

# High Availability IPSec Connection

Herry Darmawan

[BelajarMikroTik.COM](http://BelajarMikroTik.COM)

MikroTik User Meeting 2013, Yogyakarta

# Tentang Saya

Nama : Herry Darmawan

Kesibukan

Trainer di BelajarMikroTik.COM

Consultant Engineer di Duxtel Pty Ltd

Technology Consultant di Harvi Technology

Volunteer di IIX Jawa Timur

Peran dalam bidang MikroTik

Konsultan

Trainer (semua kelas sertifikasi)

Koordinator Akademi (untuk MikroTik Academy Partner Program)

# BelajarMikroTik.COM

Didirikan oleh beberapa Trainer independen

Kami memiliki 4 trainer utama dan 6 co-trainer yang tersebar di berbagai kota

Kami berpartner dengan lebih dari 10 perusahaan di Indonesia, Malaysia, Filipina, dan Australia

Kelas bervariasi mulai dari kelas regular, kelas weekend, kelas bootcamp, dan inhouse

Konsep :

Kelas kecil, intensif, inovatif, tingkat kelulusan tinggi

# Tentang Client

1. Sebuah perusahaan CARGO yang berpusat di Filipina
2. Menggunakan perangkat non-mikrotik untuk mengkoneksikan cabang ke kantor pusat melalui TUNNEL
3. Memiliki 29 cabang di Filipina (Cavite, Alabang, Cebu, dll) dan beberapa cabang di negara lain (Vietnam, Hongkong, Jerman, Guam, China, dll)
4. Alasan beralih ke MikroTik : AFFORDABLE PRICE

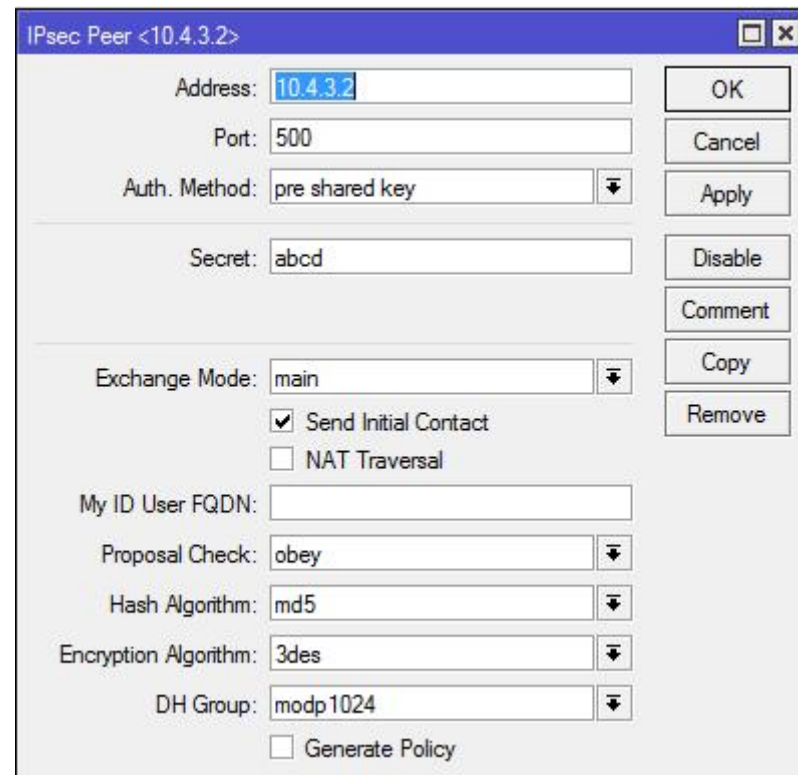
# Kondisi Awal

1. Menggunakan IPSecurity sebagai metode tunnel
2. Terdapat 2 router \*non-mikrotik\* yang terkoneksi ke 2 ISP yang berbeda, setiap cabang terhubung ke salah satu router
3. Semua cabang memiliki IP Publik tapi beberapa menggunakan NAT sebelum mencapai IPSec router
4. Tidak ada backup router (yang alive), sehingga bila ada pergantian router, harus ada downtime

# IPSecurity PEER (\*winbox config)

Peer harus dibuat di kedua router

Konfigurasi PEER ini akan menentukan jenis enkripsi dan otentikasi dari koneksi antar-router dalam IPSecurity

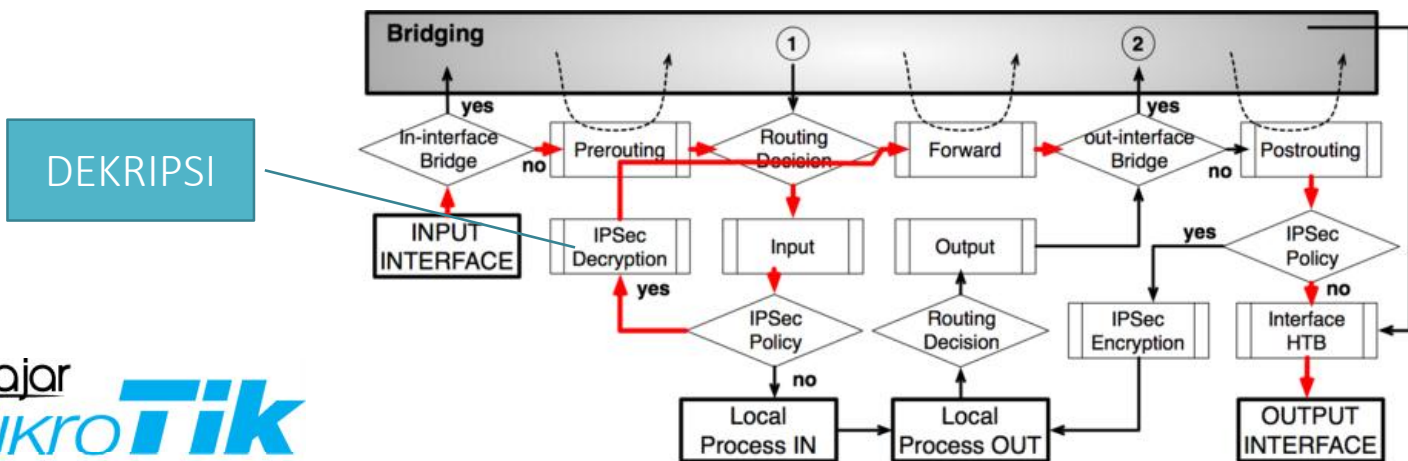
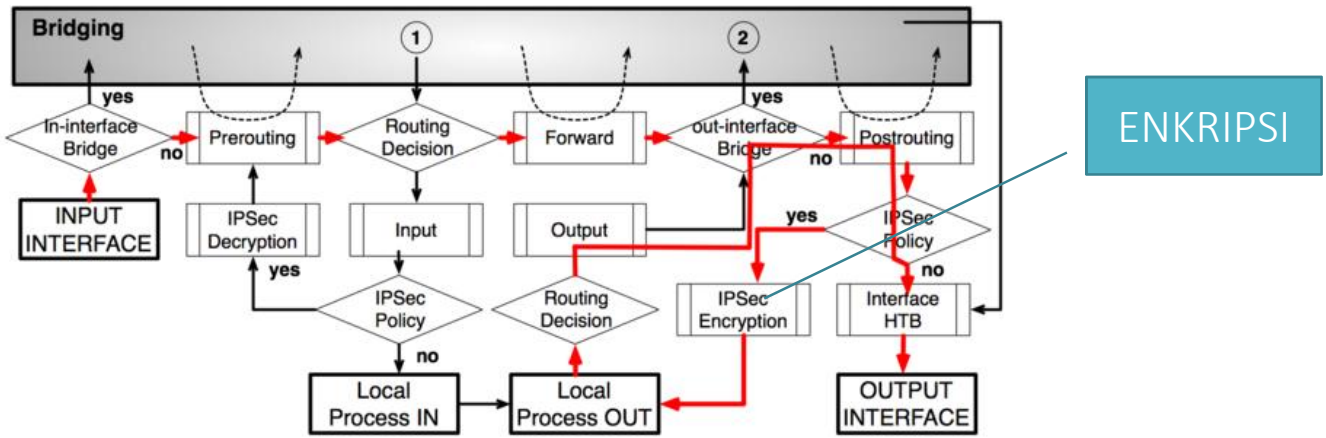


The screenshot shows the 'IPsec Peer <10.4.3.2>' configuration window in Mikrotik WinBox. The window contains the following fields and options:

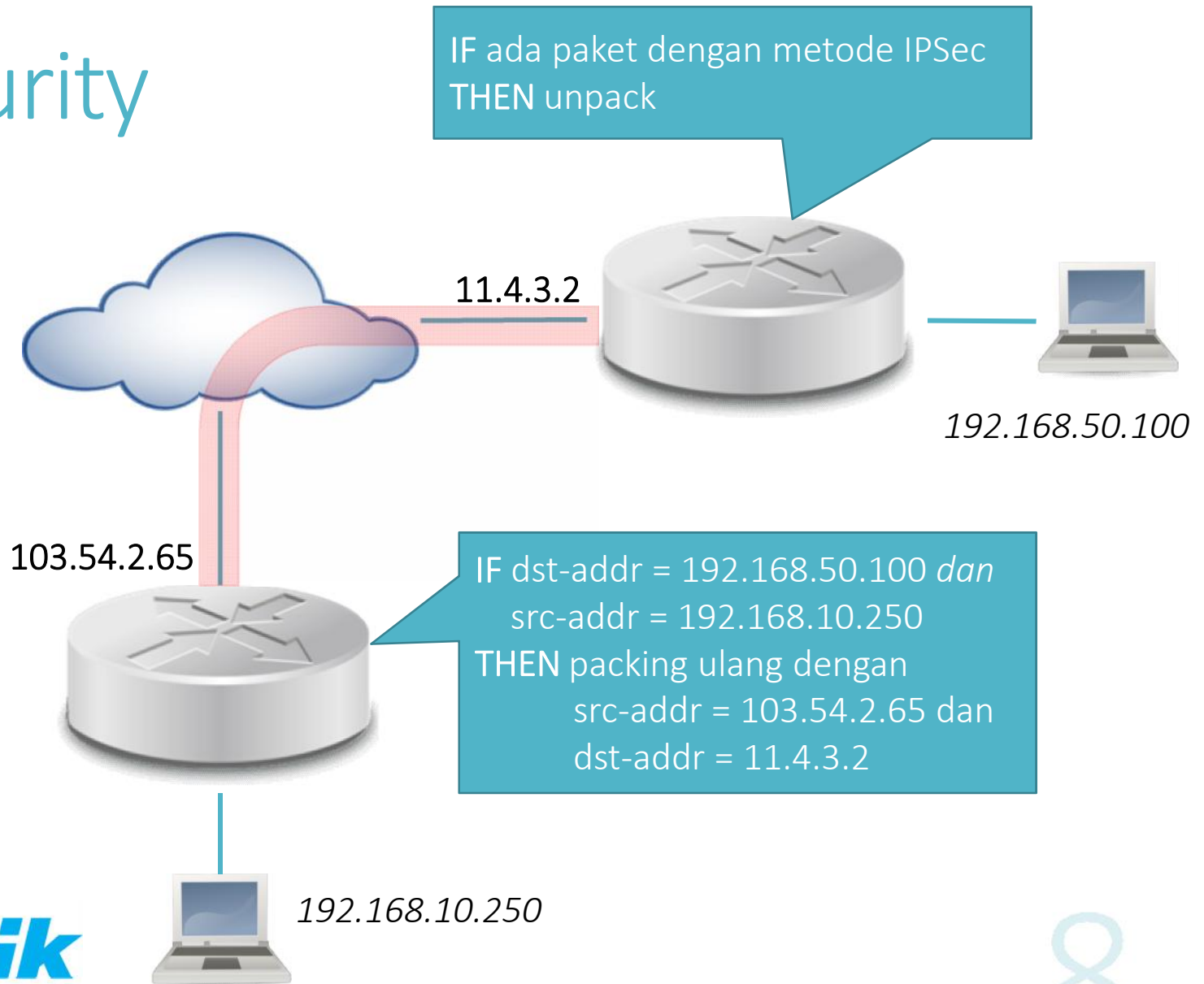
- Address: 10.4.3.2
- Port: 500
- Auth. Method: pre shared key
- Secret: abcd
- Exchange Mode: main
- Send Initial Contact
- NAT Traversal
- My ID User FQDN: (empty)
- Proposal Check: obey
- Hash Algorithm: md5
- Encryption Algorithm: 3des
- DH Group: modp1024
- Generate Policy

On the right side of the window, there are buttons for: OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

# IPSecurity (\*menurut PacketFlow)

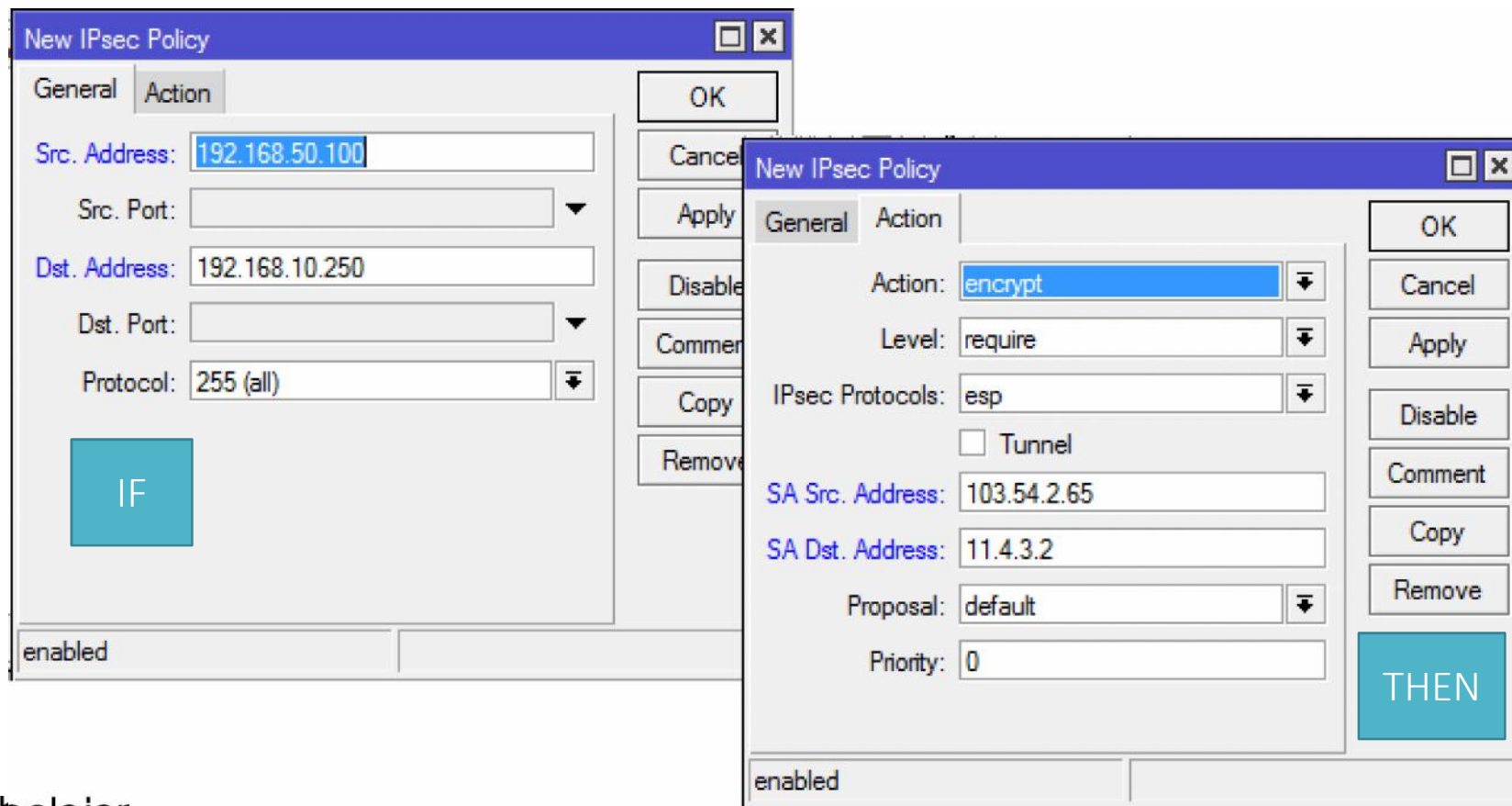


# IPSecurity





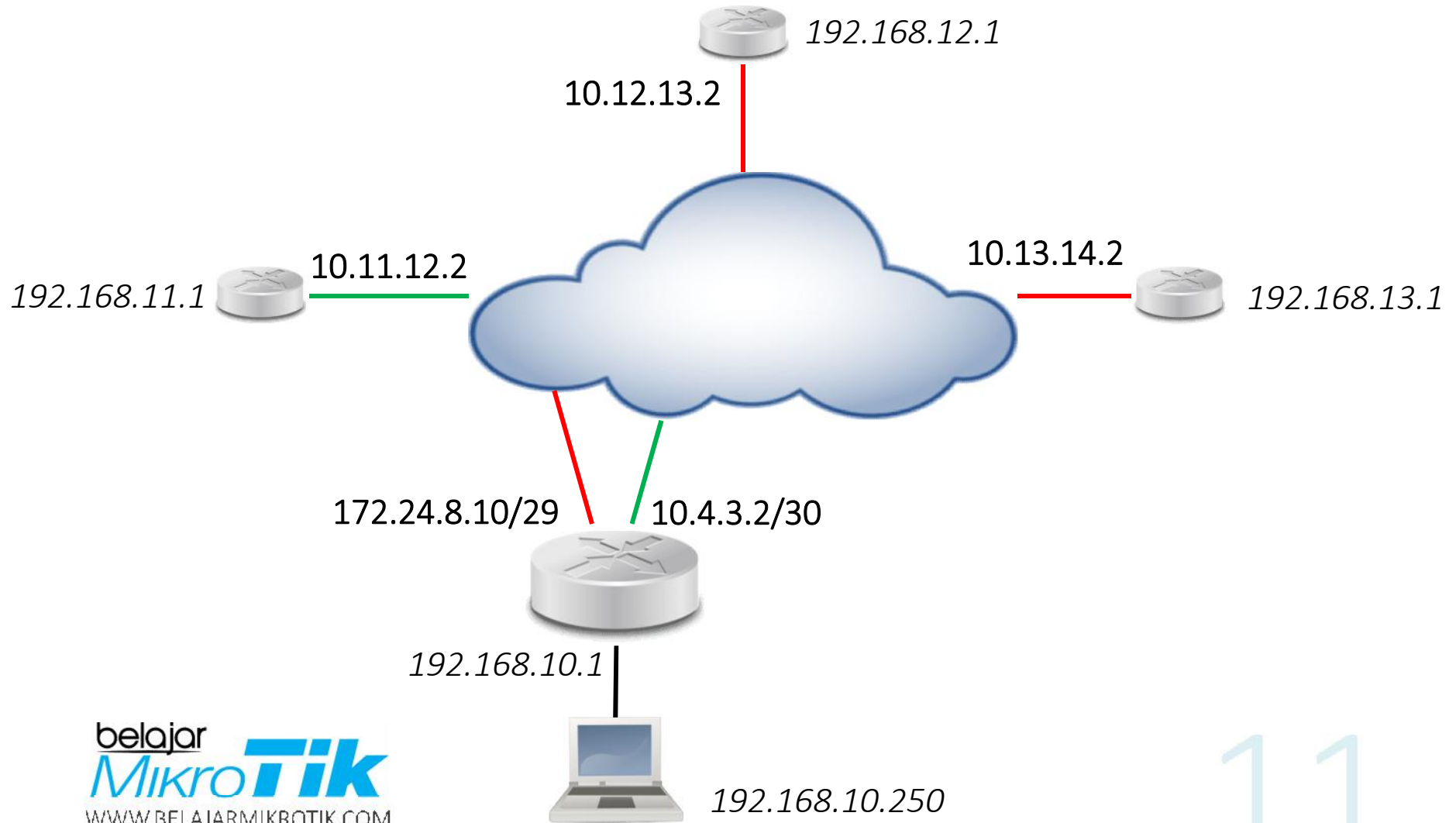
# IPSecurity RULE (\*winbox config)



# Sistem Baru yang di Usulkan

1. Single Gateway dengan Policy Routing
2. Load-balance IPSec \*manual\* (pengaturan secara manual cabang mana yang lewat ke ISP1 dan ISP2)
3. Fail-over IPSec (kalau ISP satu putus, bisa otomatis pindah ke ISP backup)
4. Fail-over router (kalau router utama down, langsung di-takeover oleh router backup)

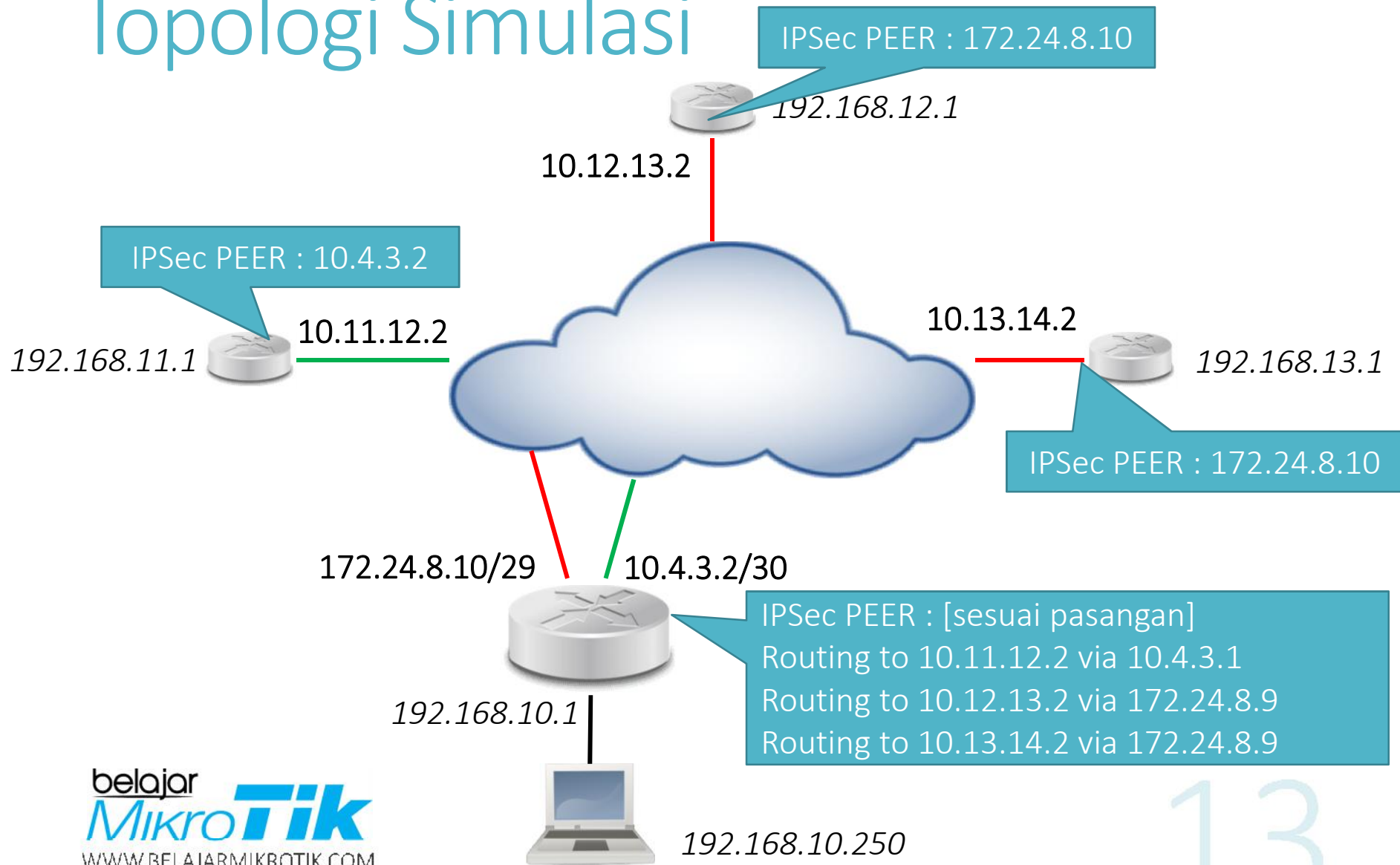
# Topologi Simulasi



# Sistem #1

Single Gateway dengan Policy Routing

# Topologi Simulasi



# RouterOS Config (routing)

Route List

Routes | Nexthops | Rules | VRF

	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	via-isp-1
AS	0.0.0.0/0	172.24.8.9 reachable to-isp-2	1	via-isp-2
DAC	10.4.3.0/30	to-isp-1 reachable		
DAC	172.24.8.8/29	to-isp-2 reachable		
DAC	192.168.10.0/24	local reachable		

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists

Name	Address
isp1	10.11.12.2
isp2	10.12.13.2
isp2	10.13.14.2

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

#	Action	Chain	Dst. Address List	New Routing Mark	Bytes	Packets
0	mark routing	output	isp1	via-isp-1	31.4 KB	423
1	mark routing	output	isp2	via-isp-2	27.7 KB	250

# RouterOS Config (peer)

Via ISP1

The screenshot displays two overlapping WinBox windows for configuring IPsec peers. The background window is titled 'admin@10.11.12.2 (REMOTE-1) - WinBox v5.25 on RB MetaROUTER (mipsbe)'. The foreground window is titled 'admin@10.4.3.2 (HQ1) - WinBox v5.25 on RB MetaROUTER (mipsbe)'. It shows the configuration for an IPsec Peer with the following fields:

- Address: 10.4.3.2
- Port: 500
- Auth. Method: pre shared key
- Secret: abcd

A second, smaller window titled 'IPsec Peer <10.11.12.2>' is overlaid on top, showing the configuration for a peer with the following fields:

- Address: 10.11.12.2
- Port: 500
- Auth. Method: pre shared key
- Secret: abcd

Buttons for 'OK', 'Cancel', 'Apply', and 'Disable' are visible on the right side of the smaller window.

# RouterOS Config (peer)

Via ISP2

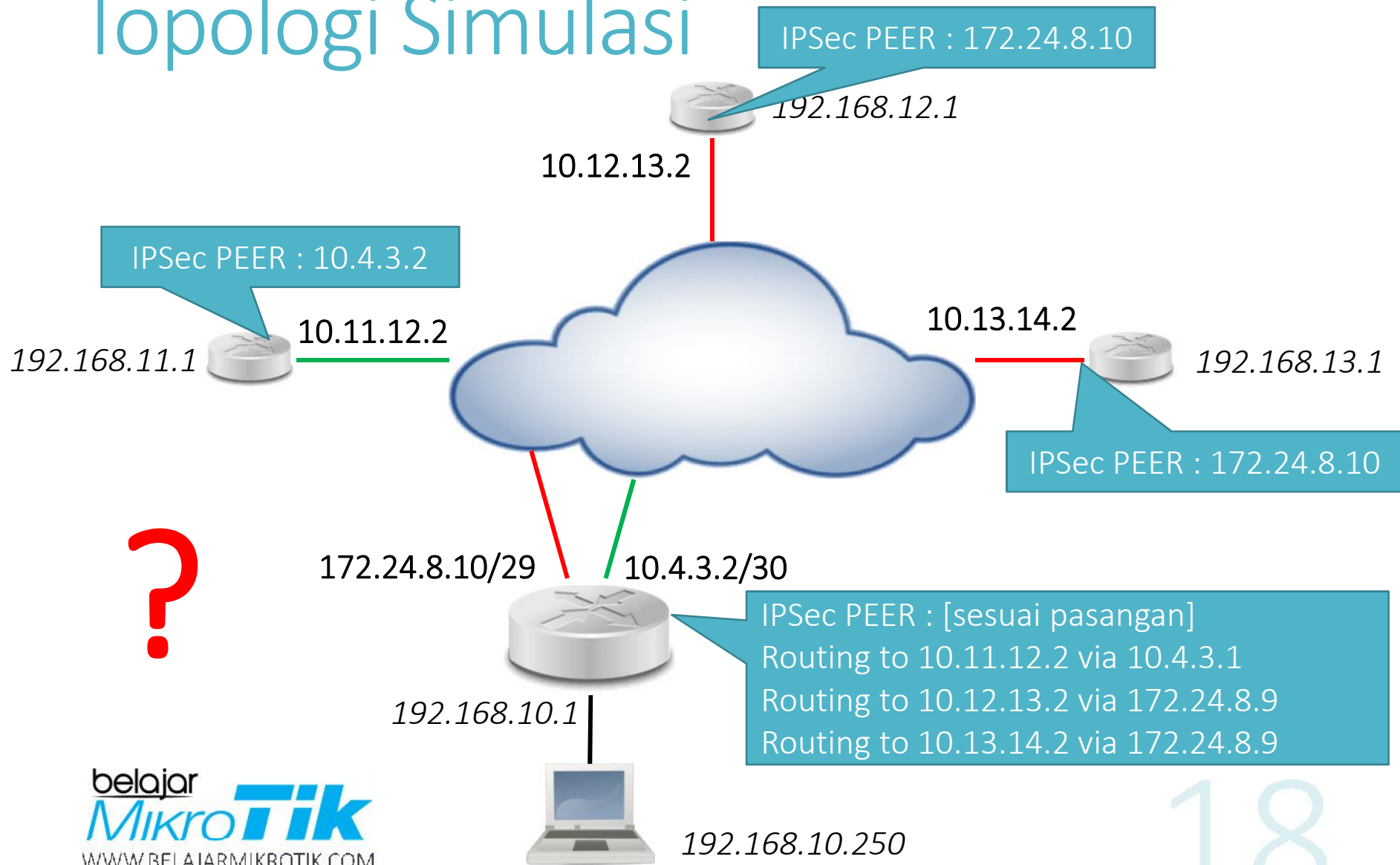
The image displays three screenshots of the RouterOS WinBox interface, showing the configuration of IPsec peers. The top-left screenshot shows the configuration for a peer at 172.24.8.10, with fields for Address (172.24.8.10), Port (500), Auth. Method (pre shared key), and Secret (ab12). The top-right screenshot shows the configuration for a peer at 10.12.13.2, with fields for Address (10.12.13.2), Port (500), Auth. Method (pre shared key), and Secret (ab12). The bottom-left screenshot shows the configuration for a peer at 172.24.8.10, with fields for Address (172.24.8.10), Port (500), Auth. Method (pre shared key), and Secret (1234). The bottom-right screenshot shows the configuration for a peer at 10.13.14.2, with fields for Address (10.13.14.2), Port (500), Auth. Method (pre shared key), and Secret (1234).



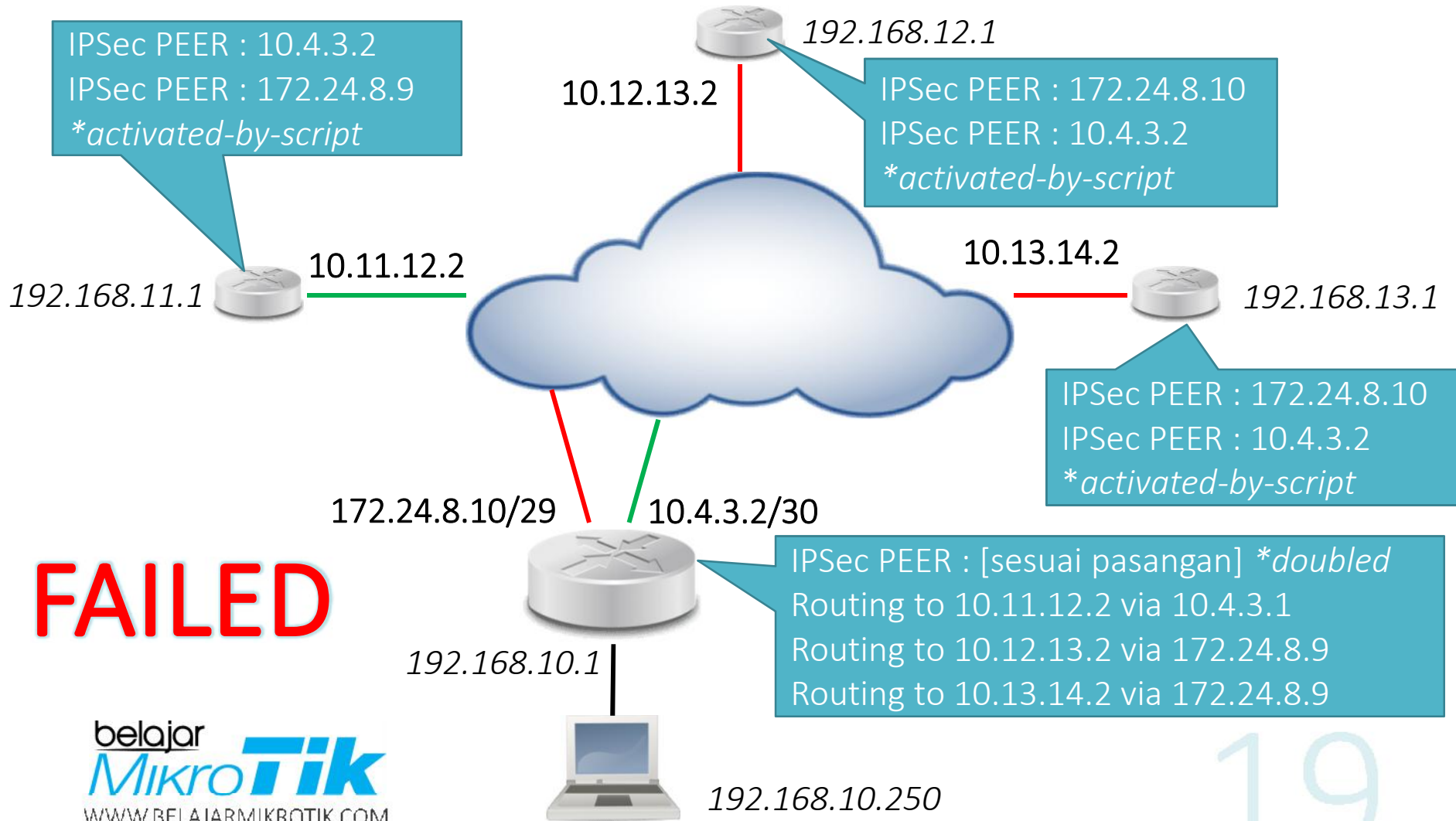
# Sistem #2

Load-balance IPSec *\*manual\** (pengaturan secara manual cabang mana yang lewat ke ISP1 dan ISP2)

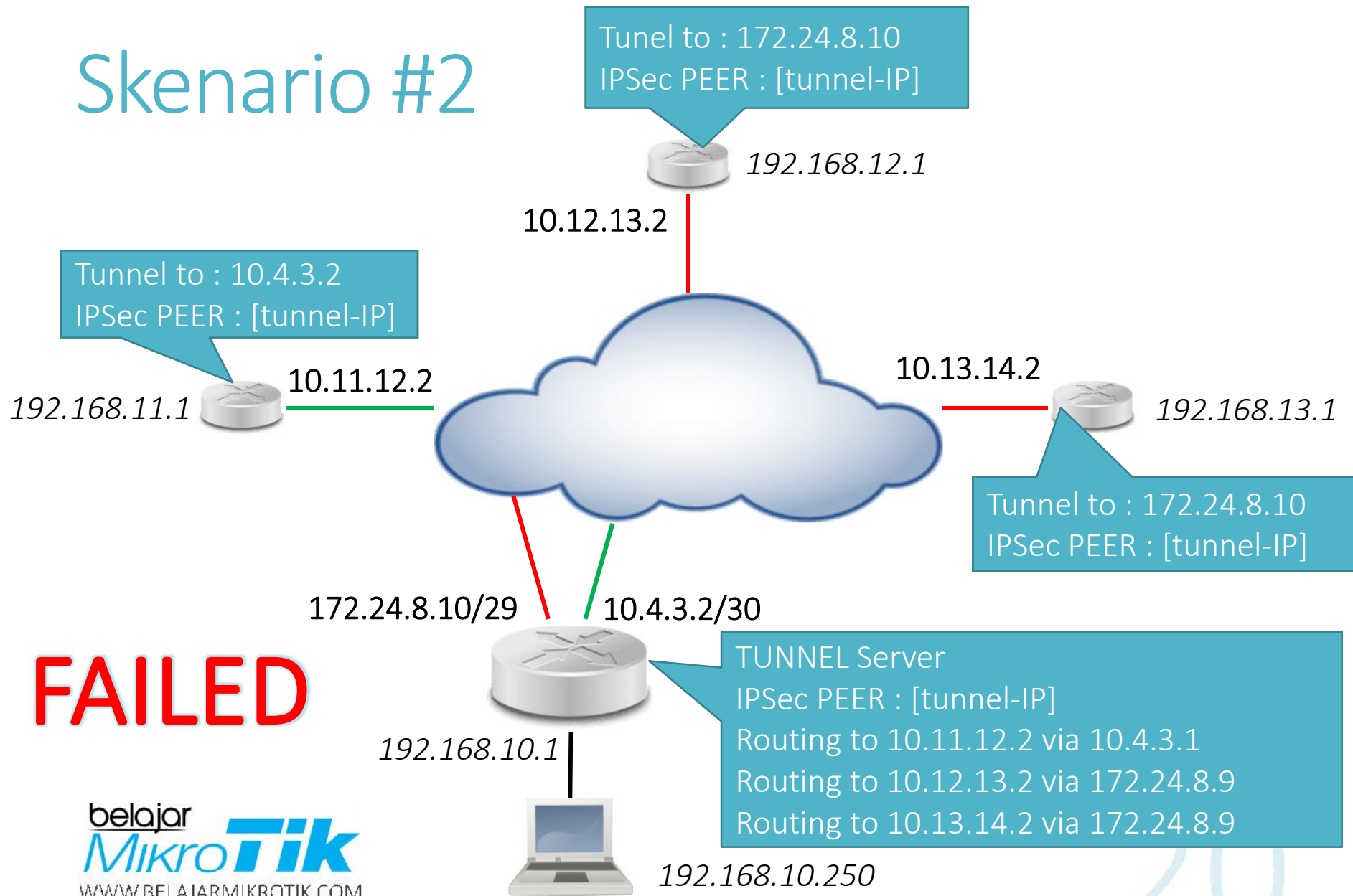
# Topologi Simulasi



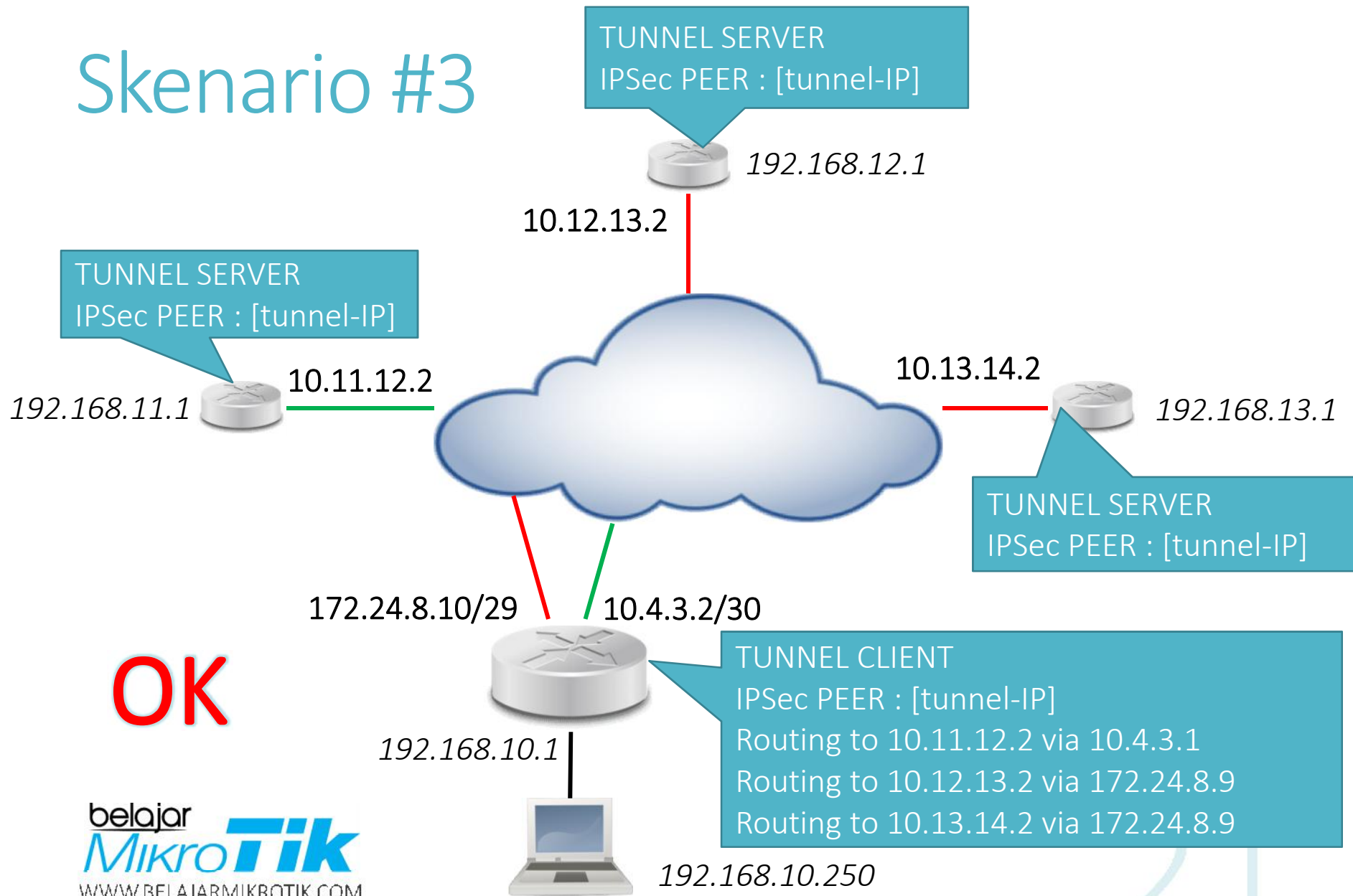
# Skenario #1



# Skenario #2



# Skenario #3



OK

# RouterOS Config - TUNNEL

REMOTE-SITE (Tunnel Server)

admin@10.11.12.2 (REMOTE-1) - WinBox v5.25 on RB M

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections

	Name	Local Address	Remote Address	Bridge
*	default			
*	default-encryption			
	profile1	10.1.1.11	10.1.1.111	

PPP Secret <10.11.12.2>

Name: 10.11.12.2

Password: 123

Service: sstp

Caller ID:

Profile: profile1

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

# RouterOS Config - TUNNEL

HQ SITE (Tunnel Client)

PPP

Interface | PPPoE Servers | Secrets | Profiles | Ac

+ | - | ✓ | ✗ | 📄 | 🏠 | PPP Scann

	Name	Type
R	❖❖sstp-out-remote-11	SSTP Client
R	❖❖sstp-out-remote-12	SSTP Client
R	❖❖sstp-out-remote-13	SSTP Client

Interface <sstp-out-remote-11>

General | Dial Out | Status | Traffic

Connect To: 10.11.12.2

Port: 443

Proxy: [dropdown]

Proxy Port: 443

Certificate: none

Verify Server Certificate

Verify Server Address From Certificate

User: 10.11.12.2

Password: 123

Profile: default-encryption

Keepalive Timeout: 10

Add Default Route

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Torch

# RouterOS Config - PEER

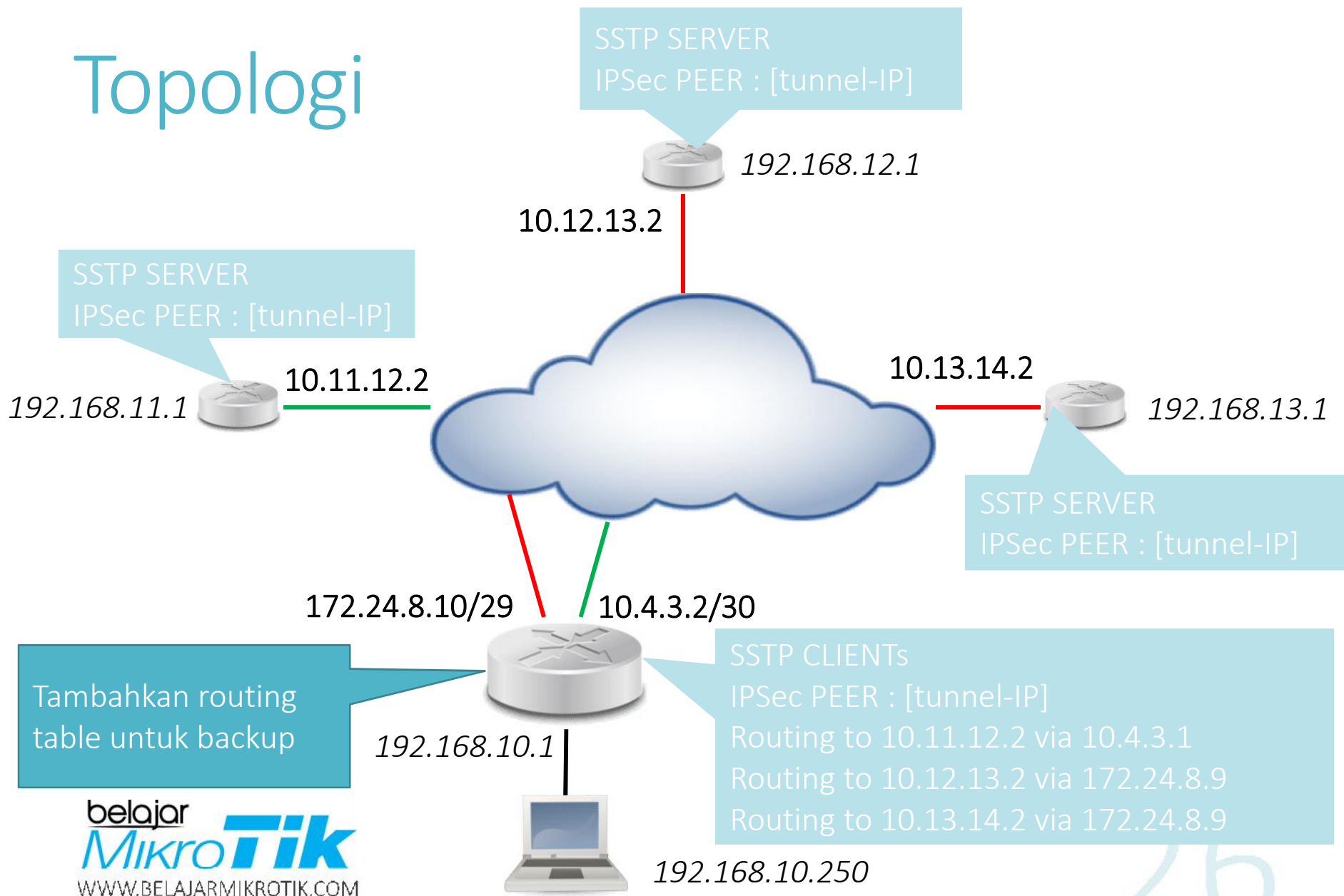
The image shows two overlapping Mikrotik WinBox windows. The background window is titled 'admin@02:42:1B:43:F3:30 (HQ1) - WinBox v5.25 on RB' and displays the configuration for an IPsec Peer with address 10.1.1.11. The configuration includes: Address: 10.1.1.11, Port: 500, Auth. Method: pre shared key, Secret: abcd, Exchange Mode: main, and checkboxes for Send Initial Contact (checked) and NAT Traversal (unchecked). The foreground window is titled 'admin@10.11.12.2 (REMOTE-1) - WinBox v5.25 on RB MetaR' and displays a smaller dialog box for an IPsec Peer with address 10.1.1.111. This dialog box has the same configuration: Address: 10.1.1.111, Port: 500, Auth. Method: pre shared key, Secret: abcd, Exchange Mode: main, and checkboxes for Send Initial Contact (checked) and NAT Traversal (unchecked). The dialog box also features buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove.



# Sistem #3

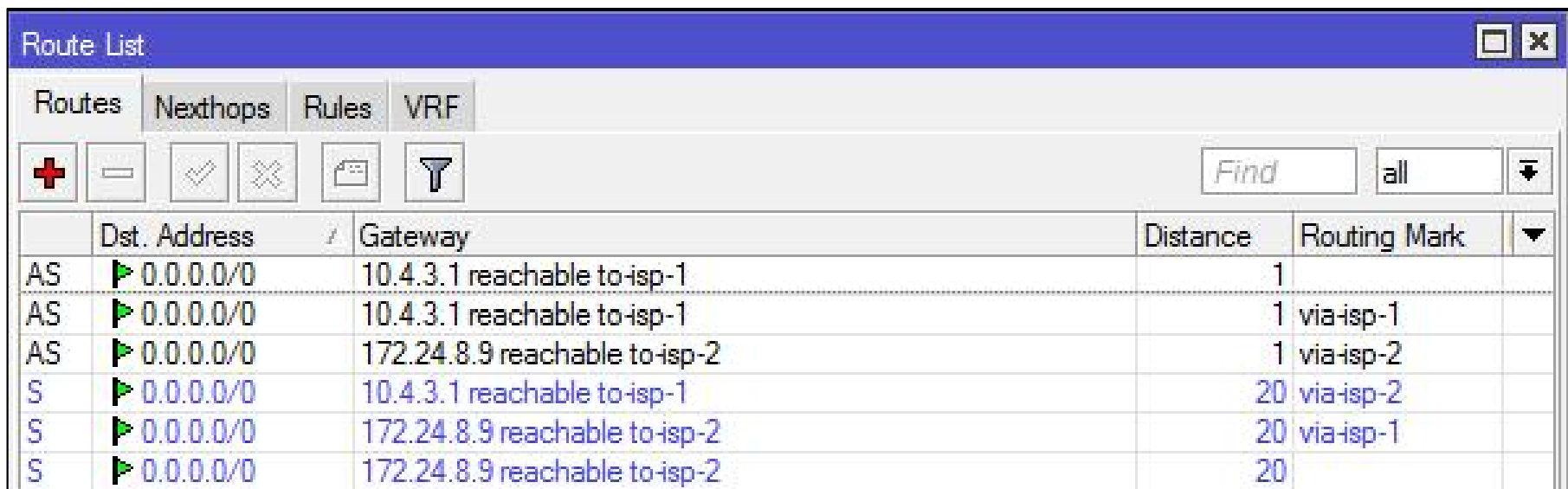
Fail-over IPsec (kalau ISP satu putus, bisa otomatis pindah ke ISP backup)

# Topologi



# FailOver RouterOS Config

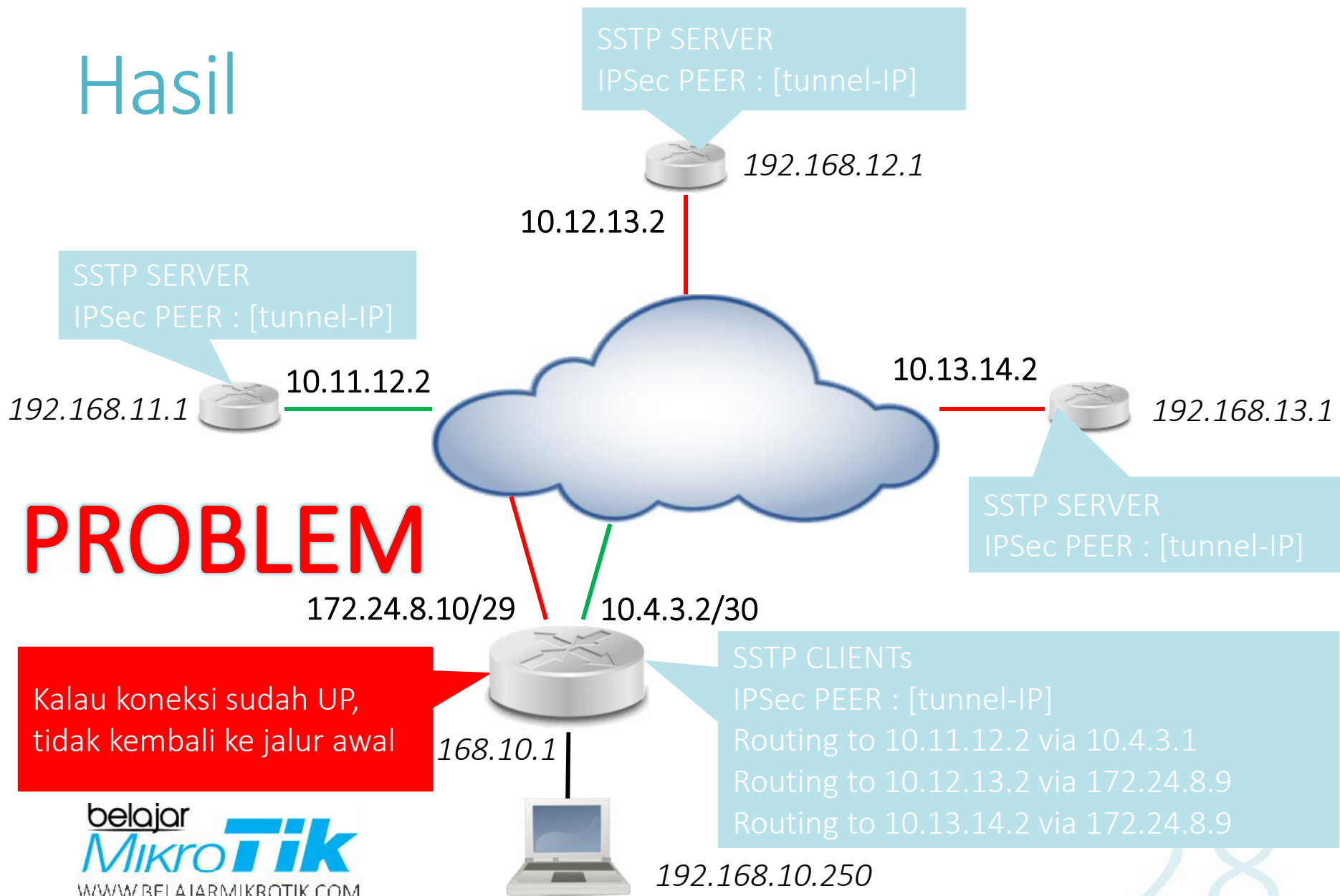
Tambahkan routing dengan routing-mark terbalik dan dengan distance lebih tinggi



The screenshot shows the RouterOS 'Route List' window. It features a toolbar with icons for adding, deleting, and filtering routes, along with a search field. The main table displays routing entries for the destination 0.0.0.0/0. The entries are categorized by source (AS or S) and include details on the gateway, distance, and routing mark.

	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	via-isp-1
AS	0.0.0.0/0	172.24.8.9 reachable to-isp-2	1	via-isp-2
S	0.0.0.0/0	10.4.3.1 reachable to-isp-1	20	via-isp-2
S	0.0.0.0/0	172.24.8.9 reachable to-isp-2	20	via-isp-1
S	0.0.0.0/0	172.24.8.9 reachable to-isp-2	20	

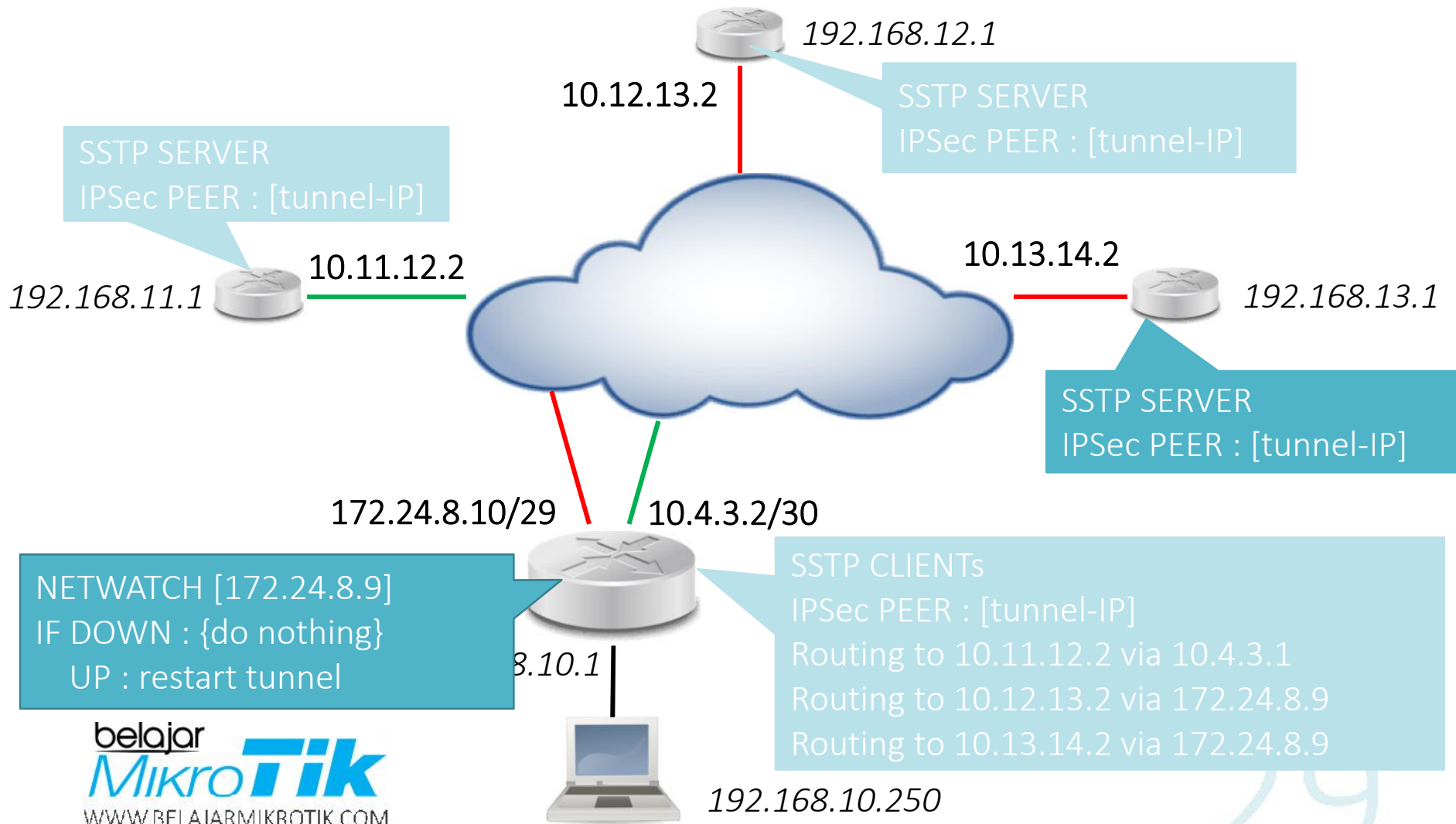
# Hasil



# PROBLEM

Kalau koneksi sudah UP, tidak kembali ke jalur awal

# FailOver Desain



# FailOver

Netwatch		
Host	/	Interval
10.4.3.1		00:00:10
172.24.8.9		00:00:10

```
Netwatch Host <10.4.3.1>
Host Up Down
On Up:
:local main isp 1
:delay delay-time=5
for id from=0 to=([/ip firewall address-list print count-only]-1) do={
:local list [/ip firewall address-list get $id list];
if ($list=$main) do={
:local ip [/ip firewall address-list get $id address];
/interface sstp-client disable [find user=$ip]
:delay delay-time=3
/interface sstp-client enable [find user=$ip]
}
}
}
enabled
```

# FailOver

The screenshot shows two windows from Mikrotik WinBox. The top window is titled 'Netwatch' and displays a table with columns: Host, Interval, Timeout (ms), Status, and Since. It shows two entries: 10.4.3.1 (up) and 172.24.8.9 (down). The bottom window is titled 'Route List' and shows a table with columns: Dst. Address, Gateway, Distance, and Routing Mark. It lists routes for 0.0.0.0/0 with various gateways and distances, including unreachable and reachable states.

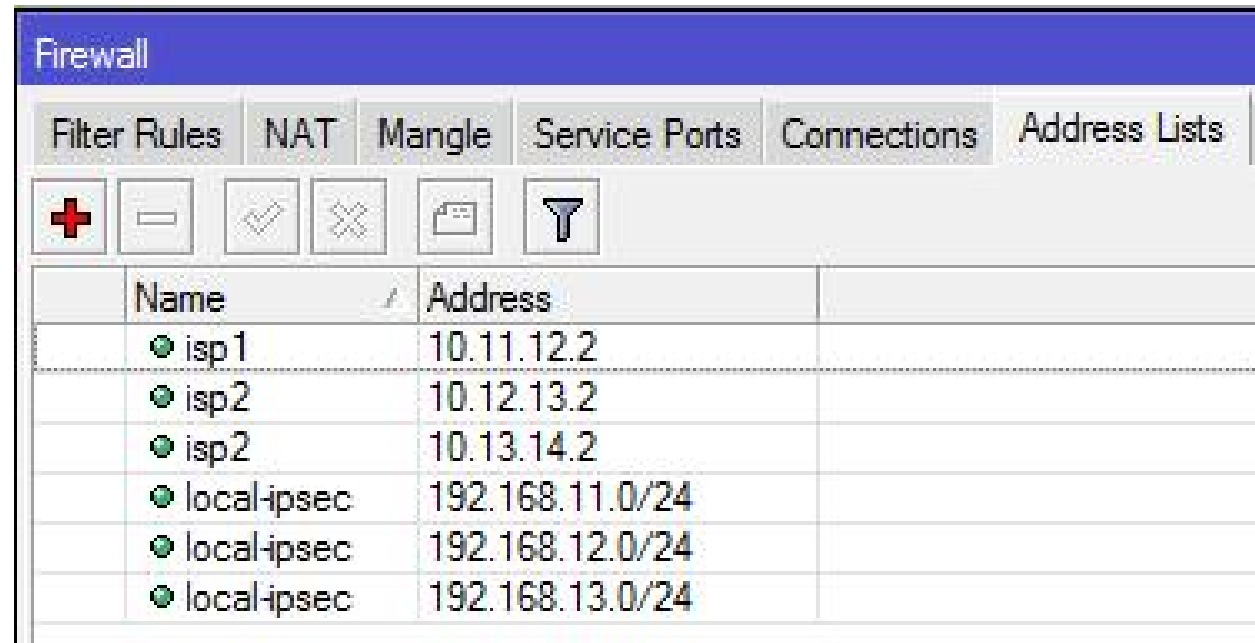
Host	Interval	Timeout (ms)	Status	Since
10.4.3.1	00:00:10	1000	up	Jan/02/1970 00:09:20
172.24.8.9	00:00:10	1000	down	Jan/02/1970 00:34:23

	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	via-isp-1
S	0.0.0.0/0	172.24.8.9 unreachable	1	via-isp-2
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	20	via-isp-2
S	0.0.0.0/0	172.24.8.9 reachable to-isp-2	20	via-isp-1
S	0.0.0.0/0	172.24.8.9 reachable to-isp-2	20	

# Pengaturan Jalur

Via Address-List



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Address Lists. The 'Address Lists' tab is selected. Below the navigation tabs, there are several icons: a red plus sign for adding, a minus sign for deleting, a checkmark for enabling, a cross for disabling, a document icon for editing, and a funnel icon for filtering. The main table displays the following data:

Name	Address
isp 1	10.11.12.2
isp2	10.12.13.2
isp2	10.13.14.2
local-ipsec	192.168.11.0/24
local-ipsec	192.168.12.0/24
local-ipsec	192.168.13.0/24



# Sistem #4

Fail-over router (kalau router utama down, langsung di-takeover oleh router backup)

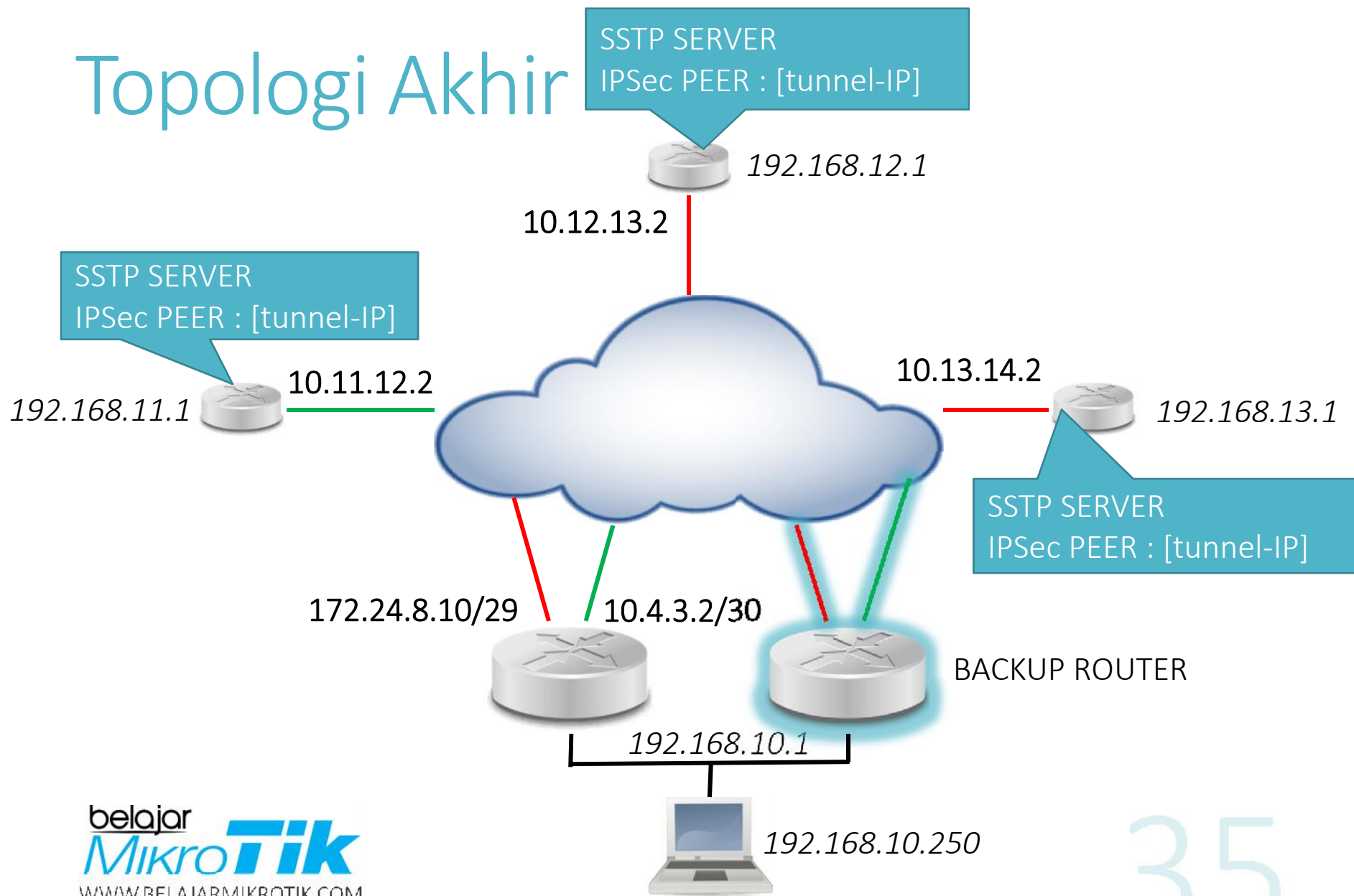
# VRRP

Metode auto-backup secara hardware (atau bisa juga jadi load-balance gateway router)

Menciptakan IP Virtual pada jaringan lokal dan dapat segera mengaktifkan router lain bila terindikasi router utama DOWN

Bekerja sangat responsif

# Topologi Akhir



# TANTANGAN

Salah satu IP Publik memiliki subnet /30

Sinkronisasi setting antar 2 router

SOLUSI : gunakan SCRIPT/SCHEDULER

# VRRP

IP Publik dipakai bergantian

Address List			
	Address	Network	Interface
X	10.4.3.2/30	10.4.3.0	to-isp-1
X	172.24.8.10/29	172.24.8.8	to-isp-2
	192.168.10.1	192.168.10.1	vmp 1
	192.168.10.253/24	192.168.10.0	local

Interface <vmp 1>

General VRRP Scripts Traffic

On Master:

```
/ip address enable [find interface=to-isp-1]  
/ip address enable [find interface=to-isp-2]
```

On Backup:

```
/ip address disable [find interface=to-isp-1]  
/ip address disable [find interface=to-isp-2]
```

enabled  running  slave

# VRRP

Sinkronisasi setting

MASTER

*Buat script untuk membackup beberapa setting secara regular, misal address-list, sstp-client, routing-table, dll (yang dirasa perlu)*


BACKUP

*Buat script untuk mem-fetch file ke router MASTER secara regular*

*Hapus semua konfig di BACKUP router sesuai dengan konfig yang diambil, misal address-list*

*Apply (import) file backup dari router MASTER*

# Kredit

 **UnitedPlexus** Philippines (partner)

Tokim Wong

Samuel Cadeliña

# Terima Kasih

Pertanyaan

Email : [herry@belajarmikrotik.com](mailto:herry@belajarmikrotik.com)

Web : [www.belajarmikrotik.com](http://www.belajarmikrotik.com)

Phone : +628179343779