

DMZ (De-Militarized Zone)

Internet untuk saat ini sangat berkembang cepat. Dengan banyaknya company yang telah menyediakan Link Backbone baik untuk teresterial maupun untuk langsung terconnect dengan dunia luar. Di Indonesia setau saya telah ada beberapa company yang melayani jasa tersebut. Contoh Indosat, Satelindo, XLComindo, IconPLN, Telkom, etc. Memang disitu adalah perusahaan yang cukup besar dan profesional di bidangnya.

Dengan begitu maraknya dunia telekomunikasi di Indonesia tentunya tidak lepas dari security network di setiap client pengguna jasa network. Beberapa alasan yang membuat security network sangat penting yaitu :

- Keamanan data
- Keamanan rahasia perusahaan
- Dan lain-lain

Mau tidak mau dengan adanya perkembangan teknologi di dunia ini setiap perusahaan harus sudah siap untuk melakukan sebuah perubahan di dalam infrastruktur usahanya, dari sisi telekomunikasi dan networknya tersebut.

Disini akan terdapat sedikit pembahasan kecil tentang keamanan network yang dibangun dengan topology yang sederhana yang dengan tujuan untuk keamanan network tersebut. DMZ adalah sebuah topology network yang di sini mengutamakan management dan security didalamnya. Untuk contoh sederhana dari gambar network topologynya saya sertakan disini.

<http://noc.iconpln.net.id/~syam/Stuff/dmz.jpg>

Pejelasanannya akan saya mulai dari atas sisi internet samapi ke dalam. Untuk disisi internet, dengan siapa pun kita mempunyai uplink tidak akan mempunyai masalah disini.

Disisi Router kita bisa memakai cisco dengan konfigurasi VLAN di dalamnya. Mengapa pakai VLAN hal ini dikarenakan VLAN akan memperkecil Broadcast Domain di setiap port di switchnya tersebut.

Dari cisco akan keluar terconnect dengan switch yang dimana switch tersebut juga terconfigure VLAN. Dari switch akan menuju ke 2 server yaitu server yang berfungsi sebagai Firewall dan NAT. untuk konfigurasi 2 server ini kita menggunakan 2 metode yang berbeda.

Untuk Firewall server tentunya kita menggunakan Server yang mempunyai 2 eth yang berfungsi atau terhubung sebagai Bridge. Saya sarankan untuk Friewall server menggunakan OS yang bener. aman untuk default nya. Saya disini menggunakan OpenBSD untuk server tersebut. Ada banyak type OS server yang bagus. Disamping Firewall Server terconfigure sebagai Bridge juga disana bisa kita configure untuk limiter bandwidth bagi setiap server farm nya.

Dibawah Firewall kita bisa menggunakan Hub untuk menghubungkan Server Farmnya dengan dunia luar. Disini kita bisa mendapatkan keuntungan dimana kita bisamensegmentasi network kita dan bisa mengatur network kita dengan baik. Dan juga konsumsi setiap traffic bandwidthnya bisa tidak terlalu berlebihan.

Kemudian dari sisi keluar Switch yang lainnya keluar menemui Server NAT. yang mempunyai 2 eth juga yang satunya memakai IP publish dan satuna lagi memakai IP Privat sebagai gateway LAN tersebut.Keuntungan dari network ini adalah :

- Management network mudah
- Kita bisa plug and play
- Konsumsi bandwidth tidak overload
- Dan yang terpenting adalah security dari setiap data bisa termonitor dengan baik

Sedangkan kelemahan dari network ini: * Harus menghubungi Administrator network apabila diinginkan ada perubahan network.

Author: yanuar@iconpln.net.id

From:

<http://wiki.corebsd.or.id/> - **CoreBSD Wiki**

Permanent link:

<http://wiki.corebsd.or.id/doku.php/dmz?rev=1128530869>

Last update: **2025/10/25 17:09**

