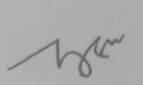
ANALISIS AKSES KEAMANAN JARINGAN LAPAN BERDASARKAN *LOG FIREWALL* DI LAPAN PUSAT

ADITYO JAYA SUBAKTI
5235131557

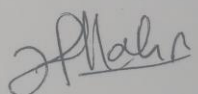
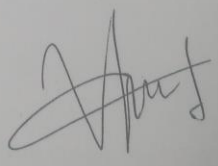
Skripsi ini Ditulis untuk Memenuhi Sebagian Persyaratan dalam Memperoleh gelar Sarjana Pendidikan

PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS NEGERI JAKARTA
2017

HALAMAN PENGESAHAN

NAMA DOSEN	TANDA TANGAN	TANGGAL
Lipur Sugiyanta, Ph.D (Dosen Pembimbing I)		22/2 2017
Drs. Bachren Zaini, M.Pd (Dosen Pembimbing II)		23/2 2017

PENGESAHAN PANITIA UJIAN SKRIPSI

NAMA DOSEN	TANDA TANGAN	TANGGAL
Dr. Yuliatri Sastrawijaya (Ketua Penguji)		23/2 2017
Hamidillah Ajie., M.T (Sekretaris Penguji)		22/2 2017
Vina Oktaviani, M.T (Dosen Ahli)		22/2 2017

ii

HALAMAN PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Karya tulis skripsi saya yang berjudul Analisis Akses Keamanan Jaringan LAPAN Berdasarkan *Log Firewall* Di LAPAN Pusat adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik sarjana, baik di Universitas Negeri Jakarta maupun di perguruan tinggi lain.
2. Karya tulis yang berjudul Analisis Akses Keamanan Jaringan LAPAN Berdasarkan *Log Firewall* Di LAPAN Pusat adalah murni gagasan, rumusan, dan penelitian saya sendiri dengan arahan dosen pembimbing.
3. Dalam karya tulis ini, tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma yang berlaku di Universitas Negeri Jakarta.

Jakarta, 8 Febuari 2017

Yang membuat pernyataan

Adityo Jaya Subakti

5235131557

KATA PENGANTAR

Puji dan syukur saya panjatkan kehadirat Tuhan Yang Maha Esa, yang telah memberikan rahmat, karunia-Nya, sehingga saya dapat menyelesaikan skripsi dengan judul "Analisis Akses Keamanan Jaringan Berdasarkan Log Firewall Di LAPAN Pusat". Skripsi ini disusun sebagai persyaratan untuk meraih gelar Sarjana Pendidikan Teknik Informatika dan Komputer pada Fakultas Teknik, Universitas Negeri Jakarta.

Dalam menyelesaikan skripsi ini penulis telah mencurahkan segala kemampuan dan penulis menyadari akan kemampuan dan keterbatasan yang dimiliki. Oleh sebab itu pada kesempatan ini saya ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Bapak Lipur Sugiyanta, Ph.D selaku pembimbing I yang telah memberikan waktu, motivasi, arahan dan kepercayaan kepada penulis dalam menyelesaikan skripsi ini.
2. Bapak Drs. Bachren Zaini, M.Pd., selaku pembimbing II yang telah memberikan waktu, motivasi, arahan dan kepercayaan kepada penulis dalam menyelesaikan skripsi ini.
3. Prof. Dr. Ir. Ivan Hanafi, M.Pd, selaku pembimbing akademik.
4. Seluruh dosen dan staf tata usaha Program Studi Pendidikan Teknik Informatika dan Komputer yang selalu membantu menyediakan informasi dan membantu proses administrasi skripsi
5. Surono Setiyo Atmojo, S.Kom., M.T.I., selaku Kepala Subbidang Infrastruktur Teknologi dan Informasi di LAPAN yang membantu proses penelitian untuk pengerjaan skripsi
6. Keluarga penulis selaku orang tua Tukul Lasiman dan Ening Kusumaningsih, selaku saudara kandung Teny Damayanti Putri yang selalu memberikan semangat, kekuatan, dan doa yang tulus dalam pengerjaan skripsi penulis
7. Abel Balbo, Sandi Rahmayadi, Engki Budhi, yang memberi bantuan doa dan semangat pada penulis

8. Keluarga PTIK 2013 dan University Of Jagad Raya, terutama Akbar Jaya, Taufiq Akbar yang senantiasa memberikan dukungan dan semangat kepada penulis
9. Bimo sebagai laboran PTIK yang membantu penyediaan sarana dan prasarana laboratorium PTIK untuk pengerjaan skripsi
10. Semua pihak yang secara langsung maupun tidak langsung membantu proses penyelesaian skripsi ini.

Saya menyadari bahwa skripsi masih jauh dari sempurna, karenanya saya mengharapkan kritik dan saran yang membangun untuk perbaikan yang lebih baik lagi di masa yang akan datang. Akhir kata, penulis berharap semoga skripsi ini dapat bermanfaat dan berguna bagi pembaca serta dapat mendukung kemajuan ilmu pengetahuan khususnya di bidang pendidikan.

Jakarta, 8 Januari 2017

Penulis.

Adityo Jaya Subakti

5235131557

ABSTRAK

ADITYO JAYA SUBAKTI, Analisis akses keamanan jaringan LAPAN berdasarkan log firewall di LAPAN Pusat. Pembimbing LIPUR SUGIYANTA, Ph.D dan Drs. BACHREN ZAINI, M.Pd.

Meningkatnya serangan Denial Of Service, dan jenis gangguan jaringan komputer lainnya, membuat keamanan menjadi isu yang penting untuk diperhatikan oleh semua pihak yang memanfaatkan keberadaan dunia maya saat ini. Sistem komputer LAPAN Pusat beserta informasi yang terkandung di dalam tidak terkecuali terdapat serangan pada akses keamanan jaringan komputer. Serangan tersebut dapat secara dini dicegah dengan menganalisa pada setiap akses yang akan masuk pada keamanan jaringan LAPAN. Tujuan penelitian ini adalah untuk mengetahui dan mempelajari akses keamanan jaringan di dalam log firewall LAPAN Pusat. Penelitian ini dilaksanakan dengan beberapa tahap observasi dan wawancara kepada karyawan infrastruktur LAPAN Pusat. Setelah tahap observasi dan wawancara, selanjutnya peneliti melakukan pengumpulan data dan analisis log firewall. Hasil penelitian menyatakan bahwa analisis akses keamanan jaringan berdasarkan log firewall di LAPAN Pusat berupa enam pesan yang terjadi pada saat sebuah jaringan akan melewati firewall. Dapat disimpulkan bahwa dengan melakukan beberapa tahap Analisis akses keamanan jaringan berdasarkan log firewall di LAPAN Pusat menghasilkan catatan setiap kejadian di dalam log firewall.

Kata kunci: Denial Of Service, Hacker, log, firewall, Analisis dan Akses.

ABSTRACT

ADITYO JAYA SUBAKTI, Analysis of Network Security Access Space Agency Based Firewall Log In LAPAN Center. Supervisor LIPUR SUGIYANTA, Ph.D dan Drs. BACHREN ZAINI, M.Pd.

Increased Denial Of Service attacks, and other types of computer network interference, making security an important issue to be considered by all those who take advantage of the presence of the virtual world today. LAPAN Pusat system along with the information contained within is no exception contained attacks on access computer network security. Such attacks can be prevented at an early stage by analyzing at each access that will go on network security in LAPAN. This research aimed to Analysis of Network Access to know and learn access of network security in log firewall LAPAN Center. This research was conducted with several stages of observation and interviews to employees LAPAN Center infrastructure. After the stage of observation and interviews, the researchers conducted further data collection and analysis of firewall logs. The study states that the analysis of security access network based firewall log in LAPAN Centre in the form of six messages that occur when a network will pass through the firewall. It can be concluded that by doing some analysis phases of network security access based firewall log in LAPAN Centre produces a record every incident inside the firewall logs.

Keywords: log, firewall, Analysis dan Access.

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pada era global saat ini, teknologi informasi (TI) telah berkembang dengan pesat, terutama dengan adanya jaringan internet yang dapat memudahkan dalam melakukan komunikasi dengan pihak yang lain. Selain itu, para pengguna atau user dapat mengakses hampir seluruh informasi yang dibutuhkan baik itu informasi yang bersifat publik maupun bersifat pribadi.

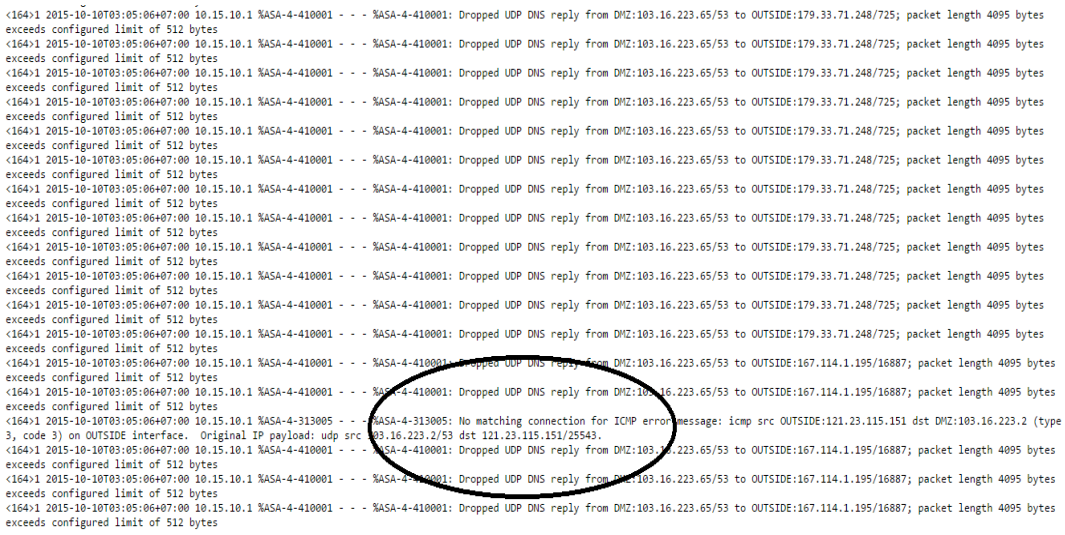
Namun dengan mudahnya pengaksesan terhadap informasi tersebut menyebabkan timbulnya masalah di LAPAN (Lembaga Penerbangan dan Antariksa Nasional) yaitu informasi atau data-data penting dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri. Sehingga suatu sistem keamanan pada jaringan LAPAN menjadi salah satu aspek yang penting untuk diperhatikan dari sebuah sistem informasi.

Internet sebagai para pencari informasi. Hampir semua jenis informasi bisa didapatkan melalui dunia maya ini, termasuk informasi kedirgantaraan. LAPAN saat ini telah banyak memanfaatkan *internet* untuk mendapatkan informasi secara cepat tanpa dibatasi dimensi ruang dan waktu. Tetapi seperti halnya teknologi baru yang membawa keuntungan ternyata *internet* juga membawa masalah baru yaitu masalah serangan informasi.

Pesatnya penggunaan *internet* sebagai sarana pencarian dan penyebaran informasi di lingkungan LAPAN, secara langsung maupun tidak langsung telah banyak mempengaruhi proses dan cara kerja di LAPAN saat ini, jika hal ini tidak

ditangani dengan baik khususnya dalam hal keamanan jaringan, maka informasi yang ada di LAPAN akan sangat rentan terhadap serangan melalui *internet*.

Besarnya kemampuan konektivitas yang dimiliki oleh jaringan komputer LAPAN pusat menimbulkan masalah yang cukup mengganggu, yaitu berupa serangan melalui jaringan *internet*. Serangan yang umum dihadapi di jaringan komputer LAPAN pusat saat ini ialah *server* LAPAN diakses oleh orang lain melalui jaringan *internet* dari dalam maupun luar, dengan menggunakan berbagai cara untuk bisa mengakses lebih jauh isinya. Hal ini dilakukan untuk merubah konfigurasi sistem komputer yang dimasuki sehingga orang tersebut dapat mengambil data-data penting yang disimpan di dalamnya.



Gambar 1.1 Pembuktiaan *No matching connection*

Pembuktian salah satu permasalahan jaringan LAPAN Pusat ialah *No matching connection* yang berakibat tidak mendapatkan akses pada keamanan jaringan di LAPAN Pusat. Saat ini sering terdapat keluhan seperti *No matching connection*, *Flooding*, dan *Port Scanning* yang selanjutnya dapat berimbas pada penurunan performa jaringan *internet* yang terhubung pada jaringan tersebut.

Akibatnya, mudahnya lalu lintas data atau paket-paket berbahaya yang tidak di izinkan masuk ke dalam jaringan.

Biasanya sistem keamanan tergantung dari ketersediaan dan kecepatan administrator dalam menangani gangguan yang akan terjadi pada jaringan LAPAN. Apabila jaringan mengalami gangguan yang menyebabkan jaringan tidak berfungsi maka administrator juga tidak dapat lagi mengakses sistem bahkan administrator tidak dapat memperbaiki atau memulihkan sistem dengan cepat.

Sistem keamanan jaringan merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas data di LAPAN. Agar sistem jaringan komputer di LAPAN tidak terganggu bahkan sampai rusak oleh serangan penyusup (*intrusion*), maka diperlukan analisa sistem keamanan jaringan yang dapat menanggulangi dan mencegah serangan penyusup tersebut.

Salah satu cara untuk meningkatkan keamanan dalam jaringan di LAPAN adalah dengan meningkatkan keamanan data, pengamanan data bisa dilakukan dengan memanfaatkan teknonolgi enkripsi dan dekripsi. Teknologi ini akan mengubah data ke dalam bentuk yang lain sehingga tidak dapat dibaca oleh orang lain.

Keamanan jaringan komputer sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersedian layanan bagi penggunanya. Agar sistem jaringan komputer tidak terganggu bahkan terjadi rusak oleh serangan penyusup, maka diperlukan sistem keamanan jaringan yang dapat menanggulangi dan mencegah serangan penyusup tersebut.

firewall pada sistem yang memiliki kemampuan hanya melewatkan trafik yang diizinkan untuk masuk ke dalam sebuah jaringan komputer, dan secara otomatis menghalangi atau memblokir semua trafik lainnya.

Serangan yang paling sering digunakan adalah *Port Scanning* dan DOS (*Denial Of Service*). *Port Scanning* adalah serangan yang bekerja untuk mencari *port* yang terbuka pada suatu jaringan komputer, dari hasil *port scanning* akan didapat letak kelemahan sistem jaringan komputer tersebut. DOS adalah serangan yang bekerja dengan cara mengirimkan *request* ke *firewall* berulang kali untuk bertujuan membuat *firewall* menjadi sibuk menanggapi *request* tersebut. Setelah itu, akan mengalami kerusakan bahkan bisa terjadi *hang* pada komputer.

Setelah melakukan observasi berupa wawancara dengan Kepala Subbidang Infrastruktur Teknologi Informasi di LAPAN diperoleh informasi bahwa keamanan *firewall* mereka masih rentan adanya penyusupan, hal itu dikarenakan LAPAN pada tahun 2016 masih mengalami kesulitan dalam menganalisa akses keamanan jaringan menggunakan *firewall*. Berdasarkan wawancara dengan empat karyawan Infrastruktur jaringan LAPAN diperoleh informasi bahwa mereka mengalami kesulitan dalam menganalisa serangan terhadap keamanan jaringan baik dari luar maupun dalam jaringan di LAPAN Pusat.

Untuk keamanan sistem serta beberapa keperluan jaringan lainnya. Didalam konsep jaringan semua *service* berjalan melalui jalur yang dinamakan *port*. Sehingga dengan *firewall* ini dapat dilakukan proses penyaringan *traffic network* apa dan bagaimana yang diperbolehkan atau dilarang.

Dari uraian maka peneliti memutuskan untuk mengambil topik “Analisis Akses Keamanan Jaringan LAPAN Berdasarkan *Log Firewall* di LAPAN Pusat”.

1.2 Identifikasi Masalah

Dari latar belakang masalah sebelumnya maka dapat di identifikasi masalah sebagai berikut :

1. Karyawan Infrastruktur LAPAN masih mengalami kesulitan dalam menganalisa akses keamanan jaringan menggunakan *firewall*.
2. Karyawan Infrastruktur LAPAN masih mengalami kesulitan dalam menganalisa serangan terhadap keamanan jaringan baik dari luar maupun dalam jaringan di LAPAN Pusat

1.3 Batasan Masalah

Untuk menghindari penyimpangan dari topik yang dipilih dan juga sesuai dengan latar belakang permasalahan yang sudah diuraikan, maka didalam hal ini masalah yang akan dibahas, yaitu : (1) Analisis akses keamanan jaringan LAPAN berdasarkan *log firewall*

1.4 Rumusan Masalah

Dari batasan masalah diatas maka dapat dirumuskan masalah sebagai berikut : (1) Bagaimana akses keamanan jaringan LAPAN berdasarkan *log firewall* di LAPAN Pusat ?

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah : (1) Untuk mengetahui dan mempelajari akses keamanan jaringan di dalam *log firewall* LAPAN Pusat.

1.6. Manfaat Penelitian

1. **Bagi penulis**

Dengan adanya penelitian yang dilakukan di LAPAN, penulis mendapatkan pemahaman lebih mendalam mengenai sistem keamanan jaringan yang bisa dikembangkan dalam dunia teknologi.

2. **Bagi Lembaga LAPAN**

Dengan adanya penelitian akan membantu LAPAN dalam meningkatkan keamanan jaringan di LAPAN Pusat

BAB II

KERANGKA TEORITIK DAN KERANGKA BERPIKIR

2.1 Kerangka Teoritik

2.1.1 Teori Sistem Keamanan Jaringan Komputer

Keamanan jaringan komputer adalah suatu kebutuhan yang sangat vital untuk diimplementasikan di dalam sebuah jaringan komputer, apalagi bila jaringan komputer tersebut terhubung ke jaringan luar yang secara teknis tentu siapa saja dapat mengakses jaringan milik suatu perusahaan tersebut. Hal ini menjadi kendala apabila *user* luar yang mengakses, mempunyai suatu niat yang buruk terhadap segala macam komponen jaringan perusahaan, mulai dari data, operating sistem dan lainnya (LAPAN, 2004:2).

2.1.2 Definisi Sistem Keamanan Jaringan Komputer

Sistem keamanan jaringan komputer dapat didefinisikan sebagai sekumpulan perangkat untuk memantau dan mengontrol jaringan. Sistem keamanan jaringan terdiri dari tambahan perangkat keras dan perangkat lunak yang diimplementasikan di antara komponen-komponen jaringan yang sudah tersedia. (Subramanian, 2000:40).

Sistem keamanan komputer dapat didefinisikan sebagai sebuah sistem yang digunakan untuk memproteksi dan menjaga semua sumber data dan unsur-unsur yang terdapat pada suatu jaringan komputer, bentuk pengamanannya bisa berupa *hardware* maupun *software* yang telah diberikan fasilitas untuk suatu pengamanan jaringan.

2.1.3 Konsep Dasar Keamanan Jaringan

Konsep dasar keamanan jaringan menjelaskan lebih banyak mengenai keamanan (*security*) dari sebuah sistem jaringan komputer yang terhubung ke internet terhadap ancaman dan gangguan yang ditunjukan kepada sistem tersebut (Jufriadif Na'Am, 2003:15).

Sistem keamanan komputer dapat didefinisikan sebagai sebuah integritas sistem yang digunakan untuk menjaga semua sumber daya dan unsur-unsur yang terdapat pada suatu jaringan komputer, bentuk pengamananya bisa berupa *hardware* maupun *software* yang telah diberikan fasilitas untuk suatu pengamanan jaringan (Achmad Fauzie, 2004:25).

Keamanan jaringan dapat digambarkan secara umum yaitu apabila komputer yang terhubung dengan jaringan yang lebih banyak mempunyai ancaman keamanan dari pada komputer yang tidak terhubung ke mana-mana. Namun dengan adanya pengendalian maka resiko yang tidak diinginkan dapat dikurangi. Adanya keamanan jaringan maka para pemakai berharap bahwa pesan yang dikirim dapat sampai dengan baik ke tempat yang dituju tanpa mengalami adanya keterlambatan yang diterima oleh si penerima, misalnya saja adanya perubahan pesan. Biasanya jaringan yang aksesnya semakin mudah, maka keamanan jaringannya semakin rawan, namun apabila keamanan jaringan semakin baik maka pengaksesan jaringan juga semakin nyaman dan semakin sulit diserang oleh hacker.

Keamanan suatu sistem berbanding terbalik dengan kemudahan, jika menginginkan akses jaringan yang mudah maka keamanannya menjadi semakin rawan, begitupun sebaliknya apabila menginginkan sistem yang lebih aman maka pengaksesan jaringan akan semakin sulit. Namun dengan langkah-langkah

pengendalian dan pencegahan yang tepat, maka dapat mengurangi resiko pada jaringan komputer di LAPAN berupa dalam bentuk ancaman fisik maupun *logic* baik secara langsung maupun tidak langsung.

Adapun upaya meningkatkan keamanan jaringan sebuah sistem harus memenuhi beberapa unsur, antara lain:

1. *Confidentiality* (kerahasiaan) : Pembatasan akses hanya pada *user* yang berhak atas suatu data atau informasi, dan mencegah akses dari *user* yang tidak memiliki hak.
2. *Integrity* (integritas) : Keaslian data atau informasi yang dikirim melalui jaringan dari sumber ke penerima secara lengkap, tanpa ada modifikasi atau manipulasi oleh pihak yang tidak berwenang.
3. *Availability* (ketersediaan) : Ketersediaan data atau informasi ketika dibutuhkan saat itu juga.

Tujuan keamanan jaringan dapat dicapai dengan suatu metode keamanan jaringan yang dapat melindungi sistem keamanan di LAPAN. Namun bukan hanya melindungi tetapi harus dapat bertindak apabila terjadi serangan yang ada di dalam jaringan LAPAN. Salah satu metode tersebut yaitu *Intrusion Detection System* (IDS). Selain metode tersebut dibutuhkan juga suatu pemahaman tentang menentukan kebijakan keamanan (*Security Policy*) dalam keamanan jaringan yang berada di LAPAN. Jika ingin menentukan apa saja yang harus dilindungi maka harus mempunyai perencanaan keamanan jaringan, karena apabila tidak direncakanan maka tidak akan sesuai dengan yang diharapkan dalam perlindungan jaringan.

2.1.4 Keamanan Jaringan

Keamanan jaringan adalah melindungi jaringan, keamanan tidak hanya tentang menjaga IP di dalam jaringan maupun dari luar. Akan tetapi juga menyediakan akses ke dalam jaringan dengan cara yang dikehendaki, mempersilakan IP di dalam jaringan itu untuk saling bekerja sama (Stallings, 2003:4).

Masalah keamanan menjadi salah satu perhatian pada sistem keamanan jaringan komputer di LAPAN karena resiko keamanan semakin bertambah maka semakin kejahatan *cyber* meluas untuk menyusup sistem keamanan jaringan komputer tanpa batas.

Berikut beberapa ancaman yang umum ditemui pada jaringan komputer di LAPAN yaitu :

1. ARP *Spoofing*

   Penyerang menangkap penyebaran paket ARP dari access point dan kemudian mengirimkan balasan ARP fiktif sehingga informasi perangkat dari penyerang akan terpetakan ke dalam table ARP untuk kemudian mendapatkan hak akses ke dalam jaringan.

2. *Denial Of Service* (DOS)

   Metode serangan dengan mengirimkan paket data dalam jumlah yang sangat besar terhadap jaringan yang menjadi targetnya secara terus-menerus. Hal ini dapat mengganggu lalu lintas data bahkan dapat merusak sistem jaringan server.

3. MAC *Spoofing*

Penyerang berusaha mendapatkan koneksi ke dalam jaringan dengan mengambil alamat NIC dari suatu perangkat komputer pada jaringan yang ditargetkan.

2.1.5 Beberapa Cara Pengamanan Jaringan Komputer

Pada umumnya, pengamanan dapat dikategorikan menjadi dua jenis yaitu Pencegahan (*preventif*) dan Pengobatan (*recovery*). Usaha pencegahan dilakukan agar sistem informasi tidak memiliki lubang keamanan, sementara usaha-usaha pengobatan dilakukan apabila lubang keamanan sudah dieksploitasi. Secara fisik, sistem dapat juga diamankan dengan menggunakan *firewall* yang memisahkan sistem dengan *internet* (Garfinkel, 2009:38).

2.1.5.1 Mengatur Akses

Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme *authentication* dan *access control*. Dengan menggunakan *firewall*, administrator diharuskan melalui proses *authentication* dengan menuliskan *userid* dan *password*. Salah satu cara untuk mempersulit *hacker* untuk mendapatkan *log* yang berisi *password* adalah dengan menggunakan *shadow password* (Madcoms, 2009:12)

2.1.5.2 Menutup Service Yang Tidak Digunakan

Perangkat keras dan perangkat lunak diberikan dengan beberapa *service* dijalankan secara *default*. Untuk mengamankan sistem, *service* yang tidak diperlukan dapat dimatikan (Garfinkel, 2009:40).

2.1.5.3 Memasang Proteksi

Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi dapat berupa *firewall* yang dapat digunakan untuk memfilter e-mail, informasi, dan akses. *Firewall* merupakan sebuah perangkat

yang diletakkan antara *Internet* dengan *server*. Informasi yang keluar atau masuk harus melalui *firewall* yang bekerja untuk mengamati paket IP (*Internet Protocol*) yang melewatinya. Berdasarkan konfigurasi dari *firewall*, maka akses dapat diatur berdasarkan IP *address*, *port*, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing *firewall*. (Madcoms, 2009: 14

2.1.6 Kebijakan Keamanan

Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi data-data di dalam sistem jaringan keamanan komputer tersebut secara efektif. (Onno W. Purbo dan Tony Wiharjito, 2000:10).

Perencanaan keamanan yang baik dapat membantu menentukan apa yang harus dilindungi, seberapa besar nilai atau biayanya, dan siapa yang bertanggung jawab terhadap data maupun aset-aset lain dalam jaringan komputer di LAPAN. Secara umum terdapat tiga hal yang harus diperhatikan dalam perencanaan kebijakan keamanan jaringan komputer: (Stallingsh, 2003:69).

1. *Risk* (resiko dan tingkat bahaya)

   Pembatasan akses hanya pada user yang berhak atas suatu data atau informasi, dan mencegah akses dari user yang tidak memiliki hak.

2. *Threat* (ancaman)

   Menyatakan sebuah ancaman yang dating dari seseorang yang mempunyai kenginginan untuk memperoleh akses illegal ke dalam suatu jaringan computer seolah-olah mempunyai otoritas terhadap jaringan tersebut.

3. *Vulnerability* (kerapuhan sistem)

Menyatakan seberapa kuat sistem keamanan suatu jaringan computer yang dimiliki dari seseorang dari luar sistem yang berusaha memperoleh akses illegal terhadap jaringan komputer tersebut.

Secara umum terdapat delapan hal yang harus diperhatikan dalam tingkat keamanan jaringan komputer: (Iwan, 2010:60).

1. *Emergency* (keadaan darurat)

   Pesan sistem yang tidak dapat digunakan lalu pesan harus dilaporkan ke CERT (*computer emergency response team*) dengan melakukan perbaikan pada sistem segera mungkin.

2. *Alert* (waspada)

   Pesan tindakan segera diperlukan untuk mengatasi bila paket yang lewat dinyatakan bahaya dengan melakukan tolak paket pada sistem yang berbahaya tersebut.

3. *Critical* (kritis)

   Pesan kondisi dimana sistem telah terjadi kerusakan yang harus diperbaiki dengan melakukan *maintence* supaya sistem tidak terjadi kerusakan.

4. *Error* (kesalahan)

   Pesan kondisi kesalahan dimana paket yang lewat telah terjadi kesalahan dengan melakukan perbaikan pada isi paket tersebut.

5. *Warning* (peringatan)

   Pesan kondisi peringatan dimana paket yang lewat berisi peringatan harus diwaspadai dengan melakukan perhatian pada paket tersebut.

6. *Notification* (pemberitahuan)

Pesan normal tetapi signifikan dimana *firewall* memberi pemberitahuan bahwa paket yang lewat tidak terlalu bahaya sehingga sistem mengizinkan paket masuk ke sistem.

7. *Information* (informasi)

   Pesan informasi dimana paket yang lewat dinyatakan aman dengan melakukan informasi kepada sistem bahwa paket diperbolehkan masuk ke sistem.

8. *Debugging* (kesalahan code)

   Pesan kondisi kesalahan pada kode dimana paket yang lewat hanya terdapat kesalahan kode sehingga sistem melakukan perbaikan kode pada paket tersebut.

2.1.7 Definisi Jaringan Komputer

Jaringan komputer merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling terhubung dalam melaksanakan tugasnya (Madcoms, 2009:2).

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan node, mencetak pada printer yang sama dan bersama-sama menggunakan *hardware* atau *software* yang terhubung dengan jaringan.

Tujuan dari jaringan komputer adalah agar setiap komputer dapat saling berbagi sumber daya, akses informasi, dan dapat saling berkomunikasi antara data

yang satu dengan yang lainnya. Manfaat dari jaringan komputer antara lain dapat melakukan pengiriman data secara cepat dan efisien, penghematan biaya untuk pembelian perangkat-perangkat keras seperti printer, scaner karena perangkat tersebut bisa dipakai bersama-sama melaluin jaringan komputer, mudahnya untuk melakukan manajemen maupun keamanan data pada setiap komputer client yang tersambung pada komputer server.

2.1.8 Jenis-Jenis Jaringan Komputer

Jenis-jenis jaringan komputer berdasarkan jangkauan area atau lokasi, jaringan komputer dibedakan menjadi 7 jenis yaitu: (Madcoms, 2009: 3).

2.1.8.1 *Local Area Network* (LAN)

Local Area Network (LAN) merupakan suatu jaringan komunikasi yang saling menghubungkan berbagai jenis perangkat dan menyediakan suatu pertukaran data diantara perangkat-perangkat tersebut. (Stallings, 2004:16). LAN merupakan suatu jaringan yang menghubungkan dua atau lebih komputer dan alat-alat yang terhubung dalam sebuah area geografis yang terbatas, berkecepatan tinggi, dan memiliki *error* yang rendah dalam sebuah perusahaan. (Lammle, 2005:670).

LAN merupakan suatu jaringan pribadi di dalam sebuah bangunan sampai beberapa kilometer dari gedung tersebut. LAN banyak digunakan untuk menghubungkan komputer dan *workstatiton* di dalam kantor perusahaan, pabrik-pabrik untuk dapat saling berbagai sumber daya dan bertukar informasi. LAN dibedakan dari tiga karakteristik, yaitu: (1) Ukuran, (2) Teknologi transmisi, dan (3) Topologi (Tanenbaum, 2003:16).

Local Area Network (LAN) merupakan jaringan yang menghubungkan sejumlah komputer yang ada dalam suatu lokasi dengan area terbatas seperti ruang atau gedung pada sebuah sekolah maupun area gedung perkantoran. Biasanya pada jaringan setiap komputer dapat mengakses data dari komputer lain, menggunakan perangkat lain yang terhubung dengan jaringan seperti printer. Jumlah komputer yang terhubung pada LAN relatif kecil dan kebanyakan menggunakan kabel sebagai media penghubung.

2.1.8.2 *Metropolitan Area Network* (MAN)

Metropolitan Area Network (MAN) merupakan suatu jaringan yang dapat menghubungkan beberapa LAN menjadi suatu jaringan yang lebih bersar. MAN termasuk jaringan yang jarak antara satu sistem dengan sistem lainnya relative lebih jauh ketimbang LAN, Jangkauan MAN dalam satu kota (Lammle, 2005:674).

Metropolitan Area Network (MAN) merupakan jenis jaringan yang lebih besar dari LAN. Sebuah MAN terdiri dari beberapa jaringan LAN yang saling terhubung dalam lingkup area yang lebih luas seperti suatu wilayah pada satu provinsi, Sebagai contoh jaringan bank, dimana beberapa kantor cabang sebuah bank pada kota besar dihubungkan antara satu dengan lainnya.

2.1.8.3 *Wide Area Network* (WAN)

Wide Area Network (WAN) merupakan jenis jaringan yang ruang lingkup sudah terpisahkan oleh batas geografis dan biasanya sebagai penghubungnya sudah menggunakan media satelit atau kabel bawah laut. Teknologi jaringan sekarang memungkinkan WAN menggunakan media *fiber optic*, di mana

kecepatan pengiriman data sangat tinggi. Bentuk WAN biasanya digunakan oleh perusahaan besar maupun departemen pemerintahan dikarenakan harga instalasinya yang terlalu besar (Stallings, 2000:9).

Wide Area Network (WAN) merupakan jenis jaringan yang memberikan layanan lebih luas lagi dibanding MAN, yaitu dapat menghubungkan suatu Negara bahkan benua. WAN biasanya menggunakan satelit dan kabel bawah laut untuk menghubungkan satu sama lain. Selain itu terdapat 2 tipe jaringan yang dapat digunakan dalam mengatur sebuah jaringan komputer, antara lain.

2.1.8.4 *Client-Server*

Diawali perkembangannya perangkat komputer adalah barang yang mahal dan mewah. Pengembangan dan pengoperasiannya rumit. Namun seiring dengan berjalannya waktu yang telah dikembangkan menjadi proses terdistribusi sampai pada *end user*. Dipengaruhi oleh adanya perkembangan teknologi LAN (*Local Area Network*) di pertengahan tahun 1980' (Fadel, 2010).

Tipe jaringan client-server menggunakan komputer *server* dengan beberapa koputer client/workstation. Komputer *server* adalah komputer yang menyediakan fasilitas atau layanan bagi komputer-komputer lain yang terhubung dalam jaringan. Sedangkan komputer client adalah komputer-komputer yang menggunakan fasilitas atau layanan yang diberikan oleh komputer *server*. Biasanya komputer *server* pada sebuah jaringan disebut juga dengan Dedicated *server* karena komputer yang digunakan hanya sebagai penyedia fasilitas atau layanan untuk komputer client/workstation.

2.1.8.5 *Peer-to-peer*

Tipe jaringan *peer-to-peer* menghubungkan beberapa komputer dalam sebuah jaringan. Pertukaran data dapat dilakukan antara komputer yang terhubung

tanpa perantara komputer *server*. Masing-masing komputer dapat berperan sebagai komputer *server* sekaligus sebagai komputer client (Warino, 2003:26).

2.1.8.6 *Internet*

Internet (*Interconnected Network*) adalah jaringan komputer yang terdiri dari ribuan jaringan komputer independen yang dihubungkan satu dengan lainnya. Secara etimologis, *internet* berasal dari bahasa inggris yaitu *inter* berarti antar dan *net* berarti jaringan sehingga dapat diartikan hubungan antar jaringan (Fadel, 2010).

Internet adalah sekumpulan jaringan yang berlokasi tersebar di seluruh dunia yang saling terhubung membentuk satu jaringan besar komputer. Dalam jaringan dibatasi layanannya sebagai berikut: (1) FTP, (2) E-Mail, (3) Telnet, dan *Mailing List*. Biasanya jaringan menggunakan *protocol* TCP/IP.

2.1.8.7 *Logging* dan *Alerting System*

Tergantung pada apa yang *Detection Engine* temukan dalam sebuah paket, lalu paket digunakan untuk mencatat aktivitas atau menghasilkan peringatan (*alert*) (Madcoms, 2009:45).

2.1.9 Arsitektur Jaringan Komputer

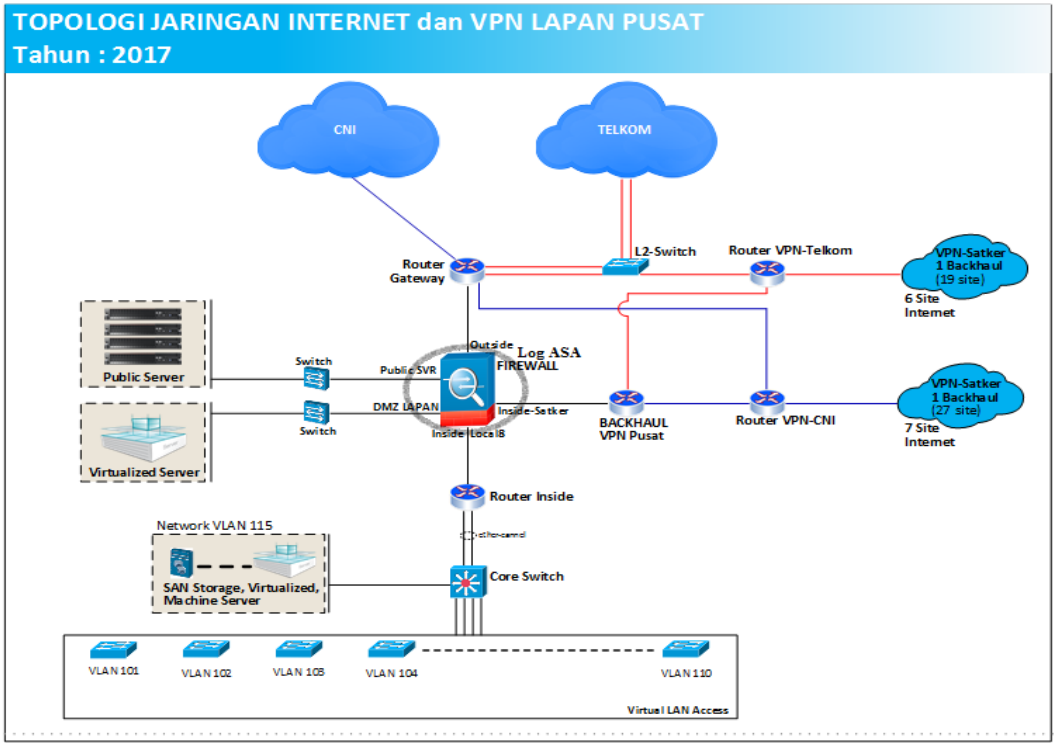
Arsitektur sebuah jaringan komputer dibedakan menjadi arsitektur fisik dan arsitektur logik. Arsitektur fisik berkaitan dengan susunan fisik sebuah jaringan komputer, bisa juga disebut dengan topologi fisik jaringan yaitu menjelaskan hubungan perkabelan dan lokasi node (simpul) atau *workstation*. Sedangkan arsitektur *logic* berkaitan dengan logika hubungan masing-masing komputer

dalam jaringan atau menjelaskan aliran data dari satu *user* ke *user* lainnya dalam jaringan (Setiawan, 2012:68).

Topologi adalah suatu cara menghubungan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Banyak cara yang digunakan adalah *Bus*, *Star*, *Token-Ring*, dan *Peer-to-peer* jaringan. (Fadel, 2010:5).

Topologi dari sebuah jaringan adalah merujuk pada konfigurasi kabel, komputer, dan perangkat lainnya. Salah satu topologi yang digunakan oleh LAPAN yaitu: Topologi *Star*.

2.1.9.1 Topologi LAPAN Pusat



Gambar 2.1 Topologi *Star* (LAPAN, 2017)

Dalam topologi LAPAN Pusat, masing-masing komputer dalam jaringan dihubungkan ke pusat *server* LAPAN dengan menggunakan jalur data yang berbeda. Dengan digunakannya jalur yang berbeda untuk masing-masing komputer maka jika terjadi gangguan atau masalah pada salah satu titik dalam

jaringan tidak akan mempengaruhi bagian jaringan yang lain. Hal ini juga memungkinkan pengaturan instalasi jaringan yang lebih mudah bila menggunakan topologi *star*.

Topologi *star* merupakan control terpusat, semua *link* harus melewati pusat yang menyalurkan data tersebut kesemua *client* yang dipilihnya. Simpul pusat dinamakan stasiun primer atau *server* dan lainnya dinamakan stasiun sekunder atau *client server*. Setelah hubungan jaringan dimulai oleh *server* maka setiap *client server* sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari *server*.

2.1.10 *Firewall*

Firewall adalah sebuah *host* yang bertujuan utama untuk melindungi jaringan. *Firewall* membatasi tipe tertentu suatu *network traffic* dari *internet* ke jaringan yang dilindungi, sebaliknya *firewall* tidak dapat membuat jaringan selalu aman. Bagaimanapun, *firewall* hanya mengamankan sejauh usaha kita untuk membuatnya menjadi aman. (Tabratas Tharom, 2002:135). *Firewall* merupakan suatu *service* yang bersifat beresiko pada keamanan jaringan. Ada beberapa alasan membutuhkan *firewall* untuk suatu jaringan antara lain:

1. Meningkatkan keamanan jaringan

   Beberapa layanan secara kesatuan tidak aman, dan tidak mungkin untuk diamankan dalam *host* individu. *Firewall* dapat membantu membagi jaringan untuk meningkatkan keamanan.

2. *Network Access Control*

Firewall dapat membantu meningkatkan keamanan *policy network* dengan secara selektif memperbolehkan layanan *network* untuk semua atau *host* yang dipilih.

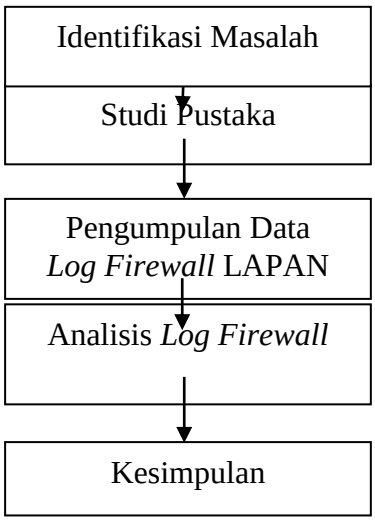
3. *Logging*

   Firewall memeriksa semua *traffic* jaringan yang diijinkan atau tidak diijinkan. Dapat membantu aktivitas yang melewati jaringan. Ada beberapa tipe *Firewall*, yaitu:

   a. *Proxy Firewall*: *proxy server* bekerja dengan membuat *request* atas nama *client*.

   b. *Packet Filtering Firewall*: *packet filter* bekerja dengan memeriksa paket IP.

2.2 Kerangka Berpikir



Gambar 2.2 Diagram Kerangka Berfikir

Berdasarkan uraian kerangka berpikir yang telah dijabarkan adalah:

1. Untuk menganalisis akses keamanan jaringan di LAPAN Pusat, diawali dengan identifikasi masalah yang telah dijelaskan pada Bab I yang bertujuan untuk mengangkat masalah yang akan diteliti.
2. Melakukan studi pustaka yang bertujuan untuk memperkuat materi pembahasan sekaligus menjadi dasar untuk menggunakan teori-teori tertentu dalam penelitian.
3. Pengumpulan data meliputi *Log Firewall* selama 3 bulan mulai dari bulan November 2015, Desember 2016, dan Januari 2017.
4. Menganalisis *Log Firewall* meliputi pengumpulan data dan identifikasi masalah terhadap akses keamanan jaringan yang terdapat di LAPAN Pusat.
5. Penarikan kesimpulan berdasarkan analisis yang telah dilakukan pada tahap sebelumnya.

BAB III

METODELOGI PENELITIAN

3.1. Tempat dan Waktu Penelitian

Penelitian dilakukan di LAPAN. Waktu penelitian dilakukan pada November 2016 sampai dengan Januari 2017.

3.2. Metode Penelitian

Metode penelitian yang digunakan adalah Metode Kualitatif. Metode kualitatif merupakan metode penelitian yang digunakan untuk mengumpulkan data dengan cara bertatap muka langsung dan berinteraksi dengan orang-orang di tempat penelitian. (McMilan & Schumacher, 2003). Menurut McMilan dan Schumacher merumuskan metode kualitatif ke dalam 6 langkah yaitu: (1) Observasi, (2) Wawancara, (3) Pengumpulan Data, (4) Analisis Data, (5) Hasil Analisis, (6) Pembahasan Hasil Analisis

3.3. Data dan Sumber Data

Pengumpulan data dilakukan untuk memperoleh informasi yang diperlukan untuk mencapai tujuan penelitian. Data berupa *log firewall* yang didapat dari Kepala Subbidang Infrastruktur Teknologi Informasi LAPAN Pusat dengan mengajukan prasyarat sebelum mendapatkan *log firewall* LAPAN berupa surat kerahasiaan data yang tidak diperbolehkan mempublikasikan IP *server*. Data yang dikumpulkan untuk bahan penelitian selama 3 bulan mulai dari bulan November 2015, Desember 2016, dan Januari 2017. Dengan data tersebut dapat mengetahui adanya kendala, dan akses keamanan jaringan yang digunakan pada *firewall* LAPAN Pusat.

3.4. Teknik dan Prosedur Pengumpulan Data

Teknik pengumpulan data yang disusun dalam penelitian adalah sebagai berikut:

1. Observasi

Observasi disebut juga dengan pengamatan. Dalam penelitian, observasi dilakukan pada empat karyawan infrastruktur dengan melakukan observasi kepada kepala infrastruktur. Melakukan observasi untuk memperoleh informasi perihal keamanan jaringan LAPAN Pusat. observasi kepada kepala infrastruktur berisi pertanyaan tentang keluhan pada keamanan jaringan di LAPAN Pusat.

2. Wawancara

Observasi disebut juga dengan pengamatan. Dalam penelitian, wawancara dilakukan pada empat karyawan infrastruktur dengan melakukan wawancara empat karyawan infrastruktur. Melakukan wawancara untuk memperoleh data akses keamanan jaringan selama 3 bulan mulai dari bulan November 2015, Desember 2016, dan Januari 2017. Wawancara kepada empat karyawan infrastruktur berisi pertanyaan tentang akses keamanan jaringan pada *firewall* yang dirasakan oleh karyawan infrastruktur LAPAN.

3. Pengumpulan data

Pengumpulan data dilakukan untuk mendapatkan data tentang akses keamanan jaringan berupa data *log firewall* yang terdapat di LAPAN Pusat. Pengumpulan data didapatkan dengan beberapa persyaratan oleh kepala subbidang infrastruktur teknologi informasi yaitu (1) Membuat surat perjanjian kerahasian data LAPAN Pusat, (2) Fotocopy KTP, dan (3) Surat penelitan dari kampus.

4. Analisis data *log firewall*

Log firewall adalah sekumpulan data jaringan yang akan melewati *firewall* dan dicatat oleh *firewall* berupa *log firewall*. Menganalisis *log firewall* pada setiap kejadian yang terjadi untuk mendapatkan informasi jaringan *server* tersebut. Apabila ingin melakukan analisis yang harus dilakukan dengan melihat isi *log firewall*. Analisis yang dihasilkan akan berupa pesan dari *log firewall* berguna untuk mengetahui jaringan yang akan melewati *firewall* menuju *server* LAPAN Pusat.

5. Hasil Analisis data

Setelah melakukan analisis data maka mendapatkan hasil analisis berupa enam pesan mulai dari bulan November 2015, Desember 2016, Januari 2017. Pesan tersebut berisi akses pada keamanan jaringan seperti IP INSIDE-SATKER, IP INSIDE-LOCAL8, IP DMZ, IP PUBLIC-SVR, dan IP OUTSIDE.

6. Pembahasan Hasil Analisis

Setelah mendapatkan hasil analisis maka dilakukan pembahasan hasil analisis berupa persentasi banyak permasalahan data *log firewall* dalam per hari selama tiga bulan, mulai dari bulan November 2015, Desember 2016, Januari 2017. Pembahasan tersebut berisi persentasi serangan dari luar maupun serangan dari dalam jaringan LAPAN Pusat.

3.4. Prosedur Analisis Data

Dengan melakukan Observasi dan Wawancara kepada pihak LAPAN, untuk mendapatkan informasi perihal akses keamanan jaringan berdasarkan *log firewall*.

3.5. Pemeriksaan Keabsahan Data

Menjelaskan bagaimana proses dan teknik yang digunakan untuk memeriksa keabsahan data. Keabsahan data antara lain dapat mencakup: (1) Kepercayaan (credibility), dan (2) Kepastian (confirmability).

3.5.1 Kredibilitas (Credibility)

Membuat surat kerahasiaan kejaminan data, untuk menjaga kerahasiaan data dan melakukan observasi kepada kepala subbidang infrastruktur teknologi dan informasi LAPAN Pusat.

3.5.2 Konfimabilitas (Confirmability)

Mengumpulkan data log firewall LAPAN Pusat mulai dari bulan November 2015, Desember 2016, dan Januari 2017 dengan melakukan wawancara kepada empat karyawan infrastruktur LAPAN Pusat.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1. Hasil Penelitian

4.1.1. Observasi

Dalam observasi berdasarkan observasi di LAPAN Pusat oleh kepala subbidang infrastruktur teknologi informasi yaitu bapak Surono Setiyo Atmojo., S.Kom., M.T.I dengan hasil observasi yang dapat dilihat pada lampiran 2.

4.1.2. Wawancara

Dalam wawancara berdasarkan wawancara kepada empat karyawan infrastruktur di LAPAN Pusat yaitu bapak Fajar Iman Nugraha., S.Kom, Bagus Arief., S.Kom, Yanuar Abadi, Mohammad Jamil Saputra dengan hasil wawancara kepada empat karyawan infrastruktur yang dapat dilihat pada lampiran 3.

4.1.3. Pengumpulan Data

Dalam pengumpulan data dilakukan untuk mendapatkan data *log firewall* yang terdapat di LAPAN Pusat. Berdasarkan pengumpulan data mulai dari bulan November 2015, Desember 2016, dan Januari 2017 maka data *log firewall* terdapat 83 *file,* dan di dalam *log firewall* tidak diperbolehkan publikasi oleh kepala subbidang infrastruktur teknologi informasi LAPAN Pusat karena bersifat rahasia di LAPAN.

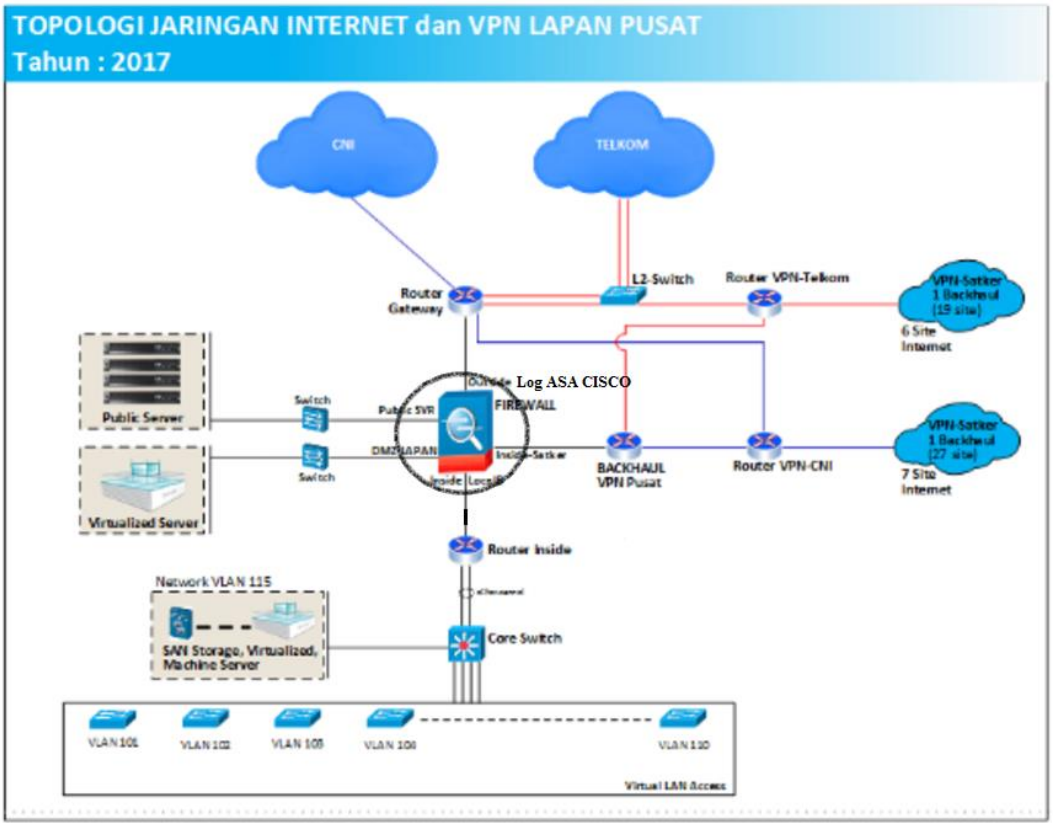
4.1.4. Analisis Data *Log Firewall*

Dalam analisis data *log firewall* berdasarkan hasil pengumpulan data selama tiga bulan maka terdapat tanggal, waktu akses, pesan, dan penjelasan akses yang masuk pada keamanan jaringan dengan analisis data *log firewall* yang dapat dilihat pada lampiran 1.

4.1.5. Hasil Analisis *Log Firewall*

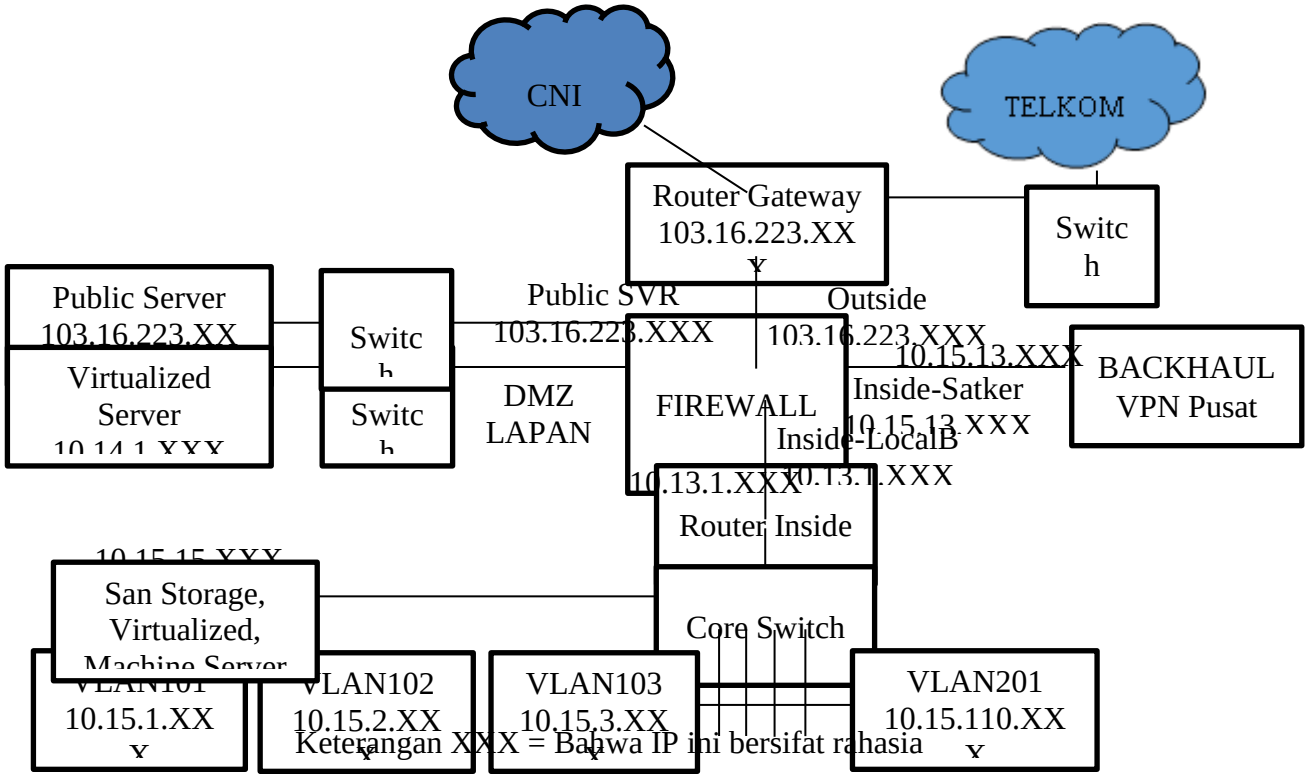
Dalam hasil analisis yang di dapat maka telah mendapatkan topologi jaringan LAPAN untuk mempermudah dalam menganalisa *log firewall* LAPAN Pusat. Pada Gambar 4.1 merupakan topologi jaringan LAPAN:

a. Topologi LAPAN Pusat 2016



Gambar 4.1 Topologi LAPAN Pusat

b. Penjelasan IP Topologi LAPAN Pusat



Gambar 4.1 Topologi yang menunjukan IP LAPAN Pusat

Topologi menunjukan alamat IP pada setiap perangkat jaringan komputer di LAPAN Pusat 2017. Mulai dari VLAN101-VLAN201 sampai menuju *Public Server*. Topologi untuk mempermudah dalam menganalisa *log firewall* LAPAN.

Berikut hasil analisis akses keamanan jaringan berdasarkan *log firewall* di LAPAN Pusat:

4.1.5.1 Hasil Analisis Akses keamanan berdasarkan *log firewall* pada bulan Januari 2017 di LAPAN Pusat.

a. Pesan dari *Log Firewall*:

1. 10.13.1.XXX %ASA-4-313005: *No matching connection for ICMP error message*: icmp src DMZ-SVR_LOCAL: 10.14.1.XXX.

   Pesan dari *firewall* yaitu Tidak mendapatkan akses koneksi pada ICMP sehingga hanya terdapat IP dari DMZ-SVR dikarenakan terdapat gangguan pada akses keamanan jaringan dan bersifat *Error*.

2. 10.13.1.XXX %ASA-4-733100: [*Scanning*] *drop rate*-1 *exceeded*. *Current burst rate is* 20 per *second, max configured rate is* 10; *Current average rate is* 44 per *second, max configured rate is* 5; *Cumulative total count is* 26515.

   Pesan dari *firewall* yaitu Paket yang lewat telah melebihi batas akses keamanan jaringan yang ditentukan sehingga di drop oleh *firewall* dan bersifat *Warning*.

3. 10.13.1.XXX %ASA-4-313004: *Denied* ICMP type = 0, *from address* 23.65.215.XXX on *interface* OUTSIDE to 103.16.223.XXX: *no matching session*.

   Pesan dari *firewall* yaitu Paket yang lewat ditolak oleh ASA karena IP berasal dari jaringan luar LAPAN dan bersifat *Warning* dapat mengganggu akses keamanan jaringan yang berada di dalam jaringan LAPAN.

4. 10.13.1.XXX %ASA-4-419002: *Duplicate* TCP SYN *from* INSIDE-SATKER: 10.18.40.XXX *to* INSIDE-SATKER: 103.31.157.XXX *with different initial sequence number.*

   Pesan dari *firewall*: IP tersebut menunjukan telah melakukan duplikasi alamat IP sebanyak mungkin dan bersifat *alert*.

5. 10.13.1.XXX %ASA-4-410001: *Dropped* UDP DNS *reply from* OUTSIDE: 202.134.1.XXX *to* INSIDE-SATKER: 10.18.60.XXX; label length 32 bytes exceeds remaining packet length limit of 5 bytes.

   Pesan dari *firewall*: Paket UDP DNS tersebut mendapatkan balasan dari IP luar ke IP dalam LAPAN sehingga dapat mengganggu akses IP pada keamanan jaringan di LAPAN Pusat selama beberapa menit dan bersifat *Warning*.

6. 10.13.1.XXX %ASA-2-106017: *Deny* IP *due to Land Attack from* 103.16.223.XXX *to* 103.16.223.XXX

   Pesan dari *firewall*: IP tersebut menunjukan telah terjadi penyerangan dari OUTSIDE IP ke *Public*-SVR IP sehingga dapat mengganggu akses yang akan masuk pada keamanan jaringan LAPAN lalu *firewall* menolak IP tersebut dan bersifat *Alert*.

b. Banyak permasalahan dari *Log Firewall* mulai tanggal 02 Januari 2017 – 22 Januari 2017:

   1. Ada (± 141.493/hari) yang tidak mendapatkan koneksi tetapi mempunyai IP
   2. Ada (± 37.736/hari) yang terjadi masalah dalam *Host*, TCP/UDP *port*, dan protokol IP melebihi batas yang ditentukan sehingga di *drop*
   3. Ada (± 16.833/hari) Paket yang lewat ditolak oleh ASA
   4. Ada (± 180.736/hari) *Duplicate* TCP SYN
   5. Ada (± 4.153/hari) Paket UDP DNS melebihi batas protokol
   6. Ada (± 37.953/hari) Menolak IP terhadap serangan jaringan dari luar

Keterangan: Angka tersebut menunjukan perhitungan dalam per hari di dalam *log firewall* LAPAN Pusat.

4.1.5.2 Hasil Analisis Akses keamanan berdasarkan *log firewall* pada bulan Desember 2016 di LAPAN Pusat.

a. Pesan dari *Log Firewall*:

   1. 10.13.1.XXX %ASA-4-313005: *No matching connection for ICMP error message*: icmp src INSIDE-SATKER: 10.15.13.XXX.

Pesan dari *firewall* yaitu Tidak mendapatkan akses koneksi pada ICMP sehingga hanya terdapat IP dari INSIDE-SATKER dikarenakan terdapat gangguan pada akses keamanan jaringan dan bersifat *Error*.

2. 10.13.1.XXX %ASA-4-733100: [*BAD Packet*] *drop rate*-1 *exceeded*. *Current burst rate is* 217 per *second, max configured rate is* 400; *Current average rate is* 553 per *second, max configured rate is* 100; *Cumulative total count is* 320301.

   Pesan dari *firewall* yaitu Paket yang lewat telah melebihi batas akses keamanan jaringan yang ditentukan sehingga di *drop* oleh *firewall* dan bersifat *Alert*.

3. 10.13.1.XXX %ASA-4-419002: *Duplicate* TCP SYN *from* INSIDE-SATKER: 10.18.40.XXX *to* INSIDE-SATKER: 103.31.157.XXX *with different initial sequence number.*

   Pesan dari *firewall*: IP tersebut menunjukan telah melakukan duplikasi alamat IP sebanyak mungkin dan bersifat *Alert*.

4. 10.13.1.XXX %ASA-4-410001: *Dropped* UDP DNS *reply from* OUTSIDE: 202.134.0.XXX *to* INSIDE-SATKER: 10.18.130.XXX; label *length* 32 *bytes exceeds remaining packet length limit of* 1 *bytes.*

   Pesan dari *firewall*: Paket UDP DNS tersebut mendapatkan balasan dari IP luar ke IP dalam LAPAN sehingga dapat mengganggu akses IP pada keamanan jaringan di LAPAN Pusat selama beberapa menit dan bersifat *Warning*.

5. 10.13.1.XXX %ASA-2-106017: *Deny* IP *due to Land Attack from* 103.16.223.XXX *to* 103.16.223.XXX

Pesan dari *firewall*: IP tersebut menunjukan telah terjadi penyerangan dari OUTSIDE IP ke *Public*-SVR IP sehingga dapat mengganggu akses yang akan masuk pada keamanan jaringan LAPAN lalu *firewall* menolak IP tersebut dan bersifat *Alert*.

b. Banyak permasalahan dari *log firewall* selama tanggal 01 Desember 2016 – 31 Desember 2016:

1. Ada (± 164.685/hari) yang tidak mendapatkan koneksi tetapi mempunyai IP
2. Ada (± 27.673/hari) yang terjadi masalah dalam *Host*, TCP/UDP *port*, dan protokol IP melebihi batas yang ditentukan sehingga di drop
3. Ada (± 256.073/hari) *Duplicate* TCP SYN
4. Ada (± 2.758/hari) Paket UDP DNS melebihi batas protokol
5. Ada (± 13.975/hari) Menolak IP terhadap serangan jaringan dari luar

Keterangan: Angka tersebut menunjukan perhitungan dalam per hari di dalam *log firewall* LAPAN Pusat.

4.1.5.3 Hasil Analisis Akses keamanan berdasarkan *log firewall* pada bulan November 2015 di LAPAN Pusat.

a. Pesan dari *Log Firewall*:

1. 10.13.1.XXX %ASA-4-313005: *No matching connection for ICMP error message*: icmp src OUTSIDE: 173.240.247.XXX.

Pesan dari *firewall* yaitu Tidak mendapatkan akses koneksi pada ICMP sehingga hanya terdapat IP dari INSIDE-SATKER dikarenakan terdapat gangguan pada akses keamanan jaringan dan bersifat *Error*.

2. 10.13.1.XXX %ASA-4-733100: [SYN *Attack*] *drop rate*-1 *exceeded. Current burst rate is* 344 per *second, max configured rate is* 200; *Current*

average rate is 419 per *second, max configured rate is* 100; *Cumulative total count is* 251647.

Pesan dari *firewall*: Paket yang lewat telah melebihi batas akses keamanan jaringan yang ditentukan sehingga di drop oleh *firewall* dan bersifat *Critical*.

3. 10.13.1.XXX %ASA-4-419002: *Duplicate* TCP SYN *from* DMZ: 116.211.0.XXX *to* DMZ: 103.16.223.XXX *with different initial sequence number.*

   Pesan dari *firewall*: IP tersebut menunjukan telah melakukan duplikasi alamat IP dalam jaringan LAPAN sebanyak mungkin sehingga dapat mengganggu jalur akses pada keamanan jaringan dan bersifat *Alert*.

4. 10.13.1.XXX %ASA-4-410001: *Dropped* UDP DNS *reply from* DMZ: 103.16.223.XXX *to* OUTSIDE: 68.200.209.XXX; label *length* 4095 *bytes exceeds remaining packet length limit of* 512 *bytes.*

   Pesan dari *firewall*: Paket UDP DNS tersebut mendapatkan balasan dari DMZ IP dalam ke OUTSIDE IP Luar LAPAN sehingga IP tersebut melebih batas yang ditentukan oleh *firewall* sehingga dapat mengganggu jalur akses pada keamanan jaringan di LAPAN Pusat selama beberapa jam dan bersifat *Emergency*.

5. 10.13.1.XXX %ASA-2-106017: *Deny IP due to Land Attack from* 103.16.223.XXX *to* 103.16.223.XXX.

   Pesan dari firewall: IP tersebut menunjukan telah terjadi penyerangan dari OUTSIDE IP ke *Public*-SVR IP sehingga dapat mengganggu akses yang akan masuk pada keamanan jaringan LAPAN lalu *firewall* menolak IP tersebut dan bersifat *Critical*.

b. Banyak permasalahan dari *log firewall* selama tanggal 01 November – 31 November 2015:

1. Ada (± 4.927/hari) yang tidak mendapatkan koneksi tetapi mempunyai IP
2. Ada (± 10.580/hari) *Host*, TCP/UDP *port*, dan protokol IP melebihi batas yang ditentukan sehingga di *drop*
3. Ada (± 297.772/hari) *Duplicate* TCP SYN
4. Ada (± 194.834/hari) Paket UDP DNS melebihi batas protokol
5. Ada (± 46.268/hari) Menolak IP terhadap serangan jaringan dari luar

Keterangan: Angka tersebut menunjukan perhitungan dalam per hari di dalam *log firewall* LAPAN Pusat.

4.2. Pembahasan

Tahap-tahap penelitian adalah (1) Observasi, (2) Wawancara, (3) Pengumpulan Data, (4) Analisis data, (5) Hasil analisis, (6) Pembahasan hasil analisis. Tahap penelitian identifikasi masalah dan pengumpulan data telah dijabarkan hasilnya pada Sub Bab Latar Belakang, sehingga penelitian analisis *log firewall* dijabarkan mulai tahap Pengumpulan Data dan Analisis *log firewall*.

Pada analisis *log firewall*, penelitian mencari informasi tentang permasalahan yang terjadi melalui pengumpulan data LAPAN. Langkah awal analisis *log firewall* adalah dengan mengumpulkan data dari bulan November 2015, Desember 2016, dan Januari 2017. Langkah selanjutnya adalah menganalisis *log firewall* untuk mencari permasalahan yang sering terjadi di LAPAN Pusat, berikut merupakan pembahasan hasil analisis *log firewall*:

1. Pembahasan Analisis Akses keamanan jaringan berdasarkan *log firewall* pada bulan Januari 2017 di LAPAN Pusat.

a. Pesan dari *Log Firewall*:

1. Pada pesan pertama terdapat gangguan akses pada keamanan *firewall* sehingga pesan tidak mendapatkan koneksi pada keamanan jaringan di LAPAN Pusat tetapi hanya terdapat IP pada DMZ-SVR_LOCAL sebagai alamat pada jaringan.
2. Pada pesan kedua terdapat gangguan jalur alamat pada keamanan *firewall* sehingga pesan memberitahukan bahwa *Host*, TCP/UDP *port*, *protocol* IP melebihi batas yang ditentukan sehingga di *drop* oleh *firewall* ASA CISCO.
3. Pada pesan ketiga terdapat gangguan akses pada keamanan jaringan sehingga pesan menolak IP OUTSIDE atau IP luar jaringan LAPAN Pusat oleh *firewall* ASA CISCO.
4. Pada pesan keempat terdapat gangguan akses pada keamanan jaringan berdasarkan pesan *log firewall* yaitu IP INSIDE-SATKER duplikasi TCP sebanyak 280.736 PING sehingga terjadi gangguan pada akses keamanan jaringan di LAPAN Pusat.
5. Pada pesan keempat terdapat gangguan pada akses keamanan jaringan sehingga pesan terdapat paket UDP DNS melebihi batas sebesar 148 berdasarkan protokol yang lewat
6. Pada pesan keenam terdapat gangguan pada akses keamanan jaringan sehingga pesan menolak IP OUTSIDE karena IP tersebut menyerang pada akses keamanan jaringan di LAPAN Pusat

Pada bulan Januari 2017 terdapat 68% serangan dari luar jaringan yang terjadi pada akses keamanan jaringan, 32% serangan dari dalam jaringan LAPAN Pusat. Berdasarkan pada banyak permasalahan pada *log firewall* LAPAN per hari.

2. Pembahasan Analisis Akses keamanan berdasarkan *log firewall* pada bulan Desember 2016 di LAPAN Pusat.

a. Pesan dari *Log Firewall*:

1. Pada pesan pertama terdapat gangguan akses pada keamanan *firewall* sehingga pesan tidak mendapatkan koneksi pada keamanan jaringan di LAPAN Pusat tetapi hanya terdapat IP pada INSIDE-SATKER sebagai alamat pada jaringan.
2. Pada pesan kedua terdapat gangguan jalur alamat pada keamanan *firewall* sehingga pesan memberitahukan bahwa *Host*, TCP/UDP *port*, *protocol* IP melebihi batas yang ditentukan sehingga di *drop* oleh *firewall* ASA CISCO.
3. Pada pesan ketiga terdapat gangguan akses pada keamanan jaringan sehingga pesan menolak IP OUTSIDE atau IP luar jaringan LAPAN Pusat oleh *firewall* ASA CISCO.
4. Pada pesan keempat terdapat gangguan akses pada keamanan jaringan berdasarkan pesan *log firewall* yaitu IP INSIDE-SATKER duplikasi TCP sebanyak 480.736 PING sehingga terjadi gangguan pada akses keamanan jaringan di LAPAN Pusat.
5. Pada pesan keempat terdapat gangguan pada akses keamanan jaringan sehingga pesan terdapat paket UDP DNS melebihi batas sebesar 148 berdasarkan protokol yang lewat.
6. Pada pesan keenam terdapat gangguan pada akses keamanan jaringan sehingga pesan menolak IP OUTSIDE karena IP tersebut menyerang pada akses keamanan jaringan di LAPAN Pusat.

Pada bulan Desember 2016 terdapat 75% serangan dari luar jaringan yang terjadi pada akses keamanan jaringan, 15% serangan dari dalam jaringan LAPAN Pusat. Berdasarkan pada banyak permasalahan pada *log firewall* LAPAN per hari.

3. Pembahasan Analisis Akses keamanan berdasarkan *log firewall* pada bulan November 2015 di LAPAN Pusat.

a. Pesan dari *Log Firewall*:

1. Pada pesan pertama terdapat gangguan akses pada keamanan *firewall* sehingga pesan tidak mendapatkan koneksi pada keamanan jaringan di LAPAN Pusat tetapi hanya terdapat IP pada OUTSIDER sebagai alamat pada jaringan.
2. Pada pesan kedua terdapat gangguan jalur alamat pada keamanan firewall sehingga pesan memberitahukan bahwa *Host*, TCP/UDP *port*, *protocol* IP melebihi batas yang ditentukan sehingga di *drop* oleh *firewall* ASA CISCO.
3. Pada pesan ketiga terdapat gangguan akses pada keamanan jaringan sehingga pesan menolak IP OUTSIDE atau IP luar jaringan LAPAN Pusat oleh *firewall* ASA CISCO.
4. Pada pesan keempat terdapat gangguan akses pada keamanan jaringan berdasarkan pesan *log firewall* yaitu IP INSIDE-SATKER duplikasi TCP sebanyak 786.061 PING sehingga terjadi gangguan pada akses keamanan jaringan di LAPAN Pusat.
5. Pada pesan keempat terdapat gangguan pada akses keamanan jaringan sehingga pesan terdapat paket UDP DNS melebihi batas sebesar 148 berdasarkan protokol yang lewat.

6. Pada pesan keenam terdapat gangguan pada akses keamanan jaringan sehingga pesan menolak IP OUTSIDE karena IP tersebut menyerang pada akses keamanan jaringan di LAPAN Pusat.

Pada bulan November 2015 terdapat 85% serangan dari luar jaringan yang terjadi pada akses keamanan jaringan, 25% serangan dari dalam jaringan LAPAN.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitan yang dilakukan dapat diambil kesimpulan bahwa:

1. Analisis akses keamanan jaringan LAPAN dilakukan penelitian selama 3 bulan, mulai dari bulan November 2015, Desember 2016, dan Januari 2017 terdapat tiga gangguan sebagai berikut:

   a. *No matching connection*: Tidak mendapatkan akses koneksi dari *log firewall* sehingga hanya mempunyai alamat IP karena adanya akses koneksi IP jaringan dalam terhalang oleh akses koneksi jaringan luar LAPAN Pusat , cara mengatasi kendala tidak mendapatkan akses koneksi dengan melakukan pembatasan akses hanya pada *user* yang berhak atas suatu data, dan mencegah akses dari *user* yang tidak memiliki hak akses.

   b. *Flooding*: Penyerangan yang dilakukan berupa duplikasi TCP sehingga dapat mengganggu akses pada keamanan jaringan di LAPAN Pusat, cara mengatasi kendala penyerangan duplikasi TCP dengan melakukan proteksi pada akses keamanan jaringan melalui penambahan *rules* di *log firewall*.

   c. *Port Scanning*: Penyerangan yang dilakukan berupa manipulasi *port* untuk mencari akses yang terhubung pada keamanan jaringan, cara mengatasi kendala penyerangan manipulasi *port* dengan melakukan pencarian keaslian data yang dikirim melalui akses dari sumber ke penerima secara lengkap, tanpa ada modifikasi atau manipulasi oleh pihak yang tidak berwenang.

2. Pembahasan hasil analisis yang telah dilakukan selama tiga bulan didapatkan data sebagai berikut: (1) Pada bulan November 2015 terdapat 85% serangan jaringan dari luar dan 15% serangan jaringan dari dalam LAPAN Pusat. Berdasarkan banyak permasalahan dalam per hari terhitung tanggal 01 November 2015 – 31 November 2015. (2) Pada bulan Desember 2016 terdapat 75% serangan jaringan dari luar dan 15% serangan jaringan dari dalam LAPAN Pusat. Berdasarkan banyak permasalahan dalam per hari terhitung tanggal 01 Desember 2016 – 31 Desember 2016. (3) Pada bulan Januari 2017 terdapat 68% serangan jaringan luar dan 32% serangan jaringan dalam LAPAN Pusat. Berdasarkan banyak permasalahan dalam per hari terhitung tanggal 02 Januari 2017 – 22 Januari 2017.

5.2. Saran

Berdasarkan kesimpulan penelitian, maka dapat diberikan saran sebagai berikut:

1. Membuat aturan dalam LAPAN Pusat, yang mengatur agar tidak memasang modem lain yang terhubung ke internet. Hal ini berfungsi agar setiap akses data yang masuk ke jaringan dalam ataupun luar jaringan tetap melewati *firewall*.
2. Dibutuhkan admin yang dapat memahami *firewall* ASA CISCO.

DAFTAR PUSTAKA

Fadel. (2010). *Jenis Jaringan Komputer*. Jakarta: PT Gramedia Pustaka Utama.

Fauzie, Achmad. (2004). Analisis Penerapa Firewall Sebagai Sistem Keamanan Jaringan Pada PT. PLN (Persero) Penyaluran Dan Pusat Pengaturan Beban. Jurnal Sistem Keamanan Komputer, 25:24-26.

[LAPAN] Lembaga Penerbangan dan Antariksa Nasional. (2004). *Peningkatan Keamanan Jaringan LAPAN*. Jakarta: 979-8554-82-5.

Lammle, T. (2005). *Cisco Certified Network Profesional LAN Switch Configuration Study Guide*. Jakarta: PT Sybex Network.

Madcoms, A. (2009). *Membangun Sistem Jaringan Komputer*. Yogyakarta: Andi Offset.

Na'Am, J. (2003). Firewall Sebagai Pengamanan Internet, *Jurnal Akadimika*, 14:14-20.

Purbo, O. W & Wiharjito, Tony. (2000). *Keamanan Jaringan Internet*. Jakarta : PT Elex Media Komputindo.

Schumacher & McMillan. (2003). Research Qualitative: *A conceptual introduction*. Ed ke-5. New York: Longman.

Stallingsh. (2003). *Cryptography and Network Security*: *Principles and Practice*. New Jersey: Prentice-Hall.

Subramanian, (2000). *Sistem Keamanan Jaringan Komputer*. Jakarta: Balai Pustaka.

Tharom Tabratas. (2002). *Keamanan Jaringan Komputer*. Jakarta: Elex Media Komputindo.

Tim Penyusun. 2015. *Buku Pedoman Skripsi/Komprehensif/Karya Inovatif*. Jakarta: Univeristas Negeri Jakarta.

Lampiran 1

Tabel *Log Firewall* LAPAN Pusat

Tanggal	Waktu	Problem	Pesan	Penjelasan
2017-01-02	23:14:30 - 03:32:49	122.029 24.598 1.201 15.300 56 37.953	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-03	22:38:35 - 18:59:25	134.969 30.780 94 5.902 2.022 11.966	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-04	18:59:25 - 14:03:55	124.937 27.880 149 23.448 4.153 9.119	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2017-01-05	14:03:55 - 04:38:32	141.493 22.387 22 16.244 139 1.786	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-06	18:58:29 - 12:54:00	123.752 24.242 16.833 14.724 966 13.882	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-07	12:54:00 - 07:19:55	125.986 28.112 9.575 19.619 315 4.724	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-08	07:19:55 - 03:58:08	117.934 38.337 12.721 16.529 134 1.265	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			410001 %ASA-2- 106017	
2017-01- 09	08:08:58 - 06:01:20	122.805 37.537 11.831 12.079 313 623	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01- 10	19:01:21 - 12:24:12	127.339 28.198 9.392 16.653 750 6.040	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01- 11	12:24:12 - 06:16:37	131.195 34.786 9.196 1.055 470 8.151	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2017-01-12	20:44:57 - 15:26:44	127.175 33.339 8.593 877 820 20.488	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-13	15:26:44 - 08:53:37	126.808 30.634 5.261 5.065 547 23.769 263 0 0	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-14	23:58:28 - 23:59:14	42 25 26	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-15	23:58:40 - 23:59:26	28 4 0 340 0 107	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2017-01-16	12:32:13 - 18:55:14	52.599 12.575 6 157.117 147 8.091	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-18	14:18:10 - 10:40:14	133.619 37.736 209 1.005	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-17	18:55:14 - 14:18:10	132.285 9.456 34.579 38 1.218 911 19.610	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-19	10:40:15 - 07:41:55	119.977 32.004 60 12.579	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP.
		306 32.976	%ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2017-01-20	21:47:11 - 03:11:49	28.183 8.301 8 180.736 29 24.332	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2017-01-21	14:28:52 - 06:43:58	131.139 34.421 14.818 1.400 332 1.123	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2017-01-22	17:56:05 - 04:25:07	91.079 22.003 11.596 1.027 370 280	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-01	20:26:07 - 23:36:51	164.685 5.530 0 1 2 3.166	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2016-12-02	20:49:09 - 23:00:16	162.535 4.221 0 245 1 9.813	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-03	19:23:28 - 23:04:36	162.964 3.904 0 5.978 7 10.362	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-04	17:06:14 - 21:24:55	46.743 47 0 166.061 44 13.975	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-05	16:36:54 - 20:08:54	58.035 4.528 0 68.915 741 5.146	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			410001 %ASA-2- 106017	
2016-12- 06	14:33:07 - 14:47:24	4.238 1.595 0 5.421 129 524	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12- 07	17:16:03 - 21:24:23	44.352 389 0 7.621 143 69	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12- 08	19:51:58 - 22:56:57	161.507 180 0 2.028 60 259	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2016-12-09	08:34:35 - 15:52:34	134.456 128 0 15.253 160 1.237	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-11	19:03:44 - 12:52:42	133.650 316 0 3.571	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-10	05:13:42 - 19:03:44	123.897 70 912 1.290 0 2.758 78 126	%ASA-4-313005 %ASA-4-313004 %ASA-4-419002 %ASA-4-733100 %ASA-4-410001 %ASA-4-313004 %ASA-2-106017 %ASA-4-419002	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-12	12:52:44 - 22:02:33	102.223 631 0	%ASA-4-313005 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded.
2016-12-13	22:02:33 - 16:32:08	106.738 18.490 1,126 282 5.236 0 50.258 598 8.394	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-313004 %ASA-4-410001 %ASA-4-419002 %ASA-2-106017 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. Denied Packet ICMP. Duplicate TCP SYN. DNS drop rate-1 exceeded. Dropped UDP DNS. Deny IP due to Land Attack. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-14	16:32:08 - 15:39:58	116.988 188 0 28.443 870 9.551	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			%ASA-2-106017	
2016-12-15	15:39:58 - 11:29:15	117.911 233 0 39.180 370 633	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-16	16:36:19 - 16:45:54	619 5 0 256.053 1 61	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-18	16:45:54 - 00:23:28	59.879 2 0 85.833 663 4.925	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2016-12-19	18:22:25 - 18:27:38	119 3 0 352 0 24	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-20	09:23:26 - 18:32:05	47.024 319 0 148.156 258 11.086	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-21	14:21:45 - 16:06:03	159.385 100 0 15.622 43 1.577	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-22	03:13:35 - 18:52:19	65.420 1 0 100.621 743 8.087	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			410001 %ASA-2- 106017	
2016-12- 23	07:26:41 - 13:54:49	107.831 160 0 67.928 773 3.826	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12- 24	13:54:49 - 22:58:38	106.706 68 0 24.597 583 2.789	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12- 25	22:58:39 - 12:22:22	153.364 360 0 8.266 143 238	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2016-12-26	12:22:24 - 00:12:57	158.653 230 0 7.792 42 304	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-27	17:32:44 - 19:31:17	66.451 302 0 98.091 2.425 10.431	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-28	19:31:17 - 11:37:13	138.025 983 60 12.579 306 4.928	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-29	11:37:13 - 08:32:21	94.443 4.666 51 45.470 1.103 11.170	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			%ASA-4-410001 %ASA-2-106017	
2016-12-30	09:38:00 - 21:43:57	143.211 17.207 253 21.066 455 1.982	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12-31	20:43:58 - 23:14:30	130.395 27.673 363 13.416 95 3.618	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2015-10-01	03:54:27 - 04:22:34	742 10.580 0 963 228 566	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2015-10-02	05:20:24 - 06:00:50	1.279 8.730 0 902 10.829 46.268	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-03	04:47:25 - 05:21:45	945 7.268 0 2.245 10.679 45.814	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-04	03:57:36 - 04:16:30	19 6.986 0 65.986 497 8.364	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2015-10-05	09:50:41 - 10:15:49	3.657 248 0 786.061 230 3.876	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-06	07:10:26 - 07:13:30	126 8.726 0 78.012 843 1.247	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-07	07:04:35 - 07:51:33	1.818 7.690 0 1.428 829 2.623	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-08	06:40:40 - 07:21:03	1.264 580 0 11.628 443 868	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			410001 %ASA-2- 106017	
2015-10- 09	02:08:54 - 02:23:23	1.621 780 0 5.078 468 659	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 10	03:03:32 - 03:24:46	1.875 598 0 58.253 360 837	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 11	18:57:37 - 19:07:42	1.505 840 0 68.458 863 1.482	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2015-10-12	19:27:55 - 19:45:32	1.583 448 0 49.872 980 1.618	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-13	19:54:17 - 20:02:21	1.404 231 0 8.492 626 1.290	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-14	19:08:25 - 19:20:55	4.927 189 0 30.168 328 1.344	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-15	23:42:05 - 23:55:52	534 136 0 16.112 278 557	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			410001 %ASA-2- 106017	
2015-10- 16	02:32:38 - 02:55:10	769 189 0 6.170 225 806	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 17	16:36:19 - 16:45:54	3.477 5 0 225 54.714 7.912	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 18	03:12:36 - 03:31:26	622 936 0 140 179.213 2.571	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4-	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			410001 %ASA-2- 106017	
2015-10- 19	02:46:56 - 03:05:17	1.325 3 7 352 173.687 4.044	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 20	02:51:17 - 03:08:35	652 1.095 0 224 165.541 3.544	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 21	06:04:40 - 06:25:12	239 968 0 229 49.227 1.895	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

2015-10-22	03:18:00 - 03:37:02	1.187 986 0 57.013 180.690 2.054	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-23	05:38:38 - 06:17:21	932 1.955 0 199 36.374 7	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-24	06:31:45 - 06:47:40	600 651 0 203 193.759 52	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

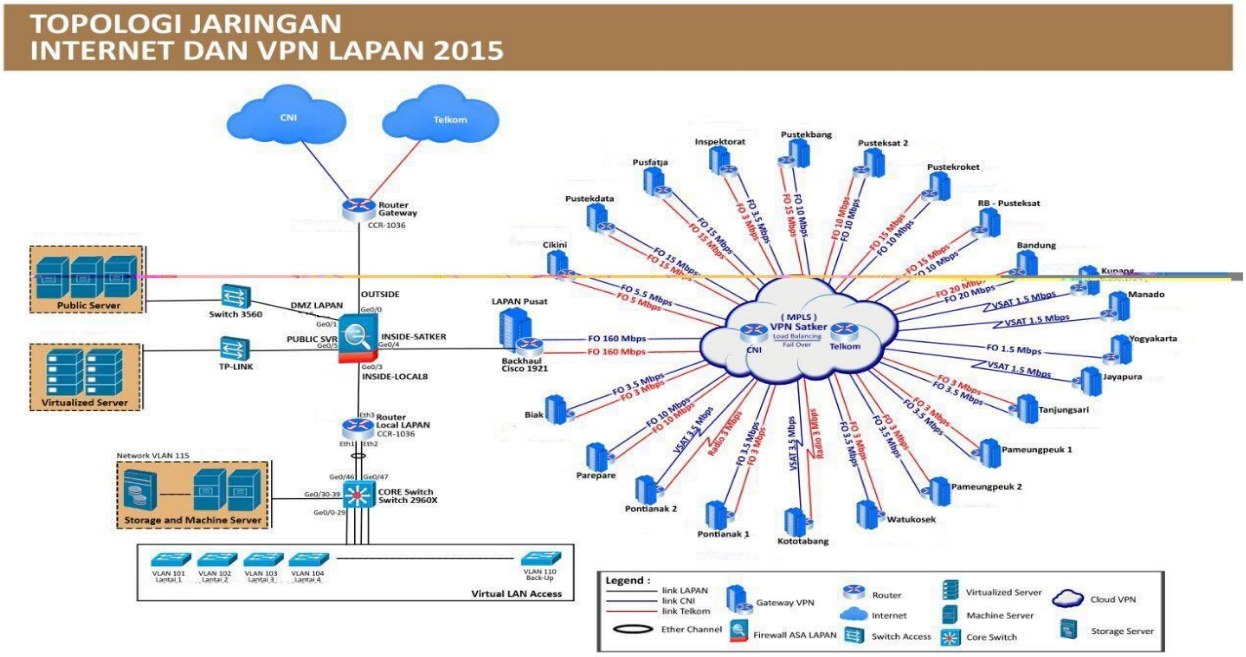
2015-10-25	03:11:09 - 03:29:29	660 17 0 43.365 194.8349	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-26	02:33:45 - 02:52:33	437 21 0 74.008 169.13471	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-27	03:11:47 - 03:31:42	3.432 34 0 58.392 175.9113.548	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-410001 %ASA-2-106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10-28	16:25:17 - 16:25:52	12 1 0 270.468 6257	%ASA-4-313005 %ASA-4-733100 %ASA-4-313004 %ASA-4-419002 %ASA-4-	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

			410001 %ASA-2- 106017	
2015-10- 29	28:23:38 - 18:27:15	472 2 0 220.319 40.746 1.494	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 30	03:33:31 - 03:55:27	749 1.282 0 56.803 177.937 8.498	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2015-10- 31	02:39:49 - 03:04:43	287 22 0 81.763 161.452 1.146	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

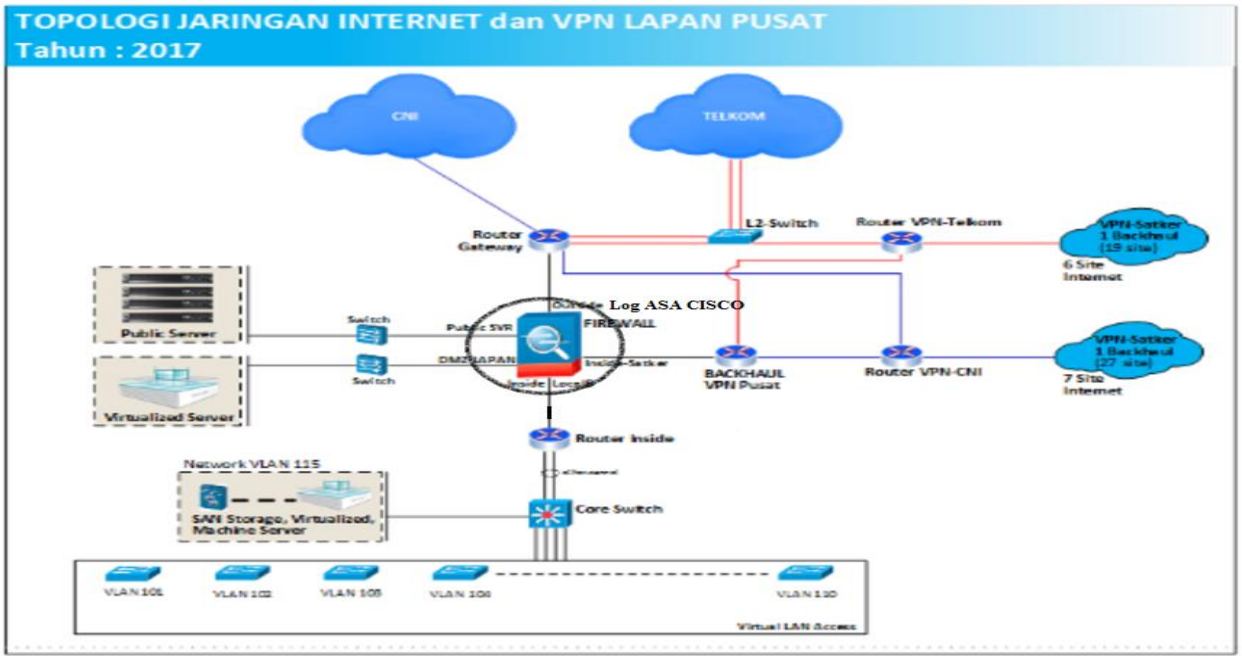
Lampiran 5

Foto Dokumentasi Penelitian LAPAN

Gambar 1. Topologi LAPAN 2015



Gambar 2. Topologi LAPAN 2017



Gambar 3. Kepala Subbidang Infrastruktur Teknologi dan Informasi, dan Tiga Karyawan Infrastruktur LAPAN Pusat

Gambar 4. Ruangan Infrastruktur LAPAN Pusat

Gambar 5. Ruangan Server LAPAN Pusat

Gambar 6. Pada Saat Pengambilan Data *Log Firewall* LAPAN Pusat

DAFTAR RIWAYAT HIDUP

Penulis bernama Adityo Jaya Subakti, lahir di Jakarta 02 Maret 1995. Anak pertama dari dua bersaudara dari pasangan Tukul Lasiman dan Ening Kusumaningsih. Riwayat pendidikan formal yang pernah ditempuh oleh peneliti, Pendidikan Dasar 17 Pg, Jakarta (2006-2007), Pendidikan Menengah di SMPN 137, Jakarta (2009-2010), Pendidikan Tingkat Atas di SMAN 72, Jakarta (2012-2013) dan melanjutkan ke jenjang universitas di Universitas Negeri Jakarta, Jakarta Timur (2013-2017), Fakultas Teknik, Program Studi Pendidikan Teknik Informatika dan Komputer dengan Konsentrasi Peminatan Teknik Komputer dan Jaringan pada tahun 2015 dan lulus pada tahun 2017.

Kegiatan yang telah diikuti selama kuliah di Universitas Negeri Jakarta adalah Praktek Kerja Lapangan di Lembaga Antariksa dan Penerbangan Nasional (LAPAN) di bagian divisi Infrastrutur tahun 2016. Kegiatan selama kuliah di Universitas Negeri Jakarta antara lain Program Praktek Kerja Lapangan (PKM) di SMK Diponegoro 1 Jakarta (2016).