ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN MENGGUNAKAN TEKNIK DEMILITARIZED ZONE(DMZ)

Benny Wijaya, Dedi Rianto Rahadi, Alex Wijaya

Magister Teknik Informatika
Universitas Bina Darma
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstrak

Ancaman keamanan terhadap jaringan komputer semakin hari semakin beragam dan semakin canggih. Ketika suatu jaringan lokal terhubung ke jaringan internet maka potensi untuk ancaman keamanan akan semakin meningkat. Untuk itu perlu dilakukan langkah-langkah untuk mencegah dan meminimalisir ancaman keamanan yang berpotensi menyerang jaringan internal. Ada beberapa teknik yang bisa diterapkan, salah satunya menggunakan teknik Demilitarized Zone (DMZ). Dengan DMZ maka akan terbentuk zona penyangga pada jaringan sehingga akses dari luar tidak bisa langsung memasuki zona internal, akan tetapi harus melalui zona penyangga tersebut. Ada banyak cara yang berbeda untuk merancang sebuah jaringan dengan DMZ, metode dasar adalah dengan menggunakan firewall tunggal. Implementasi DMZ kedalam jaringan bisa dilakukan menggunakan firewall secara hardware maupun software. Bisa juga memanfaatkan firewall linux untuk merancang DMZ.

Kata kunci: *DMZ, Firewall*

1 PENDAHULUAN

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, walaupun terkadang ada beberapa organisasi yang menempatkan masalah keamanan ini pada urutan yang ke sekian setelah tampilan dan lain sebagainya. Tapi ketika jaringan mendapat serangan dan terjadi kerusakan sistem, investasi yang dikeluarkan cukup besar untuk melakukan perbaikan sistem. Untuk itu sudah selayaknya investasi dibidang keamanan jaringan lebih diperhatikan, untuk mencegah kerusakan dari ancaman serangan yang saat ini semakin beragam serta semakin canggih. Terlebih lagi ketika jaringan lokal sudah terhubung ke internet maka ancaman serangan terhadap keamanan jaringan akan semakin meningkat, berbagai macam teknik serangan terus dikembangkan misalnya syn flood attack, Dos attack dan lain sebagainya, tidak menutup kemungkinan juga serangan hacker, virus, Trojan yang semuanya merupakan ancaman serangan yang tidak bisa diabaikan. Untuk itu perlu disiapkan teknik yang dapat setidaknya meminimalisir ancaman serangan yang bisa memasuki sistem jaringan sehingga kerusakan dapat diperkecil.

Untuk menangkal ancaman serangan terhadap jaringan ada beberapa langkah yang bisa diterapkan, salah satu teknik yang bisa digunakan adalah teknik demiliterizedzone (DMZ). Dengan DMZ maka jaringan internal dapat diamankan dari akses eksternal. Ada banyak cara yang berbeda untuk merancang sebuah jaringan dengan DMZ. Metode dasar adalah dengan menggunakan firewall tunggal.

Ada banyak cara pula untuk menerapkan DMZ ini kedalam jaringan, seperti yang sudah di ketahui ada 2 (dua) jenis firewall yaitu secara hardware maupun software. Untuk yang jenis hardware, ada beberapa firewall keluaran vendor besar seperti contoh Cisco PIX Firewall. Sedangkan untuk firewall jenis software seperti Black Ice. Selain itu, bisa juga memanfaatkan firewall linux untuk merancang DMZ.

2 METODOLOGI PENELITIAN

2.1 Bahan penelitian

Bahan penelitian yang digunakan dalam penelitian ini adalah firewall untuk membatasi akses eksternal ke jaringan internal.

2.2 Alat penelitian

Penelitian ini menggunakan perangkat firewall, switch, kabel untuk membangun sistemDMZ.

3 HASIL DAN PEMBAHASAN

3.1 Konfigurasi DMZ

- Konfigurasi Jaringan untuk penerapan DMZ memiliki karakteristik sebagai berikut:
  - Web server dihubungkan pada antarmuka DMZ firewall PIX 515E.
  - HTTP klien pada jaringan privat dapat mengakses web server di DMZ dan juga dapat berkomunikasi dengan perangkat di Internet.
  - Klien di Internet diijinkan akses HTTP ke web server DMZ; semua trafik lainnya ditolak.
  - Jaringan memiliki dua alamat IP routable yang tersedia untuk Publik: satu untuk antarmuka luar firewall pix 515E (209.165.200.225), dan satu untuk alamat IP publik dari server web DMZ (209.165.200.226).
- konfigurasi firewall pix 515E meliputi aturan- aturan sebagai berikut:
- Aturan kontrol akses memungkinkan trafik diperuntukkan untuk server web DMZ dan untuk perangkat di Internet.
- Aturan terjemahan alamat menerjemahkan alamat IP privat sehingga alamat privat tidak terlihat ke Internet. Untuk trafik yang ditujukan ke server web DMZ, alamat IP privat diterjemahkan ke alamat IP dari alamat IP pool.

  Untuk trafik yang ditujukan untuk Internet, alamat IP privat diterjemahkan ke alamat IP publik dari firewall pix 515E. Trafik keluar tampaknya datang dari alamat ini.

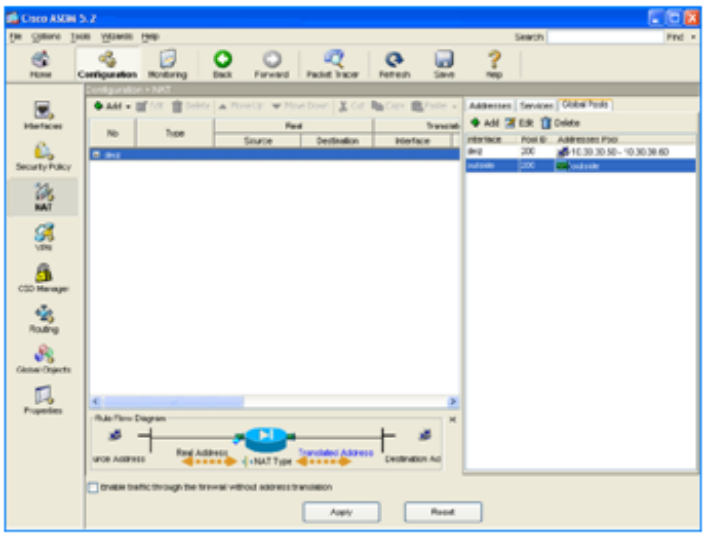
- Untuk mengizinkan trafik masuk untuk mengakses web server DMZ, konfigurasi firewall pix 515E meliputi :
  - Sebuah aturan terjemahan alamat menerjemahkan alamat IP publik dari web server DMZ untuk alamat IP privat dari server web DMZ.
  - Aturan kontrol akses mengizinkan trafik HTTP masuk yang diperuntukkan bagi webserver DMZ.

3.2 Konfigurasi PIX 515E untuk DMZ Deployment

Akan digunakan Adaptive Security Device Manager (ASDM) untuk mengkonfigurasi firewall pix 515E. ASDM adalah antarmuka berbasis garafis yang memungkinkan untuk mengatur dan memonitor Cisco Pix firewall 515E. untuk skenario konfigurasi, prosedur yang dilakukan sesuai dengan parameter berdasarkan skenario yang telah ditentukan sebelumnya.

Prosedur Konfigurasi ini mengasumsikan bahwa firewall pix 515E telah dilakukan konfigurasi untuk bagian antarmuka dalam, antarmuka DMZ, dan antarmuka luar. Mengatur interface dari firewall pix 515E dengan menggunakan Startup Wizard di ASDM. Pastikan bahwa tingkat keamanan antarmuka DMZ diatur antara 0 dan 100. (Pilihan umum adalah 50)

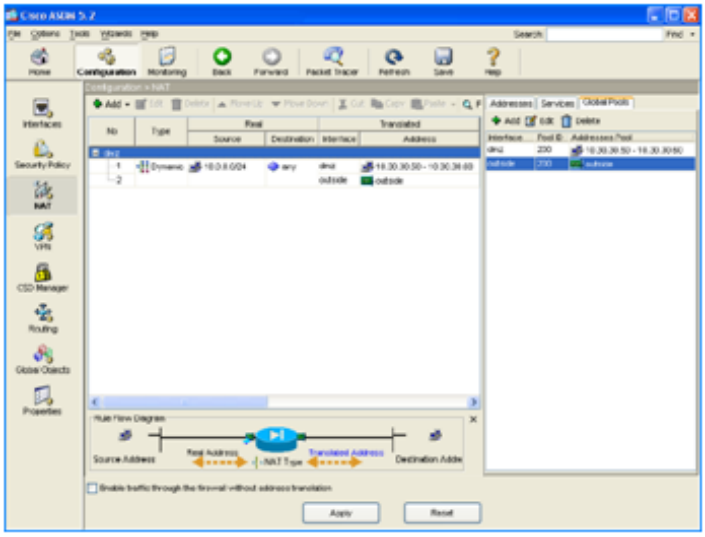
3.3 Persyaratan Konfigurasi



Gambar 1: hasil konfigurasi Pool pada jendela utama ASDM

Konfigurasi firewall pix 515E untuk penyebaran DMZ ini membutuhkan tugas konfigurasi berikut:

- Untuk klien internal agar memiliki akses HTTP ke web server DMZ, maka akan dibuat alamat IP Pool untuk terjemahan alamat dan mengidentifikasi klien mana yang harus menggunakan alamat dari IP Pool. Untuk menyelesaikan tugas ini, akan dilakukan konfigurasi berikut :



Gambar 2: Hasil konfigurasi Dynamic NAT Rule

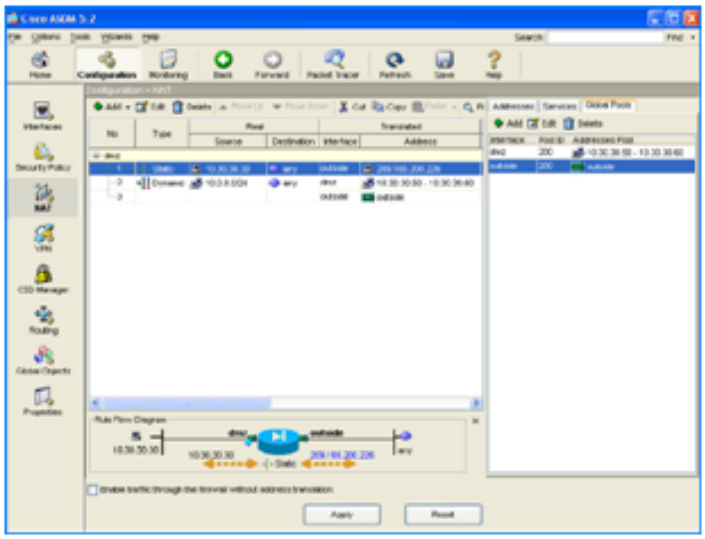
- Sebuah pool alamat IP untuk antarmuka DMZ. Dalam skenario ini, IP Pool adalah 10.30.30.50-10.30.30.60.
- Sebuah aturan terjemahan dynamic NAT untuk antarmuka dalam yang menentukan alamat IP klien mana yang dapat diberikan alamat dari IP Pool.
- Untuk klien internal agar memiliki akses ke HTTP dan HTTPS pada Internet, akan dibuat aturan yang menerjemahkan alamat IP dari klien internal ke alamat eksternal yang dapat digunakan sebagai alamat sumber.

Untuk menyelesaikan tugas ini, akan dilakukan konfigurasi aturan terjemahan PAT (aturan terjemahan alamat port, kadang-kadang disebut antarmuka NAT)untuk antarmuka internal yang menerjemahkan alamat IP internal ke alamat IP eksternal dari firewall pix 515E.

Dalam skenario ini, alamat internal yang akan diterjemahkan adalah yang dari subnet jaringan privat (10.10.10.0). Alamat dari subnet ini diterjemahkan ke alamat publik dari firewall pix 515E (209.165.200.225).

- Untuk klien eksternal agar memiliki akses HTTP ke web server DMZ, akan dikonfigurasi identitas eksternal untuk server web DMZ dan aturan akses yangmengizinkan permintaan HTTP yang berasal dari klien di Internet. Konfigurasi yang akan dilakukan sebagai berikut :
  - Buat aturan NAT statis. Aturan ini menerjemahkan alamat IP sebenarnya dari Server web DMZ ke alamat IP publik. Dalam skenario ini, alamat publik web server adalah 209.165.200.226.
  - Buat aturan akses keamanan yang mengizinkan trafik dari Internet jika trafik adalah permintaan HTTP maka akan ditujukan ke alamat IP publik dari server web DMZ.

3.4 Menciptakan IP Pools untuk Network Address Translation



Gambar 3: hasil konfigurasi NAT statis

Firewall pix 515E menggunakan Network Address Translation (NAT) dan Port Address Translation (PAT) untuk mencegah alamat IP internal di- ekspose ke eksternal. Prosedur ini menjelaskan cara membuat pool dari alamat IP yang bisa digunakan oleh antarmuka DMZ dan antarmuka luar untuk menterjemahkan alamat. Sebuah IP pool tunggal dapat mengandung NAT dan PAT entri, dan dapat berisi entri untuk lebih dari satu antarmuka.

3.5 Konfigurasi NAT untuk Klien internal Berkomunikasi dengan Web Server DMZ

Dalam prosedur sebelumnya, sudah dibuat pool alamat IP yang dapat digunakan oleh firewall pix 515E untuk menutupi alamat IP privat dari klien pada jaringan internal. Dalam prosedur ini, akan dikonfigurasi aturan Network Address Translation (NAT) untuk mengasosiasi alamat IP dari pool ini dengan klien bagian dalam(internal) sehingga mereka dapat berkomunikasi secara aman dengan server web DMZ. Konfigurasi akan seperti Gambar 2.

3.6 Konfigurasi NAT untuk Klien internal Berkomunikasi dengan Perangkat di Internet

Dalam prosedur sebelumnya, telah dikonfigurasi aturan Network Address Translation (NAT) yang mengasosiakan alamat IP dari IP pool dengan klien internal sehingga mereka dapat berkomunikasi secara aman dengan server web DMZ.

Bagi beberapa konfigurasi, perlu juga membuat aturan NAT antara antarmuka dalam dan antarmuka luar untuk memungkinkan klien dari jaringan internal untuk berkomunikasi dengan internet.

Namun, dalam skenario ini tidak perlu membuat aturan ini secara eksplisit. Alasannya adalah bahwa IP pool (pool ID 200) mengandung kedua jenis alamat yang diperlukan

untuk terjemahan alamat: kisaran alamat IP yang akan digunakan oleh antarmuka DMZ, dan alamat IP yang digunakan untuk antarmuka luar. Hal ini memungkinkan untuk ASDM membuat terjemahan aturan kedua.

3.7 Konfigurasi Identitas Eksternal untuk Web Server DMZ

Web server DMZ harus dapat diakses oleh semua host di Internet. konfigurasi ini membutuhkan menerjemahkan alamat IP privat dari server web DMZ ke alamat IP publik. Untuk memetakan alamat IP server web yang sebenarnya (10.30.30.30) statis ke alamat IP publik (209.165.200.226)

3.8 Menyediakan HTTP Akses Publik ke Server Web DMZ

Aturan kontrol akses pada firewall pix 515E harus dibuat untuk mengizinkan jenis trafik dari jaringan publik untuk sumber daya di DMZ. Aturan kontrol akses ini menentukan antarmuka dari firewall pix 515E yang akan memproses trafik, apakah trafik masuk atau keluar, asal dan tujuan trafik, dan jenis protokol trafik dan layanan yang diizinkan.

Akan dibuat aturan akses yang mengizinkan trafik HTTP masuk berasal dari semua host atau jaringan di Internet, jika tujuannya adalah web server pada jaringan DMZ. Semua trafik lainnya yang datang dari jaringan publik akan ditolak.

4 KESIMPULAN

1. Dengan membuat segmen jaringan menggunakan DMZ, maka akses dari luar ke jaringan internal dapat dibatasi sehingga tidak bisa langsung menuju jaringan internal dan ini meningkatkan kemanan jaringan.

2. Penerapan DMZ pada infrastruktur jaringan mampu melindungi jaringan komputer dari ancaman.

5 Referensi

1. Alsa, Asmadi. (2004) Pendekatan Kuantitatif Kualitatif dalam Penelitian Psikologi. Pustaka Pelajar, Yogyakarta.

2. Amon, Cherie n friends. (2006) Designing and Building Enterprise DMZs.Syngress Publishing, Inc, Canada. 3. Gay, L.R. (1983). Educational Research Competencies for Analsis & Application. 2nd Edition. A Bell & Howell Company, Ohio.

3. Goldman, James E.(2003). Applied data communications : a business oriented approach. Wiley, United StatesLusignan, Russel, Oliver Steudler, Jacques Allison. (2000). Managing Cisco Network Security : Building rock solid Network. Syngrees Publishing, Inc, Rockland.

4. Mansfield, Niall. (2002). PRACTICAL TCP/IP Mendesain, Menggunakan, dan Troubleshooting Jaringan TCP/IP di Linux dan Windows. Jilid 1. Penerbit Andi,Yogyakarta.

5. Mansfield, Niall. (2003). PRACTICAL TCP/IP Mendesain, Menggunakan, dan Troubleshooting Jaringan TCP/IP di Linux dan Windows. Jilid 2. Penerbit Andi, Yogyakarta.

6. Osipov, Vitalty, Mike Sweeney dan Wondy Weaver. (2002). Cisco Security Specialists Guide to PIX Firewall.Syngress Publishing,Inc, Rockland.

7. Salim, Hartojo . (1990). Virus Komputer : teknik pembuatan dan langkah-langkah penanggulangannya. 1st Edition. CV. Andi Offset, Yogyakarta.

8. Sofana, Iwan. (2009). Pengantar JARINGAN KOMPUTER & CISCO CCNA. Informatika, Bandung.

9. Sopandi, Dede, 2008, Instalasi dan konfigurasi Jaringan Komputer, Informatika, Bandung.

10. Sukardi. (2011). Metodologi Penelitian Pendidikan Kompetensi dan Praktiknya. PT Bumi Aksara, Jakarta

11. Suyatno, A. (2009). Aplikasi Model Sistem Keamanan Jaringan Berbasis De-Militarised Zone. Jurnal Informatika Mulawarman, 6-12.

12. Wahana komputer, 2004, Kamus Lengkap Jaringan Komputer, Salemba Infotek, Jakarta.

13. Wirija, Sudantha, 2005, Microsoft Windows Server 2003, Elek Media Komputindo, Jakarta.

14. Zwicky, Elisabeth D, Cooper, Simon, and Chapman, D. Brent. (2000). Building Internet Firewalls. Second Edition.ORcitly & Associates, Sebastopol, California.