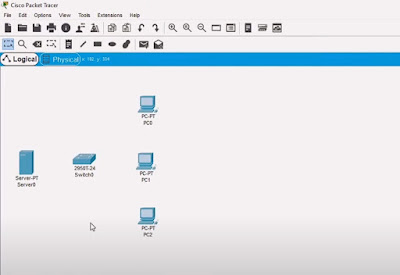
**Langkah-langkah Konfigurasi Firewall dengan Cisco**

**1. Buka Aplikasi Konfigurasi Firewall sederhana**

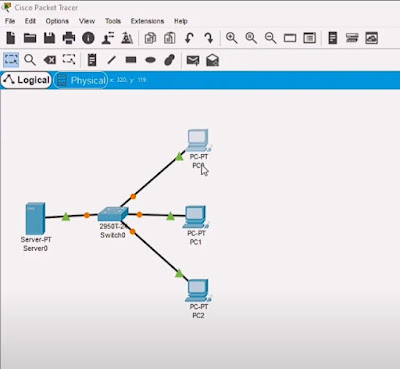
Pertama-tama, buka aplikasi untuk konfigurasi firewall, yaitu menggunakan software Cisco Packet Tracer. Jadi, pastikan software tersebut sudah terinstal di PC atau laptop yang kamu gunakan.

**2. Mengatur Server dan Switch**

Pada lembar kerja, tambahkan satu server, satu switch, dan tiga PC atau lebih di Cisco Packet Tracer. Setelah itu, tambahkan connection untuk menyambungkan antarperangkat.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi-fJ3zxRcl4d2aliJx2FJVXRgU-eGRZZiqwUooD55JAoAZgKW4g2Y0RX5NoHtQbk9cIeVS6zLk7aKfezShC9ovQHhCSIZWwz62Y7Lddz3D-40PxTxJbldiaRJZ5IgvVL1JTRZnhvj7i2yTwefm-QUt0NpRgwCYvgMHy87SeT6yBmO8skaY9q65FtXRtE4/s884/130-01.jpg)

Untuk pemula bisa menggunakan automatic choose connection untuk mempermudah tahapan ini. Sambungkan server ke switch dan switch ke tiga PC tadi menggunakan connection tersebut.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhuvHmUhGk6ytmDTIzClg4RNFouVzTiQLKi28j5t2Ik2uVhth385iStzbOdOflSculRK7lqGrpjKLiWAlxRHKEq3JL_YqsoI77fOQVC9yVOK9QUACel0gFDv2GwJxb3o3quTHVcP-z1Qj7KTdYLQ5o_W7n7djMnW69cWfzuJHRW_VmCEzxhRQf-TB4lrKU/s659/130-02.jpg)

Sebelum melanjutkan konfigurasi, pastikan bahwa server sudah terhubung dengan baik. Pastikan juga bahwa switch-switch yang digunakan telah diatur dengan benar.

Klik dua kali pada bagian nama perangkat dan kamu bisa mengubahnya dengan IP Address yang kamu gunakan. Sebagai contoh, pada ketiga perangkat menggunakan IP Address sebagai berikut:

Server: 192.168.10.1

PC 1: 192.168.10.2

PC 2: 192.168.10.3

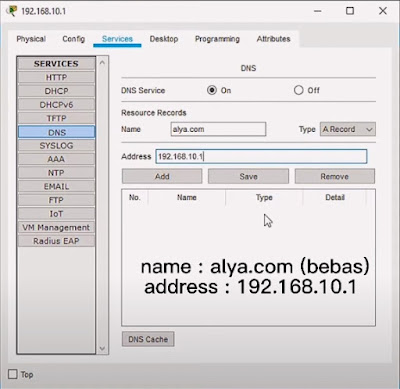
PC 3: 192.168.10.4

Jika semua komponen perangkat telah terhubung, kamu dapat melanjutkan ke langkah berikutnya.

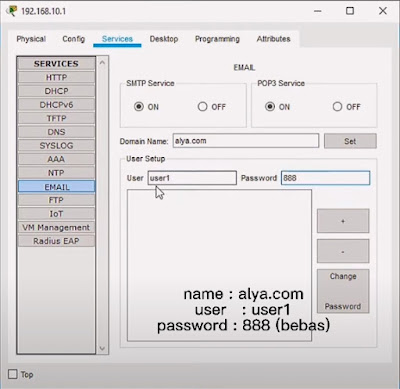
**3. Konfigurasi Awal**

Setelah semua komponen terhubung, masuk ke pengaturan server dengan klik pada gambar Server untuk melakukan konfigurasi awal.

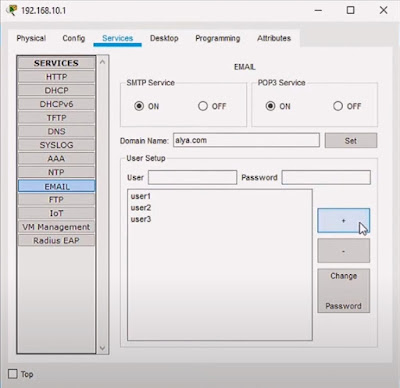
Masuk ke menu Services, pilih DNS, dan aktifkan DNS Service dengan memilih opsi On. Lalu, berikan nama pada Resource Records sesuai keinginan dan ketikkan 192.168.10.1 pada kolom Address. Klik Save untuk menyimpan pengaturan DNS Server.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhJ5-ZRf6cpuMOOOI9x2wDkq2vFhmgbG2VuLIxyuSpwK9eKc8LZa_IfrwoxzgWkEbPaXdqtGeZ-9k9eBFfSWLDoIsagdSRUuKLrCFecTHJStUoa4N-u-SYmgSKcjWOcOoU8hMLv94jWFbS9UBWXifhWQb75-q7hHpy3fOw737J7kd9dT6l2PnGYQzH0Dpo/s576/130-03.jpg)

Lanjutkan proses ini dengan masih di tab Services dan pilih menu Email di sebelah kiri window yang sedang terbuka saat ini dan masukkan Domain Name, User, dan Password bebas sesuai keinginan. Setelah itu, tekan tombol + yang ada di sebelah kanan.

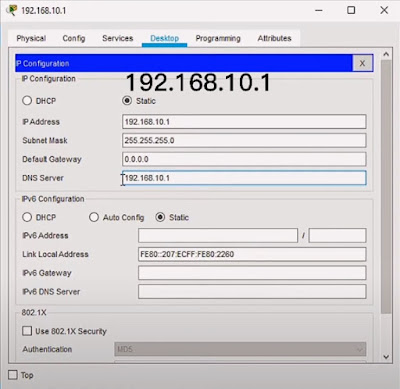
[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhafTQ1ZaXUbAKwRQuwVIk1WWQu8RQPsa4SojEM5NCq2H_IOYA7iOaG-cyw30RpDjm4-P1AoNVu79PIk5rdDIzCQZS6BubRsxB-6ufJtFLQwVkYtXTDzZciNwjHYAJQChHOlk6MypkTWuLX_gcyStVCun9vHDJvKTobtV6IuCspoxmnyTCkXKoyq5EvWIU/s576/130-04.jpg)

Buat user sebanyak jumlah PC yang kamu gunakan untuk mengonfigurasi firewall di Cisco Packet Tracer.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjhIE4DCTuqayJRj9QcgkWdKBKHn2CJXO7chp_lXnIzDLcYjZ03B6cW-FsgSSPPHlDRz-xHNYZt4GPGptMJpiuLHS7gbQA2OLf35_hxTDc03cqvONud6C1g1gcZ5ptK48WXxMDy1ogYWFsLYOmGgoiJ8sl2FK7S2LUmoyTQxNf28ys2AStMzA_n_j1Gdjw/s575/130-05.jpg)

Pindah ke tab Desktop dan di menu IP Configuration, kolom IP Address isikan dengan 192.168.10.1 (ini adalah IP Address dari Server yang kamu buat).

Tambahkan juga Subnet Mask 255.255.255.0 dan DNS Server sama seperti IP Address Server, yaitu 192.168.10.1.

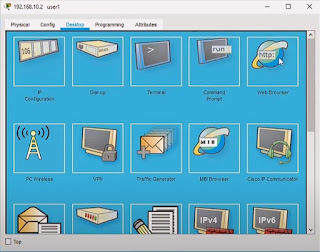
[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiOuLtR6B7DuGF_sHjdDG_owWbLLqUMo-0gKwAiS44KRXBy7ZoGCUaQTLhjyWFjvGZqtnQwY8n7Cz27V_iHQdosqQayXewPFhnmQdJAxa7tKWO0yc6aA0_NduNWtDXk9RXgf078hmPNJlRhyu6aRcjwFwxRr5rVoeVM34Gvmmsy8xTsIYdEUL0OkrDGZaQ/s574/130-06.jpg)

Klik gambar PC 1 dan masuk ke tab Desktop. Masukkan kolom IP Address sesuai dengan IP Address pada PC, Subnet Mask 255.255.255.0, Default Gateway 192.168.10.1, dan DNS Server 192.168.10.1.

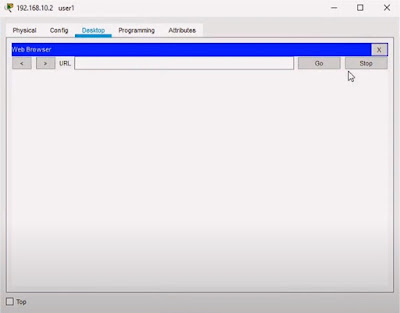
Ulangi langkah di atas pada PC 2 dan PC 3 dengan mengganti kolom IP Address sesuai IP Address yang digunakan di masing-masing perangkat PC.

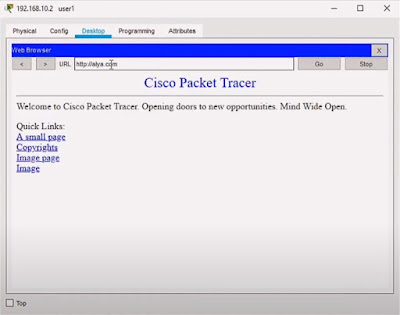
**4. Mengatur Web Browser**

Setelah konfigurasi awal selesai, cek hasil pengaturan ke web browser untuk memastikan bahwa koneksi internet sudah berfungsi dengan baik. Pastikan kamu mendapatkan hasil yang diinginkan saat mencoba membuka halaman web.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj4kYM1wWEoc4uqtgAvVFp6DqccLDPbOyPuxwSVqT4PcL1_fC_VYmWPPl38M1nMQUVnuyE6xfdz70bJg1O7M5nBLWOl-7FpnQZx4kvQFioTzhkirzOwmLR5jAzatqe1XulNqehfH6aFl91KAyvyN42EAWre2lQpqaH-XENXSDPo5erKh-cEhn3thRT4zMY/s712/130-08.jpg)

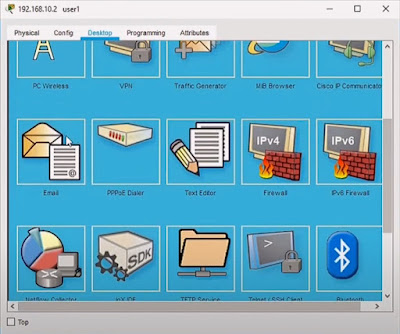
Klik pada salah satu PC, misalnya PC 1, kemudian pada tab Desktop, klik gambar Web Browser. Pada kolom URL yang tersedia, ketikkan Domain Name yang sudah dibuat tadi dan coba tes apakah konfigurasi sudah bekerja dengan baik atau belum.

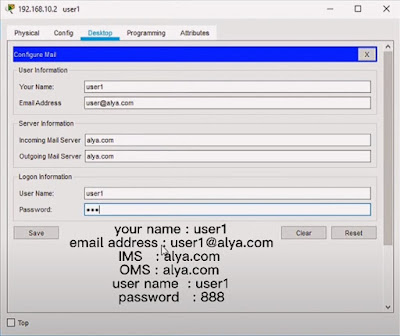
[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjdcqiGY_HybbAmtTkKktl_TSHPJGRP3V9I7ioLHxfCmAWpn6up0CBCaIdzAU39ueiZZLm7xPVRXld2t61kFlzopB1wYXFbo7ibMQCOl2nyV4S3bAhBGK3y5dd5yqV6L4JaSiTdGc-P29cRmQgOY_yuzRjd17kLLmNJ-D_LKR267R_t3gwTsKjK_0rSXjY/s711/130-09.jpg)

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiilMNTQHJ_b3x8-fiudXcpnecPbOyx7bQogK4Fwwy0W6xJnbN9EQxO5fq0vZyYLdAaxw3xitj3VoUamwSqkjZE7hFXUbMvJ_LZfScKuoOdTe2W_41zzv5DM5SHt2kUkSENHsX74YIRq7LgplVwSM3fiHq6Vc5NnrMjHb7zKX_0nQeLPCs7Bcxx08Paeak/s711/130-10.jpg)

**5. Konfigurasi Email**

Pada pengaturan PC, pergi ke tab Desktop dan klik Email. Kamu bisa mencoba menggunakan pengaturan email seperti di bawah ini dan bisa menyesuaikannya dengan preferensi masing-masing.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhOJzpztabgPZGO03MEETvYJvalaMh5XFXk4riFz3qQywRASwI3caH9n8reikLq-IZrDEaT2Oc3HXrD6xrvRHMp_RbZ3xoyailiW0TR3rVKfYKw6UbLdKJbWYjBkz_qLpDmi6vBmiGlibw4aB9XGt67IgA84n_ZsMsG1qEgIfjrArynGPDipA0tjfOzPSc/s668/130-10.5.jpg)

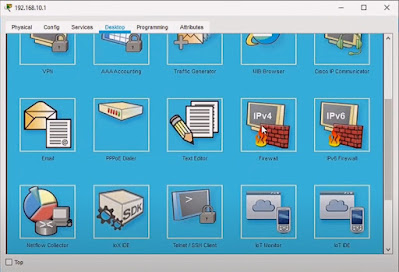
[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiF_xH2gbUoU3rSRaSJCLZ30TIL8SmQkmJIuZwvxAQn4G-E2vcYdz7F72R-SBujqxcgLuxv8t6NcZKxQIO4dfd8ERuYGix4yowLNKLri0znClq4_vYGUJoAS4f9adwuM2wS-o5dDg0nU5GhatkohsgEQVU2LMPp0zWHlmQjXTKJCrG9l00-E-hYyQraRGg/s667/130-11.jpg)

Klik tombol Save untuk menyimpan perubahan konfigurasi Email Lakukan prosedur yang sama pada PC lainnya.

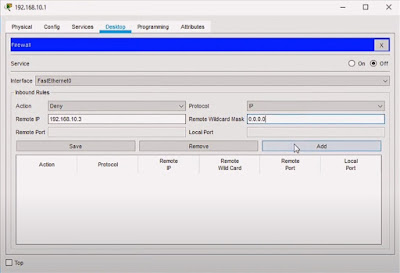
**5. Konfigurasi Firewall**

Sekarang kita akan beralih ke konfigurasi firewall. Konfigurasi ini dapat dilakukan dengan mengatur aturan-aturan yang diperlukan sesuai kebutuhan.

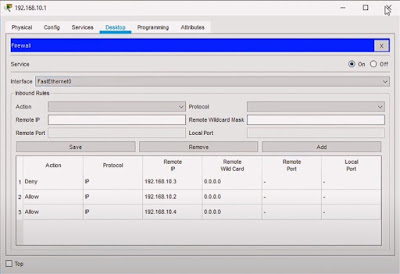
Klik pada salah satu PC dan masuk ke tab Desktop, cari dan klik opsi Firewall.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhsRr_Z8Os150i0db_K4dW1znevJzxiyJtwNhRtd0FDEVmJINE6btNCFiP9xnqJhcnOgwhLfrTHp5JgVHM_M2laWaK2j_7nBoRw66iS4ZHZk0XyvcQ4epIwoVlIJlBCNtxV0KOXcjgaMvGqjrmi-J1pZUEaDKzdqyB57c-qpXROE0BHNfcaiIcUGB5s7jI/s820/130-12.jpg)

Pada kolom Action, pilih Deny.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiEXvbriMaobxLenhcPkIISfdCBArRkFTfh7AR3b9nGq3gy1hUfauHDF35nUPy1HUqt2_fApopgsSNk5_KxRJ7dgB0BHxIenEJfq4jAAumIDKrYVpWPdVULrHmTRS_rtLbVOWYtJKL9tm24coWmPbKFSM3rMjT3K4ANcJUZf7kve-DZmbQVmg6LMHInGc8/s818/130-13.jpg)

Pada kolom Remote IP masukkan IP Address yang digunakan pada perangkat, sebagai contoh 192.168.10.3. Masukkan 0.0.0.0 pada kolom Remote Wildcard Mask. Klik Add untuk menambahkan Service pada konfigurasi Firewall.

[](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhX-y26de_xgAHBMr2-w1Hom6kmVbeB5sXYzitE6KlKNzFslqvMNQ0PcGyzPrBJUaj2yL1vwreQSJ0Q8j0xNr8smGGMPXaAPp71Td0R9YC4dhfYWVk5SshjCG5md1yk3SUZSGxaq_2YyNJEqHXiXuruxp5py4gJxVFeC9QgPnBcT7InqsKNlboCdKhBJio/s818/130-14.jpg)

Tambahkan Service baru sebanyak dua atau lebih sesuai jumlah [PC](https://www.buatkuingat.com/2023/06/cara-konfigurasi-firewall-di-cisco-packet-tracer.html). Bedanya, Action yang digunakan adalah Allow dengan menggunakan IP Address sesuai yang terdapat pada perangkat.

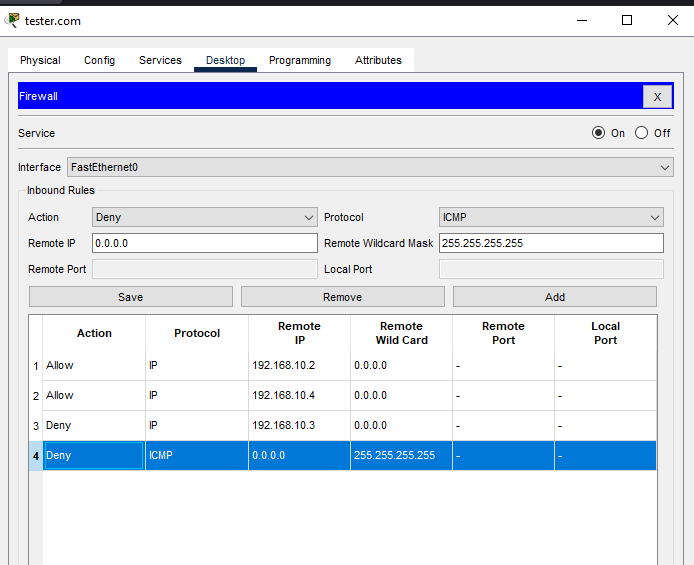
**6. Verifikasi Konfigurasi**

Setelah semua konfigurasi selesai, verifikasi keberhasilan konfigurasi firewall dengan melakukan beberapa pengujian.

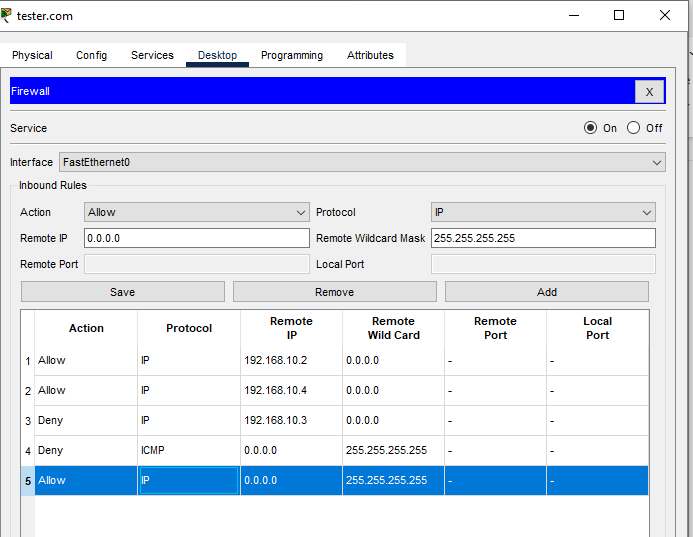
Coba tes dengan mengirimkan mail ke PC yang dituju dan bisa kamu lihat jika Successfull, berarti PC tersebut menggunakan Action Allow atau diperbolehkan dan apabila Failed, PC tersebut diblokir oleh Firewall karena Action Deny.

**Konfigurasi Blok Ping Flood**

Buka firewall (IPv4) Kembali lalu pilih ICMP (Ping Flood). Selanjutnya isi Remote IP dengan 0.0.0.0 dan untuk Remote Wildcard Mask nya 255.255.255.255

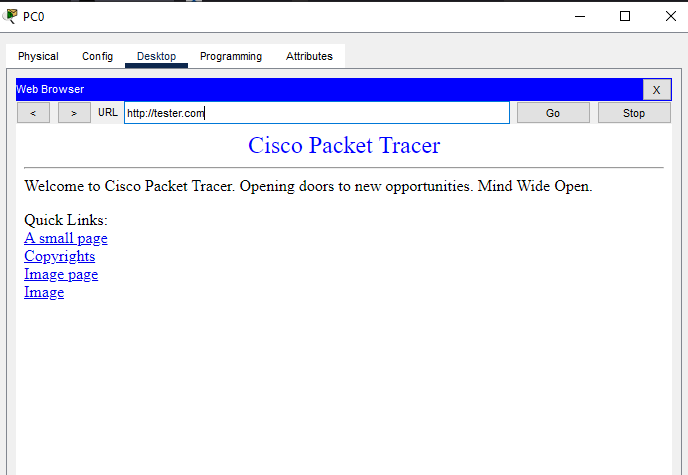


Untuk Allow Ip Traffic silahkan inputkan protocol IP untuk action nya Allow. Selanjutnya untuk Remote IP masih sama yaitu 0.0.0.0 dan Remote Wildcard Mask 255.255.255.255

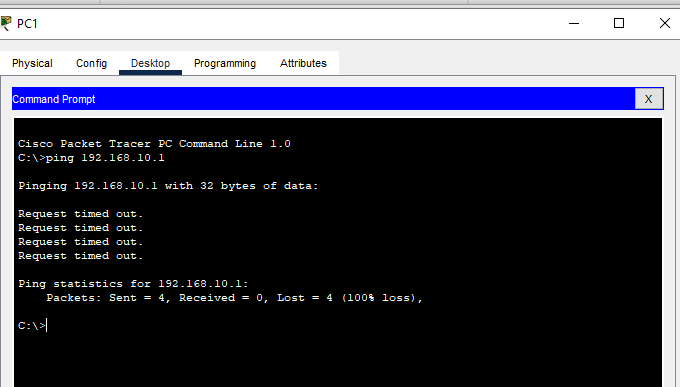


Selanjutnya untuk verifikasi konfigurasi.

Buka PC0 lalu pilih Desktop 🡪 Browser selanjutnya inputkan tester.com jika halaman terbuka berarti untuk port http aksesnya allow



Selanjutnya untuk konfirmasi blok ping floodnya silahkan masuk ke salah satu PC lalu pilih Desktop 🡪Command Prompt selanjutnya perintahkan ping 192.168.10.1 (Dimana ini Adalah IP Server). Jika mengalami Request Timed Out Berarti konfigurasi sukses



**Teori Keamanan Firewall pada Cisco ASA**

*Firewall* atau disebut juga dengan tembok api dapat melindungi dan juga mengantur informasi, data atau apapun kegiatan dalam jejaring internet pada sebuah komputer atau mencegah segala kemungkinan akses pada jaringan pribadi. *Firewall* biasanya dianalogikan seperti dinding pembatas untuk membatasi akses ke dalam suatu sistem. Pada artikel ini kita akan membahas *firewall* secara mendalam yaitu dengan topik *firewall* pada Cisco ASA.

Cisco Adaptive Security Appliance (ASA) merupakan perangkat keamanan jaringan tingkat lanjut yang mengintegrasikan *firewall stateful*, VPN, dan kemampuan lainnya. ASA digunakan untuk membuat *firewall* dan melindungi jaringan internal perusahaan dari penyusup eksternal dengan mengizinkan *host* internal mengakses Internet.

Berikut adalah gambar perangkat Firewall buatan Cisco corp:



Perangkat fisik Cisco ASA dan Cisco ASA pada Cisco Packet Tracer

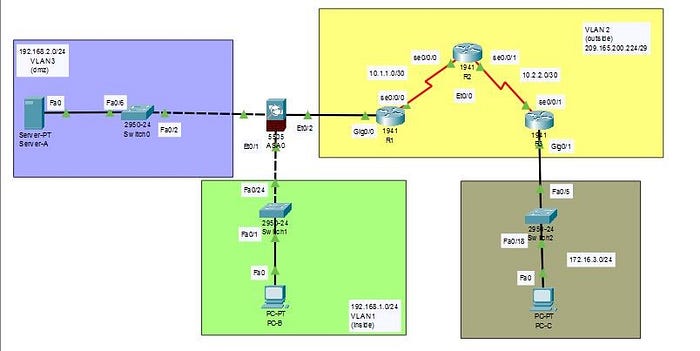
ASA menciptakan tiga antarmuka keamanan yaitu Luar, Dalam, dan DMZ. Hal ini memberi pengguna luar akses terbatas ke DMZ dan tidak ada akses ke sumber daya internal. Pengguna dalam dapat mengakses DMZ dan sumber daya luar. Metode yang digunakan pada artikel ini yaitu Command Line Interface (CLI).

**Simulasi dan Konfigurasi Cisco ASA menggunakan Cisco Packet Tracer**

Pada simulasi ini kami akan melakukan konfigurasi keamanan *firewall* menggunakan Cisco ASA yang dimana Cisco ASA ini juga terdapat beberapa konfigurasi yang dapat kita masukkan untuk memperkuat keamanan dari Cisco ASA tersebut.

**1. Desain Model Jaringan**

Press enter or click to view image in full size



Desain topologi jaringan simulasi

Berdasarkan gambar desain jaringan diatas, maka perangkat yang dibutuhkan adalah:

* 1 buah Cisco ASA

Cisco ASA (Adaptive Security Appliance) merupakan alat keamanan jaringan yang yang menyatukan antara *firewall, antivirus*, dan VPN. Cisco ASA dapat memberhentikan serangan sebelum meluas melalui jaringan dengan memanfaatkan pertahanan ancaman proaktif yang dimilikinya.

* 3 buah Router

*Router* merupakan alat jaringan yang dapat menghubungkan dua atau lebih jaringan. *Router* juga dapat memantau lalu lintas antar jaringan dan menyalurkan paket data ke alamat IP yang dituju. Melalui *router* juga, perangkat pengguna yang lain dapat menghubungkan koneksi internet pada jaringan yang sama.

* 3 buah Switch

*Switch* merupakan perangkat jaringan yang memliki fungsi untuk menghubungkan beberapa perangkat computer yang berbeda dalam sebuah jaringan. Dengan adanya *switch*, pengguna dapat bertukar data maupun informasi ke perangkat yang berbeda.

* 1 buah Server

*Server* adalah suatu sistem yang dapat menyimpan data yang dikrim oleh *client*. Data yang disimpan oleh *server* ini dapat berisikan dokumen atau berbagai informasi lainnya yang dimiliki oleh *client*.

* 2 buah PC

PC atau Personal Computer, sesuai dengan namanya perangkat ini biasa digunakan untuk perorangan atau pribadi. PC berfungsi untuk mengolah, memasukkan dan menghasilkan data maupun informasi berdasarkan arahan dari pengguna. PC biasa digunakan di rumah, sekolah, kantor, toko, dan di beberapa tempat lainnya.

Dan untuk kabel yang digunakan adalah:

* 5 buah kabel Straight-Through

Kabel ini merupakan sebutan untuk kabel yang kedua ujungnya memiliki cara pemasangan yang sama. Kabel ini digunakan untuk menghubungkan antara PC dengan *switch* yang memiliki konektor *up-link*.

* 2 buah kabel Cross-Over

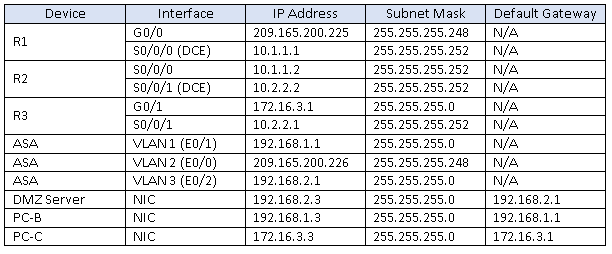
Kabel ini kebalikan dari kabel *Straight-Through*, yakni kedua ujungnya berbeda satu sama lain. Biasanya, kabel ini digunakan untuk menghubungkan perangkat yang serupa.

* 2 buah kabel Serial DCE

Kabel DCE (Data Circuit Equipment) ialah kabel yang berada diantara kabel DTE (Data Terminal Equipment) dan kabel Data Transmisi. DCE berfungsi untuk memberikan sinyal konversi, *coding* dan garis *clocking* yang termasuk kedalam perangkat DTE

**2. Tabel Pengalamatan**

Press enter or click to view image in full size



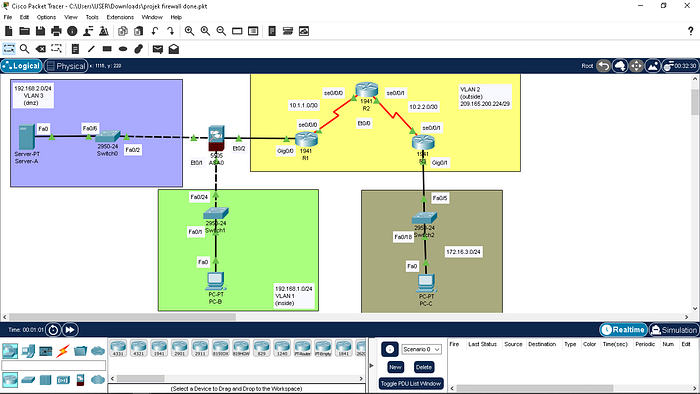
Routing table simulasi

**3. Langkah-langkah Konfigurasi**

Berikut merupakan langkah-langkah dalam konfigurasi simulasi Cisco ASA:

1. Buat Topologi Jaringan

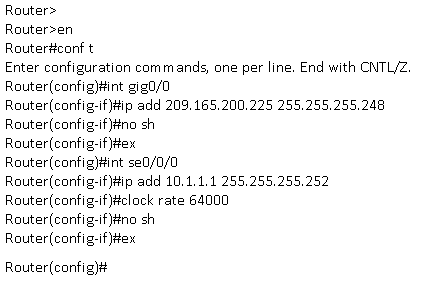
Press enter or click to view image in full size



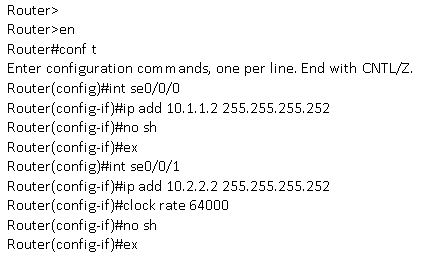
2. Konfigurasi Router dan PC

Sebelum kita mengkonfigurasi di Cisco ASA kita akan mengkonfigurasi router terlebih dahulu dan membuat PC-C bisa terhubung ke masing-masing router dengan cara :

* Memasukkan IP Address Router 1 pada CLI dengan klik Router, kemudian pilih CLI dan masukkan command seperti berikut:

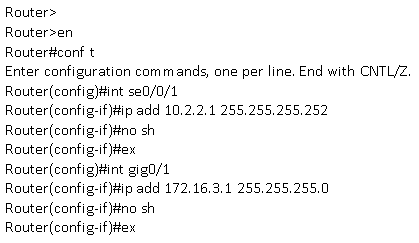


* Masukkan IP Address Router 2 pada CLI dengan klik Router 2, kemudian klik CLI dan masukkan command seperti berikut:



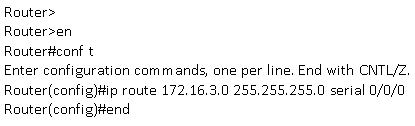
* Masukkan IP Address Router 3 pada CLI, dengan klik Router 3, kemudian klik CLI dan masukkan command berikut:

Press enter or click to view image in full size

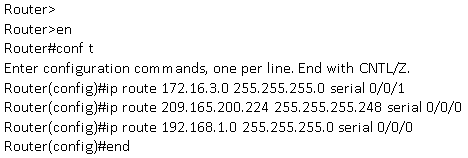


* Selanjutnya konfigurasi IP Route pada router agar router satu dengan yang lainnya dapat terhubung, dengan memasukkan command:

Pada R1:

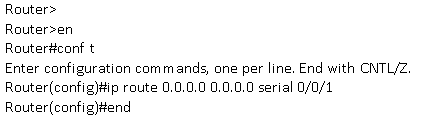


Pada R2:

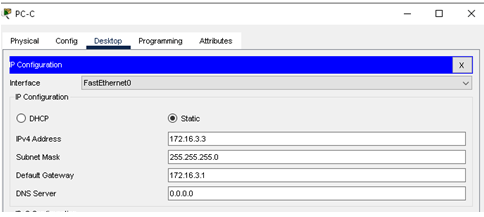


Pada R3:

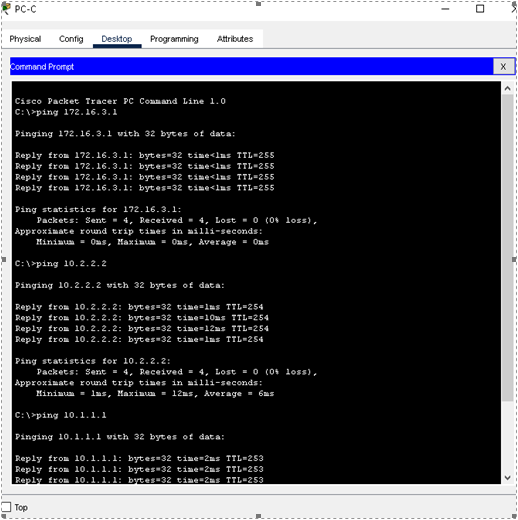
Press enter or click to view image in full size



* Masukkan IP Address PC-C dengan cara klik PC-C, kemudian pilih Desktop, dan klik IP Configuration, dan masukkan IP seperti gambar dibawah:



* Melakukan ping test dari PC-C ke masing-masing router untuk melihat apakah konfigurasi diatas telah berhasil:



Dari hasil ping test PC-C ke router, terlihat bahwa PC-C seling terhubung dengan setiap router.

* Masukkan IP Address pada PC-B dan Server dengan cara klik perangkat, kemudian klik Desktop, dan masukkan command:

PC-B:

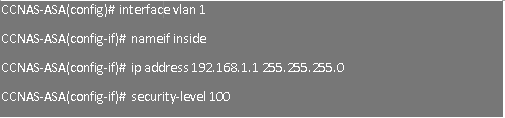


Server:

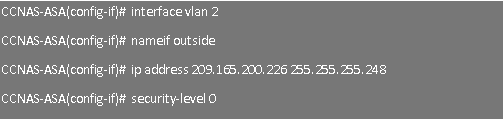


3. Konfigurasi keamanan pada CISCO ASA:

* Disini kita akan mengkonfigurasi interface VLAN 1 (inside) dan VLAN 2 (outside). Untuk interface VLAN 1 (inside 192.168.1.0/24) dan kita atur tingkat keamanan ke pengaturan tertinggi yaitu 100.

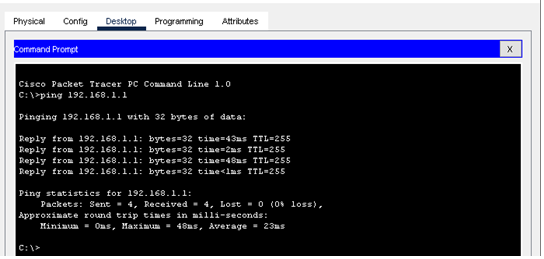


* Selanjutnya untuk interface VLAN 2 (outside 209.165.200.224/29),kita atur tingkat keamanan ke pengaturan terendah yaitu 0.



Untuk Konfigurasi VLAN 1 (inside) dapat diartikan bahwa cakupan VLAN 1 adalah jaringan Privat. Dan VLAN 2 (outside) adalah jaringan Publik.

* Lakukan ping test dari PC-B ke ASA:



Berdasarkan gambar diatas, test ping dari PC-B ke Asa(Vlan1) berhasil.

**Get Alysa Salsabila’s stories in your inbox**

Join Medium for free to get updates from this writer.

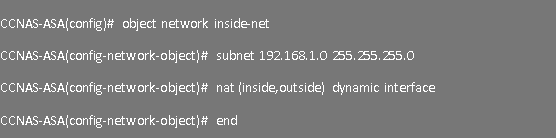
4. Konfigurasi routing, address translation, dan inspection police menggunakan CLI

* Konfigurasikan routing pada jaringan outside ASA (Et0/2) agar ASA menjangkau jaringan Router dan PC-C dengan memasukkan perintah :



* Konfigurasikan terjemahan alamat menggunakan PAT dan objek jaringan

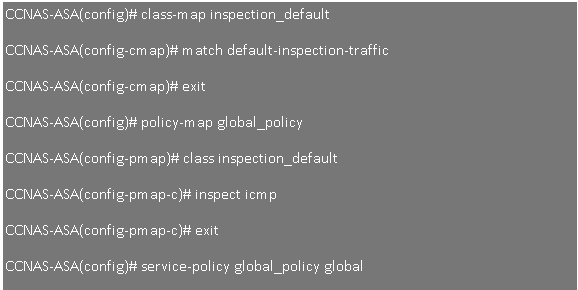
Buat objek jaringan di dalam net dan tetapkan atributnya menggunakan perintah **subnet** dan **nat** .



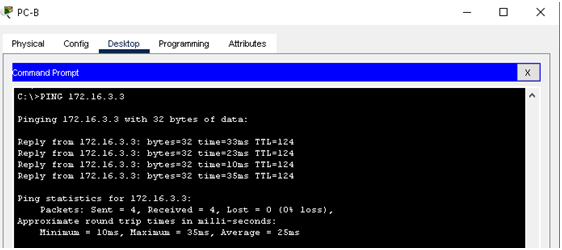
* Ubah kebijakan layanan global inspeksi aplikasi MPF default

Perangkat Packet Tracer ASA tidak memiliki peta kebijakan MPF ​​secara default. Sebagai modifikasi, kita dapat membuat peta kebijakan default yang akan melakukan pemeriksaan lalu lintas luar-dalam. Ketika dikonfigurasi dengan benar, hanya lalu lintas yang dimulai dari dalam yang diizinkan masuk kembali ke antarmuka luar. Anda perlu menambahkan ICMP ke daftar inspeksi.

Buat class-map, policy-map, dan service-policy. Tambahkan pemeriksaan lalu lintas ICMP ke daftar peta kebijakan menggunakan perintah berikut:



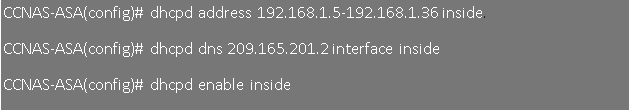
Dari konfigurasi ini PC-B akan bisa terhubung ke VLAN 2 (outside) untuk membuktikan kita bisa lakukan ping test dari PC-B ke PC-C



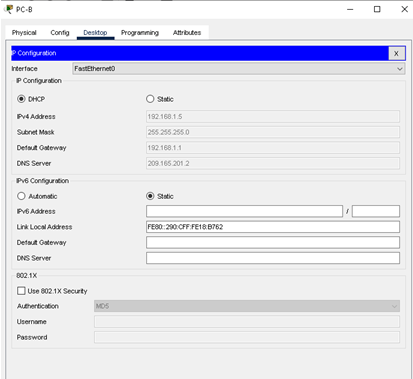
5. Konfigurasi DHCP, AAA, dan SSH

* Konfigurasi ASA Sebagai server DHCP

Pada percobaan ini kita juga dapat mengkonfigurasi ASA sebagai server DHCP dengan cara:



* Konfigurasi ubah PC-B dari alamat IP Static ke client DHCP:

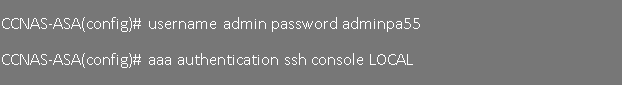


IP DHCP yang didapat yaitu:

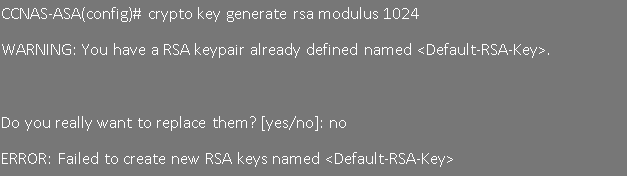


* Konfigurasikan AAA untuk menggunakan database lokal untuk otentikasi

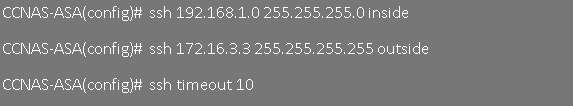
Tentukan pengguna lokal bernama **admin** dengan memasukkan perintah nama pengguna. Tentukan kata sandi **adminpa55** . Sehingga jaringan dalam dan luar jika ingin mengakses ASA dari jarak jauh harus memasukkan User dan password.



* Konfigurasikan akses jarak jauh ke ASA. Ketika langkah konfigurasi diatas selesai, kita telah membuat user dan password. Jika terdapat user jaringan dalam dan luar yang mengakses ASA, langkah selanjutnya ASA dapat dikonfigurasi untuk menerima koneksi dari satu host atau berbagai host di dalam atau di luar jaringan. Pada langkah ini, host dari jaringan luar hanya dapat menggunakan SSH untuk berkomunikasi dengan ASA. Sesi SSH dapat digunakan untuk mengakses ASA dari jaringan dalam.

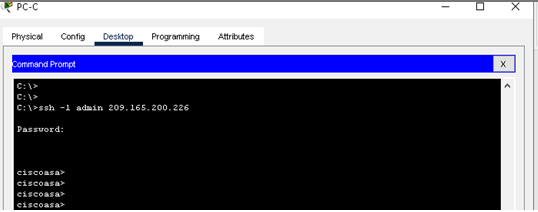


* Konfigurasikan ASA untuk mengizinkan koneksi SSH dari host manapun di jaringan dalam (192.168.1.0/24) dan dari host manajemen jarak jauh di kantor cabang (172.16.3.3) di jaringan luar. Atur batas waktu SSH ke 10 menit (standarnya adalah 5 menit), sehingga akses yang diberikan asa untuk remote jarak jauh adalah 10 menit.



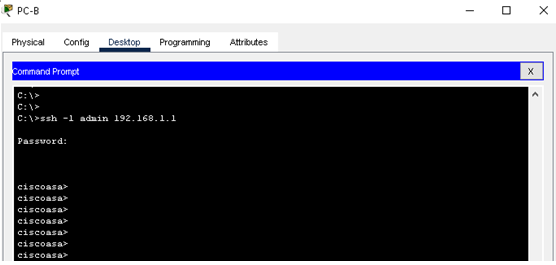
* Periksa SSH dari PC-C ke ASA (209.165.200.226)





* Periksa SSH dari PC-B ke ASA (192.168.1.1)





6. Konfigurasikan DMZ, NAT Static, dan ACL

R1 G0/0 dan interface outside ASA masing-masing sudah menggunakan 209.165.200.225 dan .226. Anda akan menggunakan alamat publik 209.165.200.227 dan NAT statis untuk menyediakan akses terjemahan alamat ke server.

* Konfigurasikan interface DMZ VLAN 3 pada ASA

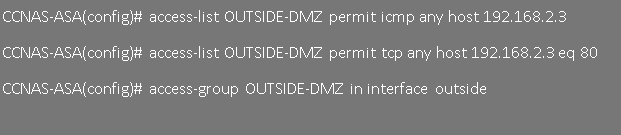
Konfigurasikan DMZ VLAN 3, di mana server web akses publik berada. Tetapkan alamat IP 192.168.2.1/24, beri nama **dmz** , dan tetapkan tingkat keamanan 70. Karena server tidak perlu memulai komunikasi dengan pengguna dalam, nonaktifkan penerusan ke interface VLAN 1.



* Konfigurasikan NAT Static ke server DMZ menggunakan objek jaringan



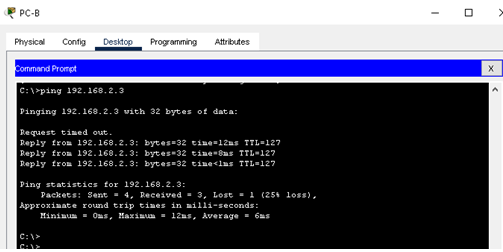
* Konfigurasikan ACL untuk mengizinkan akses ke server DMZ dari internet



**Dari langkah konfigurasi NAT dan ACL diatas kita membuat keamanan pada web server agar tidak dapat di jangkau oleh ip publik dengan menggunakan keamanan firewall Cisco ASA.**

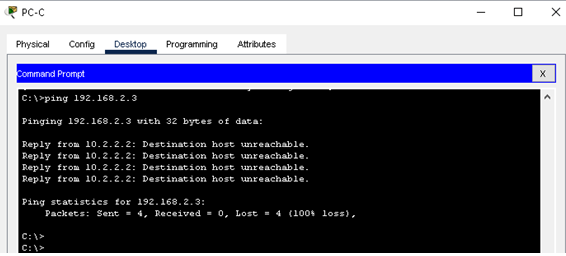
**4. Hasil Test Ping**

* Melakukan uji ping test dari PC-B ( inside) Ke server



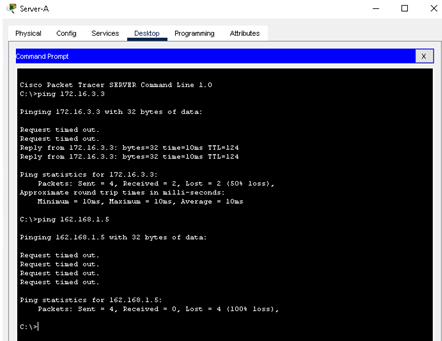
Ping test dari PC-B (inside) ke server, terhubung.

* Melakukan uji ping test dari PC-C ( Outside) Ke server



Ping test dari PC-C (Outside) ke server, tidak terhubung.

* Melakukan uji ping test dari server DMZ ke PC-B dan PC-C



Hasil ping test dari server ke PC-C, berhasil

Hasil ping test dari server ke PC-B, tidak berhasil

**5. Hasil Analisis**

Pada topologi yang kami buat terdapat beberapa tingkat keamanan Cisco ASA. Pada vlan 1 diberikan keamanan 100 yang dimana server dan jaringan outside vlan 2 tidak dapat terhubung ke vlan 1, karena disini vlan 1 kami tetapkan sebagai jaringan privat perusahaan. Dan pada vlan 2 kami berikan tingkat keamanan rendah yaitu 0, karena jaringan tersebut adalah jaringan publik sehingga perangkat dalam maupun server dapat terhubung kesana. Untuk jaringan server dmz kami berikan keamanan 70, disini server dapat diakses oleh jaringan privat (VLAN 1) dan tidak dapat diakses oleh jaringan publik (VLAN 2) yaitu PC-C. Disini juga kami memberikan akses jarak jauh ke Cisco ASA agar perangkat dalam maupun luar dapat me-*remote* ASA dari jarak jauh walaupun begitu, saat melakukan akses jarak jauh client harus mengetahui user dan password dari konfigurasi yang sudah dibuat agar dapat mengakses asa dari jarak jauh.

Sehingga dapat disimpulkan untuk keamanan firewall menggunakan cisco asa PC-B ( jaringan inside) dapat mengakses server, sedangkan PC-C (jaringan outside tidak dapat terhubung keserver karena diblock oleh cisco asa).