



PENCARIAN PRODUK

Artikel

10 Cara Mengamankan Router Mikrotik

Kategori: Tips & Trik (artikel.php?kategori=3)

Dalam melakukan konfigurasi router mikrotik untuk jaringan yang kita miliki, hal yang sangat penting dan perlu diperhatikan adalah mengenai keamanan router. Sebagai Admin jaringan jangan sampai lupa untuk melakukan proteksi atau mengamankan router dari pihak pihak luar yang tidak bertanggung jawab.

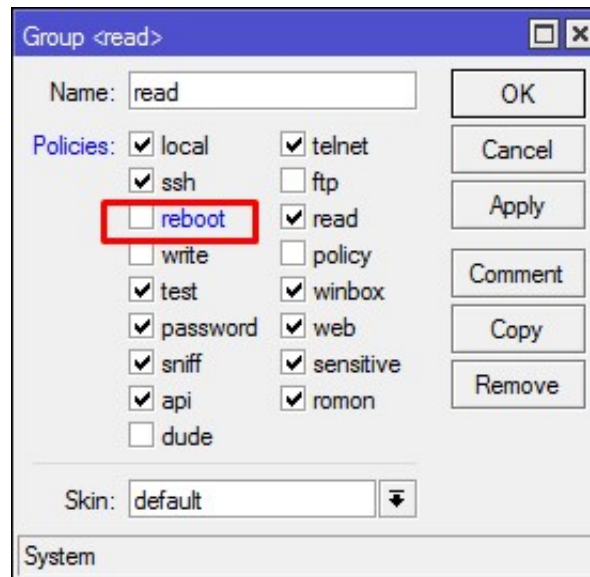
Langkah - langkah yang perlu dilakukan untuk mengamankan Router Mikrotik sebagai berikut :

1. Ganti Username dan Password Router Mikrotik

Sudah bukan rahasia lagi kalau Router Mikrotik mempunyai Username dan Password bawaan pabrik yaitu Username : Admin, dan Password : (blank). Sebaiknya Username Password default tersebut kita disable, dihapus atau kita ubah, agar tidak digunakan orang lain. Untuk menghapus dan melakukan disable User Default silakan buat terlebih dahulu User yang memiliki hak akses (group) Full. Untuk melakukan management User bisa masuk ke menu **System -> Users**



Selain disable, kita juga bisa membuat user baru dengan hak akses Read. Dalam memberikan hak akses Read yang perlu diperhatikan adalah jangan sampai lupa nonaktifkan (un-cek) policies "reboot". Karena Secara default Group Read masih bisa melakukan Reboot.



Group <read>

Name: read

Policies:

- ☒ local
- ☒ ssh
- ☐ reboot
- ☐ write
- ☒ test
- ☒ password
- ☒ sniff
- ☒ api
- ☐ dude
- ☒ telnet
- ☐ ftp
- ☒ read
- ☐ policy
- ☒ winbox
- ☒ web
- ☒ sensitive
- ☒ romon

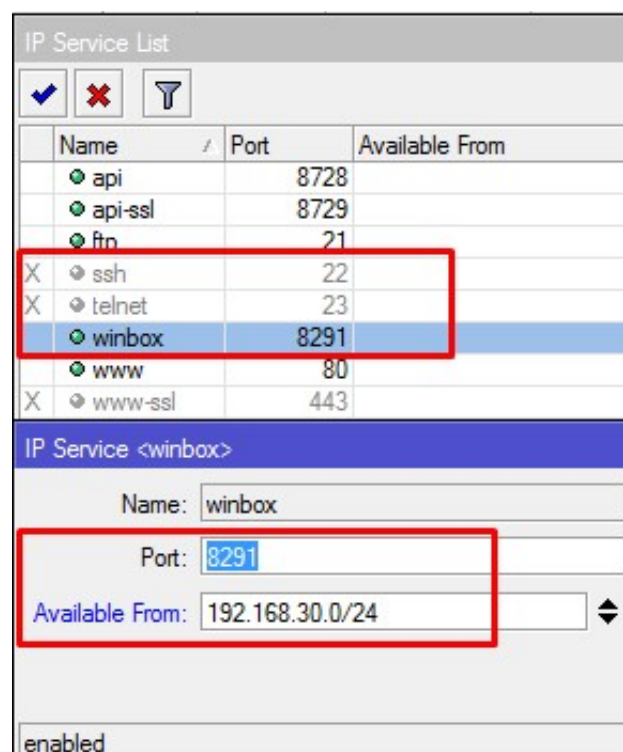
Skin: default

System

2. Ubah atau Matikan Service yang Tidak Diperlukan

Service di Router Mikrotik secara default sudah terbuka, jadi kita harus mengantisipasi beberapa service yang kita gunakan untuk melakukan remote ke router. Caranya kita bisa menonaktifkan service tersebut, mengubah port defaultnya atau membatasi hanya beberapa ip address saja yang boleh akses menggunakan port tersebut.

Pengaturan ini dapat dilakukan pada menu IP  Services



IP Service List

Name	Port	Available From
api	8728	
api-ssl	8729	
ftn	21	
X ssh	22	
X telnet	23	
winbox	8291	
www	80	
X www-ssl	443	

IP Service <winbox>

Name: winbox

Port: 8291

Available From: 192.168.30.0/24

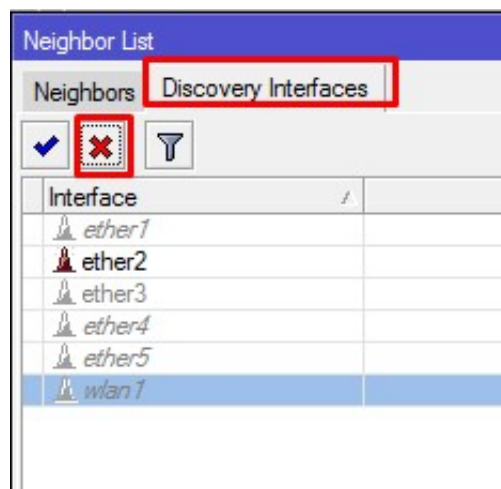
enabled

3. Non-Aktifkan Neighbors Discovery

Mikrotik memiliki protocol yang dapat melakukan broadcast domain melalui layer 2 sehingga membuat perangkat Mikrotik bisa saling menemukan jika berada di jaringan layer 2 yang sama, namanya adalah Mikrotik Neighbor Discovery Protocol(MNDP). Perangkat yang support MNDP dan CDP dapat menemukan atau mengetahui informasi router lain seperti informasi identity Router, MAC-Address,dan IP-Address. Contoh paling mudah saat kita akan melakukan winbox di tab Neighbors akan terlihat beberapa informasi Router yang terkoneksi layer 2 dengan laptop kita.

Agar Router tidak memberikan informasi tersebut, sebagai admin jaringan sebaiknya lakukan disable discovery interface. Terutama Interface yang terkoneksi langsung dengan pihak umum misalnya interface wireless untuk jaringan hotspot, interface ethernet untuk jaringan PC client warnet, dan sebagainya.

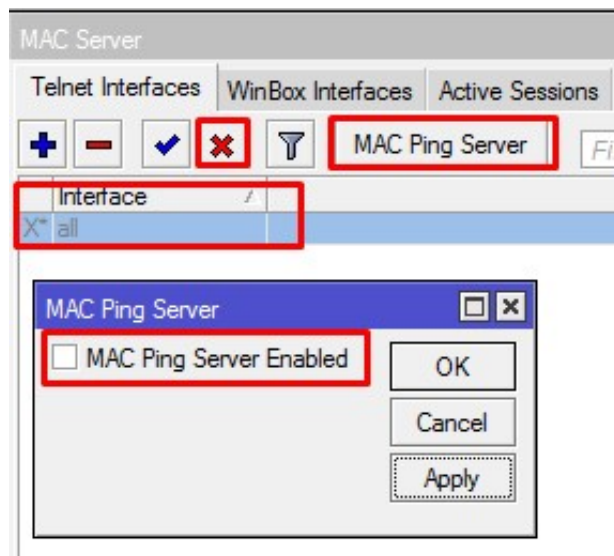
Pengaturan ini dapat dilakukan pada menu IP  Neighbors



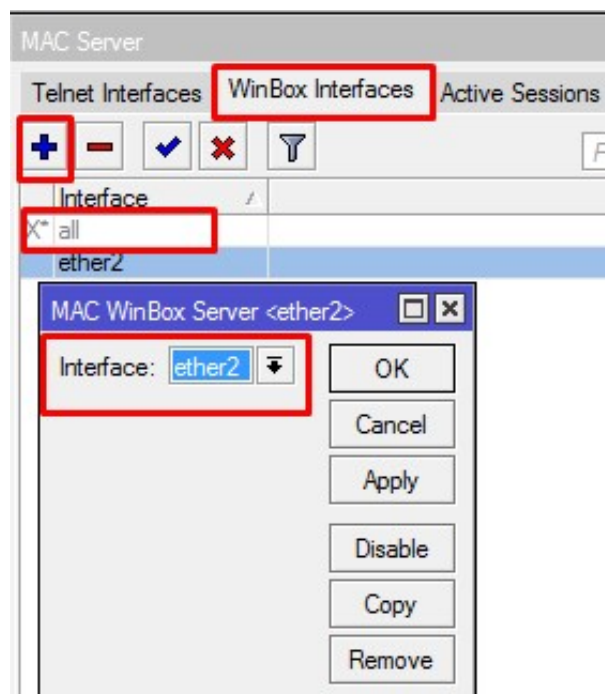
Tiga langkah cara mengamankan Router Diatas secara detail sudah pernah dibahas pada artikel Langkah Pertama Menjaga Keamanan Router (/artikel_lihat.php?id=79)

4. Non-Aktifkan atau Ubah Fitur MAC Server

Dengan melakukan disable pada discovery interface bukan berarti Router tidak bisa di remote menggunakan MAC-Address. Jika sebelumnya sudah menyimpan atau mengetahui MAC-Address Router, masih bisa di remote menggunakan MAC-Address. Jika menginginkan Router tidak bisa di remote menggunakan MAC-Address baik melalui Winbox ataupun via telnet, matikan Fitur MAC-Server di Router. **Tools -> MAC-Server**



Atau Anda hanya ingin MAC-Winbox dari interface yang terkoneksi dengan PC Anda saja misal Ether2. Cara melakukannya buat terlebih dahulu MAC-Winbox Interface ke Arah Ether2 selanjutnya disable interface "all"



5. Aktifkan Firewall Filter Untuk Akses Service Router (DNS dan Web Proxy)

Router Mikrotik yang kita tempatkan sebagai Gateway Utama, sering mengaktifkan fitur Allow-remote-request DNS dan web proxy. Kedua fitur tersebut bisa dimanfaatkan oleh pihak luar terutama web proxy yang kadang membuat trafik international kita sering penuh padahal tidak ada user lokal yang menggunakannya.

Untuk mengatasi hal tersebut kita harus mengaktifkan filter pada Firewall agar pihak luar tidak bisa memanfaatkan DNS kita dan Web Proxy kita.

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 8080,53

Any. Port:

P2P:

In. Interface: ☐ ether3

Out. Interface:

In. Interface List:

Out. Interface List:

New Firewall Rule

General Advanced Extra Action Statistics

Action: drop

☐ Log

Log Prefix:

Jangan lupa buat juga action drop untuk trafik DNS yang menggunakan protocol udp.

Firewall Rule <53>

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ 17 (udp)

Src. Port:

Dst. Port: ☐ 53

Any. Port:

P2P:

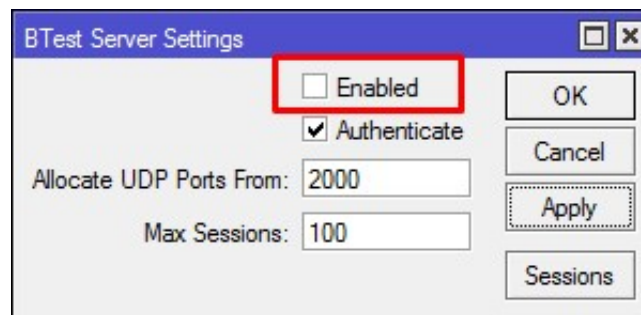
In. Interface: ☐ ether3

Out. Interface:

6. Non-Aktifkan Btest Server

Router Mikrotik juga memiliki fitur Btest Server, yang bisa digunakan untuk melakukan test koneksi yang sudah terbentuk. Tetapi fitur ini jika tiba-tiba di dimanfaatkan oleh pihak luar, Router kita di paksa untuk men-generate trafik atau menerima trafik bandwidth test bisa jadi bandwidth yang kita miliki habis atau tiba-tiba CPU load kita menjadi 100%. Tentu sebagai admin jaringan tidak menginginkan hal itu, lebih baik fitur ini dimatikan.

Pengaturan dapat dilakukan pada menu Tools  > BTest Server



Artikel mengenai penggunaan Bandwidth test bisa di lihat di halaman berikut [Bandwidth Test Menggunakan Mikrotik \(/artikel_lihat.php?id=51\)](/artikel_lihat.php?id=51)

7. Ubah pin atau Non-Aktifkan Fitur LCD

Beberapa Router Mikrotik sudah dilengkapi dengan LCD yang juga bisa digunakan untuk menambahkan perintah-perintah sederhana langsung dari LCD tersebut. Jika router yang memiliki LCD tersebut di tempatkan di tempat yang terjangkau orang banyak sebaiknya lakukan pengubahan pin atau Non-Aktifkan Fitur LCD agar orang lain tidak iseng mengotak atik router kita. Penjelasan mengenai LCD di Mikrotik bisa di lihat di [Artikel Pengaturan LCD Display Mikrotik \(/artikel_lihat.php?id=100\)](/artikel_lihat.php?id=100)

8. Lakukan Backup secara berkala serta Enkripsi dan Ambil File backupnya

Agar tidak perlu konfigurasi ulang sebaiknya kita lakukan Backup secara berkala. Apalagi setelah selesai konfigurasi lakukan backup konfigurasi, dan jangan lupa pindahkan file backup tersebut ke PC atau laptop Anda. Untuk menjaga keamanan file backup bisa Anda lakukan Enkripsi saat akan melakukan backup konfigurasi. Untuk detailnya bisa dilihat di [Artikel Backup Konfigurasi Mikrotik \(/artikel_lihat.php?id=71\)](/artikel_lihat.php?id=71)

9. Aktifkan Bootloader Protector

Fitur Bootloader Protector digunakan untuk melakukan proteksi terhadap gangguan fisik yang bisa saja terjadi pada routerboard terutama proteksi terhadap tombol reset yang ada di router Mikrotik. Contoh implementasinya sudah pernah kami bahas artikel [Protected Bootloader \(/artikel_lihat.php?id=241\)](/artikel_lihat.php?id=241)

10. Amankan Fisik Router

Mikrotik adalah perangkat hardware elektronik sebagaimana perangkat elektronik lainnya yang membutuhkan perawatan Fisik seperti :

- Proteksi kabel power agar jangan terlalu sering di cabut colok
- Ruang pendingin untuk menjaga suhu perangkat mikrotik
- Perlindungan terhadap lonjakan listrik menggunakan UPS, atau yang melewati POE sebaiknya gunakan Arester.

10 langkah mengamankan router mikrotik diatas juga sudah kami sajikan dalam bentuk video juga, silahkan langsung menuju ke link berikut [10 Cara Mengamankan Router Mikrotik \(https://www.youtube.com/watch?v=ICPJwq4u4Fc\)](https://www.youtube.com/watch?v=ICPJwq4u4Fc)

Kembali ke :

[Halaman Artikel \(artikel.php\)](#) | [Kategori Tips & Trik \(artikel.php?kategori=3\)](#)

FOLLOW OUR SOCIAL MEDIA

 [@mikrotik_id](#)

 [@mikrotik.indonesia](#)

 <http://mikrotik.id/r/youtube/>

Menu Utama

[Halaman Muka \(/\)](#)
[Produk \(/produk.php\)](#)
[Training \(/training.php\)](#)
[Layanan \(/layanan.php\)](#)
[RMA \(/user_RMA.php\)](#)
[Artikel \(/artikel.php\)](#)

Menu Lainnya

[Aturan dan Tata Cara \(/index_lihat.php?id=4\)](#)
[Tentang Kami \(/index_lihat.php?id=1\)](#)
[Kontak Kami \(/kontak.php\)](#)
[Pendaftaran Anggota \(/member_daftar.php\)](#)

Links

[Citraneet \(ISP\) \(http://www.citra.net.id\)](http://www.citra.net.id)
[Citraweb \(System Developer\) \(http://www.citra.web.id/\)](http://www.citra.web.id/)
[Citraweb \(Web Hosting\) \(http://www.citrahost.com\)](http://www.citrahost.com)
[Citraweb \(RFelements Distributor\) \(http://www.rfelements.id\)](http://www.rfelements.id)
[MikroBits \(http://www.mikrobits.com\)](http://www.mikrobits.com)
[GudegNet \(Portal Jogja\) \(http://www.gudeg.net\)](http://www.gudeg.net)

Jogjastreamers (<http://www.jogjastreamers.com>)

Kontak Kami

Citraweb Solusi Teknologi, PT
Jalan Petung 31 Papringan
Yogyakarta 55281
INDONESIA
Telp: +62-274-554444

Copyrights ©2005-2018 PT. Citraweb Solusi Teknologi. All Rights Reserved. Generated in 0.0045 second(s). Your IP: 116.206.41.66