeda; (3) Meningkatkan Fleksibilitas pada pengelolaan jaringan, VLAN memungkinkan administrator untuk mengkoneksikan komputer mana saja ke suatu VLAN tanpa memperhatikan lokasi fisik dari komputer tersebut.[7]

Keanggotaan Pada VLAN : (1) Static, administrator jaringan mengkonfigurasi manual port pada switch pada VLAN tertentu; (2) Dynamic, port secara otomatis ditugaskan pada VLAN tertentu melalui server yang disebut VMPS (VLAN Membership Policy Server); (3) Trunk, Switch menggunakan port trunk untuk melepas frame dari semua VLAN ke switch lainnya. Port Trunk digunakan untuk mengkoneksikan antar switch. Dilakukan dengan menandakan setiap frame dengan nomor VLAN.[7]

III. METODE PENELITIAN

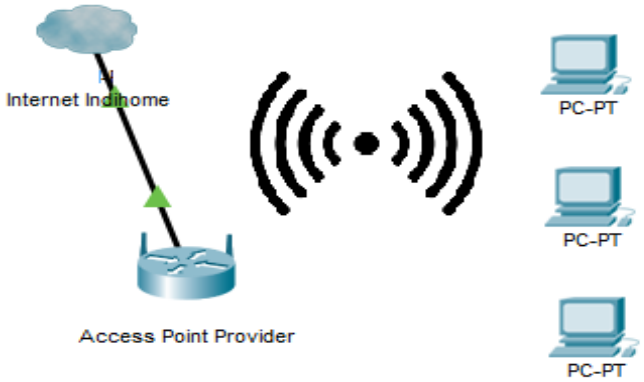
Penelitian ini akan merancang jaringan kantor yang aman dari pencurian data, tetapi praktis dalam implementasinya. Studi kasus pada PT. Dimensi Mandiri Teknologi yang beralamat di Jalan Rose Garden 2 No 66 Grand Galaxy Bekasi.

Metode yang digunakan untuk mengumpulkan data dalam penelitian ini sebagai berikut :

1. Studi Observasi : Pengumpulan data dilakukan dengan meninjau dan mengamati langsung sistem jaringan yang berjalan saat ini, untuk mengetahui bagaimana solusi untuk koneksi dan keamanan jaringan komputer.
2. Studi Literatur : Mencari dan mempelajari bahan atau informasi yang berhubungan dengan jaringan komputer, VLAN dan ACL di berbagai sumber seperti jurnal dan internet..
3. Wawancara : Melakukan proses tanya jawab kepada pihak terkait untuk penelitan yang penulis lakukan. Narasumber dalam penelitian ini adalah Direktur PT. Dimensi Mandiri Teknologi.
4. Praktik Simulasi : Melakukan praktik menggunakan sumber daya virtual dan perangkat fisik yang berkaitan dengan bagaimana solusi yang akan diimplementasikan. Penulis menggunakan software Cisco *Packet Tracer* dan *Router Firewall* Sangfor.

IV. HASIL DAN PEMBAHASAN

Dari hasil pengumpulan data selama melakukan penelitian di PT. Dimensi Mandiri Teknologi khususnya di bagian teknisi, saat ini sistem jaringan di kantor PT. Dimensi Mandiri Teknologi masih sederhana dikarenakan kondisi kantor masih baru dan jumlah karyawan yang masih sedikit. Berikut merupakan topologi yang berjalan saat ini di PT. Dimensi Mandiri Teknologi.

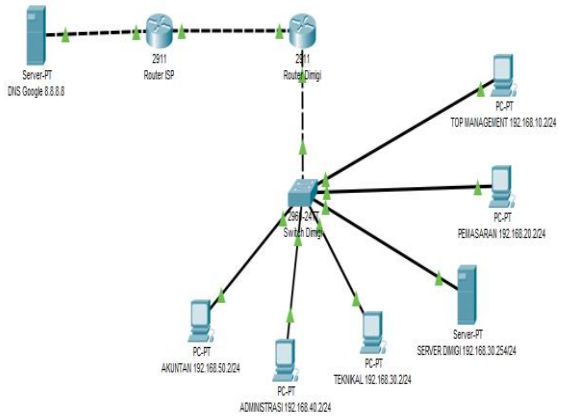


Gambar 1. Topologi Jaringan Yang Berjalan

Berdasarkan topologi yang sedang berjalan, kelebihan jaringan PT. Dimensi Mandiri Teknologi saat ini antara lain : (1) mudah dalam melakukan instalasi; (2) Praktis dalam implementasi jaringannya; (3) Biaya instalasi yang tidak memakan banyak biaya; (4) Perangkat yang digunakan tidak banyak.

Sedangkan kekurangan topologi yang sedang berjalan, saat ini antara lain : (1) Tidak memiliki *backup* perangkat karena koneksi internet hanya melalui *Access Point* yang disediakan *Internet Service Provider*; (2) Setiap pegawai di satu divisi bisa mengakses PC lain yang berbeda divisi; (3) Rawan pencurian atau pengubahan data oleh pihak yang tidak berkepentingan ketika melakukan data sharing; (4) Kualitas jaringan tidak baik untuk diimplementasikan ketika perusahaan sudah mempunyai banyak karyawan.

Meskipun jaringan saat ini sangat mudah dalam instalasi dan implementasinya karena kebutuhan yang belum kompleks dan karyawan yang masih sedikit, tapi untuk kedepannya ketika perusahaan semakin berkembang akan membutuhkan tambahan karyawan dan pengaturan setiap divisi yang jelas. Ketika kondisi tersebut terjadi, tentu akan menjadi masalah serius dalam hal manajemen dan keamanan data. Untuk mengatasi permasalahan tersebut, penulis mengusulkan solusi untuk mencegah permasalahan di masa depan, yaitu dengan mengimplementasikan *Static Virtual Local Area Network* dan *Access List* menggunakan *router firewall* dan *switch* untuk menjaga hak akses data setiap divisi di PT. Dimensi Mandiri Teknologi. Agar Static VLAN dan Access List dapat diterapkan, PT. Dimensi Mandiri Teknologi diharuskan untuk mempunyai perangkat yang dibutuhkan. Berikut merupakan rancangan topologi dan alokasi segment yang akan dilakukan dalam penelitian ini.



Gambar 2. Topologi yang diusulkan

Dalam melakukan simulasi, harus ditentukan *IP Address* dan alokasi *Static Virtual Local Area Network* bagi setiap perangkat. Berikut alokasi *IP Address dan Static Virtual Local Area Network* yang akan diberikan pada masing-masing perangkat simulasi menggunakan Cisco *Packet Tracer* sebagaimana terlihat pada Tabel 1.

Tabel 1. Alokasi VLAN dan IP Address untuk Simulasi

DEVICES	***INTERFACE***	***IP ADDRESS***	***SUBNET MASK***	***GATEWAY***
Router Dimigi	*G 0/0* *G 0/1.10* *G 0/1.20* *G 0/1.30* *G 0/1.40* *G 0/1.50*	192.168.100.149 192.168.10.1 192.168.20.1 192.168.30.1 192.168.40.1 192.168.50.1	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	192.168.100.1
Router ISP	*G 0/0* *G 0/1*	192.168.100.1 8.8.4.4	255.255.255.0	
Switch Dimigi	*VLAN 10* *VLAN 20* *VLAN 30* *VLAN 40* *VLAN 50*			
PC Top Management	*NIC/VLAN 10*	192.168.10.2	255.255.255.0	192.168.10.1
PC Pemasaran	*NIC/VLAN 20*	192.168.20.2	255.255.255.0	192.168.20.1
Storage Server Dimigi	*NIC/VLAN 30*	192.168.30.254	255.255.255.0	192.168.30.1
PC Teknikal	*NIC/VLAN 30*	192.168.30.2	255.255.255.0	192.168.30.1
PC Administrasi	*NIC/VLAN 40*	192.168.40.2	255.255.255.0	192.168.40.1
PC Akuntan	*NIC/VLAN 50*	192.168.50.2	255.255.255.0	192.168.50.1
DNS Google	*NIC*	8.8.8.8	255.0.0.0	8.8.4.4

4.1 Simulasi Jaringan Menggunakan Cisco *Packet Tracer*

Menjalankan aplikasi Cisco *Packet Tracer* dan memasukkan perangkat virtual yang dibutuhkan sesuai dengan perencanaan dan topologi. Lalu memulai untuk melakukan konfigurasi.

4.1.1 *Show Running Config* pada *Router* Simulasi

Berikut merupakan konfigurasi *interface* dan *access list* pada *router* simulasi menggunakan Cisco *Packet Tracer*. Juga diperlukan konfigurasi *Source Network Address Translation* agar *IP Address* lokal bisa terhubung ke internet.

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip access-group 120 in
 ip nat inside
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group 130 in
 ip nat inside
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 ip access-group 140 in
 ip nat inside
!
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50
 ip address 192.168.50.1 255.255.255.0
 ip access-group 150 in
 ip nat inside
!
```

Gambar 3. Konfigurasi *Interface Router* Simulasi

```
!
ip nat pool LAN-INTERNET 192.168.100.1 192.168.100.254 netmask 255.255.255.0
ip nat inside source list LAN-INTERNET interface GigabitEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
ip flow-export version 9
!
!
access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 130 permit ip any any
access-list 140 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 140 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 140 deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 140 permit ip any any
access-list 120 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 120 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 120 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 120 permit ip any any
access-list 150 deny ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 150 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 150 deny ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 150 permit ip any any
ip access-list extended LAN-INTERNET
 permit ip any any
!
```

Gambar 4. Konfigurasi *ACL Router* Simulasi

4.1.2 *Show Running Config* pada *Switch* Simulasi

Untuk konfigurasi Static Virtual Local Area Network pada interface switch Cisco, berikut merupakan konfigurasinya.

```
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 10,20,30,40,50
 switchport mode trunk
!
```

Gambar 5. Konfigurasi Interface Switch Simulasi Penelitian

4.1.3 *Show VLAN* pada *Switch* Simulasi

Berikut merupakan alokasi untuk konfigurasi Static virtual Local Area Network pada router simulasi

```
DIMIGI_SWITCH_2960#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1
10   TOP_MANAGEMENT                   active    Fa0/1
20   PEMASARAN                        active    Fa0/5
30   TEKNIKAL + SERVER                active    Fa0/10, Fa0/11
40   ADMINISTRASI                     active    Fa0/15
50   AKUNTAN                          active    Fa0/20
```

Gambar 6. Konfigurasi VLAN Switch Simulasi

4.2 Pengetesan Hasil Konfigurasi Jaringan Simulasi Cisco

Berikut merupakan hasil pengetesan untuk simulasi jaringan virtual sesuai skenario yang sudah direncanakan.

1. *Storage Server* dapat diakses oleh Divisi Teknikal dan *Top Management*. Hasil pengujian menunjukan perintah *ping* dari server (192.168.30.254) ke komputer *top management* (192.168.10.2) dan teknikal (192.168.30.2) berhasil dilakukan. Hal ini menunjukan ada jalur komunikasi diantara *server*, *top management*, dan teknikal.
2. *Storage Server* tidak dapat diakses oleh selain Divisi Teknikal dan *Top Management*. Hasil pengujian menunjukan perintah *ping* dari server (192.168.30.254) ke komputer divisi administrasi (192.168.40.2) dan divisi pemasaran (192.168.20.2) tidak berhasil dilakukan dengan menampilkan pesan *Destination host unreachable*. Hal ini menunjukan tidak ada jalur komunikasi antara *server* dengan divisi administrasi dan divisi pemasaran.

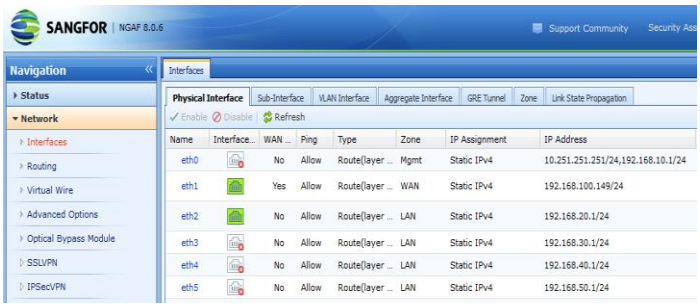
3. *Storage Server* terhubung dengan jaringan internet. Hasil pengujian menunjukan perintah *ping* dari server (192.168.30.254) ke Google (8.8.8.8) berhasil dilakukan. Hal ini menunjukan ada jalur komunikasi antara *server* dan jaringan internet.
4. Sub jaringan *top management* (192.168.10.2) dan divisi pemasaran dapat saling berkomunikasi. Hasil pengujian menunjukan perintah *ping* dari divisi pemasaran (192.168.20.2) ke jaringan *top management* (192.168.10.2) berhasil dilakukan. Hal ini menunjukan ada jalur komunikasi diantara sub jaringan *top management* dan sub jaringan divisi pemasaran.
5. Sub jaringan divisi pemasaran hanya terkoneksi dengan sub jaringan *Top Management* saja dan tidak dapat mengakses sub jaringan yang lain. Hasil pengujian menunjukan perintah *ping* dari sub jaringan divisi pemasaran (192.168.20.2) ke sub jaringan divisi administrasi (192.168.40.2) tidak berhasil dilakukan dengan menampilkan pesan *Destination host unreachable*. Hal ini menunjukan tidak ada jalur komunikasi antara divisi pemasaran dengan divisi administrasi.
6. Sub jaringan divisi pemasaran terhubung dengan jaringan internet. Hasil pengujian menunjukan perintah *ping* dari divisi pemasaran (192.168.20.2) ke Google (8.8.8.8) berhasil dilakukan. Hal ini menunjukan ada jalur komunikasi antara divisi pemasaran dan jaringan internet.
7. Sub jaringan divisi teknikal hanya terkoneksi dengan sub jaringan *Top Management* dan *server* saja dan tidak dapat mengakses sub jaringan yang lain. Hasil pengujian menunjukan perintah *ping* dari sub jaringan divisi teknikal (192.168.30.2) ke sub jaringan divisi administrasi (192.168.40.2) dan sub jaringan divisi akuntansi (192.168.50.2) tidak berhasil dilakukan dengan menampilkan pesan *Destination host unreachable*. Hal ini menunjukan tidak ada jalur komunikasi antara divisi teknikal dengan divisi administrasi dan akuntansi.
8. Begitupun hasil pengujian terhadap sub jaringan divisi administrasi dan divisi akuntansi yang tidak dapat terhubung dengan sub jaringan yang lain kecuali sub jaringan *top management*. Dan sub jaringan divisi administrasi dan divisi akuntansi dapat terhubung dengan jaringan intenet.

4.3 Implementasi Jaringan Menggunakan Router Firewall Sangfor

Setelah selesai melakukan simulasi menggunakan sumber daya virtual. Selanjutnya akan dilakukan implementasi menggunakan perangkat fisik. Perangkat yang digunakan untuk implementasi rancangan adalah *router firewall* Sangfor.

4.3.1 Konfigurasi Interface Router Firewall Simulasi

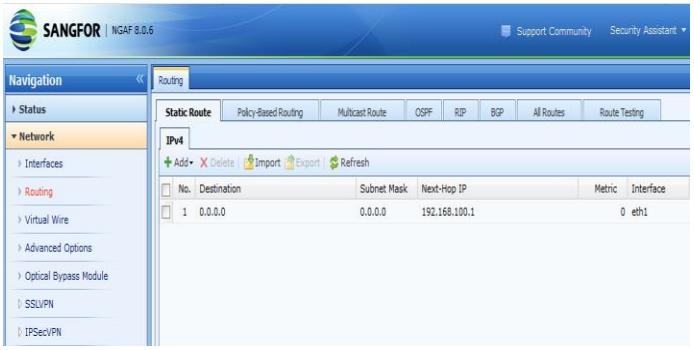
Dikarenakan tidak memiliki sebuah Manageable Switch untuk konfigurasi Static Virtual Local Area Network, sebagai gantinya digunakan port interface fisik yang tersedia pada Router Firewall Sangfor. Pilih menu Network -> Interface.



Gambar 7. Interface Router Firewall Sangfor

4.3.2 Konfigurasi Static Route pada Router Firewall Simulasi

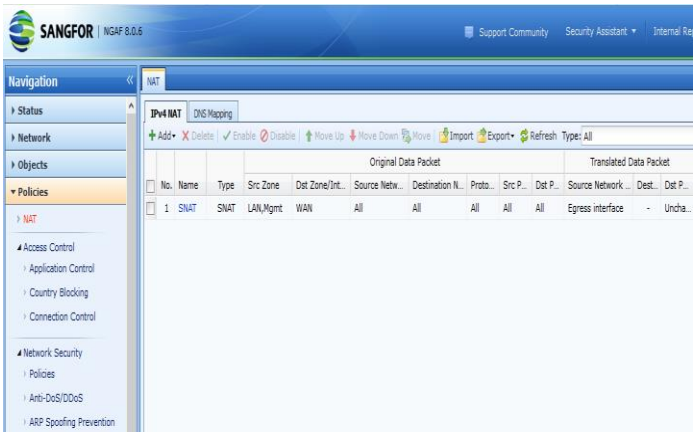
Dibutuhkan konfigurasi Static Route agar perangkat router firewall dapat terhubung dengan perangkat ISP. Pilih menu Network -> Routing



Gambar 8. Static Route pada Router Firewall Sangfor

4.3.3 Konfigurasi SNAT pada Router Firewall Simulasi

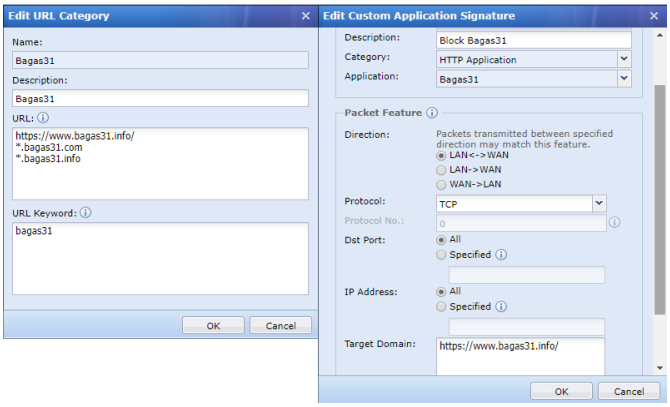
Dibutuhkan konfigurasi Source Network Address Translation agar IP Address lokal dapat terhubung dengan perangkat internet. Pilih menu Network -> NAT



Gambar 9. SNAT Router Firewall Sangfor

4.3.4 Custom URL dan Aplikasi pada Router Firewall Simulasi

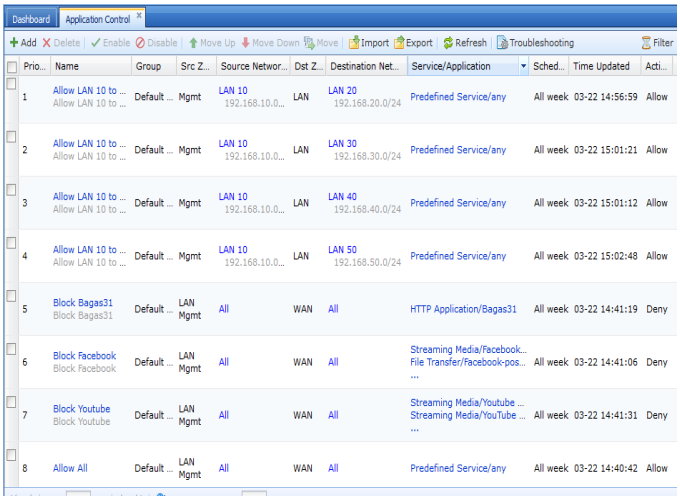
Untuk memblokir sebuah website yang belum terdaftar di database router firewall Sangfor. Maka dibutuhkan untuk menambah data URL dan aplikasi yang ingin diblokir. Untuk custom URL pilih menu Objects -> Content Control Databases -> URL Databases. Untuk Custom Application Signatures pilih menu Application Signature -> Custom Rule.



Gambar 10. Custom URL dan Application Signature

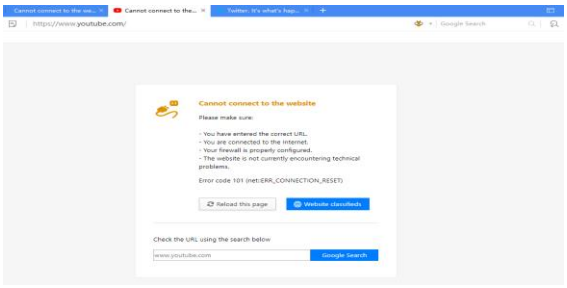
4.3.5 Konfigurasi ACL pada Router Firewall Simulasi

Buatlah konfigurasi access list pada router firewall Sangfor sesuai skenario yang sudah direncanakan. Pilih menu Policies -> Access Control -> Application Control.



Gambar 11. Rule Allow-Deny Router Firewall Sangfor

Dari gambar 11 diatas terlihat bahwa ACL juga dapat digunakan untuk memblokir akses terhadap situs-situs yang ada di internet.



Gambar 12. Akses terhadap youtube yang sudah diblokir

Sebagai contoh pada pengaturan yang dilakukan, akses terhadap situs bagas31, facebook dan youtube dilakukan pemblokiran sehingga karyawan tidak dapat mengakses situs-situs tersebut melalui jaringan kantor.

V. KESIMPULAN

Dari hasil penelitian yang dilakukan dapat disimpulkan bahwa penerapan Static VLAN dan Access List telah mampu membatasi komunikasi antar divisi pada jaringan, sehingga mengurangi akses data pada suatu divisi oleh divisi lain yang tidak berkepentingan. Pemanfaatan Access List juga dapat digunakan untuk melakukan pemblokiran terhadap situs-situs internet yang tidak boleh diakses melalui jaringan kantor. Static VLAN menjadi alternatif solusi yang dapat diimplementasikan agar penggunaan jaringan untuk setiap divisi memiliki pembagian akses yang jelas. Komputer dengan alokasi Static VLAN yang berbeda, akan diatur oleh Access List untuk hak akses source dan destinationnya, sehingga keamanan data setiap divisi dan server menjadi lebih baik untuk menghindari akses dari pihak yang tidak berkepentingan. Komputer dengan Static VLAN yang diizinkan oleh Access List, dapat saling terkoneksi sehingga pekerjaan bisa dilakukan bersama-sama.

REFERENCES

[1] A. S. Tanenbaum, *Computer Networks*. New Jersey: Pearson Education, 2003.

[2] B. A. Forouzan, *Data Communications and Networking*, 4th ed. New York: McGraw-Hill Higher Education, 2007.

[3] B. Sandberg, *The Complete Reference : Networking*, 3rd ed. New York: McGraw-Hill Education, 2015.

[4] I. W. B. B. Yoga and M. A. Raharja, "Implementasi VLAN (Virtual Local Area Network) pada Rumah Sakit Mata Ramata," *J. Elektron. Ilmu Komput. Udayana*, vol. 2, no. 7, pp. 177–186, 2019.

[5] A. D. Purwanto and M. Badrul, "Implementasi Access List Sebagai Filter Traffic Jaringan (Studi Kasus PT. Usaha Entertainment Indonesia)," *J. Tek. Komput. AMIK BSI*, vol. 2, no. 1, pp. 78–88, 2016.

[6] P. Simanjuntak, C. E. Suharyanto, and Jamilah, "Analisis Penggunaan Access Control List (ACL) dalam Jaringan Komputer di Kawasan Batamindo Industrial Park Batam," *J. Inf. Syst. Dev.*, vol. 2, no. 2, 2017.

[7] M. S. S. A. Easa, *CCNA in 21 Hours:'640-802' Syllabus*, 1st ed. London: bookboon.com, 2013.