



Mikrotik Certified Security Engineer

Instagram.com/vaseghi.it
youtube.com/shahin vaseghi
github.com/shahinvaseghi

گردآورنده : شاهین واثقی
ویراستار: علیرضا کهن ترابی

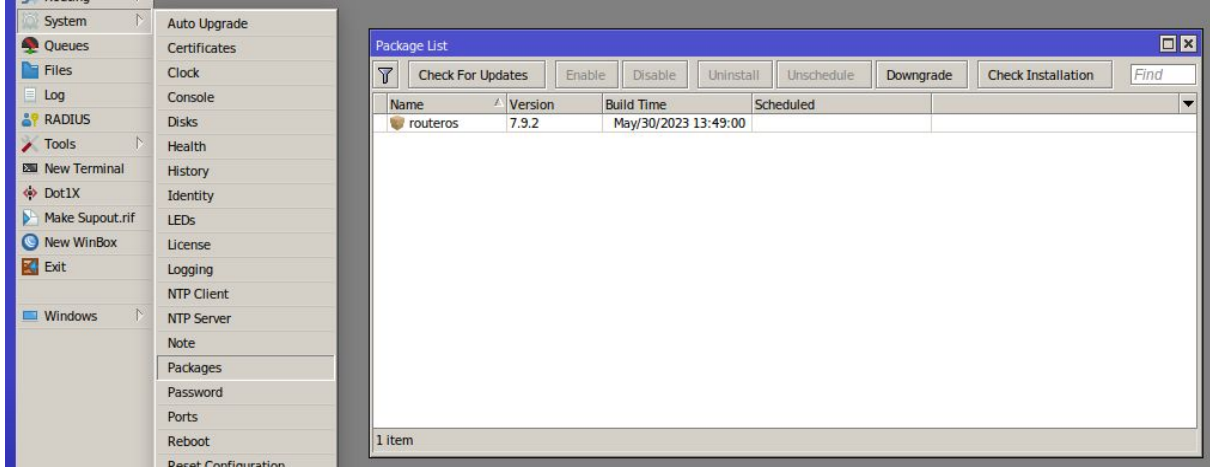
برای ایمن کردن روتر، میکروتیک مراحل زیر را پیشنهاد می کند:

۱. آپدیت نگه داشتن ورژن Router Os

برای اینکار ۴ روش وجود دارد:

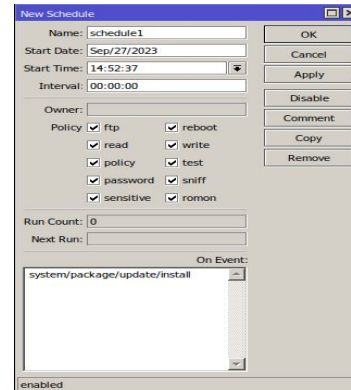
۱. به مسیر `system/packages` بروید و گزینه `check for updates` را کلیک کنید و نسخه مورد نیاز خود را انتخاب کنید

۲. مطابق با معماری پردازنده خود، پکیج **Main package** را دانلود کنید؛ پکیج را در فایل ها آپلود کنید و روتر را ریست کنید، بعد از ریست روتر با سیستم عامل جدید لود می شود.



۳. با گزینه `System Auto Upgrade` در قسمت `Update Package Source` یک روتر را به عنوان `Server` انتخاب کنید. تمامی پکیج های مورد نیاز را در `Server` آپلود کنید. به این صورت تمامی روتر های `Client` از روی `Server` پکیج ها را می بینند.

۴. می توانید در قسمت `system > Scheduler` یک اسکریپت به شکل زیر برای انجام خودکار آپدیت ایجاد کنید:



۱. Name : اسم Schedule

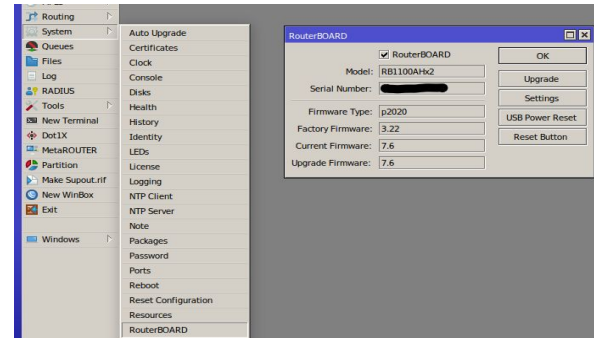
۲. Start Date : تاریخ شروع Schedule

۳. Start Time : ساعت شروع Schedule

۴. Interval : زمان تکرار این Schedule

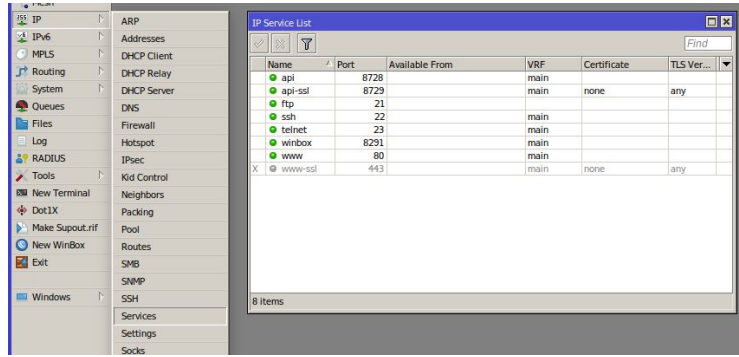
۵. On Event : دستوری که قصد دارید اجرا کنید مانند:

`system/package/update/install`



حتما توجه داشته باشید که در صورتی که قصد دارید آپدیت را روی یک روتر سخت افزاری انجام دهید، قبل از آپدیت سیستم عامل، `Firmware` برد روتر را آپگرید کنید این کار را از مسیر `System/RouterBOARD` می توانید انجام دهید

توجه کنید برای آپدیت اینترنتی حتما نیاز به `DNS Server` داریم.

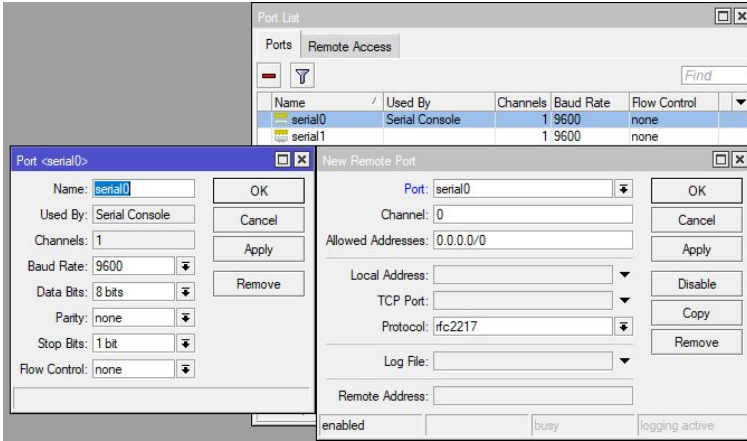


۲. مدیریت دسترسی به روتر :

برای اینکار ۵ روش وجود دارد، در منو **IP > Services** میتوانید ۴ روش را فعال یا غیر فعال کنید، پورت واسط را تنظیم کنید و دسترسی از روش این سرویس ها را کنترل کنید.

روش چهارم یا کنسول از منو **System > Port** قابل کنترل است .

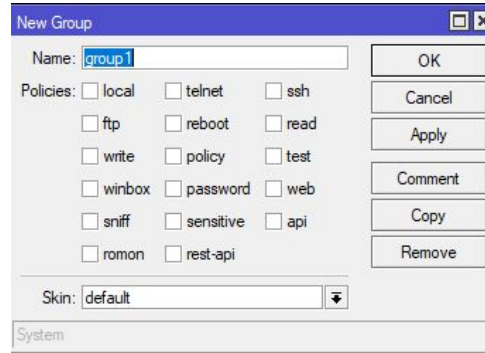
با باز کردن هر کدام می توانید شماره پورت، آدرس های مجاز برای استفاده از این سرویس و جدول مسیریابی که این سرویس مجاز است را مشاهده کنید.



برای کنترل دسترسی ها از طریق پورت سریال یا **Console** باید به منو

System>Ports رجوع کنید. میتوانید هر یک از پورت ها را باز کنید و تنظیماتی مثل **Baud Rate** و **Data bits** را کنترل کنید.

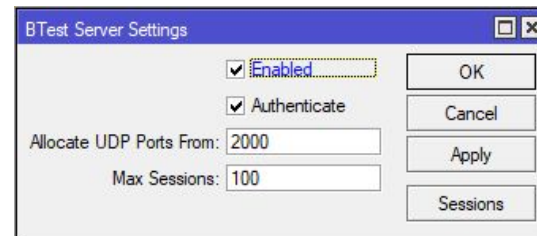
در تب **Remote Access** میتوانید تنظیمات شخصی سازی شده تری به هر پورت بدهید.



برای ایجاد یوزر، برای دسترسی کنسول باید یک گروه جدید ایجاد کنید که دسترسی **local** و باقی تنظیماتی که لازم دارید مانند **read / write** را داشته باشد سپس با آن گروه یک یوزر بسازید.

گزینه های مختلف تعریف یک گروه به شرح زیر است :

1. local دسترسی از طریق Console
 2. telnet : دسترسی از طریق telnet
 3. ssh : دسترسی از طریق ssh
 4. ftp : دسترسی به ftp روتر
 5. reboot : دسترسی ریست کردن روتر
 6. read : دسترسی خواندن تنظیمات روتر
 7. write : دسترسی نوشتن تنظیمات در روتر
 8. policy : دسترسی تنظیم یا تغییر دسترسی گروه ها
 9. test : دسترسی به ابزار های test مانند bandwidth test
 10. winbox : دسترسی از طریق winbox
 11. password : دسترسی تغییر پسورد
 12. web : دسترسی از طریق WebFig
 13. sniff : دسترسی به ابزار های sniff مانند wireless sniffer
 14. sensitive : دسترسی به اطلاعات حساس مثل کاربر های VPN
 15. api : دسترسی api زدن از یک برنامه به روتر
 16. romon : دسترسی به روتر های بعد از این روتر
- در قسمت Skin میتوانید Skin مربوط به این گروه را انتخاب کنید.



The BTest Server Settings dialog box contains the following fields and controls:

- Enabled:** A checkbox that is checked.
- Authenticate:** A checkbox that is checked.
- Allocate UDP Ports From:** A text input field containing the value 2000.
- Max Sessions:** A text input field containing the value 100.
- Buttons:** OK, Cancel, Apply, and Sessions.

به طور پیش فرض در روتر میکروتیک پورت های سرویس های فعال باز است و پورت 2000 که مربوط به Bandwidth Test است. برای امنیت دستگاه باید سرویس هایی که لازم ندارید را غیر فعال کنید و پورت سرویس های فعال خصوصی تان را تغییر دهید. در منو Tools>BTest Server Setting میتوانید Bandwidth Test را غیر فعال کنید یا پورت آن را تغییر دهید.

✓ CAPsMAN

✓ User Manager

✓ Wireless

✓ Interfaces

✓ WireGuard

✓ PPP

✓ Bridge

✓ Mesh

✓ IP

✓ MPLS

✓ IPv6

✓ Routing

✓ System

✓ Queues

✓ Dot1X

✓ Files

✓ Log

✓ RADIUS

✓ Tools

✓ Make Supout...

✓ Undo

✓ Redo

✓ Hide Password

✓ Safe Mode

Design Skin

WinBox

✓ Graphs

✓ End-User Lice...

RouterOS v7.6 (stable) Skin: default Name: My-Skin Save Revert Reset

✓ Quick Set

✓ WebFig

✓ Terminal

✓

✓

✓ Interface

✓ Interface List

✓ Ethernet

✓ EoIP Tunnel

✓ IP Tunnel

✓ GRE Tunnel

✓ VLAN

✓ VXLAN

✓ VRRP

✓ VETH

Interface List

✓ MACsec

✓ Bonding

✓ LTE

✓ VRF

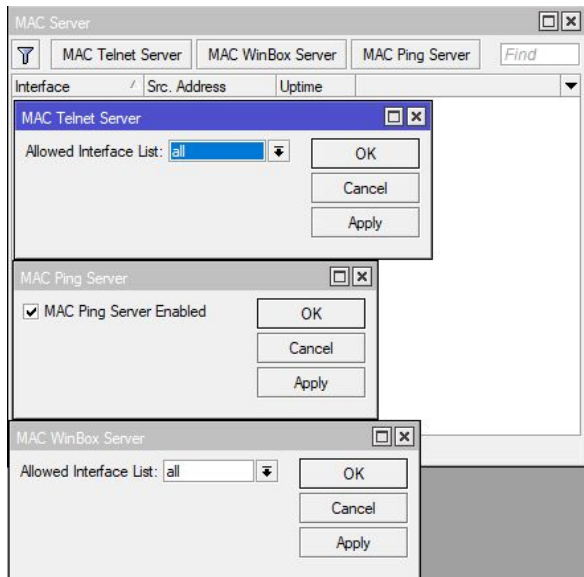
Add New

✓ Detect Internet

2 items

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)	
- D	R	bridge1	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0	
D	R	ether1	Ethernet	1500		32.5 kbps	39.0 kbps	8	59	0 bps	0 bps	0	0	

برای ساختن یک Skin جدید از طریق Web متصل شوید و گزینه Design Skin را انتخاب کنید
در این صفحه می توانید هر منویی که نمیخواهید کاربر آن گروه ببیند را غیر فعال کنید یا با دبل کلیک کردن روی هر گزینه
میتوانید یک عبارت دیگر به جای آن بنویسید.
حتی می توانید منو ها را فارسی کنید.

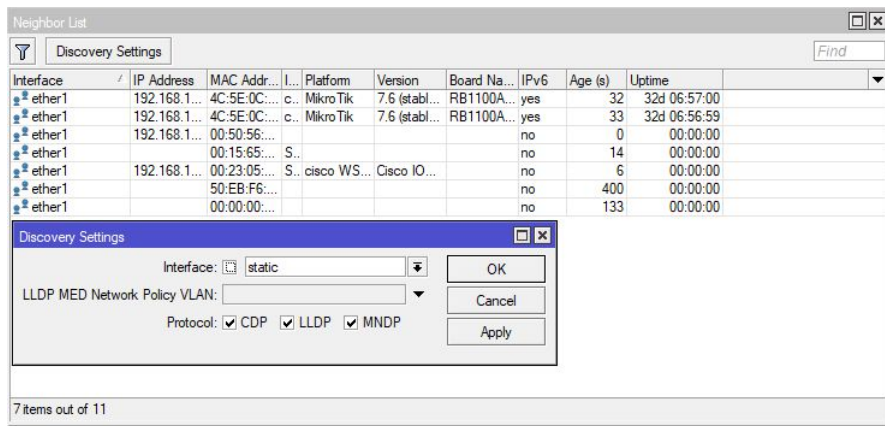


برای کنترل اتصال کاربر از طریق مک آدرس روتر به منو Tools > Mac Server رجوع کنید.
سه روش برای ارتباط با روتر از طریق مک وجود دارد:

1. Mac Telnet: می توانید دسترسی Telnet از طریق مک را با MAC Telnet Server مدیریت کنید. می توانید آن را غیر فعال کنید یا دسترسی آن را فقط به یک Interface List بدهید.
(برای ایجاد Interface List به منو Interface > Interface List مراجعه کنید و پس از ساختن یک لیست، پورت های دلخواه را به آن اضافه کنید)

2. MAC WinBox: برای مدیریت اتصال به WinBox گزینه ی MAX WinBox Server را انتخاب کنید و مانند Mac Telnet تنظیم کنید.

3. MAC Ping: در گزینه MAC Ping Server می توانید MAC Ping را فعال یا غیر فعال کنید.



برای کنترل پروتکل های Neighbor Discovery به منو

Neighbor > IP Settings رجوع کنید و گزینه Discovery Settings را

انتخاب کنید.

می توانید Interface List خاصی را انتخاب کنید و باقی پورت ها را غیر فعال کنید.

می توانید نسبت به VLAN محدود کنید .

و می توانید انتخاب کنید کدام پروتکل های Neighbor Discovery فعال باشد

در منو DNS > IP اگر گزینه Allow Remote Request را فعال کنید کاربرهای دیگر میتوانند به شما درخواست های DNS ارسال کنند.

این مساله خطر DNS Cache Attack را ایجاد می کند.

برای استفاده از Doh یا DNS over Hhttps که باعث امن شدن بسته های DNS و غیرقابل شنود شدن بسته می شود باید گزینه Use Doh Server را فعال کنید و یک DoH Server مانند :

<https://cloudflare-dns/dns-query> انتخاب کنید

برای ایجاد Transparent DNS Cache (یعنی ما بسته های DNS را دریافت کنیم اما به مقصد اصلی تحویل ندهیم و به یک DNS سرور دیگر تحویل دهیم) باید یک DST-Nat ایجاد کنید که بر روی بسته های 53 UDP اعمال شود. حال می توانید این بسته ها را در Action را روش dst-nat به پورت 53 یک DNS Server دیگر ارسال کنید یا با redirect به پورت 53 روتر خودتان تحویل دهید.

برای جلوگیری از Port Scan از ابزار PSD یا Port Scan Detect استفاده می کنیم .
برای این کار یک منگل با Chain از نوع input با prerouting برای پروتکل tcp با شروط مورد نظرتان ایجاد کنید.

حال در تب Extra گزینه PSD را فعال کنید.

Weight Threshold اعتبار برای انجام عمل Port Scan است.

Delay Threshold بازه زمانی برای نظارت به کاربر

Low Port Weight در صورتی که در بازه زمانی پورت های زیر 1024 اسکن شوند این تعداد

واحد از Weight Threshold کم می شود

High Port Weight در صورتی که در بازه زمانی پورت های بالای 1024 اسکن شوند این تعداد

واحد از Weight Threshold کم می شود

هر زمان Weight Threshold تمام شود شرط این Mangle برقرار می شود.

حال یک Action انتخاب میکنیم که روی گزینه add src to address list قرار میدهیم و یک لیست انتخاب می کنیم.

پس از جمع آوری لیست با ایجاد یک Raw Filter می توانید بسته های پورت اسکنر را دراپ کنید بدون آنکه بار زیادی برای روتر داشته باشد .

اگر در Action به جای drop، گزینه tarpit را انتخاب کنید، کانکشن ها را باز نگه میدارد و باعث هنگ کردن سیستم اتکر می شود.

مرحله ی بعدی برای ایجاد امنیت در روتر میکروتیک، خاموش کردن اینترفیس های نالازم و غیر فعال کردن LCD دستگاه از منو مربوطه است.

برای جلوگیری از حمله Brute Force یک منگل ایجاد کنید و در قسمت General شروط مناسب را انتخاب کنید، برای مثال برای جلوگیری از Brute Force در وی پی ان ها می توانید از Output Chain و پروتکل gre استفاده کنید یا از 22 , 23 tcp برای جلوگیری از Brute Force در ssh و telnet.

سپس باید در تب Advanced بخش Content یک قسمت از بسته ای که می خواهید انتخاب کنید را وارد کنید.

چرا که حمله Brute Force به طور مداوم از روتر ما پیام login failed را دریافت می کند.

New Mangle Rule

General Advanced Extra Action Statistics

Layer7 Protocol:

Content: ☒

Connection Bytes:

Connection Rate:

Per Connection Classifier:

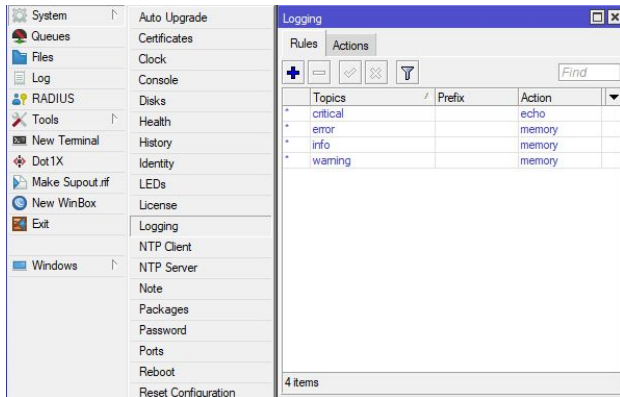
Src. MAC Address:

Out. Bridge Port:

OK Cancel Apply Disable Comment Copy Remove Reset Counters

می توانید کلمه failed را در این قسمت قرار دهید و سپس در Action گزینه add src to address list را انتخاب کنید و آدرس حمله کننده را لیست کنید.

سپس می توانید این لیست را در Raw Filter دراپ کنید. اگر میخواهید برای مثال 3 دفعه به هر کس فرصت بدهید که رمز امتحان کنند باید از منگل 2 بار کپی بگیرید و در هر بار ذکر کنید منگل اعضا لیست از قبل چک شود و در صورتی که یک آدرس در لیست منگل سوم بود دراپ شود.

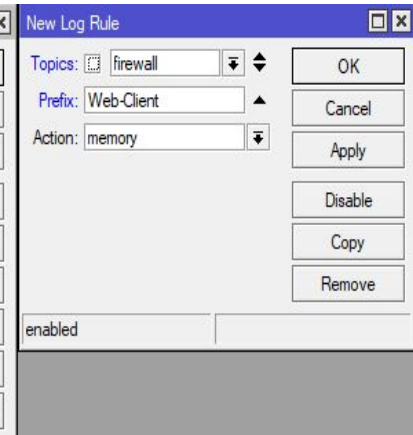
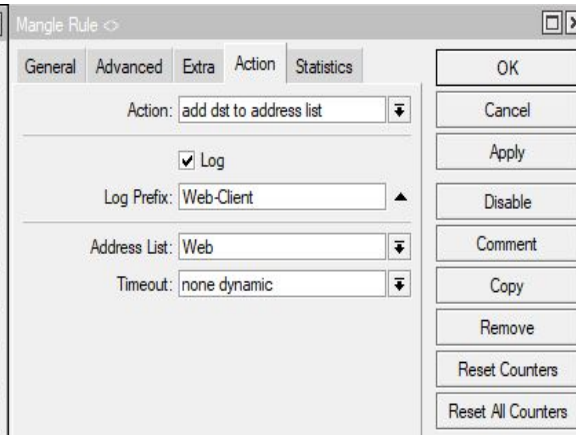
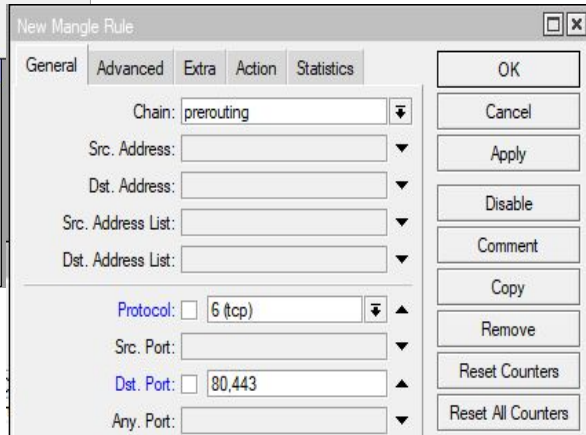
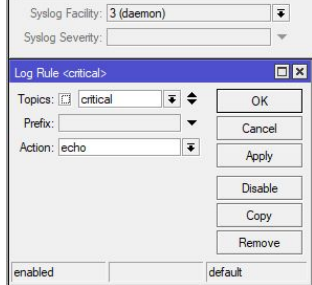
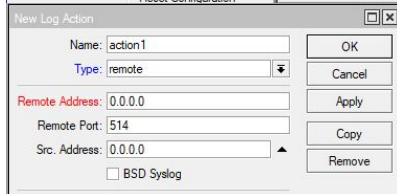


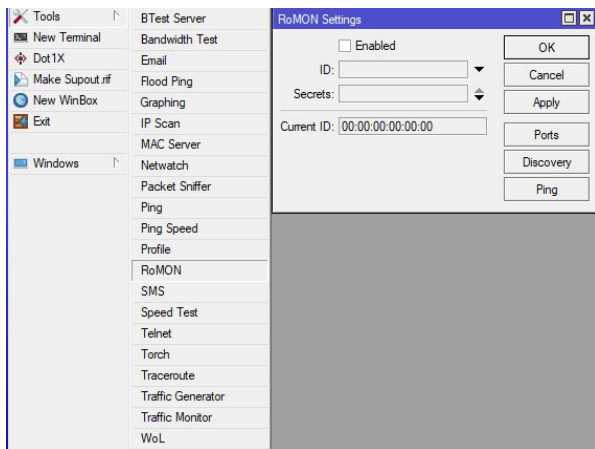
برای مدیریت Log ها به منو **System > Logging** رجوع کنید. در منو **Rules**، دسته ها را داریم و در منو **Action** روش ذخیره سازی های مختلف این دسته بندی ها وجود دارد. می توانید یکی از دسته ها را انتخاب کنید و مسیر ذخیره سازی آن را عوض کنید همچنین می توانید دسته جدیدی اضافه کنید یا می توانید اقدام جدیدی ایجاد کنید.

برای راه اندازی **Syslog Client** روی میکروتیک ابتدا باید یک **Actions** جدید با **Type = remote** ایجاد کنید و سپس گروهی که می خواهید به سرور لاگ بفرستند را باز کنید و **Action** را با **Action** جدیدی که ساخته اید عوض کنید.

برای آنکه لاگ ارتباطات خاصی را بگیرید ابتدا باید با یک منگل ترافیک ها را انتخاب کنید. برای مثال در تصویر زیر ما تمامی ترافیک **Web** یک شبکه را انتخاب کردیم و آدرس های مقصد را جمع آوری کردیم. حالا باید گزینه **Log** را انتخاب کنید و یک **Prefix** برای آن انتخاب کنید.

حالا می توانید در **Logging** یک **Rule** جدید بسازید که **Topics = firewall** و **Prefix** انتخاب شدهتان.

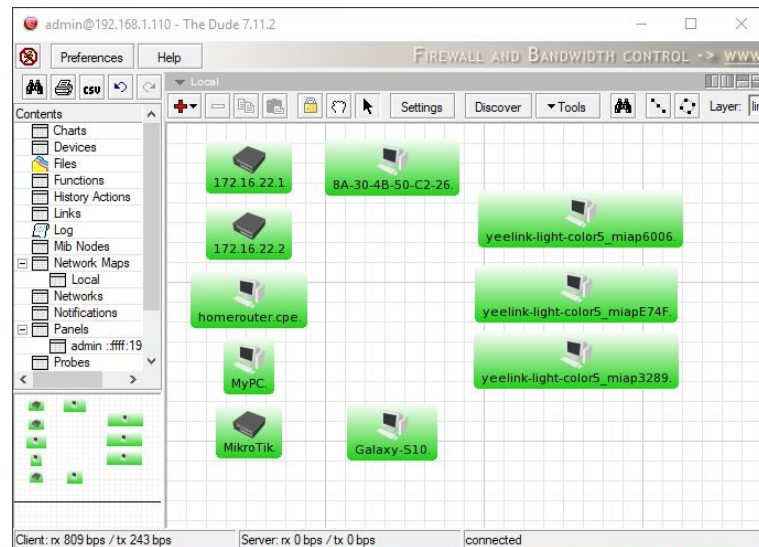
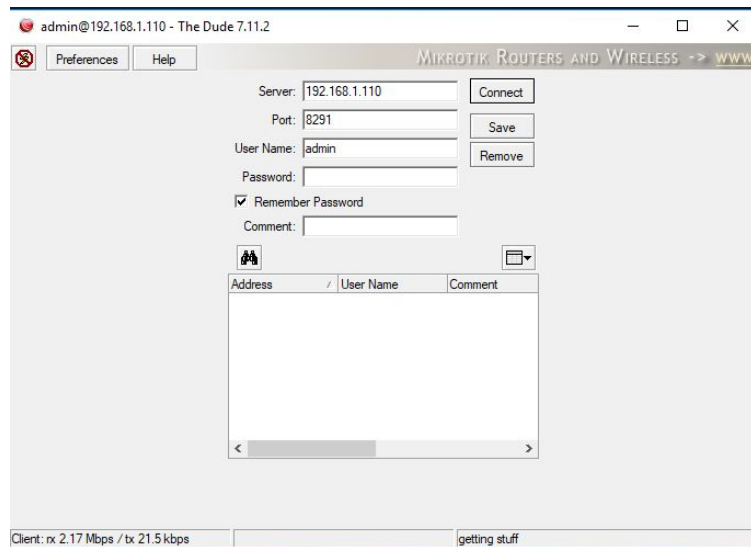




برای فعال سازی Romon بر روی روتر ها به منو Tools > Romon رجوع کنید و گزینه Enable را فعال کنید.

با اینکار با استفاده از گزینه Connect to Romon و وارد کردن آدرس و یوزر پسورد روتر Core تمامی روتر های عضو Romon را در Neighbor ببینید. برای امنیت، میکروتیک توصیه می کند Romon را غیر فعال کنید.

برای راه اندازی Dude ابتدا Extra Package مربوط به نسخه سیستم عامل خود دانلود کنید و پکیج dude را در روتر نصب کنید. سپس در منو Dude>Setting گزینه Enable را فعال کنید. اکنون Dude Client مربوط به نسخه سیستم عامل روتر خود را روی یک ویندوز نصب کنید و به سرور Dude خود متصل شوید.



میکروتیک چند Filter Rule برای روتر و چند Filter Rule برای کلاینت توصیه کرده است که در پایین توضیح میدهم:

۱. پذیرفتن ارتباطات Established و Related :

```
/ip firewall filter add action=accept chain=input connection-state=established,related
```

ارتباطات در چهار وضعیت:

۱. New : ارتباطاتی که تازه شکل گرفته اند

۲. Established : ارتباطاتی که پس از New انجام می شوند.

۳. Related ارتباطاتی که شاخه ای از ارتباط Established هستند

۴. Invalid : ارتباطاتی که منبع آن را نمی دانیم

توصیه میکروتیک این است که برای ارتباطات Established و Related منابع روتر را مصرف نکنیم زیرا در زمان New آنها بررسی شده اند.

تنظیم connection-state در تب General منو های Firewall قرار دارد.

۲. برای دسترسی به روتر یک آدرس لیست مشخص وجود داشته باشد:

```
/ip firewall filter add action=accept chain=input src-address-list=allowed_to_router
```

با تنظیم این فیلتر فقط اعضا لیست allowed_to_router (یا هر نامی که استفاده کرده اید) به روتر دسترسی دارند

۳. پذیرفتن بسته های ICMP (یا هر ترافیک دیگه ای که به سمت روتر لازم دارید) :

```
/ip firewall filter add action=accept chain=input protocol=icmp
```

۴. بستن هر نوع دیگر از ترافیک به سمت روتر :

```
/ip firewall filter add action=drop chain=input
```

برای ایجاد امنیت سمت کاربر هم چندین دستور توصیه شده است :

```
۱./ip firewall filter add action=fasttrack-connection chain=forward comment=FastTrack connection-state=established,related
۲./ip firewall filter add action=accept chain=forward connection-state=established,related
۳./ip firewall filter add action=drop chain=forward connection-state=invalid log=yes log-prefix=invalid
۴./ip firewall filter add action=drop chain=forward dst-address-list=not_in_internet in-interface=bridge1 log=yes
log-prefix=!public_from_LAN out-interface=!bridge1
۵./ip firewall filter add action=drop chain=forward connection-nat-state=!dstnat connection-state=new in-interface=ether1
log=yes log-prefix=!NAT
۶./ip firewall filter add action=drop chain=forward in-interface=ether1 log=yes log-prefix=!public
src-address-list=not_in_internet
۷./ip firewall filter add action=drop chain=forward in-interface=bridge1 log=yes log-prefix=LAN_!LAN
src-address=!192.168.88.0/24
```

۱. بسته های ارتباطات Established و Related را در ترافیک Fast Track قرار بده .

۲. بسته های ارتباطات Established و Related را بپذیر

۳. بسته های ارتباط Invalid را دراپ کن و یک لاگ با Prefix + invalid (یا هر نامی که استفاده می کنید) ایجاد کن.

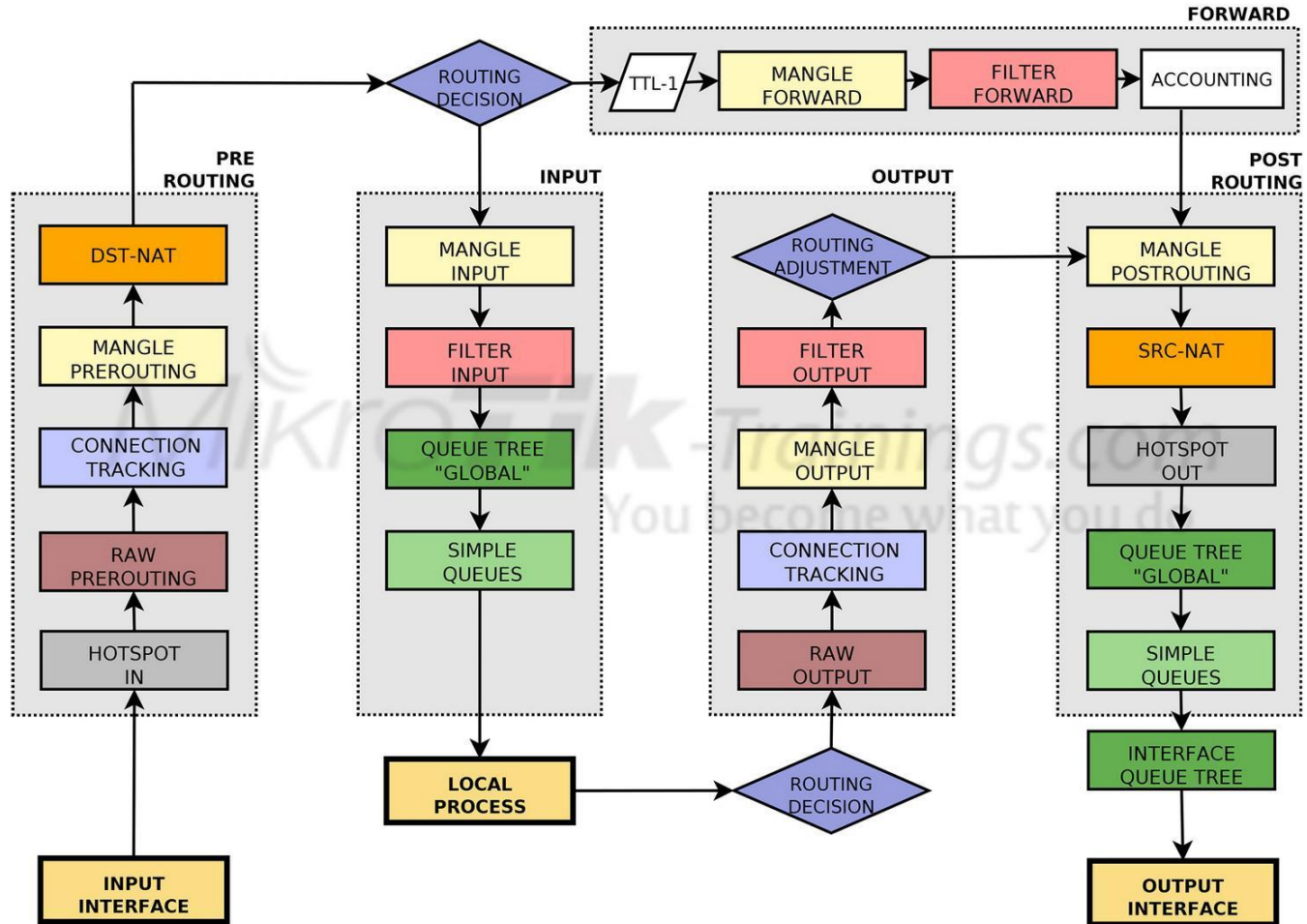
۴. بسته هایی که به سمت اینترنت به مقصد آدرس لیست not_in_internet می روند را دراپ کن. (میتوانید یک لیست به این نام یا هر نامی برای آدرس های ناموجود در اینترنت درست کنید و این فیلتر را ایجاد کنید در پایین لیستی از آدرس های ناموجود را می نویسم)

198.18.0.0/15 - 224.0.0.0/24 - 127.0.0.0/8 - 169.254.0.0/16 - 10.0.0.0/8 - 192.168.0.0/12 - 172.16.0.0/16 - 0.0.0.0/8
192.88.99.0/24 - 240.0.0.0/4 - 100.64.0.0/10 - 203.0.113.0/24 - 198.51.100.0/24 - 192.0.2.0/24 - 192.0.0.0/24 -

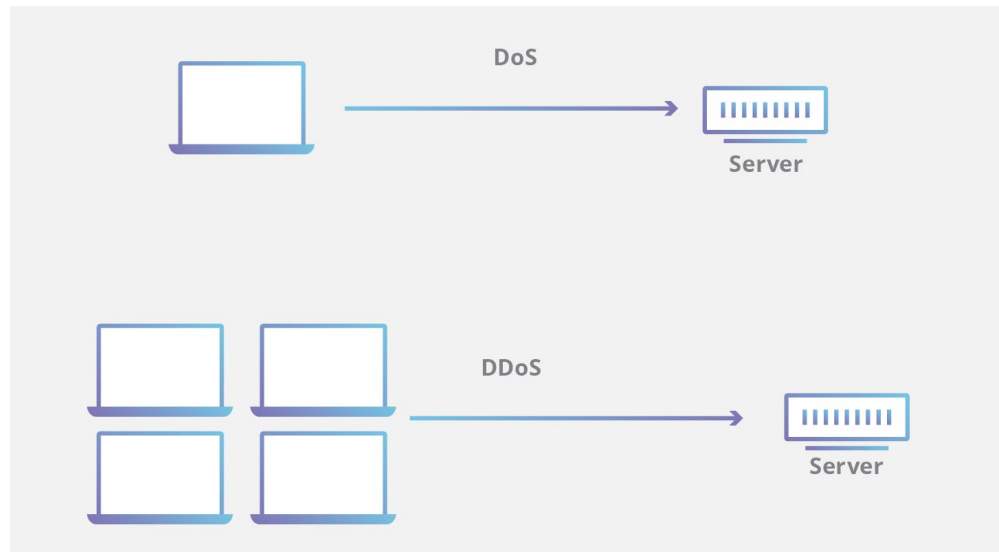
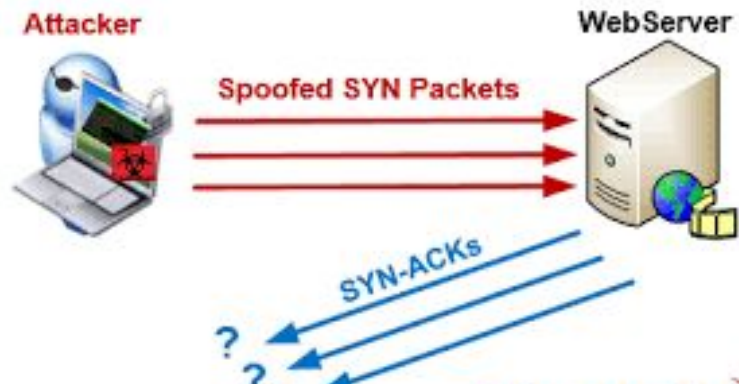
۵. بسته هایی که وضعیت ارتباطشان New باشد ولی وضعیت نت ارتباطشان dstnat نیست را به سمت اینترنت دراپ کن.

۶. بسته هایی که از سمت اینترنت با آدرس های موجود در آدرس لیست not_in_internet به سمت روتر می آیند را دراپ کن.

۷. بسته هایی که با آدرس هایی به غیر از آدرس های شبکه داخلی به سمت روتر می آید را دراپ کن.



حملات TCP SYN Attack با ایجاد کانکشن های زیاد و درگیر کردن منابع انجام می شود. حملات DOS Attack با ارسال بسته های بسیار زیادی مانند بسته های ICMP Request توسط یک کاربر انجام می شود و حملات DDOS Attack با ارسال بسته های زیادی توسط تعداد زیادی کاربر.



جلوگیری از حملات DOS و DDOS باید با استفاده از Raw Filter ها انجام شود تا منابع کمتری از روتر مصرف کند و آسیب کمتری برساند. برای اینکار ابتدا باید بسته های حمله کننده و آدرسی که مورد حمله قرار گرفته است را شناسایی کنید و سپس توسط یک Raw Filter دراپ کنید. برای شناسایی بسته ها باید فیلتر های زیر را ایجاد کنید:

۱. بسته های ورودی به روتر را به Chain جدیدی که ایجاد شده است به نام detect-ddos (یا هر اسمی که استفاده کرده اید.) منتقل کن.

```
/ip firewall filter add action=jump chain=input connection-state=new jump-target=detect-ddos
```

۲. در صورتی که یک آدرس مبدا به یک آدرس مقصد در ۱ ثانیه بیشتر از ۳۲ بسته ارسال کرد شرط را برقرار کن و این بسته را برگردان به ابتدا chain مشخص شده .

```
/ip firewall filter add action=return chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/10s
```

تنظیمات مربوط به dst-limit در تب Extra منو Filter Rule است.

۳. آدرس DST بسته را برای ۱۰ دقیقه به یک آدرس لیست به نام ddos-target در یک لیست ذخیره کن.

```
/ip firewall filter add action=add-dst-to-address-list address-list=ddos-target address-list-timeout=10m chain=detect-ddos
```

۴. آدرس SRC بسته را برای ۱۰ دقیقه به یک آدرس لیست به نام ddos-attackers اضافه کن.

```
/ip firewall filter add action=add-src-to-address-list address-list=ddos-attackers address-list-timeout=10m  
chain=detect-ddos
```

۵. بسته هایی که آدرس فرستنده آنها در لیست ddos-attackers است را با Raw Filter دراپ کن:

```
/ip firewall raw add action=drop chain=prerouting dst-address-list=ddos-target src-address-list=ddos-attackers
```

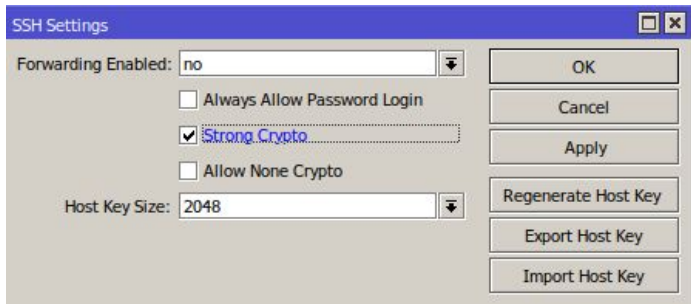
برای جلوگیری از حملات Syn باید بسته ها را شناسایی و با Raw Filter دراپ کنید .
برای این کار فیلتر های زیر را ایجاد کنید:

۱. آدرس ارتباطاتی که از نوع TCP Syn از یک آدرس بیشتر از ۲۰ ارتباط با روتر برقرار کردند را در یک آدرس لیست ذخیره کن

```
/ip firewall filter add action=add-src-to-address-list address-list="SYN Attacker" address-list-timeout=none-dynamic chain=input connection-limit=20,32 protocol=tcp tcp-flags=syn
```

۲. ارتباطاتی که آدرس فرستنده آنها در آدرس لیست بالا است را تارپیت کن.

```
/ip firewall filter add action=tarptit chain=input protocol=tcp src-address-list="SYN Attacker"
```



برای امن تر کردن کلید های ssh به منو IP > SSH رجوع کنید و گزینه Strong Crypto را فعال کنید سپس گزینه

Regenerate Host Key را انتخاب کنید و گزینه Yes را انتخاب کنید سپس یکبار روتر را ری بوت کنید تا کلید عوض شود.

برای جلوگیری از حملات Ping باید فیلتر های زیر را ایجاد کنید :

۱. ارتباطات ICMP ی که در ۱ ثانیه تا ۲ بسته ارسال می کنند را بپذیر:

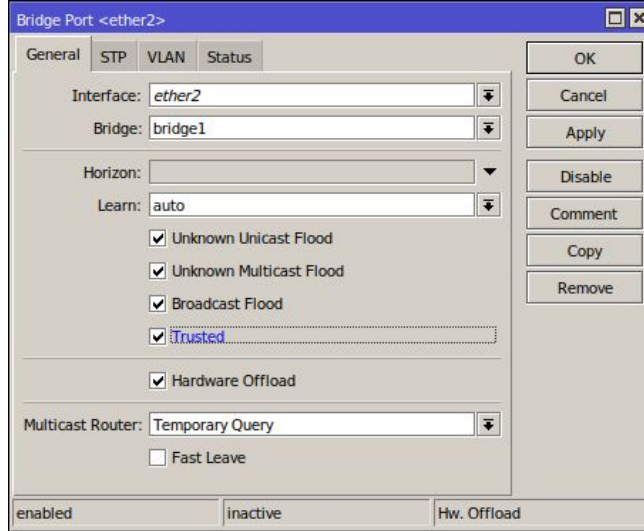
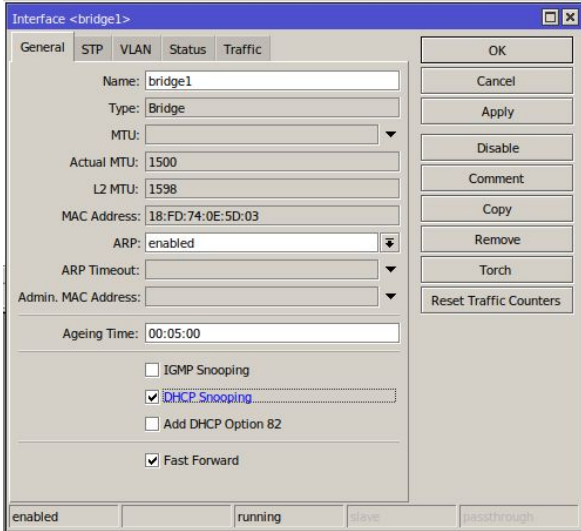
```
/ip firewall filter add action=accept chain=input limit=2,5:packet protocol=icmp
```

۲. ارتباطاتی که از فیلتر بالا عبور کرده اند را دراپ کن.

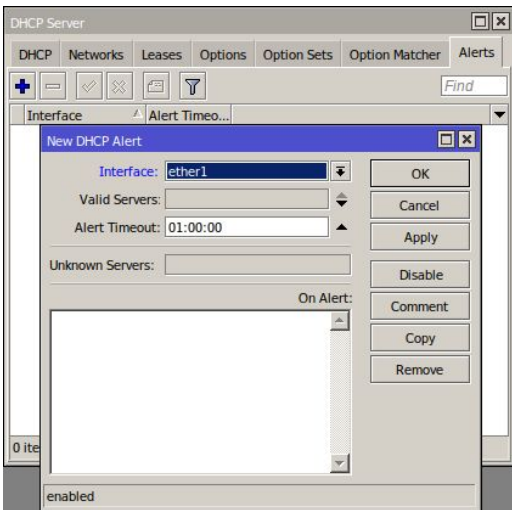
```
/ip firewall filter add action=drop chain=input protocol=icmp
```

۳. بسته های ICMP ی که از نوع Broadcast هستند را دراپ کن.

```
/ip firewall filter add action=drop chain=input dst-address-type=broadcast protocol=icmp
```

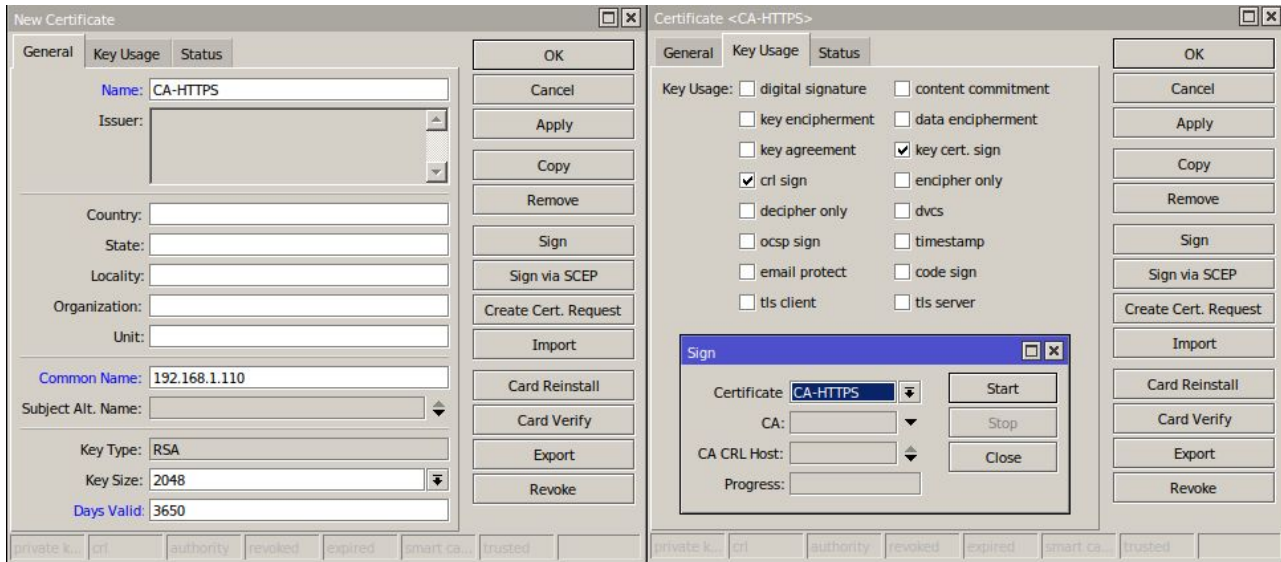


برای جلوگیری از حمله های DHCP
بر روی بریج ها، گزینه ی DHCP
Snooping در تنظیمات Bridge را
فعال کنید و در قسمت پورت در
تنظیمات آن پورتی که به DHCP
Server متصل است (اگر همان
روتر DHCP Server نیست)
گزینه Trusted را فعال کنید.



برای اینکه متوجه شویم چه کسی در شبکه DHCP Server راه اندازی کرده است در منو > IP
DHCP Server به تب Alert بروید و یک Alert جدید اضافه کنید.
Interface : پورتی که قصد دارید Alert بر روی آن فعال شود.
Valid Server : آدرس DHCP Server صحیح شبکه

برای امن کردن WebFig توسط HTTPS باید یک Certificate ایجاد کنید و آن را در Services > IP تنظیم کنید.
برای ایجاد کردن Certificate به منو System > Certificate رجوع کنید و یک Certificate جدید اضافه کنید.
برای انجام این کار به دو Certificate از نوع CA و Server احتیاج داریم.

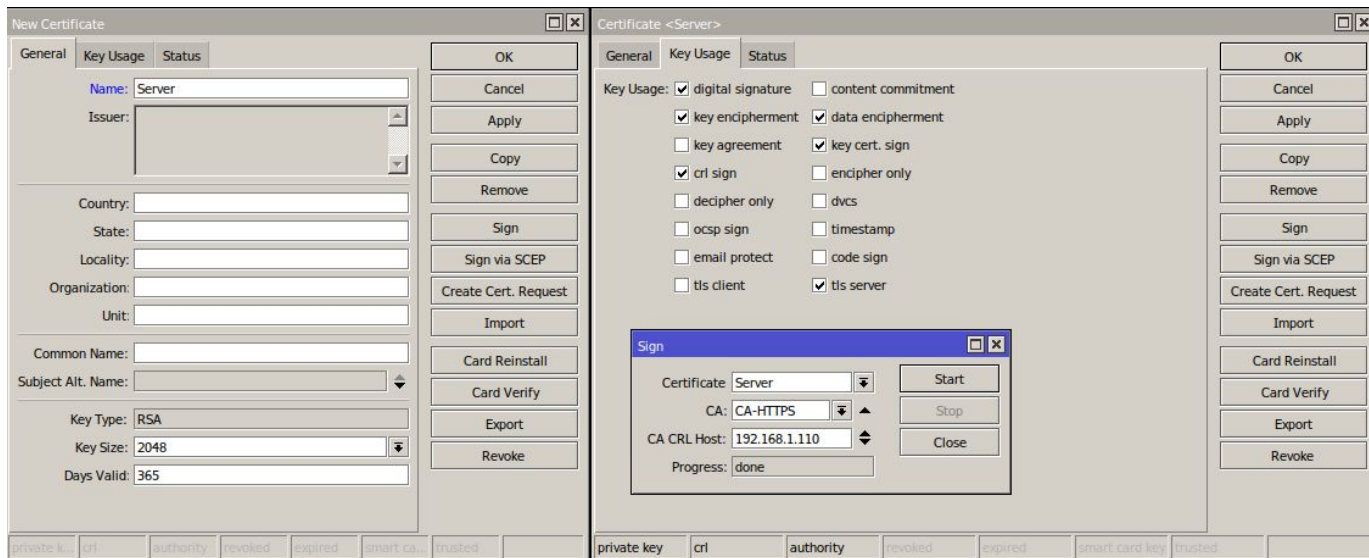


برای ساخت CA

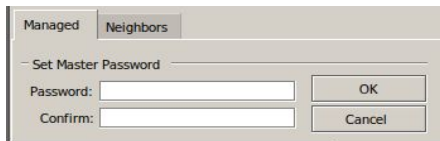
در تب General برای این Certificate یک اسم انتخاب کنید. دیگر گزینه ها انتخابی هستند اما باید گزینه Common Name را با آدرس روتر تنظیم کنید و Days Valid را مشخص کنید که در این مثال ما ۱۰ سال قرار دادیم.
سپس در تب Key Usage باید گزینه های key cert. Sign و crl sign را فعال کنید.

پس از Apply کردن باید این Certificate را Sign کنید. در سمت راست دکمه را فشار دهید در منو Sign باید Certificate خود را مشخص کنید؛ به دلیل آنکه از نوع CA هست گزینه CA را خالی میگذاریم و در CA URL Host باید آی پی روتر را وارد کنید و کلید Sign را فشار دهید.

برای ساخت Certificate از نوع Server باید یک Certificate اضافه کنید .
در تب General برای این Certificate یک اسم انتخاب کنید. دیگر گزینه ها انتخابی هستند اما باید گزینه ی Common Name را با آدرس روتر تنظیم کنید و Days Valid را مشخص کنید که در این مثال ما ۱۰ سال قرار دادیم.
سپس در تب Key Usage گزینه های digital signature , key encipherment , data encipherment , key cert. sign , crl sign , tls server را فعال کنید.



برای Sign کردن سرور باید CA را انتخاب کنید و آدرس را مجددا وارد کنید. در آخر در تب General گزینه Trusted را فعال کنید.



برای امن کردن ارتباطات ذخیره شده در Winbox حتما برای Winbox یک Master Password ذخیره کنید که اطلاعات مشخص نشود.

Port Knocking به فرایندی میگویند که ادمین شبکه برای مجاز شدن ترافیک در روتر انجام میدهد.

فرض کنید میخواهید کل ترافیک های **Input** را ببندید و فقط ادمین شبکه از پشت هر سیستمی که بخواهد دسترسی داشته باشد. برای اینکار ادمین باید یک فرایندی را انجام دهد تا روتر متوجه شود این آدرس ادمین است.

برای انجام این کار باید آدرس ادمین را در یک لیست با شرایط خاص ذخیره کنید. سپس با یک **Rule** دیگر آدرس هایی که در این لیست هستند را چک کنید و اگر شرط برقرار شد، ادمین برای مدت مشخصی دسترسی خواهد داشت.

برای این کار ما از ارتباطات **TCP** استفاده میکنیم و ادمین قبل از گرفتن دسترسی به چند پورت متفاوت کانکشن می زند تا دسترسی برقرار شود. به مثال زیر توجه کنید:

۱. آدرس فرستنده تمام ترافیک های ورودی به مقصد خود روتر با **TCP 1234** را در لیست برای **admin1** برای ۳۰ دقیقه ذخیره کن

```
/ip firewall mangle add action=add-src-to-address-list address-list=admin1 address-list-timeout=\
30m chain=input dst-port=1234 protocol=tcp
```

۲. آدرس فرستنده تمام ترافیک های ورودی به مقصد خود روتر با **TCP 12345** را در لیست برای **admin2** برای ۳۰ دقیقه ذخیره کن

```
/ip firewall mangle add action=add-src-to-address-list address-list=admin2 address-list-timeout=\
30m chain=input dst-port=12345 protocol=tcp src-address-list=admin1
```

۳. ترافیک های ورودی به مقصد خود روتر که آدرس فرستنده آنها در لیست **admin2** است را بپذیر

```
/ip firewall filter add action=accept chain=input dst-address-list=admin2
```

۴. تمام ترافیک های ورودی به روتر را ببند.

```
/ip firewall filter add action=drop chain=input
```