Jurnal Multimedia dan Teknologi Informasi
Volume 02 Number 01, 01 Apr 2020, pp. 19-29
e-ISSN : 2721-1800 pISSN : 2722-0907
doi.org/10.54209/jatilima.v2i1.140
Homepage :https://journal.cattleyadf.org/index.php/jatilima/index

Penerapan Model Protokol Aaa (Authentication, Authorization, Accounting) Pada Keamanan Jaringan Komunikasi Wan (Wide Area Network)

Article Info

Article history:

Received Feb 16, 2020
Revised March 19, 2020
Accepted Apr 01, 2020

Keywords:

AAA Protocol Model,
Communication Network, WAN

ABSTRACT

Security is the most critical aspect of a computer network—both in networks that are local or not. The main problems that are often found on computer networks include the destruction of system devices, access to information, changes in knowledge, and deletion of data by people who do not have the right to that information. The development of technology, for now, almost all agencies have used computer networks such as WAN, where the function can connect LAN networks in a large geographical area and be able to exchange data packets and frames between routers and switches. The AAA protocol model (Authentication, Authorization, Accounting) can be used one at a time or combined as needed. Using this network model will be far safer than using only one security process.

Corresponding Author:

Abdul Sani Sembiring

STMIK Budi Darma Medan,Technical Information, Medan, Indonesia
Email Address: gurkiy@gmail.com

1. Pendahuluan

Keamanan merupakan salah satu aspek terpenting dalam sebuah jaringan komputer[1], [2]. Baik dalam jaringan lokal maupun tidak [3] Di era perkembangan teknologi yang sangat pesat saat ini, hampir semua bidang menggunakan jaringan komputer [4]. Baik di instansi pemerintah maupun swasta. Wide Area Network (WAN) adalah jaringan komunikasi data yang menghubungkan pengguna pada jaringan yang berada dalam wilayah geografis yang luas [5]. WAN berbeda dengan LAN. Tidak seperti LAN yang menghubungkan stasiun kerja, peralatan, terminal, dan peralatan lain dalam sebuah gedung, WAN menghubungkan data melalui area geografis yang luas. Perusahaan yang menggunakan WAN dapat membuat koneksi antara kantor pusat dan kantor cabang yang terletak di tempat-tempat terpencil. Sebuah WAN beroperasi pada lapisan fisik dan lapisan data link dari lapisan OSI . WAN menghubungkan LAN di area geografis yang luas. WAN mampu bertukar paket data dan frame antara router dan switch [6]. Masalah utama yang sering dihadapi dalam jaringan komputer antara lain perusakan peralatan sistem, pengaksesan informasi, pengubahan informasi dan penghapusan informasi oleh orang yang tidak berhak atas informasi tersebut. Penggunaan model protokol AAA (Authentication, Authorization, Accounting) dapat digunakan secara individual atau gabungan sesuai kebutuhan. Jika ketiganya digunakan bersama-sama, konsekuensinya jaringan akan jauh lebih aman daripada hanya menggunakan

doi.org/10.54209/jatilima.v2i1.140

satu proses keamanan WAN menghubungkan LAN di wilayah geografis yang luas. WAN mampu bertukar paket data dan frame antara router dan switch [6][7]. Masalah utama yang sering dijumpai dalam jaringan komputer antara lain rusaknya peralatan sistem, pengaksesan informasi, mengubah informasi dan menghapus informasi oleh orang yang tidak berhak atas informasi tersebut. Penggunaan model protokol AAA (Authentication, Authorization, Accounting) dapat digunakan secara individual atau gabungan sesuai kebutuhan. Jika ketiganya digunakan bersama-sama, konsekuensinya jaringan akan jauh lebih aman daripada hanya menggunakan satu proses keamanan WAN menghubungkan LAN di wilayah geografis yang luas. WAN mampu bertukar paket data dan frame antara router dan switch [6]. Masalah utama yang sering dihadapi dalam jaringan komputer antara lain perusakan peralatan sistem, pengaksesan informasi, pengubahan informasi dan penghapusan informasi oleh orang yang tidak berhak atas informasi tersebut. Penggunaan model protokol AAA (Authentication, Authorization, Accounting) dapat digunakan secara individual atau gabungan sesuai kebutuhan. Jika ketiganya digunakan bersama-sama maka akibatnya jaringan akan jauh lebih aman daripada hanya menggunakan satu proses keamanan Masalah utama yang sering dihadapi dalam jaringan komputer antara lain rusaknya peralatan sistem, pengaksesan informasi, pengubahan informasi dan penghapusan informasi oleh orang yang tidak berhak atas informasi tersebut. Penggunaan model protokol AAA (Authentication, Authorization, Accounting) dapat digunakan secara individual atau gabungan sesuai kebutuhan. Jika ketiganya digunakan bersama-sama maka akibatnya jaringan akan jauh lebih aman daripada hanya menggunakan satu proses keamanan Masalah utama yang sering dihadapi dalam jaringan komputer antara lain rusaknya peralatan sistem, pengaksesan informasi, pengubahan informasi dan penghapusan informasi oleh orang yang tidak berhak atas informasi tersebut. Penggunaan model protokol AAA (Authentication, Authorization, Accounting) dapat digunakan secara individual atau gabungan sesuai kebutuhan. Jika ketiganya digunakan secara bersamaan, maka konsekuensinya jaringan akan jauh lebih aman daripada hanya menggunakan satu proses keamanan [5][8]. Model referensi OSI adalah konsep cetak biru tentang bagaimana komunikasi harus berlangsung [9]. Model ini menggambarkan semua proses yang dibutuhkan oleh komunikasi yang efektif. Model ini juga membagi proses ini ke dalam kelompok logis yang disebut lapisan. Sistem komunikasi yang dibuat mengikuti konsep ini disebut arsitektur layer [3]. Cisco Internetwork Operating System (IOS) adalah kernel (inti) dari router Cisco dan sebagian besar switch [10]. Kernel adalah bagian dasar dan tidak terpisahkan dari sistem operasi yang mengalokasikan sumber daya dan mengelola antarmuka perangkat keras dan keamanan tingkat rendah. Hampir semua router Cisco berjalan di IOS yang sama. Lapisan aplikasi pada model OSI merupakan tempat dimana pengguna berinteraksi dengan komputer [10]. Layer ini sebenarnya hanya berperan pada saat dibutuhkan akses ke jaringan. Misalnya Internet Explorer (IE). Tidak diperlukan komponen jaringan dari sistem seperti NIC, TCP/IP, dan sebagainya, tetapi Anda masih dapat menggunakan Internet Explorer untuk melihat dokumen lokal seperti HTML [11]. Lapisan jaringan mengelola pengalamatan peralatan, melacak lokasi peralatan di jaringan, dan menentukan cara terbaik untuk memindahkan data, artinya lapisan jaringan harus mengangkut lalu lintas antar perangkat yang tidak terhubung secara lokal. Router (yang merupakan perangkat yang bekerja pada lapisan ini) dikelola pada lapisan jaringan dan menyediakan layanan perutean dalam kerja internet [10]. dan sebagainya tetapi masih dapat menggunakan Internet Explorer untuk melihat dokumen lokal seperti HTML [11]. Lapisan jaringan mengelola pengalamatan peralatan, melacak lokasi peralatan di jaringan, dan menentukan cara terbaik untuk memindahkan data, artinya lapisan jaringan harus mengangkut lalu lintas antar perangkat yang tidak terhubung secara lokal. Router (yang merupakan perangkat yang bekerja pada lapisan ini) dikelola pada lapisan jaringan dan

doi.org/10.54209/jatilima.v2i1.140

menyediakan layanan perutean dalam kerja internet [10]. dan sebagainya tetapi masih dapat menggunakan Internet Explorer untuk melihat dokumen lokal seperti HTML [11]. Lapisan jaringan mengelola pengalamatan peralatan, melacak lokasi peralatan di jaringan, dan menentukan cara terbaik untuk memindahkan data, artinya lapisan jaringan harus mengangkut lalu lintas antar perangkat yang tidak terhubung secara lokal. Router (yang merupakan perangkat yang bekerja pada lapisan ini) dikelola pada lapisan jaringan dan menyediakan layanan perutean dalam kerja internet [10].

2. Metode

Dalam pembahasan ini diperlukan suatu masalah dalam tahapan penelitian dan lebih banyak lagi data yang akan dijadikan dasar pemecahan masalah yang sedang dihadapi. Implementasi model protokol AAA untuk keamanan jaringan WAN adalah:

Pengumpulan data

Pengumpulan data yang dilakukan adalah studi kepustakaan, yaitu dengan mempelajari sumber-sumber pustaka yang dapat dijadikan referensi. Pengumpulan data dengan memanfaatkan buku dan bahan bacaan lain yang berhubungan dengan jaringan komputer dengan menerapkan protokol AAA.

Analisis dan desain (Analysis and Design)

Pada tahap ini digunakan untuk mengolah data yang ada kemudian menganalisis hasil studi pustaka yang diperoleh sehingga menjadi informasi. Jaringan komunikasi yang bertukar data, suara, video, gambar dan lain-lain sangat rentan terhadap serangan penyerang. Serangan tersebut dilakukan dengan berbagai tujuan, yaitu untuk mengambil informasi berharga dan menggunakannya untuk kejahatan, ada juga yang hanya untuk memblokir jalur komunikasi untuk bersenang-senang dan lain sebagainya.

Uji

Pengujian akan menguji sistem secara keseluruhan apakah aplikasi yang dibuat telah dapat berjalan dengan baik sesuai dengan tujuan yang ingin dicapai. Proses Serangan adalah banyak cara yang dapat dilakukan penyerang untuk mendapatkan akses ke sistem dan memanfaatkan sistem. Terlepas dari jenis sistem yang ditargetkan penyerang, penyerang biasanya melakukan langkah-langkah dasar yang sama, termasuk:

1. Pengintaian dan jejak kaki
   Pengintaian dan jejak kaki adalah istilah dalam keamanan jaringan yang mengacu pada langkah-langkah persiapan cerdas yang dilakukan oleh penyerang. Langkah ini merupakan proses berkelanjutan yang diterapkan pada semua operasi yang direncanakan dan dijalankan.
2. Mendapatkan Akses
   Ini adalah asumsi yang salah bahwa penyerang ingin mengambil alih perangkat target dan itu adalah target utama serangan. Ini tidak sepenuhnya benar. Lebih tepatnya penyerang ingin mendapatkan akses ke PC target. Setelah pencacahan menunjukkan peluang untuk masuk, semakin banyak penyelidikan yang mengganggu dapat dimulai sebagai akun pengguna yang valid dan sumber daya yang kurang terlindungi dieksploitasi untuk mendapatkan akses.

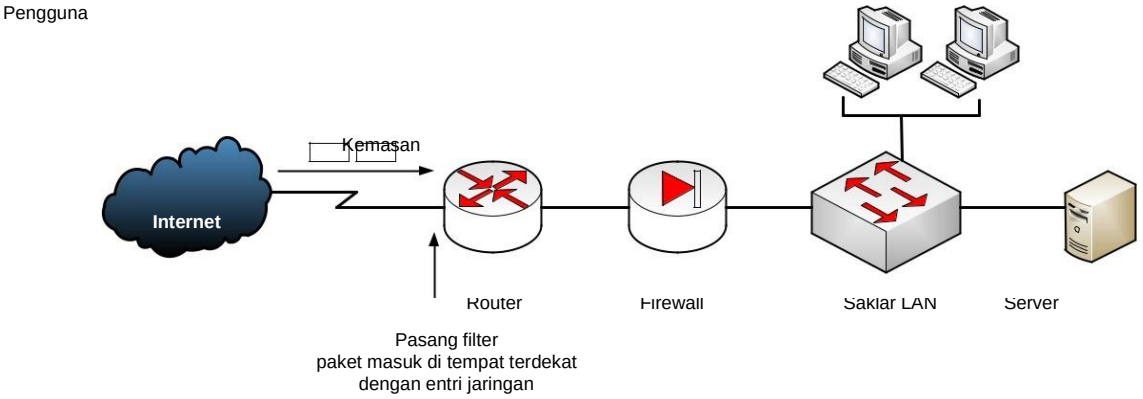
Penerapan

doi.org/10.54209/jatilima.v2i1.140

Implementasi ini akan dilakukan dengan menerapkan model protokol AAA yang digunakan sebagai acuan dalam keamanan jaringan. Pemfilteran paket adalah salah satu jenis teknologi pemantauan paket yang paling umum dan tertua. Pemfilteran paket dimulai dengan memeriksa isi paket dan menerapkan aturan untuk menentukan apakah paket tersebut ditolak atau diizinkan. Metode yang digunakan untuk mengkonfigurasi dan memfilter paket pada Router Cisco dikenal sebagai Access Control List (ACL).

3. Hasil dan Diskusi

Keamanan jaringan adalah sistem yang diimplementasikan ke dalam jaringan. Keamanan jaringan bukanlah perangkat apa yang terhubung ke jaringan. Keamanan jaringan lebih memperhatikan mekanisme kebijakan jaringan, metode yang digunakan dan pemantauan jaringan. Setiap paket dari setiap koneksi diperiksa pada kontrol akses yang lebih besar, aturan penyaringan paket yang lebih kompleks dapat mengurangi kinerja perangkat yang digunakan. Juga, karena pemfilteran paket hanya memeriksa atribut paling dasar, maka tidak aman untuk melawan kode berbahaya yang tersembunyi di lapisan lain. Penempatan packet filtering ditunjukkan pada Gambar di bawah ini.



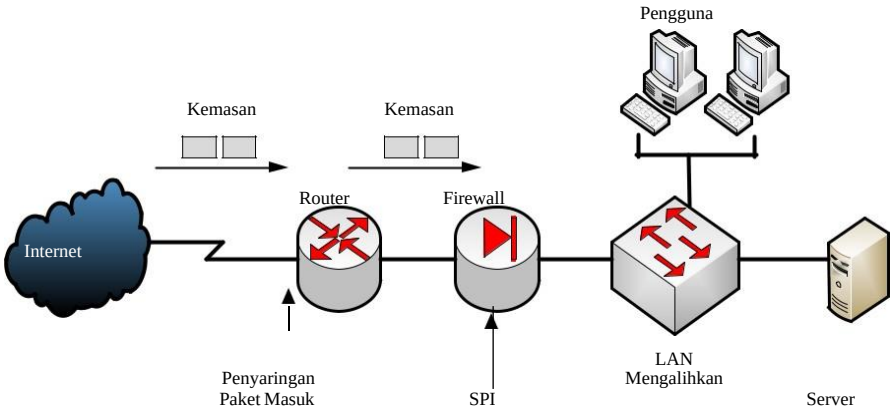
Gambar 1. Penempatan Filter Paket

Batasan packet filtering dapat dilihat pada web server DMZ dimana semua web/HTTP stream harus dapat mencapai server ini. Server ini kemudian menjalankan perangkat lunak server web IIS dari Microsoft dan penyerang memutuskan untuk menyerang server web secara langsung menggunakan aliran web/HTTP. Karena serangan menyerang kelemahan IIS, paket diperbolehkan.

Inspeksi Paket Stateful (SPI)

Packet filtering telah ditempatkan pada defense base pertama, defense base selanjutnya adalah menempatkan SPI (Stateful Packet Inspection). Penyebaran SPI dan keamanan tambahan memungkinkan pertahanan dengan melapisi di tingkat lain, dengan tujuan mengamankan jaringan melalui beberapa lapisan perlindungan. SPI biasanya diimplementasikan di firewall sehingga koneksi TCP/IP dapat diperiksa lebih dekat.

doi.org/10.54209/jatilima.v2i1.140

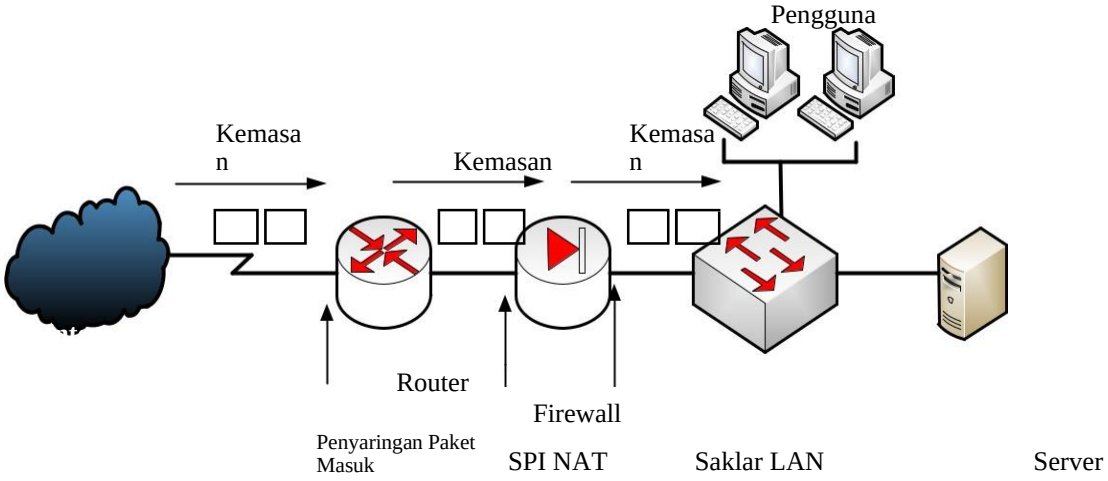


Gambar 2. Penempatan SPI

Rincian aliran paket menggunakan SPI dijelaskan sebagai berikut seperti yang ditunjukkan pada gambar di atas dengan asumsi bahwa router eksternal disebarkan dan dikonfigurasi untuk membuat rencana koneksi ke jaringan menggunakan pemfilteran paket.

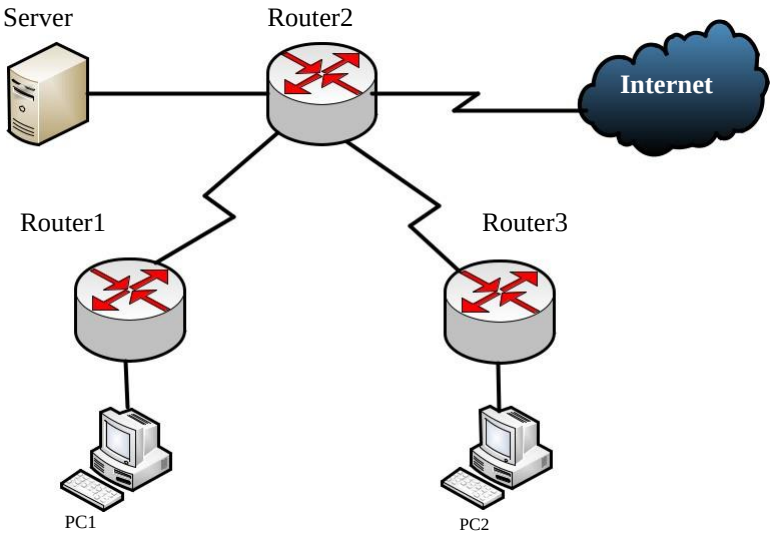
Terjemahan Alamat Jaringan (NAT)

Network Address Translation dikembangkan dan diimplementasikan pada perangkat seperti firewall, router, atau komputer yang berada di antara jaringan internal yang menggunakan alamat IP pribadi dan internet yang menggunakan alamat IP publik. Perangkat yang melakukan NAT dari jaringan pribadi ke publik biasanya firewall dan router tingkat lebih rendah. Perangkat yang melakukan NAT biasanya ditempatkan pada satu bagian yang terhubung ke jaringan internal dan bagian lainnya terhubung ke Internet (atau beberapa jaringan eksternal).



Gambar 3. Penyebaran NAT Jaringan Konfigurasi Keamanan Router Cisco

doi.org/10.54209/jatilima.v2i1.140



Gambar 4. Desain Jaringan WAN

Langkah-langkah Konfigurasi Keamanan Jaringan WAN (Wide Area Network)

Langkah-langkah untuk mengkonfigurasi keamanan jaringan ini sesuai dengan topologi jaringan yang ditunjukkan pada gambar di bawah ini adalah sebagai berikut:

1. Cloud yang mewakili jaringan internet adalah jaringan yang sangat kompleks untuk disimulasikan. Dalam simulasi ini, cloud hanya terhubung ke Router2 dengan mekanisme antarmuka loopback menggunakan protokol frame relay.
2. Dalam simulasi ini dibuat 3 router, server, 2 PC dan cloud.
3. *Protokol peruteanyang* digunakan dalam simulasi ini adalah RIP (Routing Information Protocol) versi 2.
4. Pada simulasi ini, kode enkripsi yang digunakan adalah MD5.
5. Konfigurasi keamanan hanya terfokus pada perangkat router.

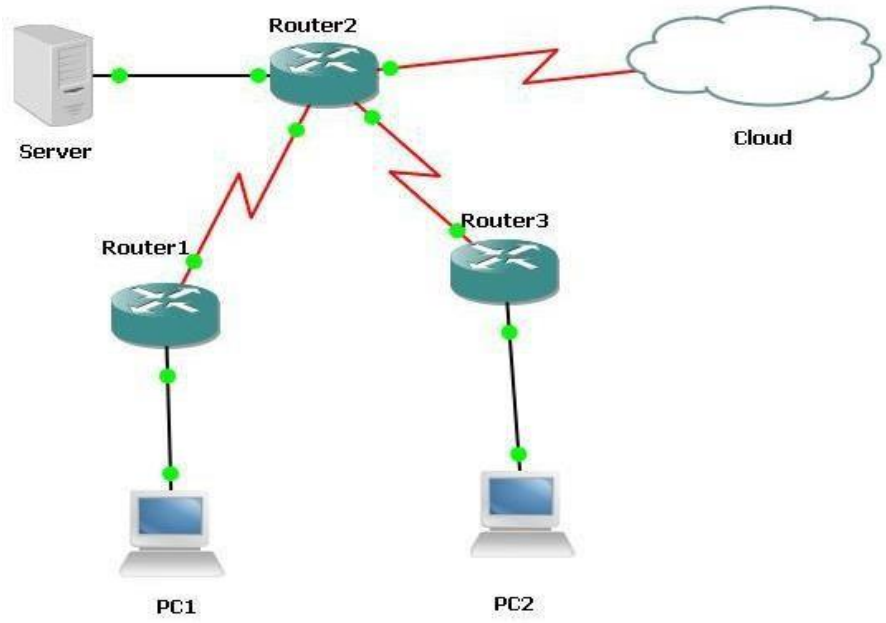
Tabel 1. Meja Pengalamatan

Perangkat	*Antarmuka*	Alamat IP	*Subnetmask*
Router1	Fa0/0	192.168.10.1	255.255.255.0
	S/1	10.1.1.1	255.255.255.252
Router2	Fa0/0	192.168.20.1	255.255.255.0
	S1/1	10.1.1.2	255.255.255.252
	S1/2	10.2.2.1	255.255.255.252
	Lo0	209.165.200.225	255.255.255.0
Router3	S1/3	10.2.2.2	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0

Tes Hasil Konfigurasi

Adapun tampilan topologi jaringan yang telah didesain dengan GNS3 yang telah disesuaikan dengan permasalahan yang ada adalah sebagai berikut :

doi.org/10.54209/jatilima.v2i1.140

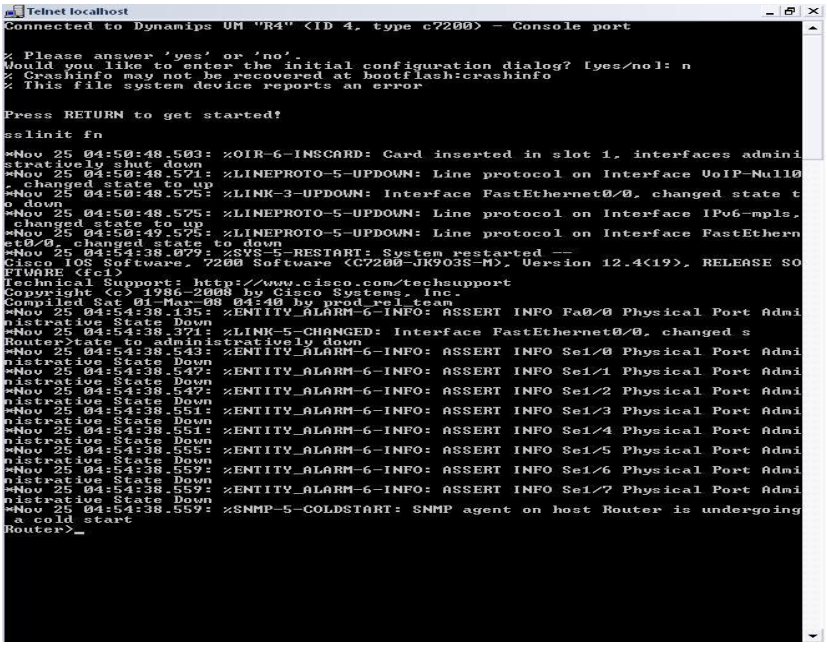


Gambar 5. Tampilan Topologi Jaringan Dengan GNS3

Gambar diatas menunjukkan topologi jaringan yang akan dikonfigurasi dimana terdapat tiga buah router yang akan dikonfigurasi untuk keamanannya.

Layar Beranda Telnet Localhost Router

Pada gambar di bawah ini, Anda dapat melihat proses awal booting router dengan dialog konfigurasi awal. Dalam proses ini, router belum dikonfigurasi.

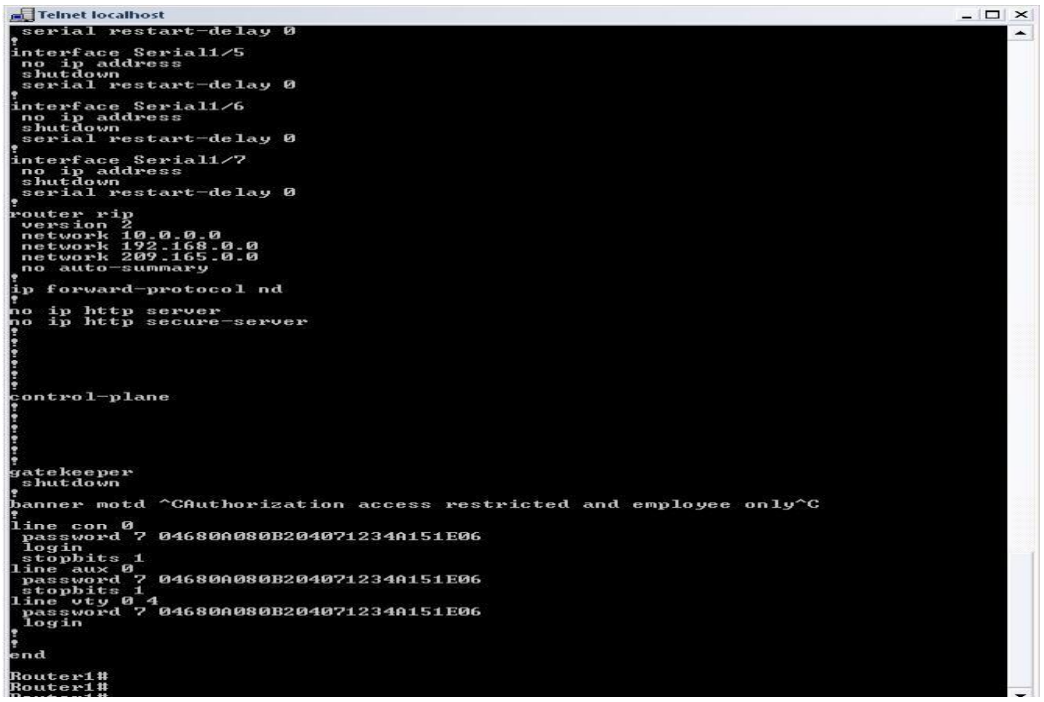


Gambar 6. Tampilan Awal Telnet Localhost Router1

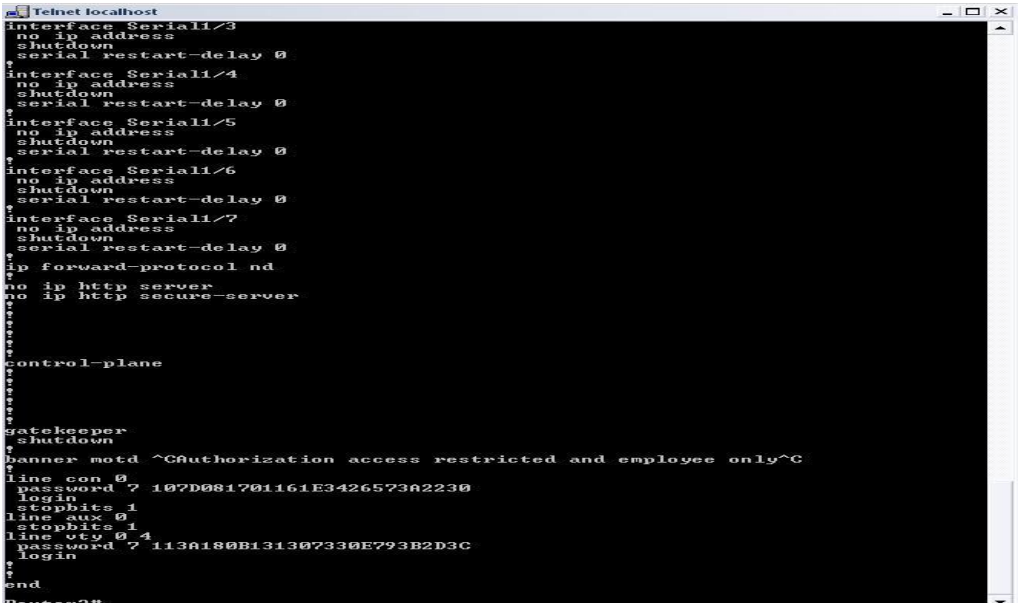
Menguji Hasil Konfigurasi Router

doi.org/10.54209/jatilima.v2i1.140

Berikut hasil pengujian konfigurasi dasar router yang dapat dilihat dengan menjalankan perintah show running-config. Terlihat bahwa semua password yang telah diset telah terenkripsi dengan menjalankan perintah service password encryption. Dan seluruh konfigurasi telah disimpan ke NVRAM dengan perintah copy running-config startup-config.

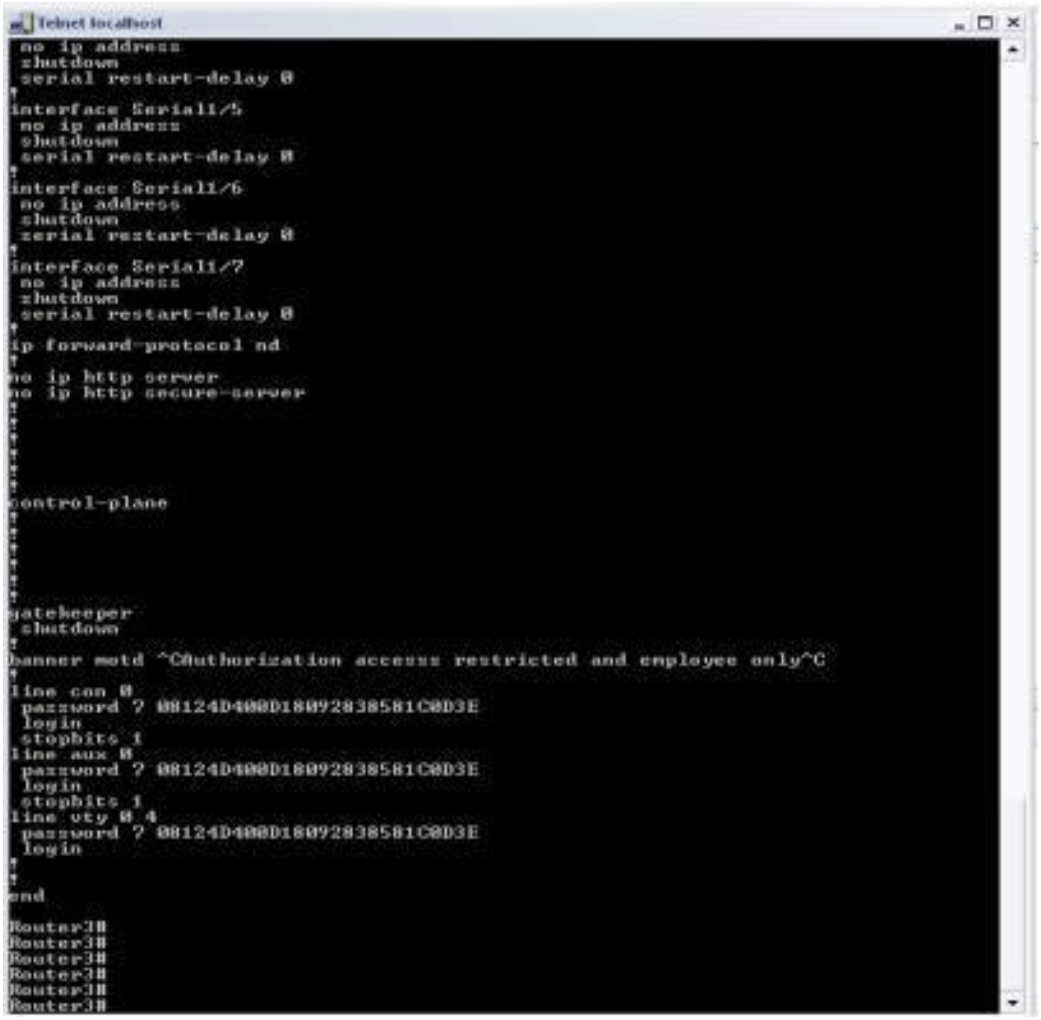


Gambar 7. Tampilan Hasil Konfigurasi Dasar Router1



Gambar 8. Tampilan Hasil Konfigurasi Dasar Router2

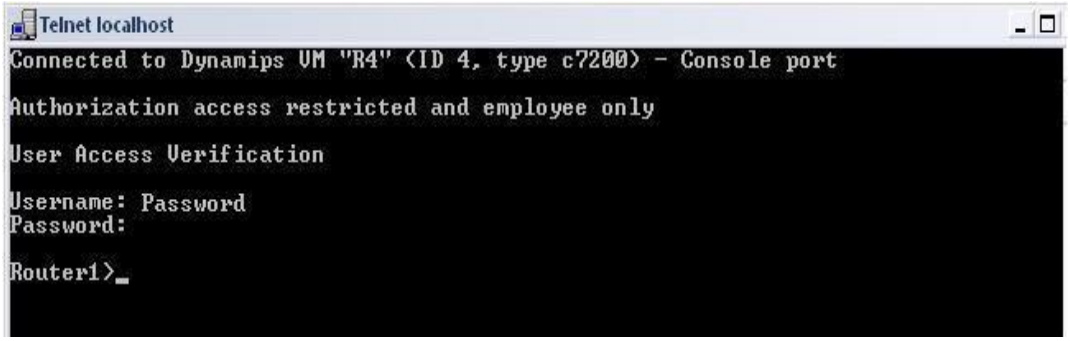
doi.org/10.54209/jatilima.v2i1.140



Gambar 9. Tampilan Hasil Konfigurasi Dasar Router3

Pengujian Hasil Konfigurasi Keamanan Router

Gambar di atas menunjukkan bahwa router akan memiliki username dan password sendiri untuk username tersebut. Ini diperlukan untuk mengotentikasi pengguna yang memiliki akses ke router. Dalam konfigurasi ini hanya satu nama pengguna yang dimasukkan ke dalam router. Terlihat juga banner motd yang sudah dikonfigurasi di awal.

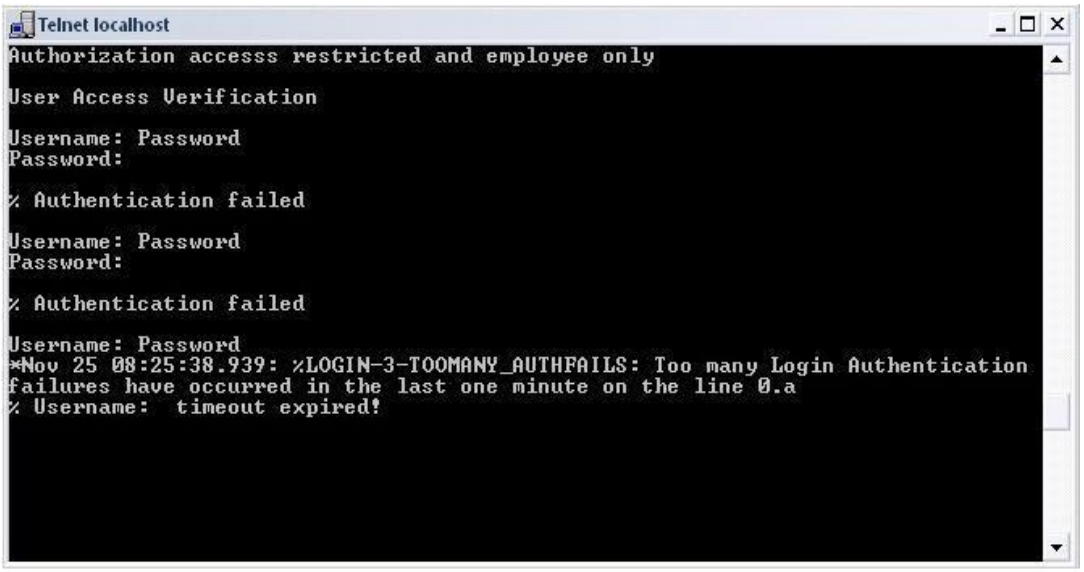


Gambar 10. Tampilan Otentikasi Telnet Localhost

Bentuk serangan yang dimaksud misalnya adalah brute force attack, yaitu serangan yang

doi.org/10.54209/jatilima.v2i1.140

mencoba menebak password dengan berulang kali login dan menebak password. Serangan ini dapat dicegah dengan memiliki teknologi AAA yang telah dikonfigurasi sebelumnya. Jika Anda sudah mencoba login 2 kali tetapi gagal dalam satu menit, akan muncul notifikasi kegagalan.



Gambar 11. Tampilan Telnet Localhost Gagal Login

4. Kesimpulan

Kesimpulan dalam keamanan jaringan dengan model protokol AAA pada keamanan jaringan WAN adalah sebagai berikut: Model protokol AAA (Authentication, Authorization, Accounting) dapat digunakan secara individual atau digabungkan sesuai kebutuhan. Serangan jaringan dapat dicegah dengan teknologi AAA yang telah dikonfigurasi sebelumnya. Telnet localhost saat login 2 kali tapi gagal dalam 1 menit, akan muncul notifikasi kegagalan.

Referensi

[1] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *AITI*, vol. 17, no. 2, pp. 143–158, 2020.

[2] R. T. Prabowo and M. T. Kurniawan, "Analisis dan Desain Keamanan Jaringan Komputer dengan Metode Network Development Life Cycle (Studi Kasus: Universitas Telkom)," *JRSI (Jurnal Rekayasa Sist. dan Ind.*, vol. 2, no. 01, pp. 1–7, 2015.

[3] I. Arnomo, "Simulasi Pengamanan Database Web Server Repository Institusi Melalui Jaringan Lan Menggunakan Remote Access," *JUST IT J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 9, no. 1, pp. 64–71, 2018.

[4] I. R. Rahadjeng and R. Ritapuspitasari, "Analisis jaringan local area network (lan) pada PT. Mustika ratu tbk jakarta timur," *Prosisko J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 5, no. 1, 2018.

[5] T. P. T. IRIADI, "IMPLEMENTASI AUTHENTICATION, AUTHORIZATION, ACCOUNTING (AAA) PADA WIRELESS MESH NETWORK MENGGUNAKAN RADIUS (REMOTE AUTHENTICATION DIAL-IN SERVICE) SERVER." University of Muhammadiyah Malang, 2013.

[6] N. Sadikin, "IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER UNTUK AKSES INTERNET MENGGUNAKAN KEY SECURITY," *Maklumatika*, pp. 20–27, 2019.

[7] M. R. Rofendi and A. Manalu, "Learning Support System With Computer Assisted Instruction Method," *J. Info Sains Inform. dan Sains*, vol. 10, no. 1, pp. 1–6, 2020.

[8] F. Y.-S. Lin, C.-H. Hsiao, Y.-F. Wen, and Y.-C. Su, "Adaptive broadcast routing assignment algorithm for blockchain synchronization services," in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018, pp. 487–492.

[9] A. Hikmaturokhman, A. Purwanto, and R. Munadi, "Analisis Perancangan Dan Implementasi Firewall

doi.org/10.54209/jatilima.v2i1.140

Dan Traffic Filtering Menggunakan Cisco Router," in *Seminar Nasional Informatika (SEMNASIF)*, 2015, vol. 1, no. 3.

10 H. Riyadi, "Memahami Lapisan OSI dan Kegunaannya serta Cara Kerja Lapisan OSI", Memahami Lapisan OSI serta Kegunaan dan Cara Kerja Lapisan OSI, 2019.

[11] S. Syofian dkk, "IMPLEMENTASI USER ACCESS MANAGEMENT UNTUK CISCO ROUTER MENGGUNAKAN METODE AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING) Studi Kasus PT. PROXIS FRIENDS INDONESIA," J. Science and Technology, vol. 8, tidak. 1, hlm. 33–40, 2018.

[12] RN Hidayat, "Implementasi Firmware Tomat Pada Router Nirkabel Linksys Dengan Proses Otentikasi, Otorisasi, Akuntansi Menggunakan Server Radius," 2010.

[13] Riska P, Sugiartawan P, Wiratama I. Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode Port Knocking. Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI). 2018 Dec 31;1(2):53-64.

[14] Huddiniah ER, Safitri EM, Priyambada SA, Nasrullah M, Angresti ND. Optimasi Rute Untuk Software Defined Networking-Wide Area Network (SDN-WAN) Dengan Openflow Protocol. Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer. 2018 Feb 28;13(1):7-13.

[15] Khasanah SN, Utami LA. Implementasi Failover Pada Jaringan WAN Berbasis VPN. Jurnal Teknik Informatika STMIK Antar Bangsa, IV (1). 2018 Jan 23:62-6.