

IMPLEMENTASI IDS

Erfin Susanto
Spectrum Indonesia

Tentang Saya

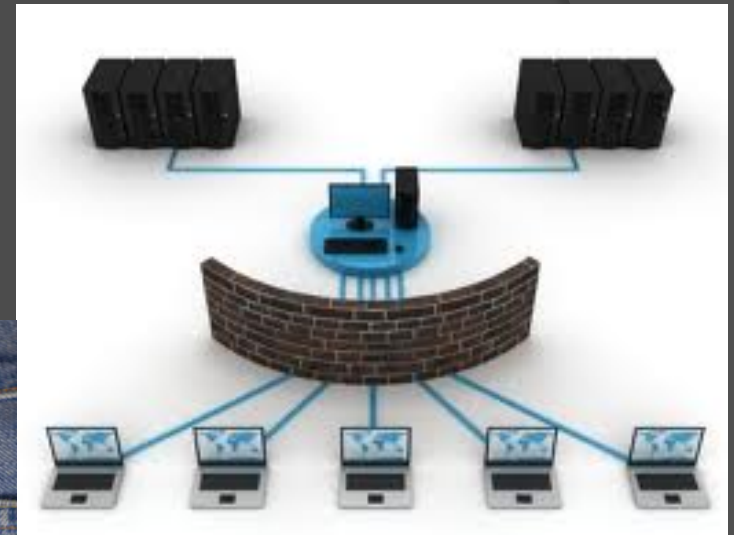
- ⦿ Erfin Susanto
- ⦿ Bekerja di Spectrum Indonesia
 - Technical & Operational Supervisor
- ⦿ MikroTik Certified Trainer
 - MTCTCE – Traffic Control Engineer
 - MTCUME – User Management Engineer
 - MTCWE – Wireless Engineer

Spectrum Indonesia

- ◎ Spectrum Indonesia – 2006
 - D~Net Surabaya divisi Wireless - 2002
- ◎ MikroTik Master Reseller – 2006
- ◎ MikroTik Certified Training Partner – 2007
 - MTCNA, MTCTCE, MTCUME, MTCRE, MTCWE
 - BootCamp Training
 - Combo Training (2 Sertifikat)
 - 5 Trainers with specific skill



Security VS Simplicity



MikroTik RouterOS

- ⦿ Mengubah PC menjadi Router yang tangguh
- ⦿ Router dengan banyak fitur dan performa tinggi tetapi murah
 - Routing (static or dynamic)
 - Firewall
 - VPN dan Tunnel
 - Quality of Service (bandwidth management)
 - Fitur User Management
 - Torch, DHCP, Hotspot, RADIUS, etc

Bagaimana Mikrotik mengamankan Jaringan anda?

- ⦿ Fitur yang ada :
 - HTTPS, SSH dan enripsi koneksi
 - Port Scan Detect
- ⦿ Use custom-made IDS
 - ICMP type limitation
 - Limit connection rates
 - Port Knocking

MikroTik Administration

The screenshot displays the MikroTik WinBox v4.5 interface. On the left, a terminal window titled "Terminal — telnet — 80x24" shows a telnet session with the following output:

```
MMM      MMM      KKK
MMMM     MMMM     KKK
MMM MMMM  MMM  III KKK
MMM MM   MMM  III KKKK
MMM      MMM  III KKK
MMM      MMM  III KKK

MikroTik RouterOS 4.5 (c
may/18/2010 12:56:17 syste
3
7.129.2 via telnet

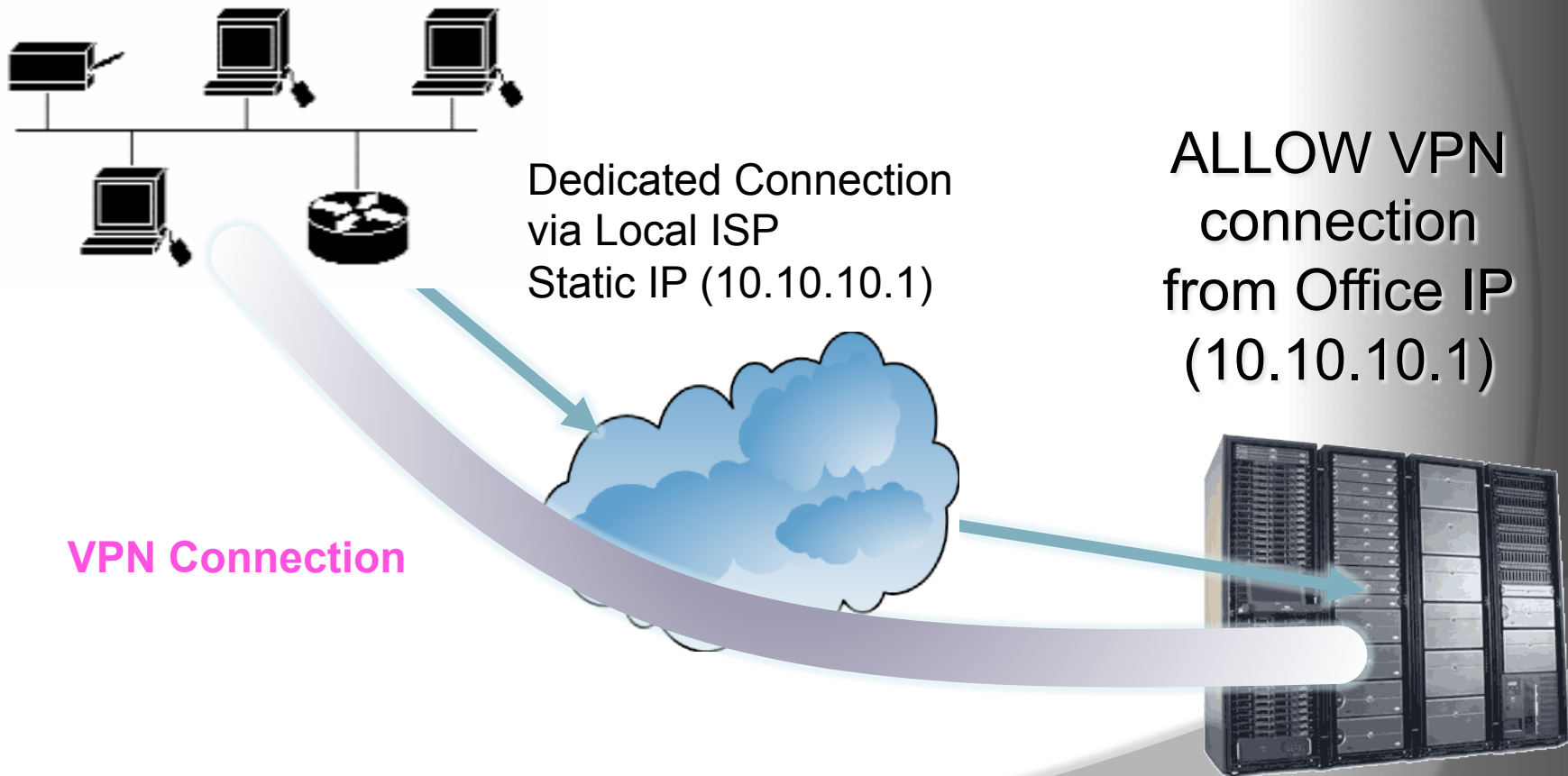
[admin@MikroTik] > ip add
Flags: X - disabled, I - i
# ADDRESS
0 10.37.129.100/24 10
[admin@MikroTik] > int pri
Flags: D - dynamic, X - di
# NAME
0 R ether1
1 R ether2
[admin@MikroTik] >
```

The main WinBox window, titled "admin@10.37.129.100 (MikroTik) - WinBox v4.5 on x86 (x86)", features a sidebar menu with categories like Interfaces, Wireless, Bridge, PPP, Mesh, IP, IPv6, MPLS, VPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, ISDN Channels, Make Supout.rif, and Manual. The "Interface List" window is open, showing a table of interfaces:

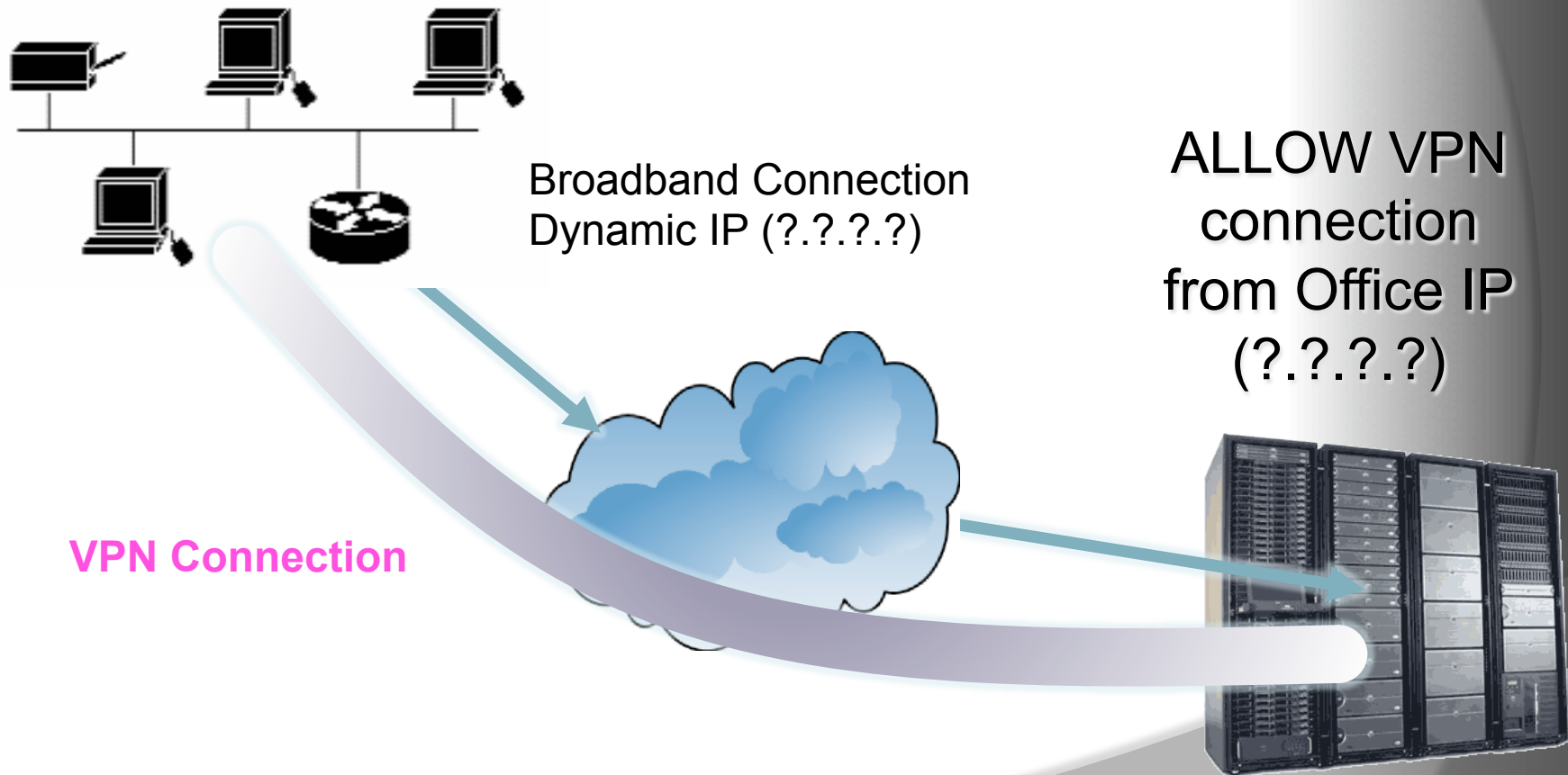
Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN	VRRP	Bonding	
Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops
R ether1	Ethernet		0 bps	0 bps	0	0	0
R ether2	Ethernet		5.6 kbps	1655 bps	1	2	0

Below the interface list, a log window shows system messages, including a critical error: "login failure for user herry from 10.37.129.2 via telnet".

Static IP



Dynamic IP



Port Knocking

- ⦿ Secara default, semua IP dan Port Tertutup
- ⦿ Menggunakan kombinasi Port dan Protocol
- ⦿ Jika Urutanya benar, maka knocker-IP akan diperbolehkan mengakses.
 - Gunakan Proses sebaliknya untuk menutup koneksi
 - Tentukan lama IP boleh mengakses

Port Knocking (ilustrasi)



Port Knocking di MikroTik



1. Kirim koneksi ke TCP-1234

2. Router menyimpan IP yang masuk selama 10 detik

3. Kirim koneksi ke TCP-4321

4. Router akan mengecek apakah IP nya sama dari sebelumnya (TCP-1234)

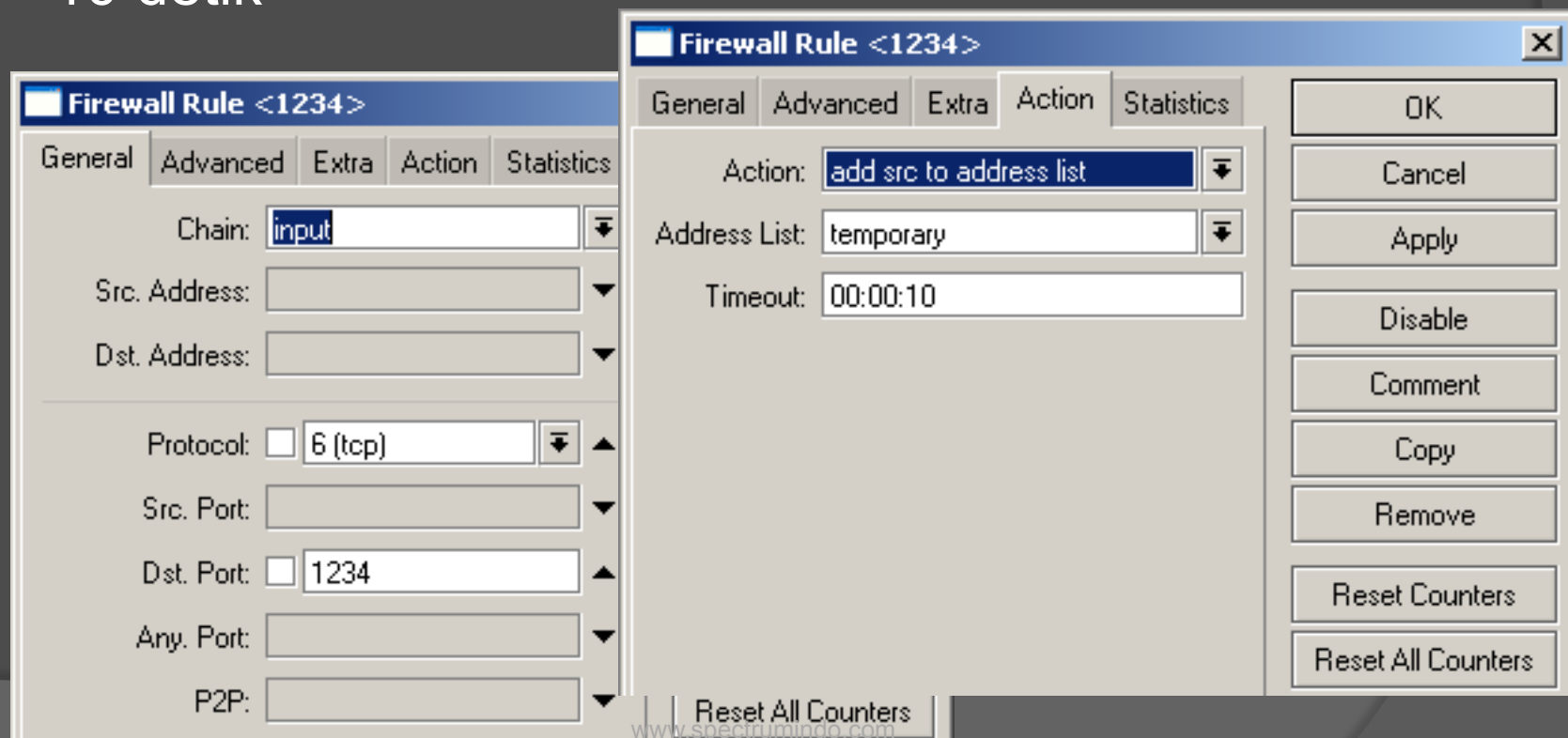
5. Jika Ipnya sama dan waktunya kurang dari 10 detik, maka IP tersebut akan diperbolehkan mengakses Router



Knocking Port
TCP 1234
TCP 4321

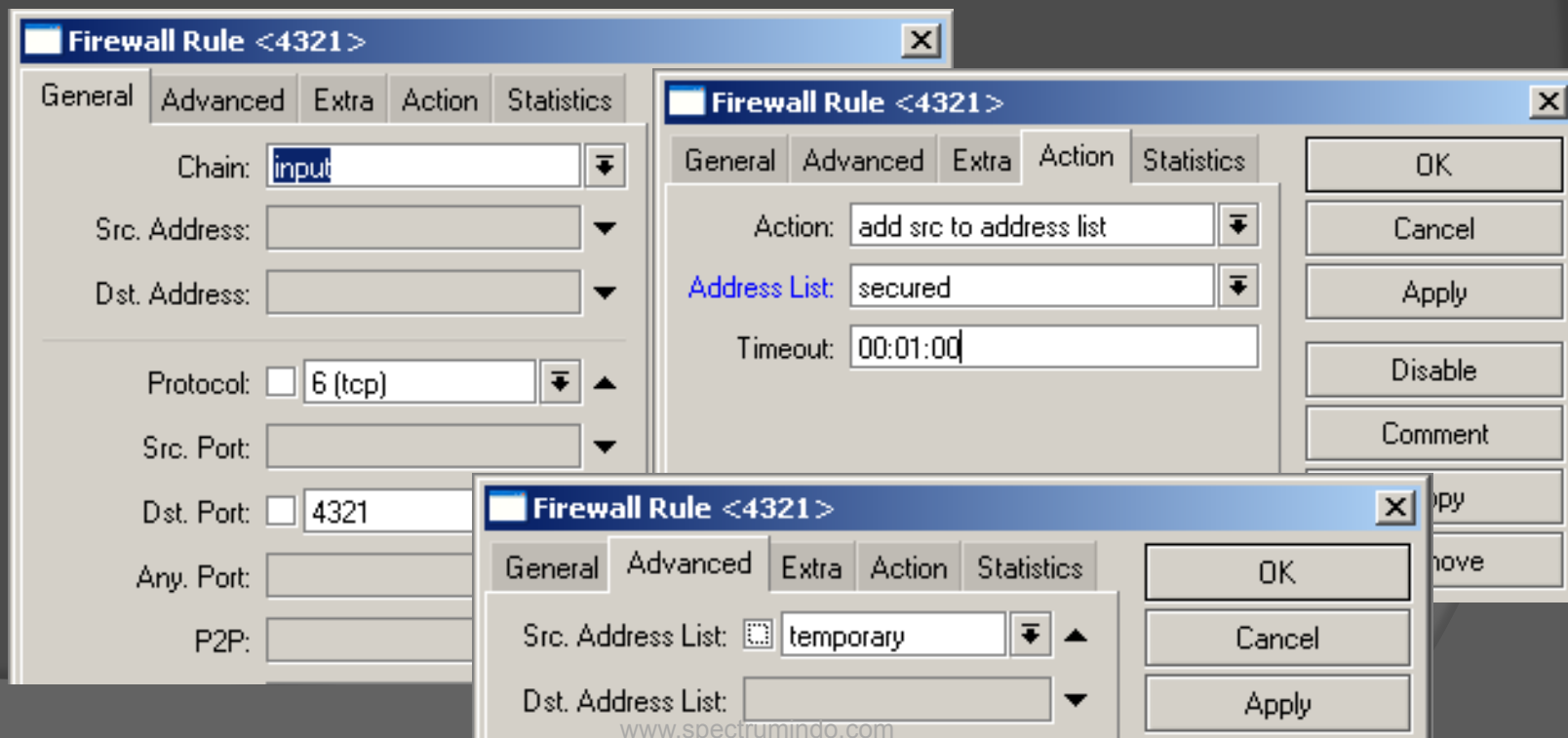
Port Knocking in MikroTik #1

- Buat Rule untuk menangkap permintaan Protocol/ Port dan menyimpan IP peminta kedaftar sementara dengan nama TEMPORARY selama 10 detik



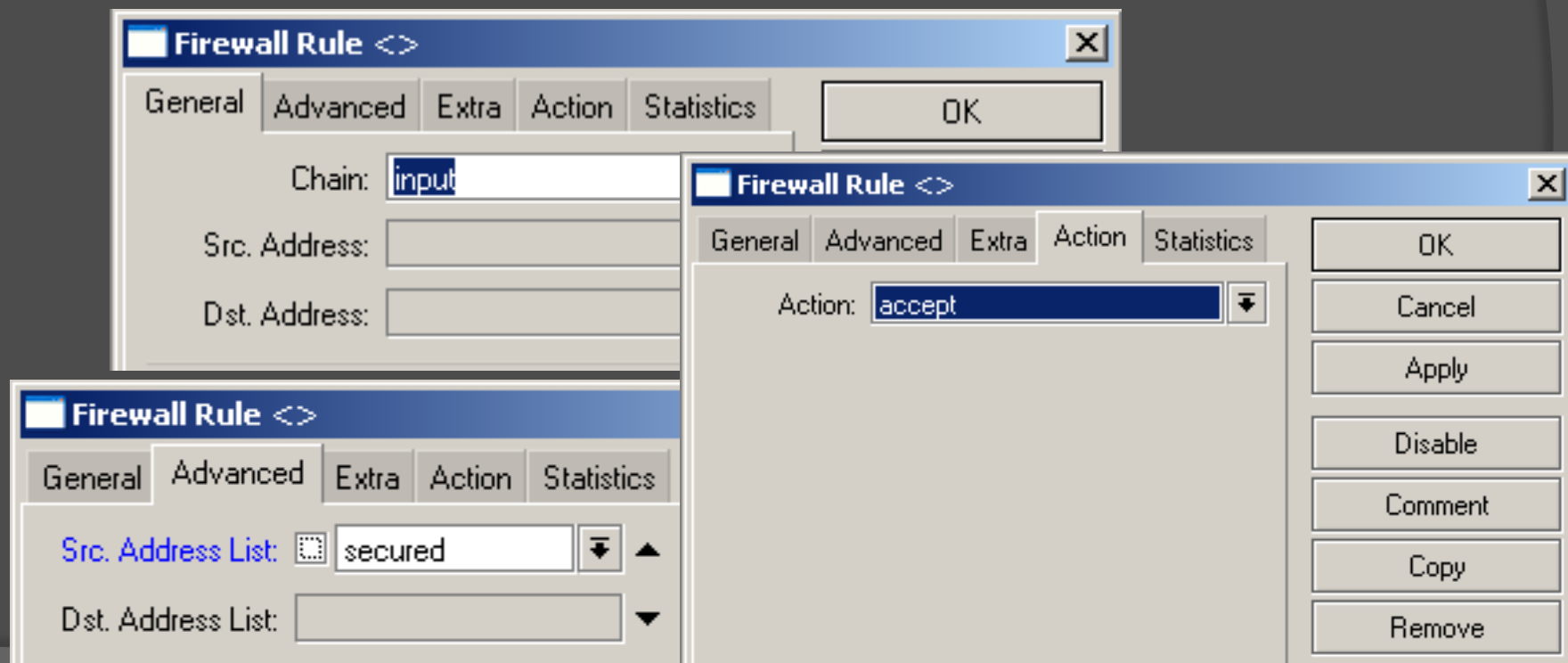
Port Knocking in MikroTik #2

- Tangkap permintaan Protocol/Port kedua dan cek apakah IP peminta sudah ada di TEMPORARY kalau ada masukan IP ke list dengan nama SECURE



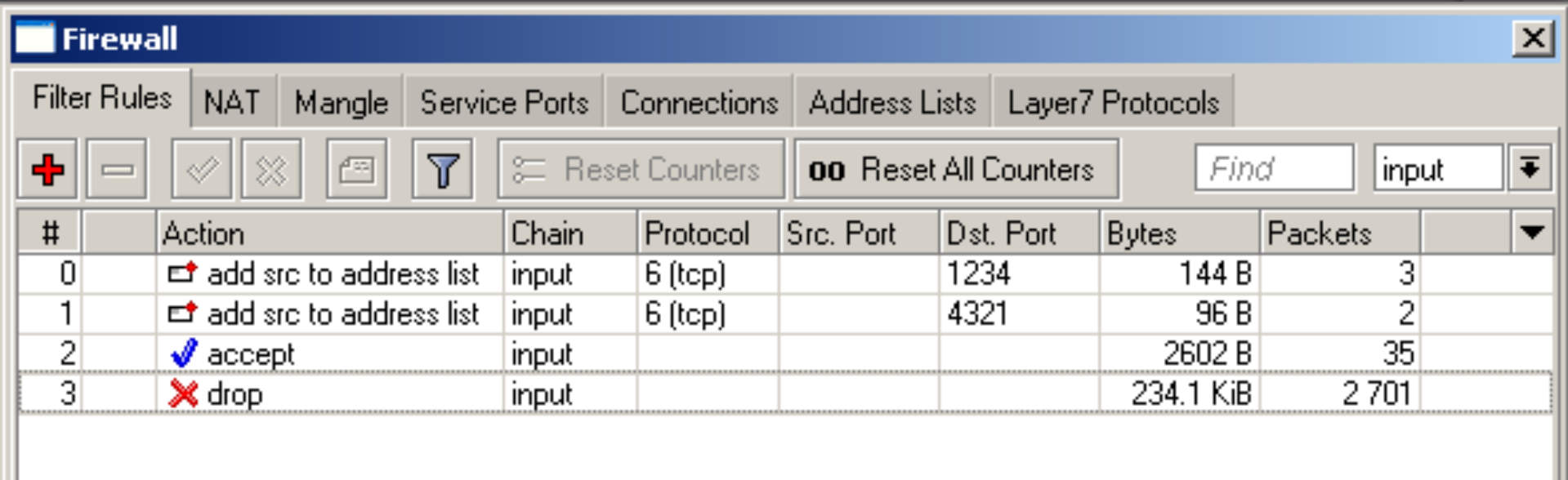
Port Knocking di MikroTik #3

- Mengizinkan IP yang ada di daftar SECURE untuk mengakses Router (atau melakukan hal yang lain)



Port Knocking di MikroTik #4

- Secara default, BLOCK semua koneksi

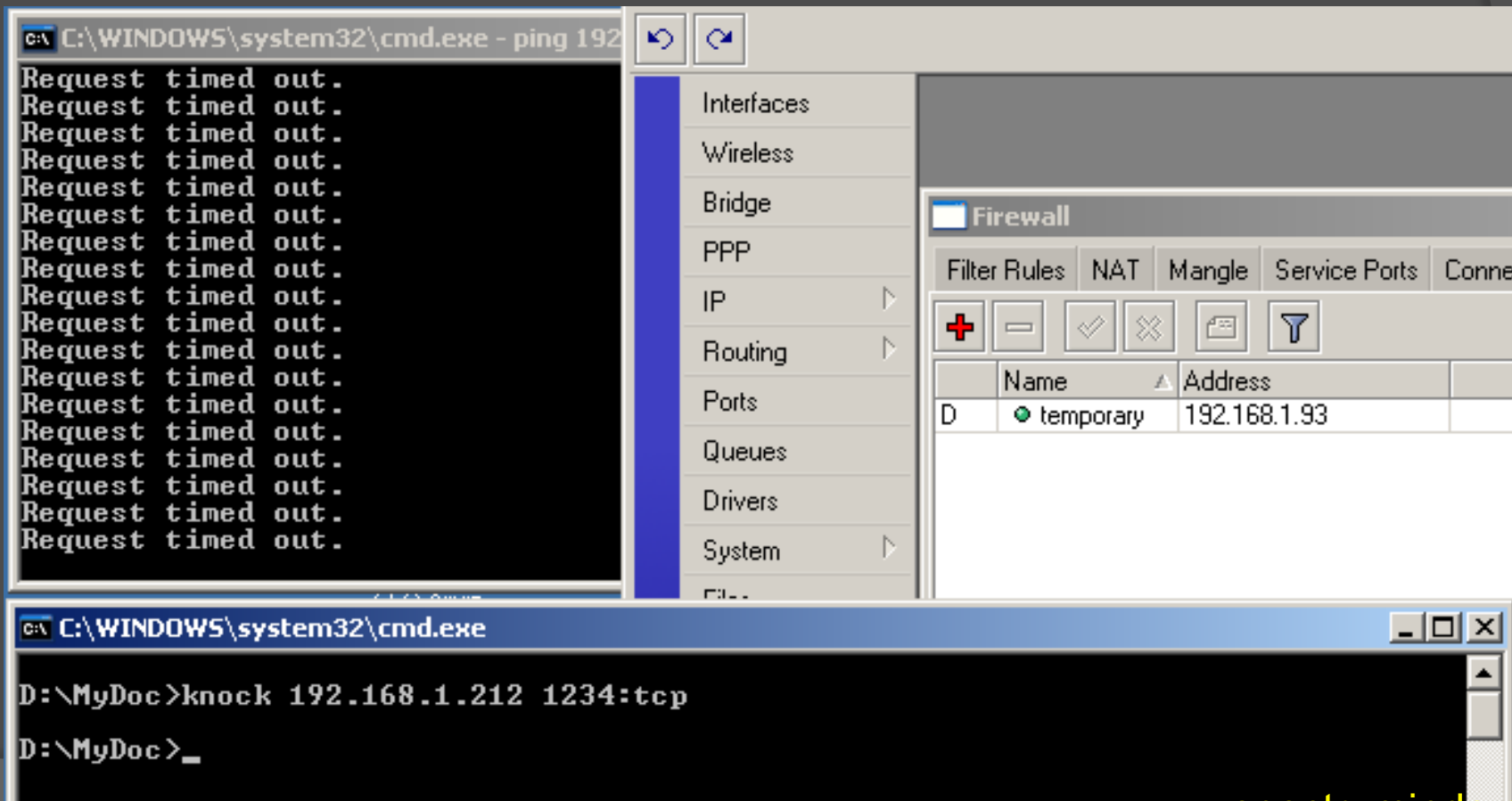


The screenshot shows the MikroTik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is selected. The table below shows the configuration of the 'input' chain. The first three rules are 'add src to address list' and the fourth rule is 'drop'.

#	Action	Chain	Protocol	Src. Port	Dst. Port	Bytes	Packets
0	add src to address list	input	6 (tcp)		1234	144 B	3
1	add src to address list	input	6 (tcp)		4321	96 B	2
2	accept	input				2602 B	35
3	drop	input				234.1 KiB	2 701

Port Knocking di MikroTik

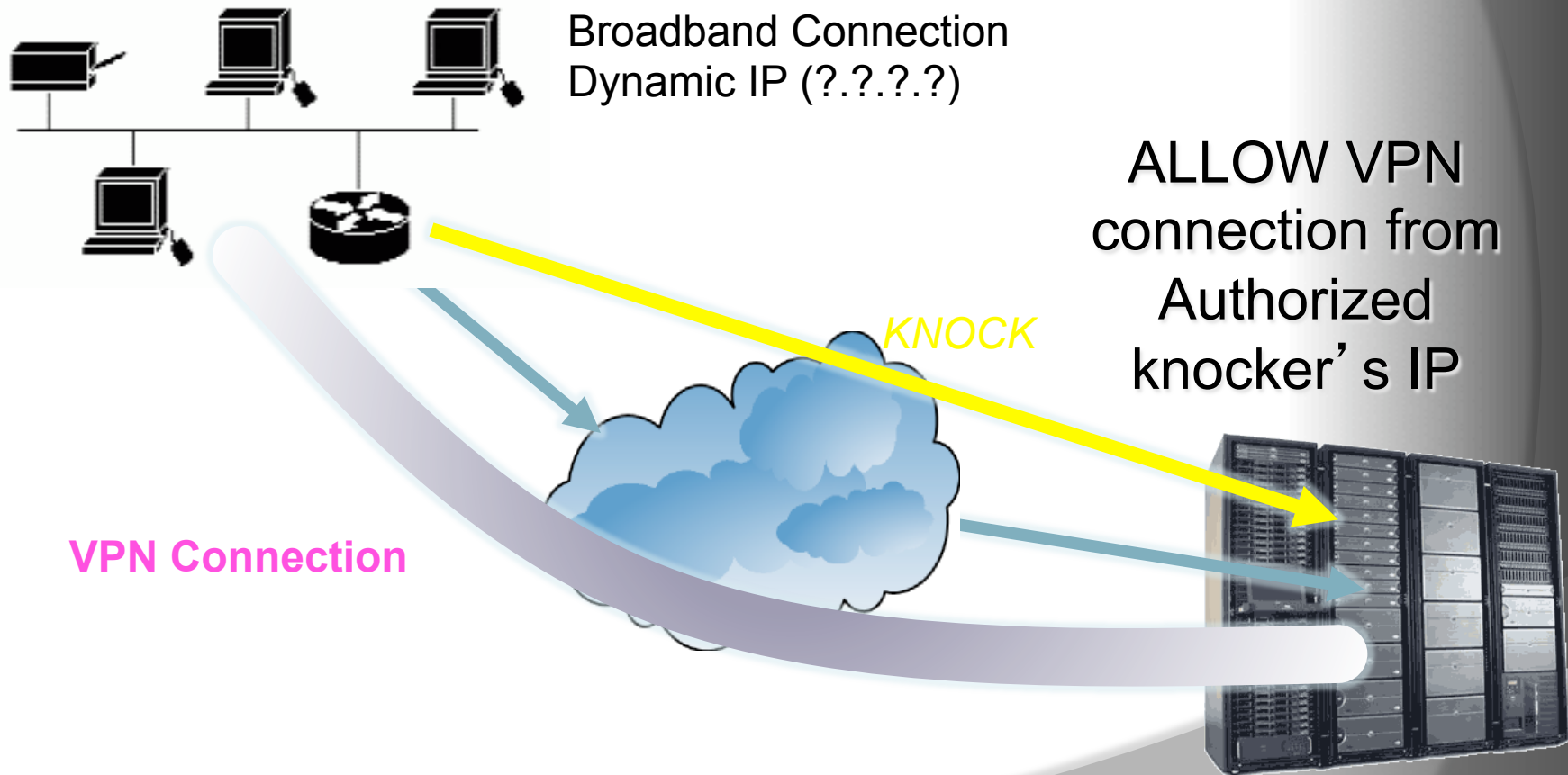
● Cara kerjanya



Port Knocking Implementasi

- ⦿ Filter pertama sebelum Autentikasi
- ⦿ Diikuti oleh enkripsi dari VPN
- ⦿ Optional
 - Spesifikasikan urutan yang berbeda untuk membuka port/service yang tidak sama
 - Berikan urutan kunci yang berbeda untuk tiap orang/IP

Implementasi



TERIMA KASIH

erfin@spectrumindo.com
training@spectrumindo.com