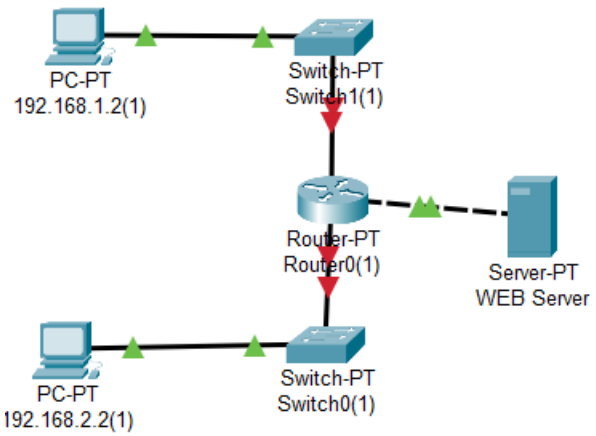
Jobsheet + Pengujian – Materi 6: Monitoring & Security

Kode Unit: J.611000.015.02
Durasi: 1,5 jam

Tujuan

1. Mengelola akun & hak akses perangkat jaringan.
2. Mengimplementasikan ACL untuk filtering lalu lintas.
3. Menjelaskan peran firewall & antivirus.
4. Menerapkan enkripsi dasar (SSH, VPN, HTTPS).
5. Memahami SLA & audit log.

Langkah Praktikum



1. Manajemen Akun & SSH

a. Buat akun admin dengan privilege 15.
b. Buat akun user dengan privilege 1.
c. Konfigurasi agar login via SSH.

Contoh perintah:
Switch(config)# username admin privilege 15 secret C1sc0!
Switch(config)# username user privilege 1 secret Usr123
Switch(config)# ip domain-name lab.local
Switch(config)# crypto key generate rsa
Switch(config)# line vty 0 4
Switch(config-line)# login local
Switch(config-line)# transport input ssh

Pengujian:

1. Tes Login via SSH dengan Admin (Privilege 15)

- ✓ Dari PC1 yang ada di jaringan sama dengan switch, buka Command Prompt:
  ssh -l admin 192.168.1.1
- ✓ Masukkan password: `C1sc0!`
- ✓ **Expected Result:**
  - Bisa login ke switch/router.
  - Prompt berubah menjadi **privileged EXEC mode (#)** → `Switch#`.
  - Bisa masuk ke mode konfigurasi global: `Switch(config)#`

2. Tes Login via SSH dengan User (Privilege 1)
   - ✓ Dari PC, jalankan:
     ssh -l user 192.168.1.1

   - ✓ Masukkan password: `Usr123`
   - ✓ Expected Result:
     - Bisa login, tapi hanya masuk ke **user EXEC mode (>)** → `Switch>`.
     - Saat coba `enable`, harus diminta password lagi, karena tidak punya privilege 15.
3. Verifikasi Hanya SSH yang Aktif (Telnet Ditolak)
   - ✓ Dari PC, coba telnet:
     telnet 192.168.1.1
   - ✓ **Expected Result:**
     - Koneksi **ditolak**, karena hanya SSH yang diizinkan (`transport input ssh`).

2. Konfigurasi ACL

Izinkan hanya subnet 192.168.1.0/24 mengakses server 192.168.2.10 (HTTP).

Contoh perintah:
R1(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.10 eq 80
R1(config)# access-list 100 deny ip any any
R1(config)# interface g0/0
R1(config-if)# ip access-group 100 in

Pengujian:

1. Uji dari Client yang Berhak (192.168.1.0/24)

- Dari **PC1 (192.168.1.11)**, coba akses server dengan browser atau command:

```bash
ping 192.168.2.10
telnet 192.168.2.10 80
```

- **Expected Output**:
  - `ping` berhasil.
  - `telnet` port 80 berhasil terhubung → artinya HTTP akses diizinkan.

---

2. Uji dari Client yang Tidak Berhak (Subnet Lain, misalnya 192.168.3.0/24)

- Dari **PC2 (192.168.3.11)**, coba akses server:

```bash
ping 192.168.2.10
telnet 192.168.2.10 80
```

- **Expected Output**:
  - `ping` → gagal (Request timed out).
  - `telnet` → ditolak, tidak bisa konek ke port 80.

3. Verifikasi ACL di Router

Gunakan perintah:

```bash
show access-lists 100
```

Expected Output (contoh):

```sql
Extended IP access list 100
    permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.10 eq www (5 matches)
    deny ip any any (3 matches)
```

- Artinya:
  - `5 matches` → ada 5 koneksi yang **diizinkan**.
  - `3 matches` → ada 3 koneksi yang **ditolak**.

3. Logging

Aktifkan logging pada router/switch:
R1(config)# logging buffered 16384
R1(config)# logging console
R1# show logging

A. Teori

1. Apa perbedaan Standard ACL dan Extended ACL?
2. Mengapa SSH lebih aman dibanding Telnet?
3. Apa fungsi Syslog server dalam monitoring jaringan?
4. Sebutkan 3 parameter umum dalam SLA jaringan.
5. Apa perbedaan privilege level 1 dan 15 di Cisco IOS