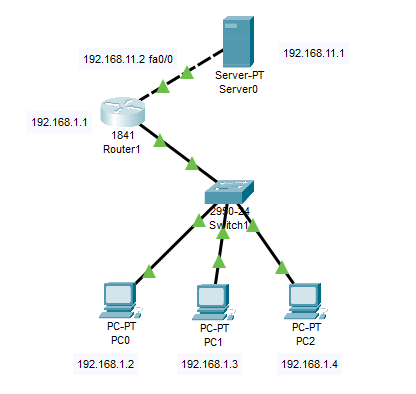
Firewall Cisco Packet Tracer

***1. Praktikum Firewall Dokumentasi Simulasi Firewall Sederhana dengan ACL di Cisco Packet Tracer***

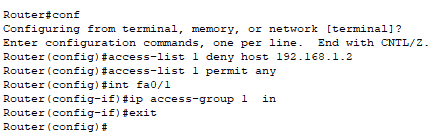
Menerapkan **firewall sederhana menggunakan Access Control List (ACL)** untuk memblokir akses dari satu host (PC0) ke jaringan server, sementara host lain tetap diizinkan.



Konfigurasi Firewall (Standard ACL) Dikerjakan pada Router:

|  |
| --- |
| **enable** |
| **configure terminal** |
|  |
| **access-list 1 deny host 192.168.1.2** |
| **access-list 1 permit any** |
|  |
| **interface fa0/1** |
| **ip access-group 1 in** |

Bukti pengerjaan

****

Tabel Hasil

|  |  |
| --- | --- |
| Uji Coba | Hasil |
| Ping dari PC0 Ke server | Gagal ❌ |
| Ping dari PC1 ke Server | ✅ Berhasil |
| Ping dari PC2 ke Server | ✅ Berhasil |

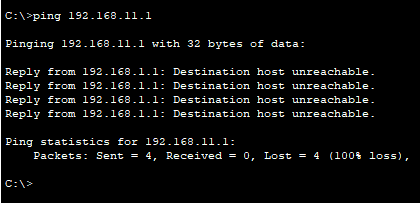


Figure . Ping dari PC0 KE SERVER GAGAL

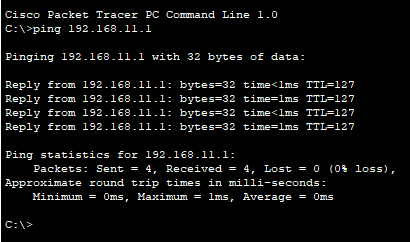


Figure . Dari PC1 Ke server berhasil

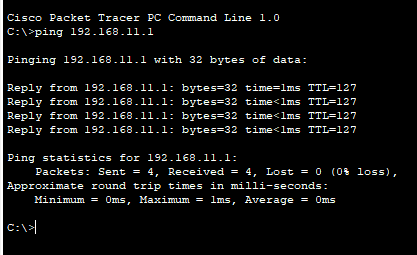
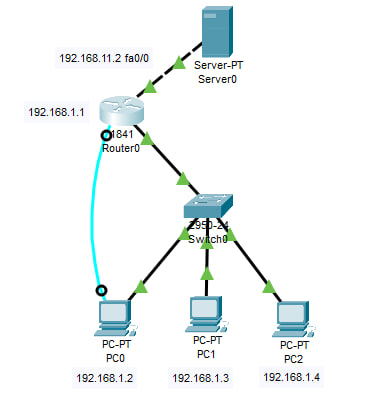


Figure . Dari PC2 ke server Berhasil

2. Konfigurasi SSH & Firewall ACL Extended di Cisco Router

Mensimulasikan koneksi remote aman menggunakan SSH pada router Cisco,  serta menerapkan kontrol akses menggunakan ACL Extended untuk membatasi IP  yang diizinkan melakukan SSH.



Konfigurasi:

1. Aktifkan SSH Pada router

|  |
| --- |
| **hostname R1** |
| **ip domain-name cisco.local** |
| **crypto key generate rsa** |
| **# Masukkan modulus 1024** |
|  |
| **username admin password 1234** |
|  |
| **line vty 0 4** |
| **login local** |
| **transport input ssh** |
|  |
| **enable password cisco** |

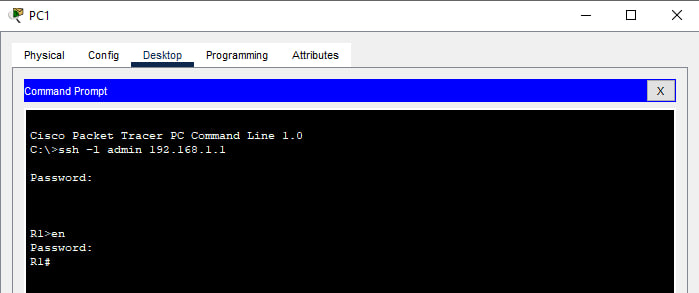
2.  Konfigurasi Firewall (ACL Extended)

|  |
| --- |
| **access-list 110 permit tcp host 192.168.1.3 host 192.168.1.1 eq 22** |
| **access-list 110 deny tcp any host 192.168.1.1 eq 22** |
| **access-list 110 deny tcp any host 192.168.1.1 eq 22** |
| **access-list 110 permit ip any any** |
| **#** Pasang ACL pada interface masuk (fa0/0) **interface fa0/0** |
| **ip access-group 110 in** |

Pengujian

|  |  |  |
| --- | --- | --- |
| device | Perintah SSH | Hasil |
| PC1 | ssh -l admin 192.168.1.1 | ✅ Berhasil login |
| PC0 | ssh -l admin 192.168.1.1 | ❌ Ditolak (ACL) |
| PC2 | ssh -l admin 192.168.1.1 | ❌ Ditolak (ACL) |

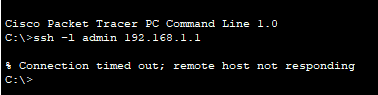
Pc 1 berhasil login



Ditolak

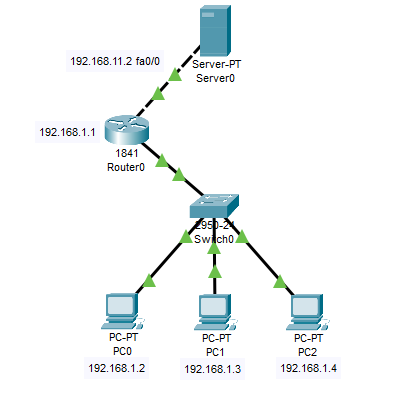


Ditolakkk



3.  Cisco Firewall HTTP ACL – Praktikum Dasar Cybersecurity

Membuat aturan firewall berbasis ACL untuk mengizinkan hanya \*\*PC1\*\* mengakses Web Server melalui port \*\*HTTP (80)\*\*, sementara \*\*PC0 dan PC2 diblokir\*\*.



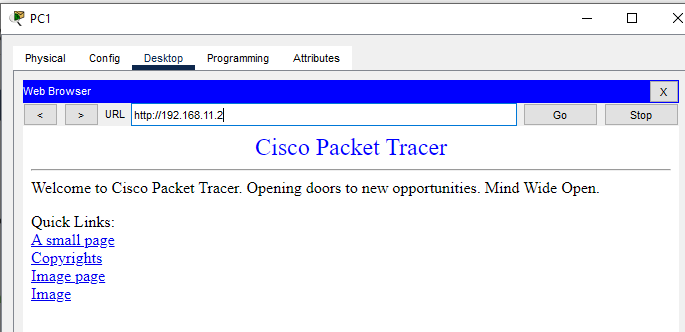
Konfigurasi ACL di Router

|  |
| --- |
| access-list 110 permit tcp host 192.168.1.3 host 192.168.11.2 eq 80 |
| access-list 110 deny tcp any host 192.168.11.2 eq 80 |
| access-list 110 permit ip any any |
| interface fa0/1 |
| ip access-group 110 in |

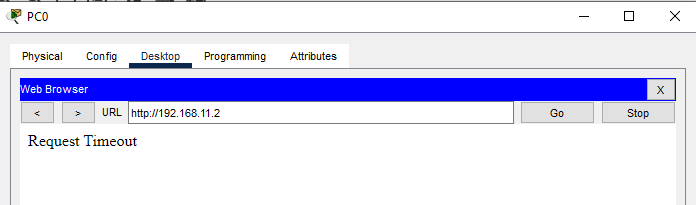
Pengujian

|  |  |
| --- | --- |
| PC | Hasil Akses HTTP |
| PC1 | ✅ Sukses (diperbolehkan) |
| PC0 | ❌ Gagal (Diblokir) |
| PC2 | ❌ Gagal (Diblokir) |

PC1



PC0



PC2

