



# RouterOS for Adaptive Security Appliance in Sekolah Tinggi Teknik Surabaya

**Iwan Chandra**  
**Sekolah Tinggi Teknik Surabaya - Indonesia**  
**for MUM Indonesia 2015**



# Tentang Saya

- » Iwan Chandra
- » Alumni Sekolah Tinggi Teknik Surabaya (S.Kom, 2012)
- » Mahasiswa S2-Teknologi Informasi, Sekolah Tinggi Teknik Surabaya (2014 - sekarang)
- » Staff IT dan Tenaga Pengajar di Sekolah Tinggi Teknik Surabaya





# Tentang Saya vs MikroTik

- » Certified for MTCNA, MTCRE, MTCTCE, MTCWE, MTCUME, MTCINE
- » MikroTik Certified Academy Trainer untuk Sekolah Tinggi Teknik Surabaya (Februari 2014 - sekarang)
- » MikroTik Certified Trainer untuk BelajarMikroTik.COM (April 2015 - sekarang)





# Sekolah Tinggi Teknik Surabaya

- » Berdiri tahun 1979
- » Berlokasi di Jl.Ngagel Jaya Tengah 73-77, Surabaya
- » Menyelenggarakan program studi D3, S1, hingga S2:
  - > D3 – Manajemen Informatika dan Komputer
  - > S1 – Teknik Elektro
  - > S1 – Teknik Informatika
  - > S1 – Teknik Industri
  - > S1 – Sistem Informasi
  - > S1 – Desain Komunikasi Visual
  - > S1 – Desain Produk
  - > S2 – Teknologi Informasi
- » Info: “<http://www.stts.edu>”





# BelajarMikroTik.COM

- » Didirikan tahun 2013 oleh Herry Darmawan dan Akbar Azwir
- » Berfokus pada pengajaran, training dan sertifikasi MikroTik (MTCNA, MTCRE, MTCTCE, MTCWE, MTCUME, MTCINE)
- » Info lebih lanjut: <http://www.belajarmikrotik.com>

**Herry Darmawan, Akbar Azwir, Slamet Suharko, Antonius Duty Susilo, Iwan Chandra / BelajarMikroTik.COM**

Rating: ★★★★★ 4.5/5 (836 votes)

Average student result: 64%

**MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE**

Surabaya, Jakarta, Malang, **Indonesia**

Tel: 62 31 60038338

[Write e-mail](#)





# Latar Belakang

- » Jaringan Internet yang “tidak aman”
- » Perangkat jaringan (Router, server, dsb) menjadi rentan terhadap ancaman serangan dari luar
- » Dibutuhkan sebuah mekanisme keamanan jaringan





# Tujuan

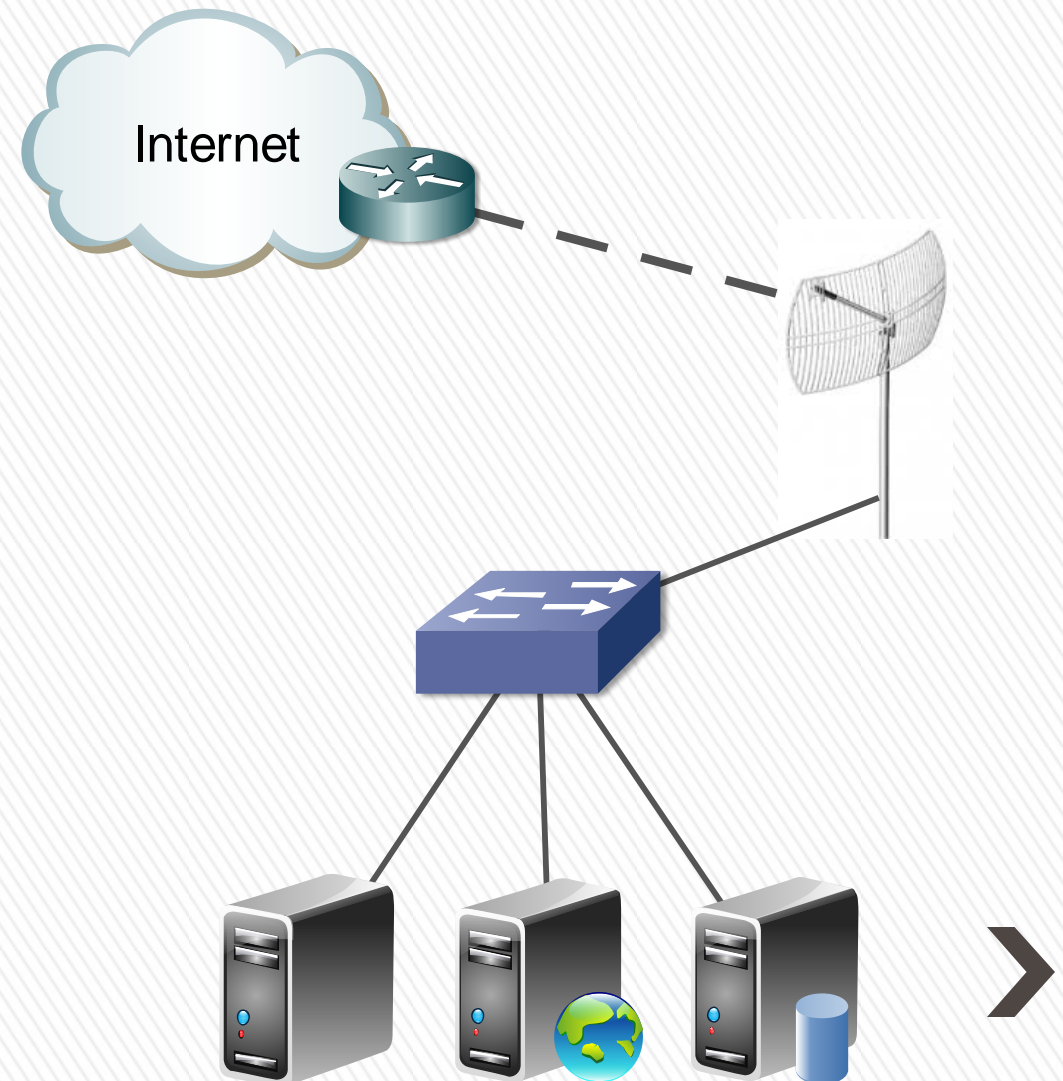
- » Membangun sebuah sistem keamanan dengan konsep Firewall menggunakan Mikrotik RouterOS untuk jaringan public Sekolah Tinggi Teknik Surabaya





# STTS Public Network “before”

- » Jaringan Server STTS terhubung dengan Internet melalui Wireless PTP menuju ISP
- » Dari wireless station, langsung terhubung dengan switch yang terhubung langsung dengan server dan perangkat jaringan lainnya
- » Tidak ada firewall yang bertugas, selain firewall pada masing-masing perangkat jaringan

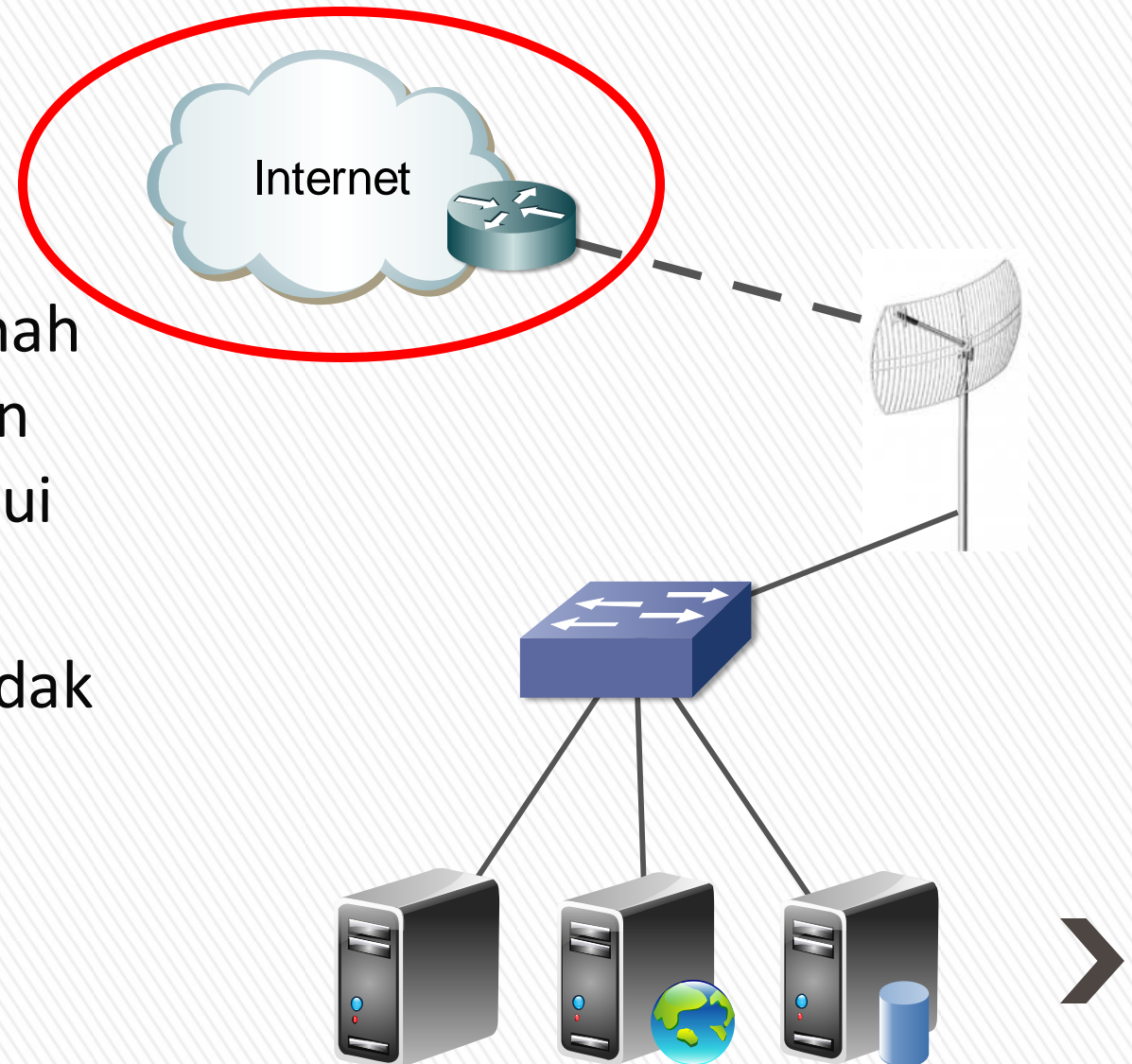






# STTS Public Network “before”

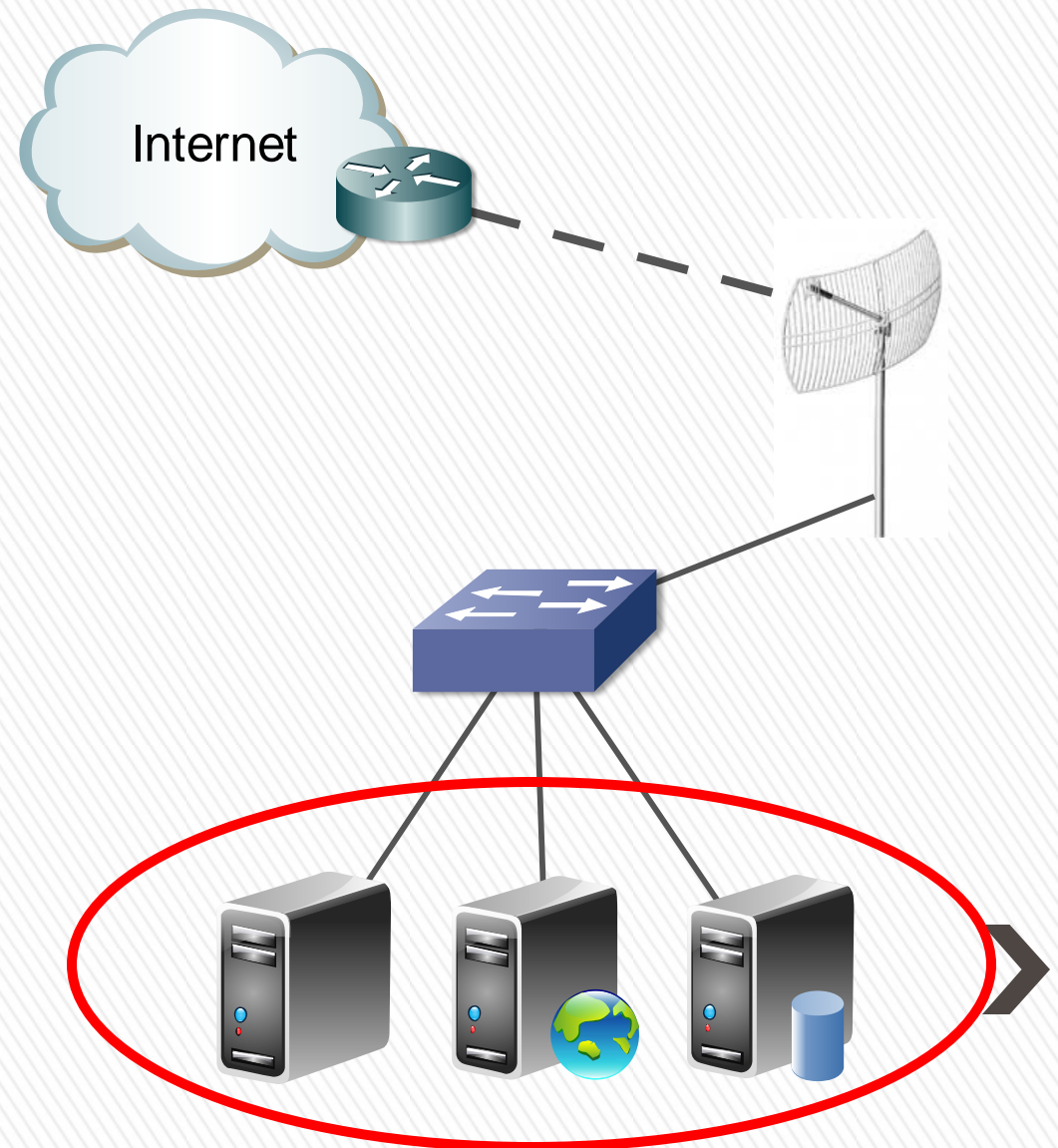
- » Client / Customer tidak pernah tahu apa yang terjadi dengan paket yang dikirimkan melalui Internet
- » Sehingga Internet disebut tidak aman





# STTS Public Network “before”

- » Server dan perangkat Jaringan terhubung langsung dengan jaringan public
- » Sehingga rentan terhadap ancaman serangan jaringan, seperti:
  - > DOS dan DDOS
  - > Ping of Death
  - > dsb





It's normal if you're being attacked,

It's not normal,

when you don't know if you're being attacked,

the attacker is gone,

and you're still didn't aware,

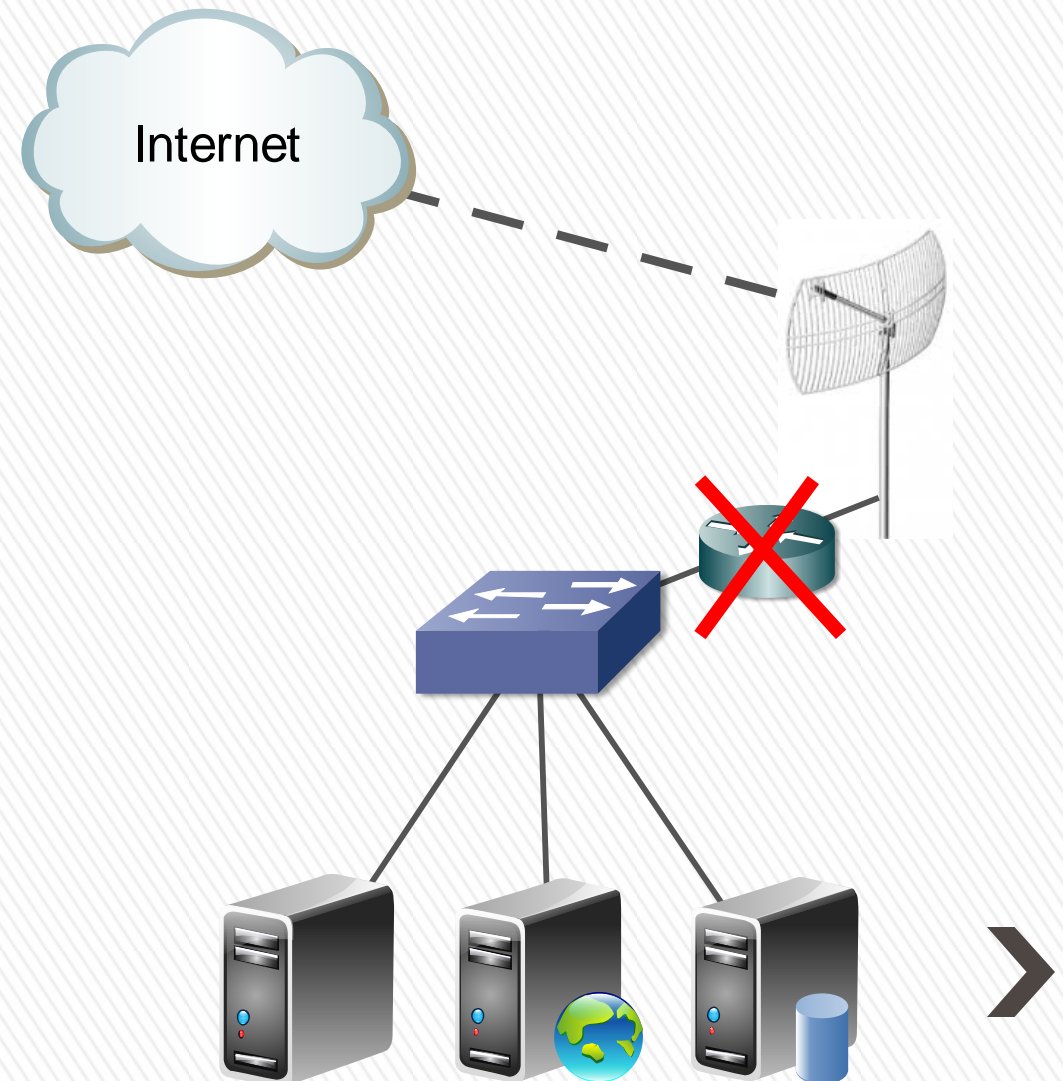
if you've been attacked before.





# Network Security

- » Untuk beberapa alasan, kami tidak dapat menempatkan router sebelum switch
- » Karena nantinya kami akan memiliki dua subnet yang berbeda
- » yang akan memaksa kami menggunakan DST-NAT, sehingga memperlambat access time menuju server





# Network Security

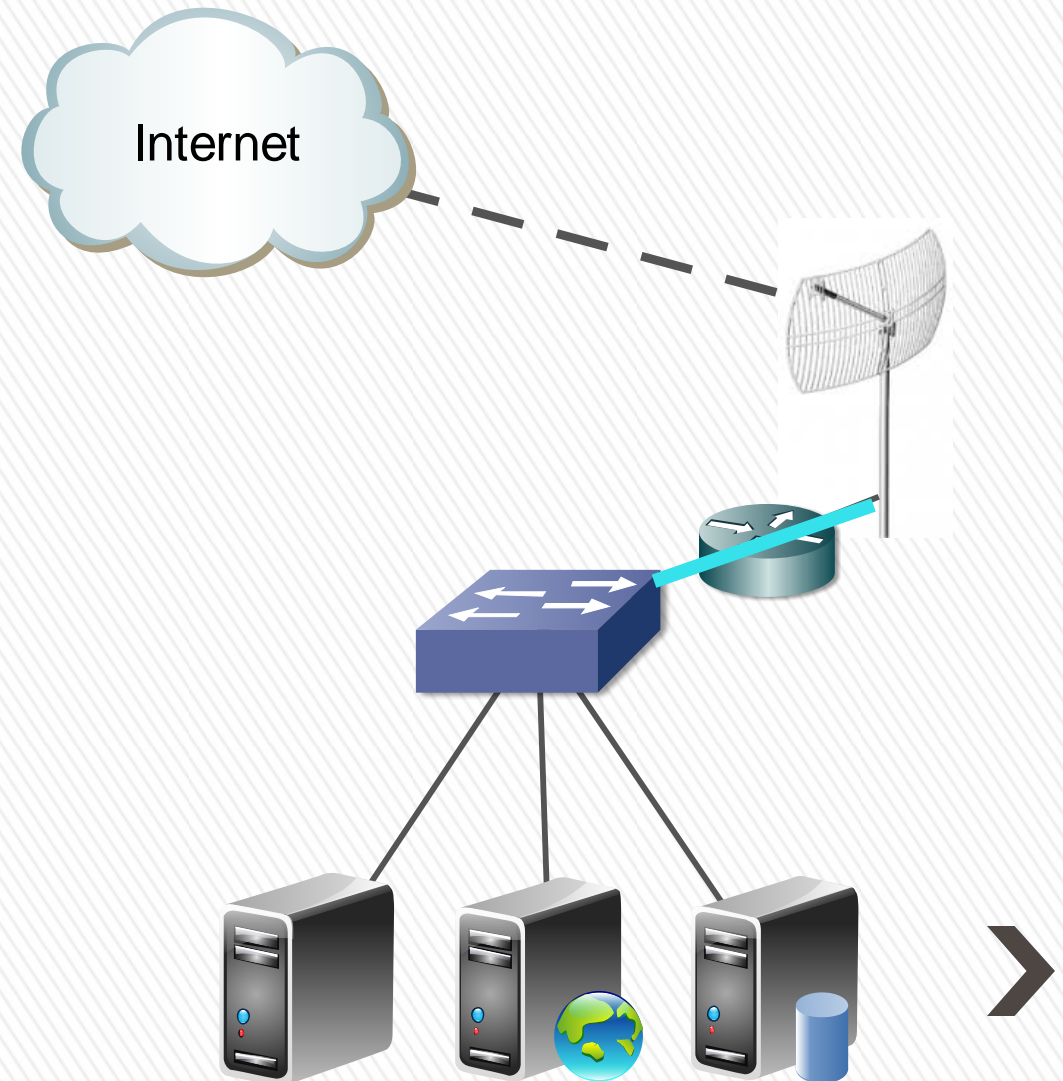
- » Solusinya, kami gunakan sebuah PC berisi RouterOS (x86), dengan 3 Network Interfaces
- » Spesifikasi:
  - > Intel Core 2 Duo 2.4GHz
  - > 2GB Memory
  - > 1GB Disk on Module
  - > 2pcs D-Link Gigabit Ethernet + 1 on Board Gigabit Ethernet
  - > Level 5, RouterOS 6.31





# Network Security

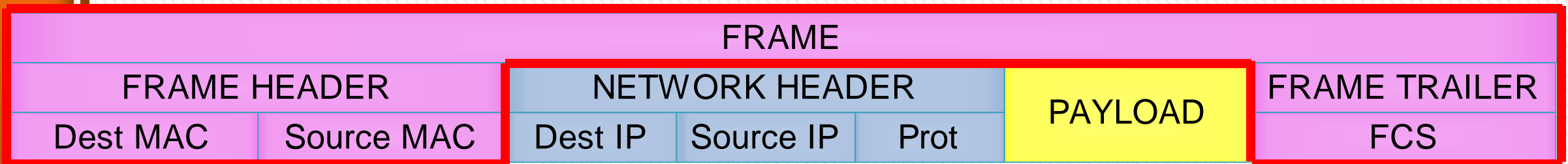
- » Terkait keterbatasan yang sudah dijelaskan sebelumnya, kami membuat bridge di antara 2 interface, sehingga tetap membentuk sebuah broadcast domain





# Adaptive Security Appliance Implementation

- » Fitur RouterOS yang digunakan untuk menerapkan sistem keamanan ini adalah fitur IP Firewall
- » Masalahnya, IP Firewall bekerja pada OSI Layer 3
- » Sedangkan Bridge dan Bridge Firewall pada RouterOS, secara default hanya bekerja hingga OSI Layer 2

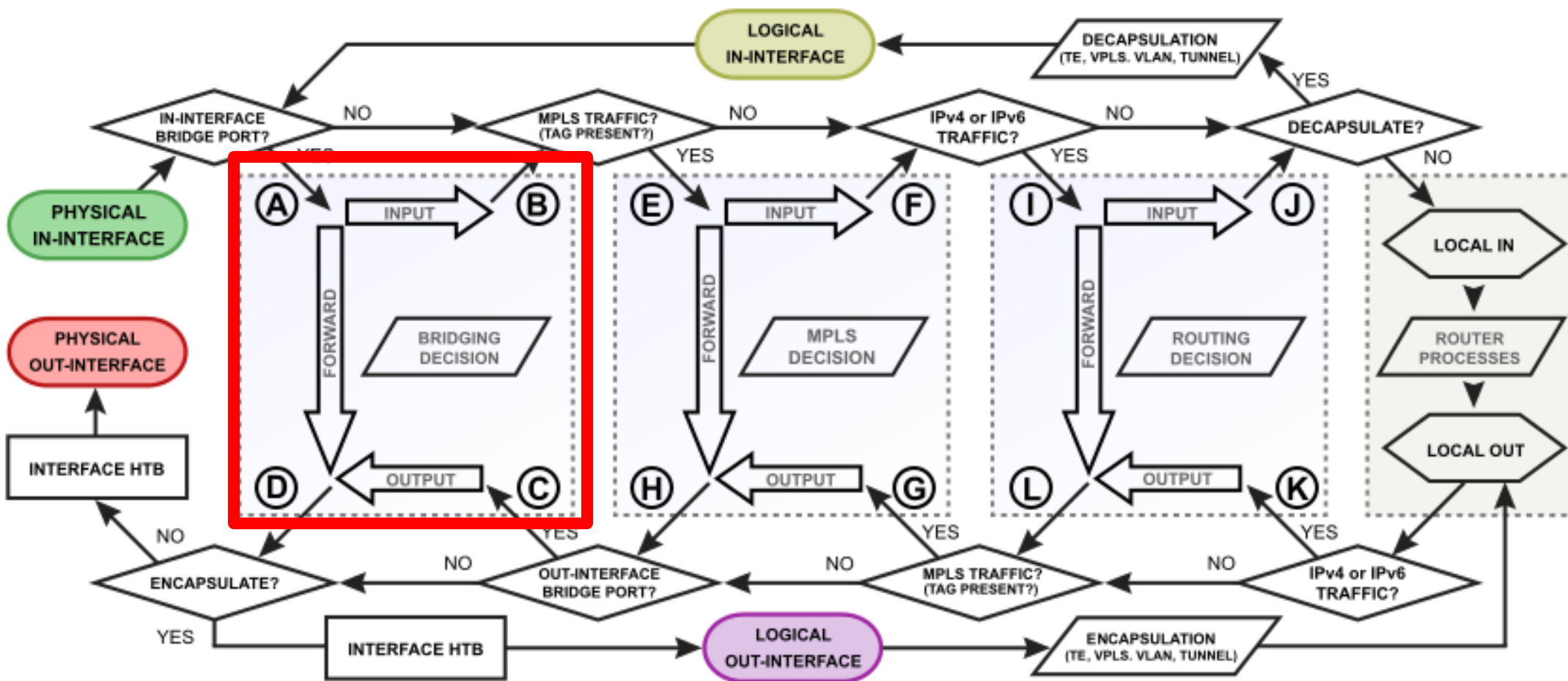


**Bridge hanya akan memproses hingga level frame saja**





# Adaptive Security Appliance Implementation

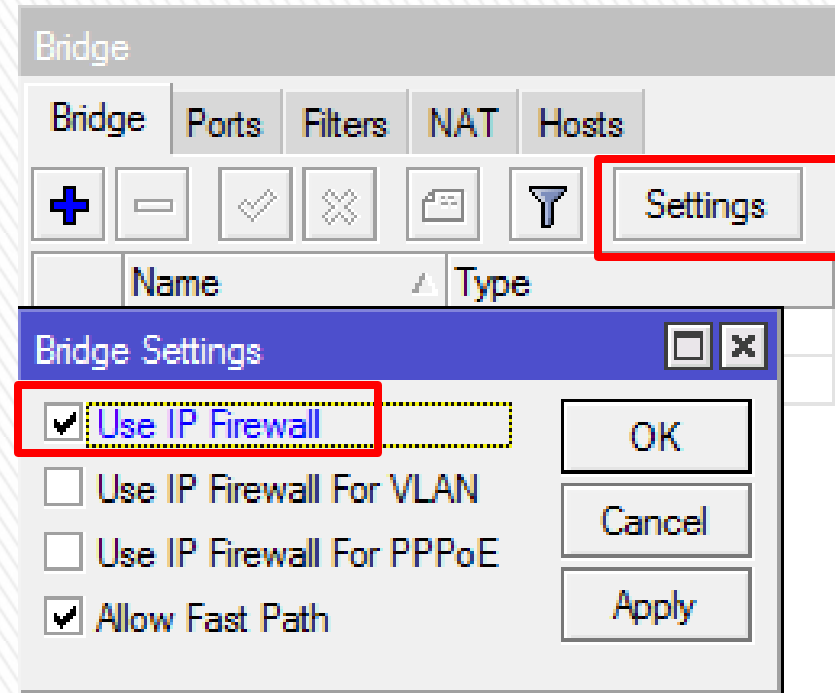






# Adaptive Security Appliance Implementation

- » Kita bisa memaksa bridge untuk membongkar frame yang diterima hingga level packet, dengan mengaktifkan menu “Use IP Firewall” pada Bridge >> Settings



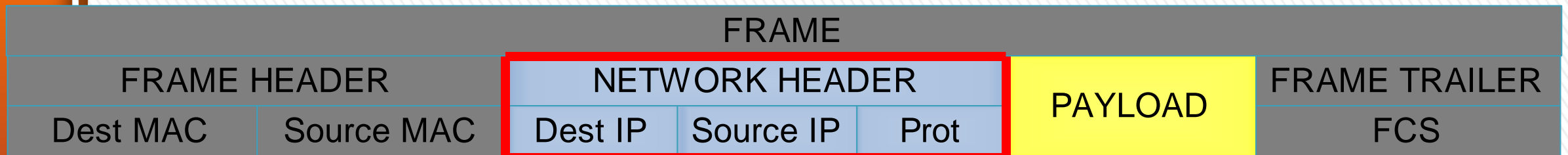
```
/interface bridge settings set use-ip-firewall=yes
```





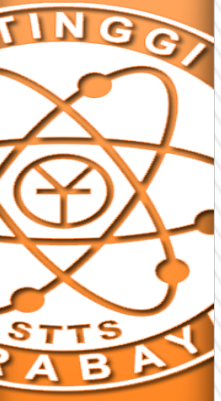
# Adaptive Security Appliance Implementation

- » Dengan demikian, bridge akan membongkar paket hingga network header
- » Sehingga kita dapat mengetahui IP Address, dan Protokol pada sebuah frame



**Opsi “use-ip-firewall” akan memaksa bridge untuk membongkar frame hingga level network**





# Adaptive Security Appliance Implementation

- » Dengan demikian kami dapat melacak connection yang sedang terjadi pada jaringan public yang melibatkan server kami.
- » Dan kemudian membuat firewall rule sesuai dengan policy yang akan diberlakukan.

The screenshot displays the Mikrotik WinBox Firewall interface. The top menu includes Filter Rules, NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocols. The 'Connections' tab is active, showing a list of active connections with columns for Src. Address, Dst. Address, Proto..., Conne..., Timeout, TCP State, and Orig./Repl. Rate. Below this, a smaller window shows the Firewall rule configuration for 'Ping Flood Detector', 'Ping Flood Warning', 'Ping Flood Critical DROP', 'DOS Detector', and 'DOS Handler'. The 'Ping Flood Critical DROP' rule is highlighted, showing it is set to 'drop' action.

	Src. Address	/	Dst. Address	Proto...	Conne...	Timeout	TCP State	Orig./Repl. Rate
C	27.111.34.131:2645		192.168.1.1:80	6 (tcp)		04:36:25	established	0 bps/0 bps
C	36.73.205.81:14925		192.168.1.1:80	6 (tcp)		02:06:58	established	0 bps/0 bps
C	36.73.205.81:14951		192.168.1.1:80	6 (tcp)		02:07:50	established	0 bps/0 bps
C	36.73.205.81:14991		192.168.1.1:80	6 (tcp)		02:10:25	established	0 bps/0 bps
C	36.73.205.81:15011		192.168.1.1:80	6 (tcp)		02:12:21	established	0 bps/0 bps
C	36.79.13.18:33021		192.168.1.1:80					
SA	36.84.69.206:14003		192.168.1.1:80					
SA	36.84.69.206:14005		192.168.1.1:80					
SA	36.84.69.206:14008		192.168.1.1:80					
SA	36.84.69.206:14013		192.168.1.1:80					
SA	36.84.69.206:18321		192.168.1.1:80					
SA	36.84.69.206:18412		192.168.1.1:80					
SA	36.84.69.206:43551		192.168.1.1:80					
SC	36.84.69.206:43553		192.168.1.1:80					
SC	36.84.69.206:43563		192.168.1.1:80					
SA	36.84.69.206:43570		192.168.1.1:80					
SC	36.84.69.206:43587		192.168.1.1:80					
SC	36.84.69.206:43595		192.168.1.1:80					
SA	36.84.69.206:43615		192.168.1.1:80					
SC	36.84.69.206:43619		192.168.1.1:80					
SA	36.84.230.170:50310		192.168.1.1:80					
SA	36.84.230.170:50317		192.168.1.1:80					
SA	36.84.230.170:50344		192.168.1.1:80					

#	Action	Chain	Src. ...	Dst. ...	Proto...
::: Ping Flood Detector					
2	✓ accept	forward			1 (ic...
::: Ping Flood Warning					
3	✓ accept	forward			1 (ic...
::: Ping Flood Critical DROP					
4	✗ drop	forward			1 (ic...
::: DOS Detector					
5	➡ add sr...	forward			6 (tcp)
::: DOS Handler					
6	X tarpit	forward			6 (tcp)



# Adaptive Security Appliance Implementation

Firewall							
Filter Rules							
NAT Mangle Service Ports Connections Ad							
+ - ✓ ✗ [Icon] [Icon] Reset Counters 00							
#	Action	Chain	Src. ...	Dst. ...	Proto...	Src. Po	
::: Ping Flood Detector							
2	✓ accept	forward			1 (ic...		
::: Ping Flood Warning							
3	✓ accept	forward			1 (ic...		
::: Ping Flood Critical DROP							
4	✗ drop	forward			1 (ic...		
::: DOS Detector							
5	➡ add sr...	forward			6 (tcp)		
::: DOS Handler							
6 X	⊗ tarpit	forward			6 (tcp)		

- » Pada IP Firewall rule, digunakan chain forward saja, karena pada topologi tersebut, paket-paket yang menuju ke jaringan kami hanya melewati router saja.
- » Beberapa rule firewall juga ditambahkan pada chain input untuk melindungi router firewall itu sendiri.





# Q & A

Iwan Chandra

- » Mail: [ichan@belajarmikrotik.com](mailto:ichan@belajarmikrotik.com)
- » Mobile: -- ask me after this session --
- » FB: [fb.com/iwan.chandra.14](https://www.facebook.com/iwan.chandra.14)
- » LinkedIn: [id.linkedin.com/in/ichan14](https://www.linkedin.com/in/ichan14)

