

Penerapan Metode Access Control List Pada Jaringan VLAN Menggunakan Router Cisco

Umar Hasan¹, Sari Dewi², Firmansyah³

^{1,2}Universitas Bina Sarana Informatika, ³Universitas Nusa Mandiri

e-mail: ¹ehasan4989gmail.com, ²sari.sre@bsi.ac.id, ³firmansyah.fmy@nusamandiri.ac.id

Abstrak - Peranan teknologi informasi sangat signifikan bagi suatu perusahaan yang bergerak di bidang teknologi di tengah pesatnya dan pesatnya perkembangan teknologi informasi saat ini. Administrasi perangkat keras dan perangkat lunak adalah faktor terpenting dalam perusahaan layanan solusi teknologi dalam hal memaksimalkan aset teknologi informasi. Untuk mengatasi masalah tersebut, peneliti akan menerapkan pengelompokan dan distribusi hak akses jaringan, yang dimaksudkan untuk melakukan aktivitas perangkat jaringan dalam siaran yang sama. Teknik AccessControlListRouting digunakan. Teknologi VLAN adalah jaringan virtual yang memungkinkan suatu perangkat untuk berbagi pengaturan jaringannya, dalam contoh ini pengaturan router Cisco, sehingga dapat berkomunikasi dengan beberapa jaringan meskipun secara fisik berada di segmen yang sama. Access Control List adalah daftar pembatasan akses..

Kata Kunci: ACL, VLAN, Cisco

***Abstract** - The role of information technology is highly significant for a company that is especially active in technology in the current rapid and rapid development of information technology. The administration of hardware and software is the most important factor in technology solution services companies when it comes to maximizing information technology assets. In order to overcome these issues, the researcher will implement network access rights grouping and distribution, which intends to perform network device activities in the same broadcast. The AccessControlListRouting technique is used. VLAN technology is a virtual network that allows a device to share its network settings, in this example the Cisco router settings, so that it can communicate with multiple networks even though they are physically in the same segment. The Access Control List is a list of restrictions on access.*

Keywords: ACL, VLAN, Cisco

PENDAHULUAN

Keamanan jaringan merupakan pertimbangan penting saat membangun jaringan komputer, terutama di lingkungan teknologi yang berkembang pesat saat ini. Banyak agensi dan organisasi besar yang tidak peduli dengan masalah keamanan jaringan komputer, dan kerentanan ini terkadang dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk menyerang atau membahayakan sistem keamanan jaringan agensi atau perusahaan. Sangat penting untuk memperhatikan kesadaran sistem keamanan jaringan ini untuk mencegah penggunaan sumber daya jaringan yang tidak tepat. Sejalan dengan pesatnya perkembangan web, web dapat memberikan dampak positif sebagai penyedia layanan informasi dan komunikasi, tetapi juga dapat berdampak negatif dan menimbulkan ancaman bagi masyarakat. Akibatnya, keamanan jaringan komputer merupakan komponen penting dari kemampuan sistem untuk menjaga validitas dan integritas data sekaligus memastikan ketersediaan layanan bagi penggunanya, dan harus dilindungi oleh bahasa Iran dari semua jenis serangan, seperti intrusi atau pemindaian oleh pihak yang tidak dapat dipercaya (Suryanto & Dewi, 2013).

Banyak organisasi dan bisnis tampaknya mengabaikan pentingnya sistem keamanan jaringan komputer ini. Sumber masalah adalah ketika jaringan keamanan tiba-tiba diserang dan sistem dirusak (Fathurrahmad, Yusuf, 2019) akibatnya banyak tenaga dan biaya yang harus dikeluarkan untuk melakukan perbaikan sistem tersebut.

Oleh karena itu, keamanan jaringan harus lebih ditekankan untuk mencegah terulangnya ancaman serangan jaringan komputer yang semakin kompleks dan beragam. Selanjutnya, setelah komputer server terhubung ke internet, serangan lebih terbuka dan dapat terjadi kapan saja. Berbagai jenis strategi serangan masih terus dibuat, dan tidak boleh diabaikan. Oleh karena itu, untuk melindungi dan meminimalisir terjadinya ancaman terhadap keamanan jaringan komputer pada suatu instansi atau korporasi, maka perlu dibangun keamanan yang sangat hati-hati (Dewi, Riyadi, Suwastitaratu, & Hikmah, 2020).

METODE PENELITIAN

Metode untuk mengevaluasi dan mengumpulkan data dibahas. Observasi, wawancara, dan analisis literatur adalah tiga jenis metode penelitian:

1. Observasi langsung (observasi) Metode observasi adalah suatu metode pengumpulan data dengan melakukan penelitian langsung terhadap objek yang diteliti, dalam hal ini peneliti mengumpulkan data dan mengamati secara langsung di kantor studio musik Purwacaraka yang beralamat di Jln. Cinere Raya no.145 komplek RB12 Cinere depok. Komputer dalam prototipe studio musik langsung mengamati jaringan.

2 Wawancara (interview)

Peneliti juga melakukan Interview (wawancara) tanya jawab langsung ke ibu Sutarmi selaku manajer kepala penanggung jawab perusahaan dan berdiskusi langsung demi mendapatkan info akurat tentang permasalahan keamanan jaringan yang ada di purwacaraka music studio.

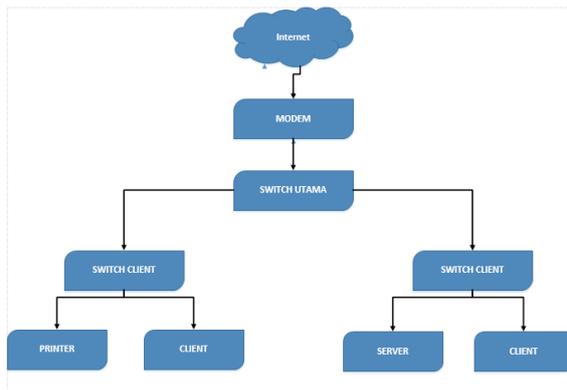
3 Studi pustaka (Literature)

Metode ini merupakan metode yang dimana pengumpulan referensi yang berkaitan dengan Virtual Local Area Network Dan ACL (Access Control List) . dengan menganalisa per topiknya . dan kemudian analisis per topiknya untuk memberikan kesimpulan tiap bagian pembahasan

HASIL DAN PEMBAHASAN

Pengelompokan paket berdasarkan daftar data yang didaftarkan menurut kategori yang dibuat dikenal sebagai Daftar Kontrol Akses. Saat Anda perlu mengontrol operasi jaringan, daftar akses bisa sangat berguna. Dalam hal mengontrol transit jaringan, daftar akses telah menjadi instrumen pilihan. Saat membuat kontrol keamanan, penggunaan daftar akses yang paling umum dan paling mudah dipahami adalah pemfilteran paket yang tidak tepat. Misalnya, kita dapat mengonfigurasi daftar akses untuk membuat keputusan yang sangat rinci tentang aturan pola lalu lintas, yang memungkinkan hanya beberapa host untuk terhubung ke jaringan sementara menolak yang lain (Novriandi, 2020). Administrator jaringan dapat menerapkan kebijakan keamanan apa pun yang mereka buat dengan kalibrasi daftar akses yang tepat. Dalam beberapa kasus, seperti dengan paket data akses Blokir, daftar akses dapat berguna. Daftar akses analog digunakan untuk mengatur jaringan mana yang mungkin atau tidak dapat diwakili oleh sistem perutean dinamis. Dengan cara yang sama, atur daftar akses. Perbedaan utama adalah bagaimana itu diterapkan pada protokol perutean daripada antarmuka saat ini. Kami juga dapat membatasi jenis data nama lalu lintas yang mengaktifkan tautan ISDN dengan menggunakan daftar akses untuk memetakan paket, antrian, atau layanan QOS (Saputra, 2016)., dan mengontrol tipe lalu lintas data nama yang akan mengaktifkan link ISDN tersebut.

ACL yang berisi string numerik alfa (nama) dapat digunakan untuk mengidentifikasi IP Standar dan ACL yang Diperluas. ACL (Daftar Kontrol Akses), Alamat IP sumber dalam paket IP adalah satu-satunya kriteria yang diverifikasi oleh standar ACL. Alamat IP sumber digunakan untuk menetapkan semua kebijakan kontrol. ACL standar, dengan kata lain, melewati atau menolak semua paket protokol. ACL ini tidak membedakan jenis trafik IP seperti WWW, telnet, UDP, dan DSP. (Novriandi, 2020)



Sumber: Penulis

Gambar 1. Blok Diagram Jaringan

Banyak bidang tambahan di header Layer 3 dan Layer 4 dari paket IP dapat dievaluasi oleh ACL yang diperluas. ACL ini dapat mengevaluasi alamat IP sumber dan tujuan, bidang protokol header lapisan jaringan, dan nomor port header lapisan transport. Hal ini memungkinkan ACL yang diperluas untuk membuat keputusan yang lebih tepat dalam hal pengendalian lalu lintas (Supriyanto, 2019)

Ancaman Terhadap Keamanan Jaringan: Mengenalinya Karena kemajuan teknologi yang pesat, serangan terhadap keamanan sistem informasi (serangan keamanan) menjadi lebih umum. Di dunia maya, kejahatan komputer/cyber crime sering dilakukan oleh sekelompok orang yang bertujuan untuk membobol suatu sistem keamanan (Manuaba, 2012). Jika informasi pada sistem benar-benar dibutuhkan, perilaku ini dibuat untuk mencari, mengambil, mengubah, dan bahkan menghancurkannya. Penyerang dapat melakukan berbagai macam bentuk serangan, menurut (Mentang, Sinsuw, Najoan, & Elektro-ft, 2015):

a) Interception, yaitu pihak yang telah memperoleh hak akses informasi meskipun tidak memiliki hak akses.

b) Interupsi, di mana penyerang telah memperoleh kendali sebagian dari sistem tetapi tidak menguasai sepenuhnya. Administrator asli masih dapat masuk.

c) Fabrikasi, yang terjadi ketika penyerang memasukkan objek palsu ke dalam sistem target.

d) Modifikasi, di mana penyerang telah merusak sistem dan mengubahnya secara teratur.

VLAN memiliki manfaat sebagai berikut: (AHMAD FITRIANSYAH, 2019)

1) Meningkatkan kinerja jaringan dengan membagi satu domain broadcast menjadi beberapa domain broadcast.

2) Meningkatkan keamanan jaringan agar paket broadcast yang dikirim dari satu unit kerja tidak diterima oleh komputer di unit kerja lain, dan mengkonfigurasi jaringan agar komputer dapat terhubung ke server atau komputer lain pada subnet yang terpisah.

3) Tingkatkan jumlah fleksibilitas pada

VLAN digunakan dalam manajemen jaringan untuk memungkinkan administrator menghubungkan komputer mana pun ke VLAN, terlepas dari lokasi

fisiknya. Penulis dapat menjelaskan hasil dari jaringan komputer yang dimanfaatkan pada sanggar musik Purwacaraka dengan menggunakan sistem jaringan komputer diatas, yang meliputi :

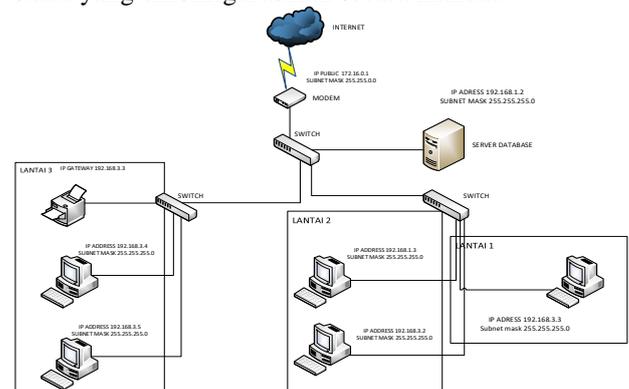
1. Pada jaringan komputer di Purwacaraka musik studio menggunakan jenis jaringan client-server, terdapat satu buah file server yang berfungsi memberikan lokasi untuk akses disk arena , yaitu penyimpanan arena file komputer seperti dokumen,data, gambar dan lainnya yang dapat diakses oleh pc-client. file server disini terhubung dengan routerboard yang berfungsi sebagai router inti jaringan ini.

2. Topologi yang digunakan pada jaringan Purwacaraka musik studio adalah topologi star.dimana setiap interface terhubung pada switch. Kemudian baru dari modem dihubungkan ke splitter kabel telpon untuk bisa terhubung ke internet.

3. Ip address yang digunakan pada jaringan komputer di Purwacaraka musik studio adalah IP kelas C dengan menggunakan subnetmask prefix/24 atau 255.255.255.

4. Jenis jaringan internet yang digunakan pada jaringan komputer Purwacaraka musik studio adalah jenis Dial-up ADSL dengan protocol PPPoE (Point to Point Protocol over Ethernet) dimana username dan password dari ISP dipasang pada modem TP-LINK TD-8817. ISP yang digunakan pada jaringan purwacaraka musik studio adalah indihome telkom speedy.

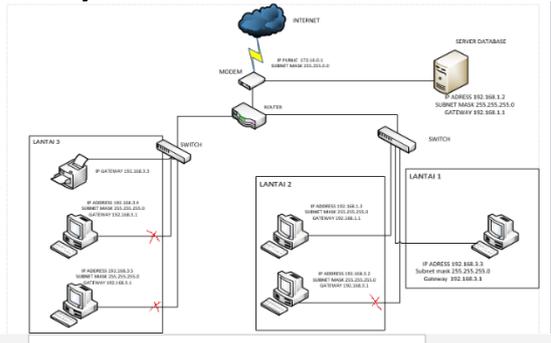
5. Menajemen IP yang digunakan pada jaringan komputer Purwacaraka musik studio adalah IP static yang dikonfigurasikan secara manual.



Sumber: Penulis

Gambar 2. Skema Jaringan Awal sesuai dengan permasalahan yang terjadi di kantor studio musik purwacaraka, jaringan yang ada saat ini sangat mudah dipasang dan diimplementasikan karena kebutuhan yang belum kompleks dan karyawan yang masih sedikit, namun seiring berkembangnya perusahaan, penambahan karyawan dan pengaturan yang jelas untuk masing-masing divisi akan diperlukan di masa depan. Jika situasi ini muncul, tentu akan memberikan tantangan yang signifikan dalam hal

pengelolaan dan keamanan data. Sebagai solusi untuk masalah ini, penulis mengusulkan pembuatan Jaringan Area Lokal Virtual Statis dan Daftar Akses menggunakan router firewall dan sakelar untuk mempertahankan hak akses data untuk setiap divisi menggunakan Daftar Akses, yang dapat digunakan untuk mencegah kesulitan di masa mendatang, dalam hal ini penulis akan membatasi akses ke server terhadap 3 PC Client dan membolehkan 2 PC Client untuk mengakses ke data server pada ruang utama. Berikut skemanya



Sumber: Penulis
Gambar 3. Skema Jaringan Akhir

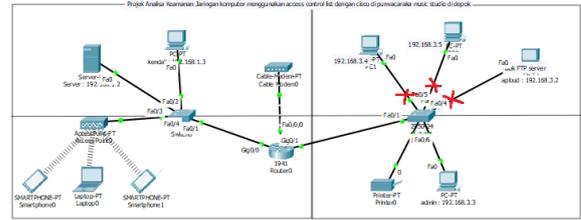
A. Pengujian Jaringan

Tes terakhir akan dilakukan untuk memeriksa apakah jaringan yang diusulkan menggunakan Daftar Kontrol Akses dan bahwa distribusi hak akses telah berjalan dengan baik. Pengujian level ini akan dilakukan dengan cara yang sama seperti sebelumnya yaitu dengan software Cisco packet tracer (Musyaffa & Sastra, 2020). Gambar dibawah ini menunjukkan sebuah Manageable Switch yang berfungsi untuk menangani kategori alamat IP yang terletak di setiap divisi selama pengujian jaringan yang diusulkan di kantor utama. Kehadiran manageable switch memberikan konsep Access InterVlan untuk mengelompokkan VLAN dari beberapa divisi menjadi satu dan menghubungkannya.

1. Cara mengkonfigurasi access control lists ke router cisco 1941

```
Router>enable
Router #configure terminal
Router(config) #access -lists 101 deny tcp host 192.168.3.2 host 192.168.1.2
Router(config) #access -lists 101 deny tcp host 192.168.3.5 host 192.168.1.2
Router(config) #access -lists 101 deny tcp host 192.168.3.8 host 192.168.1.2
Router(config) #access -lists 101 permit ip any any
Router(config) #int g0/1
Router(config-if) #ip access-groups 101 in
Router(config-if) #exit
```
- Gambar di atas adalah hasil konfigurasi Extended

di mana jalur IP pada komputer client tidak bisa mengakses ftp (file transfer protocol) pada server.



Sumber: Penulis
Gambar 4. skema skenario jaringan Usulan dengan paket tracer

Berikut adalah Konfigurasi ACL Extended pada aplikasi Packet tracer

```
Press RETURN to get started!

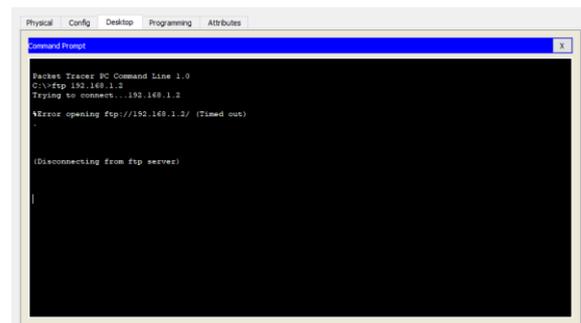
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router#enable
Router#sh acc
Router#sh access-lists
Extended IP access list 101
 10 deny tcp host 192.168.3.2 host 192.168.1.2
 20 deny tcp host 192.168.3.4 host 192.168.1.2
 30 deny tcp host 192.168.3.8 host 192.168.1.2
 40 permit ip any any

Router#
```

Sumber: Penulis
Gambar 5. konfigurasi access contro list Extended

Setelah konfigurasi selesai langkah selanjutnya mengecek CMD pada aplikasi packet tracer dan memastikan bahwa koneksi tidak terhubung antar jaringan dan telah tersetting



Sumber: Penulis
Gambar 6: Hasil Blokir Jaringan

KESIMPULAN

Setelah melakukan penelitian yang dilakukan penulis dalam hal perancangan jaringan berbasis router, maka dapat diambil beberapa kesimpulan. Pada tahap pengujian jaringan yang diusulkan, dapat dilihat bahwa hasil pemantauan paket data yang melewati jaringan Access Control List adalah routing pada CLI (Command Line Interface) yang membuat paket data dien kapsulasi. melalui perangkat router. Access

Control Daftar desain jaringan menggunakan router di server tidak memerlukan biaya tambahan atau software pendukung. Jaringan Daftar Kontrol Akses memberikan solusi keamanan karena adanya sistem otentikasi untuk klien atau karyawan yang akan mengakses jaringan lokal atau jaringan klien. Penggunaan dan konfigurasi Access Control List mudah dioperasikan. Sehingga dari segi performa, tidak memakan waktu yang relatif lama dalam pengoperasiannya. Sehingga dalam hal kinerja tidak memakan waktu yang relatif lama pada saat pengoperasiannya.

JARINGAN VPN BERBASIS IP-MPLS.
Paradigma, XV(1), 98–105.

REFERENSI

- AHMAD FITRIANSYAH. (2019). PENERAPAN STATIC VLAN DAN ACCESS LIST. *Jurnal Teknologi Informatika Dan Komputer*, 5(2), 1–6.
- Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). *Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis*. 8(1), 128–139.
- Fathurrahmad, Yusuf, S. (2019). Implementasi Jaringan VPN dengan Routing Protocol terhadap Jaringan Multiprotocol Label Switching (MPLS). *Jurnal JTJK*, 3(1).
- Manuaba, H. (2012). Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas. *JNTETI*, 1(1).
- Mentang, R., Sinsuw, A. A. E., Najoran, X. B. N., & Elektro-ft, J. T. (2015). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *E-Journal Teknik Elektro Dan Kompute*, 5(7), 35–44.
- Musyaffa, N., & Sastra, R. (2020). Implementasi Access Inter-VLAN Menggunakan Router. *InsanTek*, 1(2), 77–81.
- Novriandi, D. (2020). RANCANG DAN BANGUN SISTEM KEAMANAN JARINGAN DENGAN VIRTUAL LAN DAN ACCES CONTROL LIST PT ELECTRONIC CITY CIPINANG INDAH MALL. *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, 16(2), 45–53.
- Saputra, D. (2016). *IMPLEMENTASI VIRTUAL PRIVATE NETWORK PADA SISTEM INFORMASI PENGELOLAAN KEUANGAN*. 6(2), 18–31.
- Supriyanto, B. (2019). Perancangan Jaringan VPN Menggunakan Metode Point To Point Tunneling Protocol. *Jurnal Teknik Komputer AMIK BSI*, V(2).
<https://doi.org/10.31294/jtk.v4i2>
- Suryanto, & Dewi, S. (2013). IMPLEMENTASI