



MTCSE

Chiang Mai , Thailand

5-6 April , 2022

Schedule

- Training day: 9AM - 5PM
- 30min breaks: 10:30AM and 3PM
- 1h lunch: 12:30PM
- Certification test: last day, 1 hour

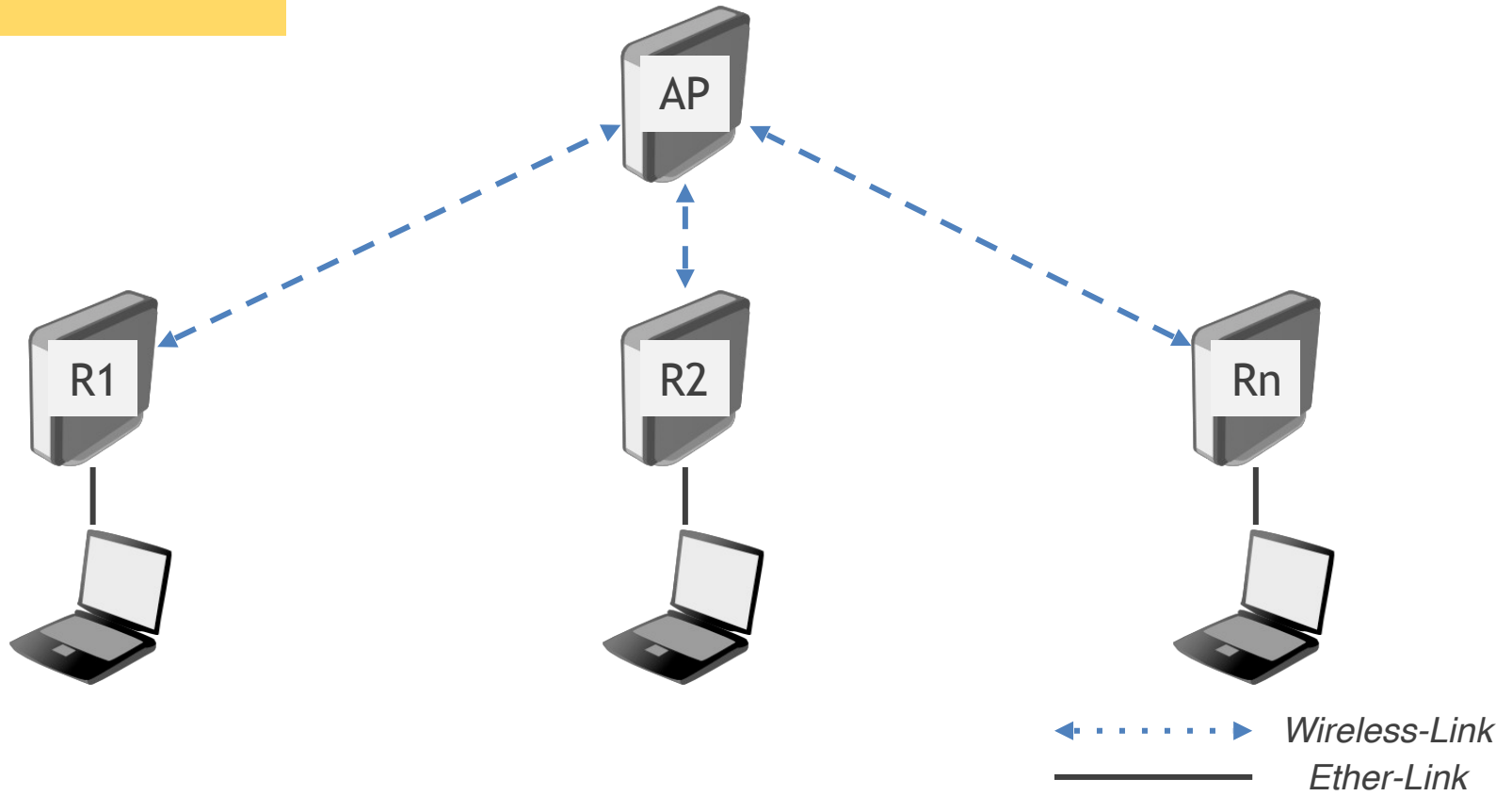
INTRODUCE Trainer

- Mana Kaewcharoen
- MTCNA, MTCTCE, MTCWE
- MTCUME, MTCRE , MTCINE
- MTCIPv6E, MTCSE
- MikroTik Academy Trainer
- MikroTik Trainer



Lab Setup

SSID : .@ VRPro Training
BAND : 2.4 / 5 Ghz
KEY : vrproservice



SECURITY INTRO

What Security is all about?

- Security is about protection of assets.
 - *D. Gollmann, Computer Security, Wiley*
- **Confidentiality** : Protecting personal privacy and proprietary information.
- **Integrity** : Ensuring information non-repudiation and authenticity.
- **Availability** : Ensuring timely and reliable access to and use of information

What Security is all about?

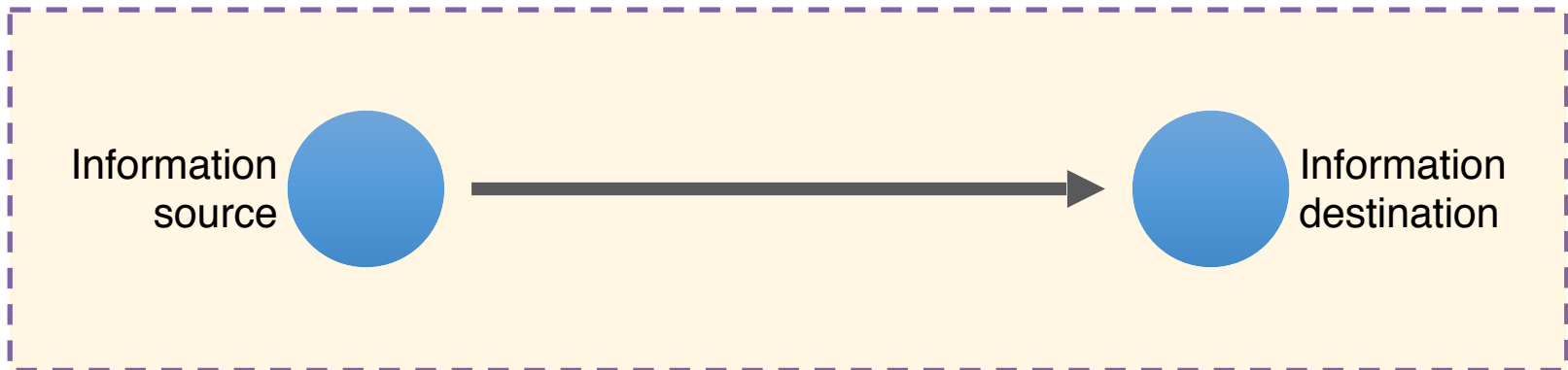
- **Prevention** : take measures that prevent your assets from being damaged (or stolen)
- **Detection** : take measures so that you can detect when, how, and by whom an asset has been damaged
- **Reaction** : take measures so that you can recover your assets

Security Attacks, Mechanisms & Services

- **Security Attack** : Any action that compromises the security of information
- **Security Mechanism** : a process / device that is designed to detect, prevent or recover from a security attack.
- **Security Service** : a service intended to counter security attacks, typically by implementing one or more mechanisms.

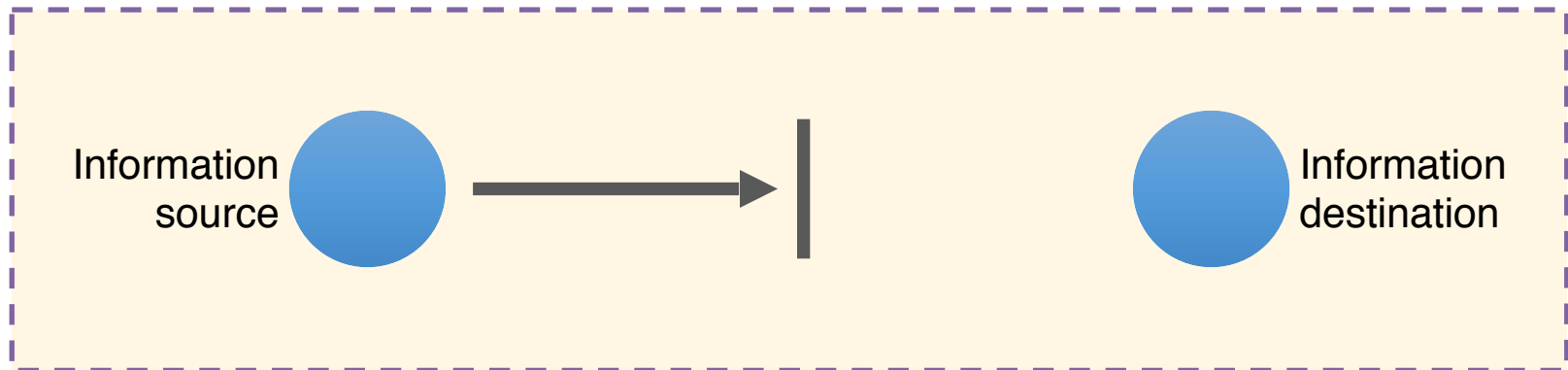
Security Threats / Attacks

NORMAL FLOW



Security Threats / Attacks

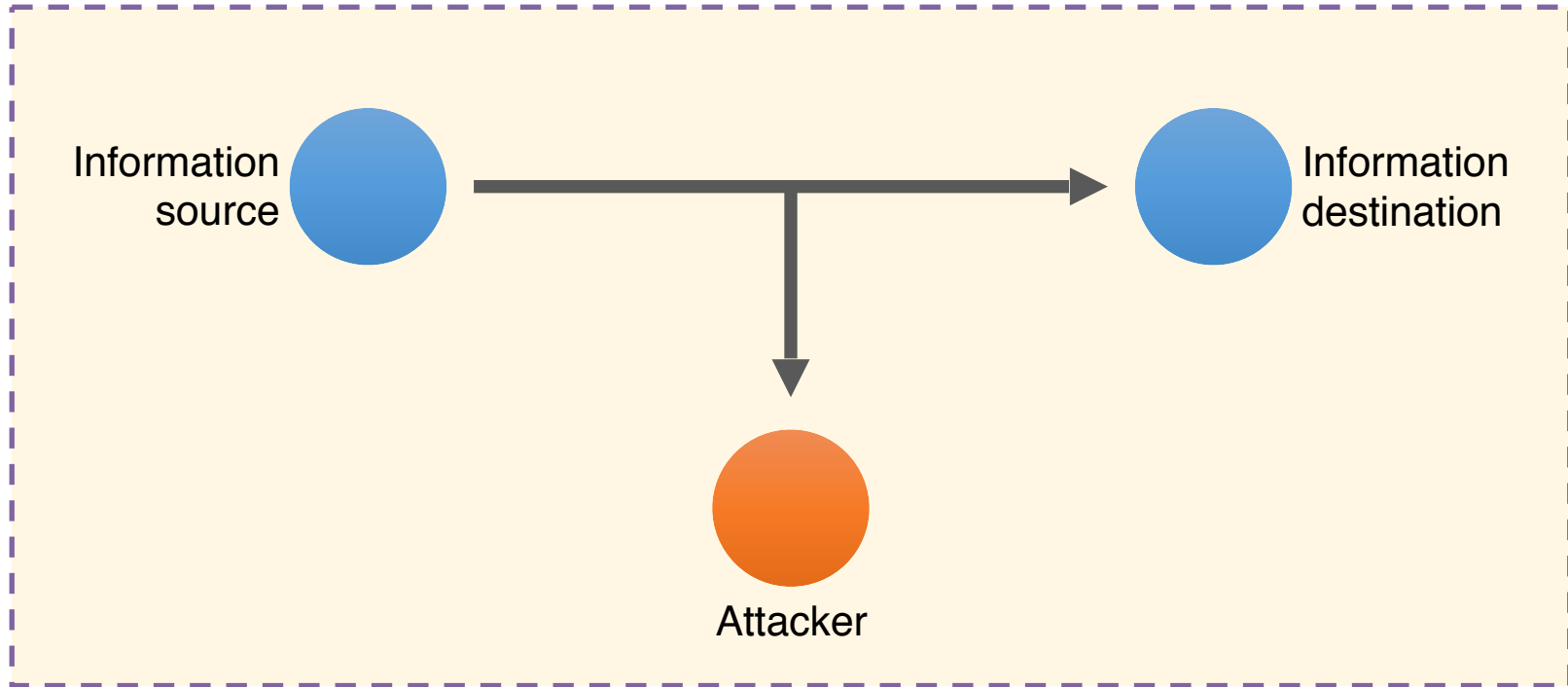
INTERRUPTION



“services or data become unavailable, unusable, destroyed, and so on, such as loss of file, denial of service, etc.”

Security Threats / Attacks

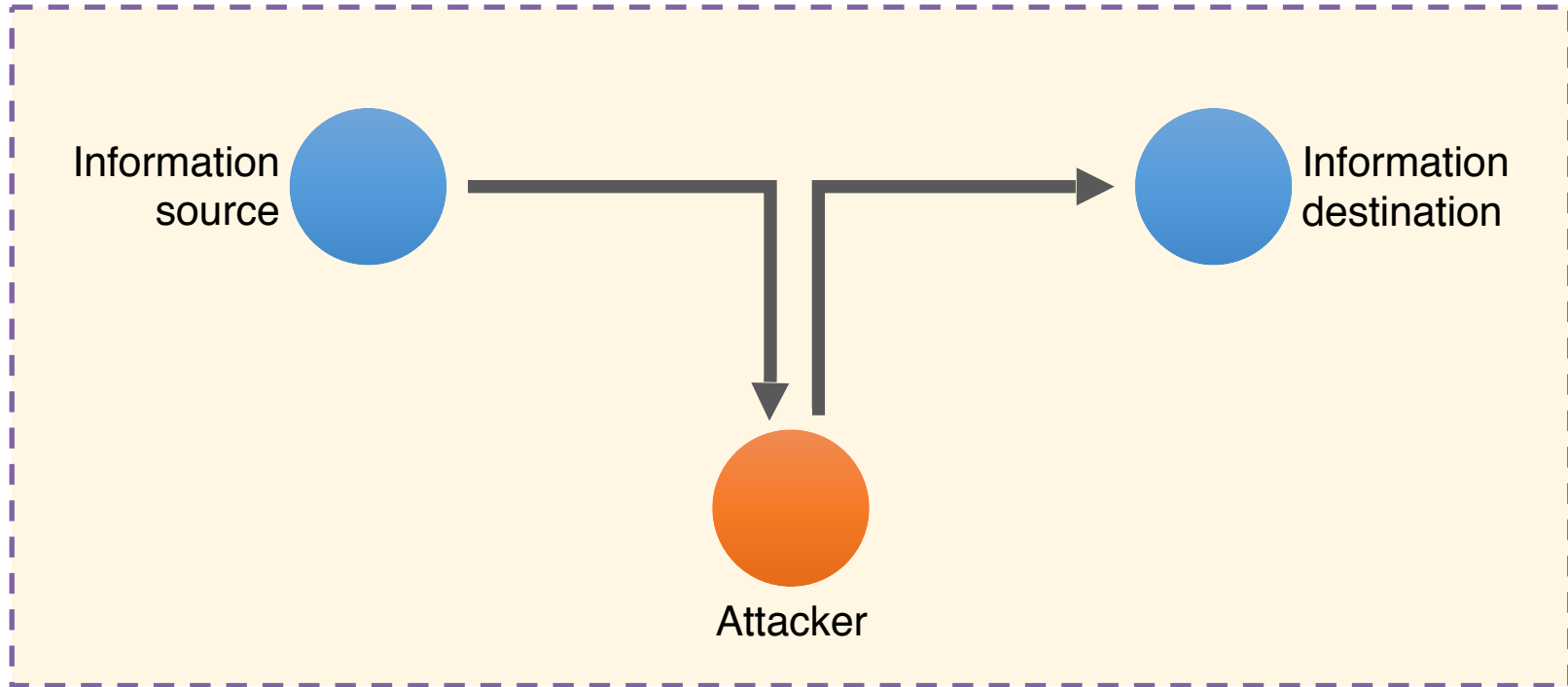
INTERCEPTION



“an unauthorized 3rd party has gained access to an object, such as stealing data, overhearing another's communication, etc.”

Security Threats / Attacks

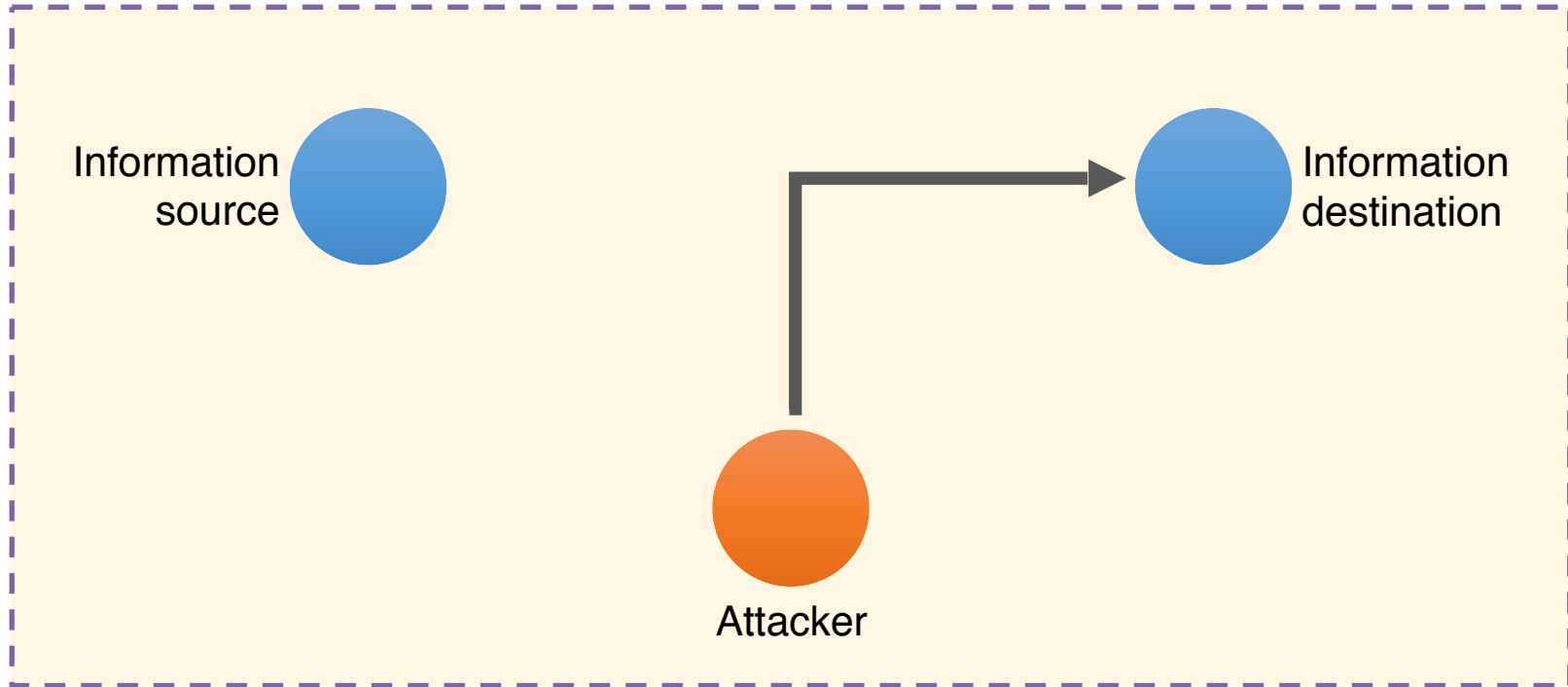
MODIFICATION



unauthorized changing of data or tampering with services, such as alteration of data, modification of messages, etc.

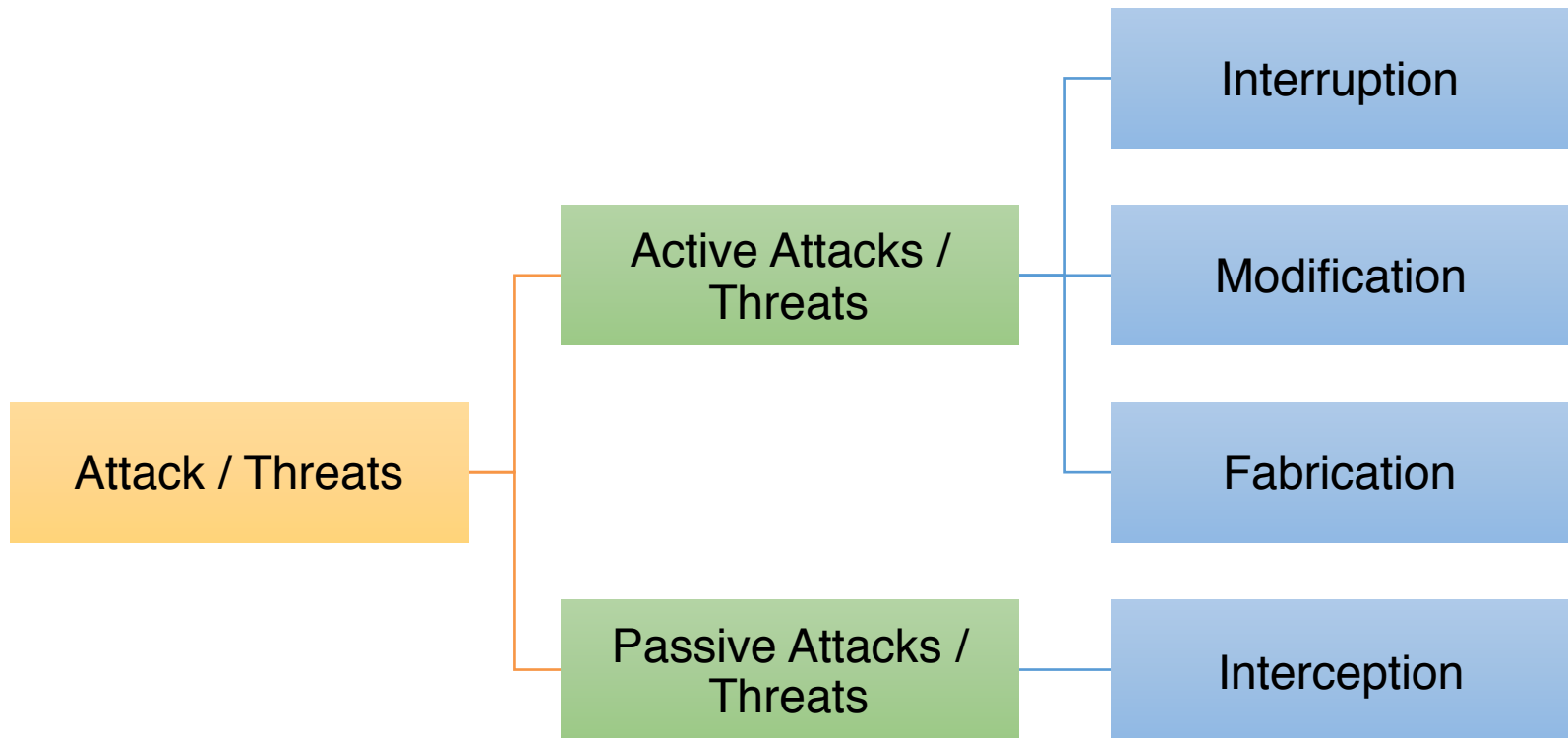
Security Threats / Attacks

FABRICATION



“additional data or activities are generated that would normally not exist, such as adding a password to a system, replaying previously sent messages, etc.”

Type of Threats / Attacks



Security Mechanisms

- **Encryption** : transforming data into something an attacker cannot understand, i.e., providing a means to implement confidentiality, as well as allowing the user to check whether data has been modified.
- **Authentication** : verifying the claimed identity of a user, such as user name, password, etc.
- **Authorization** : checking whether the user has the right to perform the action requested.
- **Auditing** : tracing which users accessed what, when, and which way. In general, auditing does not provide protection, but can be a tool for analysis of problems.

COMMON THREATS

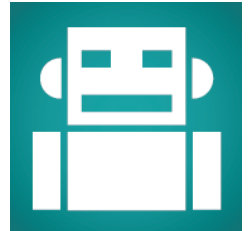
Common Security Threats

Botnet

“Collection of software robots, or 'bots', that creates an army of infected computers (known as ‘zombies’) that are remotely controlled by the originator”

What it can do :

- Send spam emails with viruses attached.
- Spread all types of malware.
- Can use your computer as part of a denial of service attack against other systems.



Common Security Threats

Distributed denial-of-service (*DDoS*)

“A distributed denial-of-service (DDoS) attack — or DDoS attack — is when a malicious user gets a network of zombie computers to sabotage a specific website or server.”

What it can do :

- The most common and obvious type of DDoS attack occurs when an attacker “floods” a network with useless information.
- The flood of incoming messages to the target system essentially forces it to shut down, thereby denying access to legitimate users.



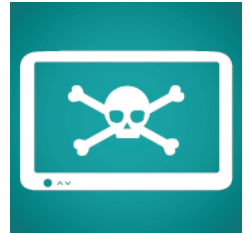
Common Security Threats

Hacking

“Hacking is a term used to describe actions taken by someone to gain unauthorised access to a computer.”

What it can do :

- Find weaknesses (or pre-existing bugs) in your security settings and exploit them in order to access your.
- Install a Trojan horse, providing a back door for hackers to enter and search for your information.



Common Security Threats

Malware

“Malware is one of the more common ways to infiltrate or damage your computer, it’s software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and adware.”

What it can do :

- Intimidate you with scareware, which is usually a pop-up message that tells you your computer has a security problem or other false information.
- Reformat the hard drive of your computer causing you to lose all your information.
- Alter or delete files.
- Steal sensitive information.
- Send emails on your behalf.
- Take control of your computer and all the software running on it.



Common Security Threats

Spam

“Spam is one of the more common methods of both sending information out and collecting it from unsuspecting people.”

What it can do :

- Annoy you with unwanted junk mail.
- Create a burden for communications service providers and businesses to filter electronic messages.
- Phish for your information by tricking you into following links or entering details with too-good-to-be-true offers and promotions.
- Provide a vehicle for malware, scams, fraud and threats to your privacy.



Common Security Threats

Spoofting

“This technique is often used in conjunction with phishing in an attempt to steal your information.”

What it can do :

- Sends spam using your email address, or a variation of your email address, to your contact list.
- Recreates websites that closely resemble the authentic site. This could be a financial institution or other site that requires login or other personal information.



Common Security Threats

Spyware & Adware

“This technique is often used by third parties to infiltrate your computer or steal your information without you knowing it.”

What it can do :

- Collect information about you without you knowing about it and give it to third parties.
- Send your usernames, passwords, surfing habits, list of applications you've downloaded, settings, and even the version of your operating system to third parties.
- Change the way your computer runs without your knowledge.
- Take you to unwanted sites or inundate you with uncontrollable pop-up ads.



Common Security Threats

Trojan Horses

“A malicious program that is disguised as, or embedded within, legitimate software. It is an executable file that will install itself and run automatically once it's downloaded.”

What it can do :

- Delete your files.
- Use your computer to hack other computers.
- Watch you through your web cam.
- Log your keystrokes (such as a credit card number you entered in an online purchase).
- Record usernames, passwords and other personal information.



Common Security Threats

Virus

“Malicious computer programs that are often sent as an email attachment or a download with the intent of infecting your computer.”

What it can do :

- Send spam.
- Provide criminals with access to your computer and contact lists.
- Scan and find personal information like passwords on your computer.
- Hijack your web browser.
- Disable your security settings.
- Display unwanted ads.



Common Security Threats

Worm

“A worm, unlike a virus, goes to work on its own without attaching itself to files or programs. It lives in your computer memory, doesn't damage or alter the hard drive and propagates by sending itself to other computers in a network.”

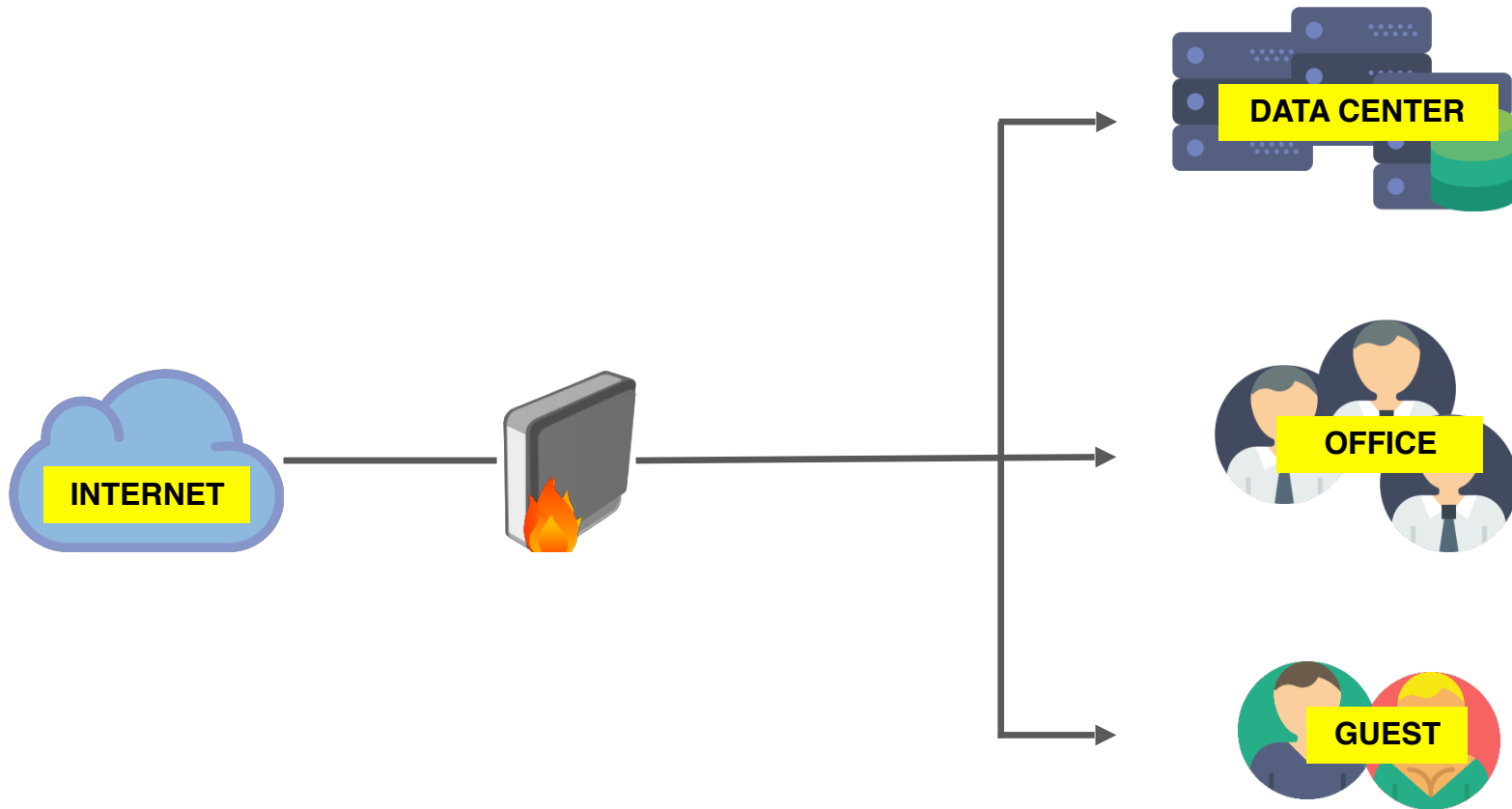
What it can do :

- Spread to everyone in your contact list.
- Cause a tremendous amount of damage by shutting down parts of the Internet, wreaking havoc on an internal network and costing companies enormous amounts of lost revenue.



MIKROTIK SECURITY DEPLOYMENT

MikroTik as a Global Firewall Router



MikroTik as a Global Firewall Router

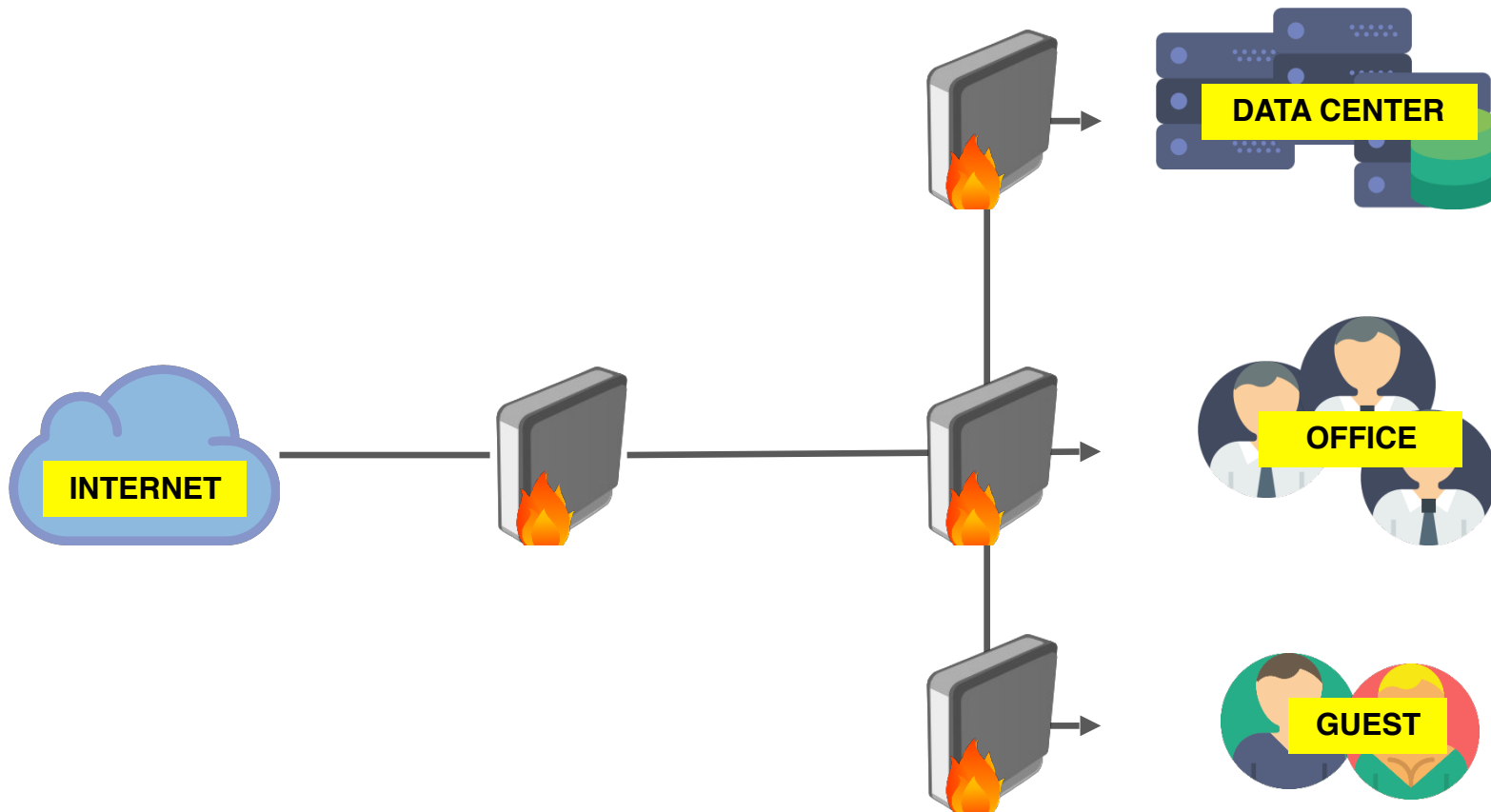
Pro's

- Simple topology
- Easy to manage

Con's

- Concentrate in one single-point-of-failure
- Demands high resources

MikroTik as a Specific Router Firewall



MikroTik as a Specific Router Firewall

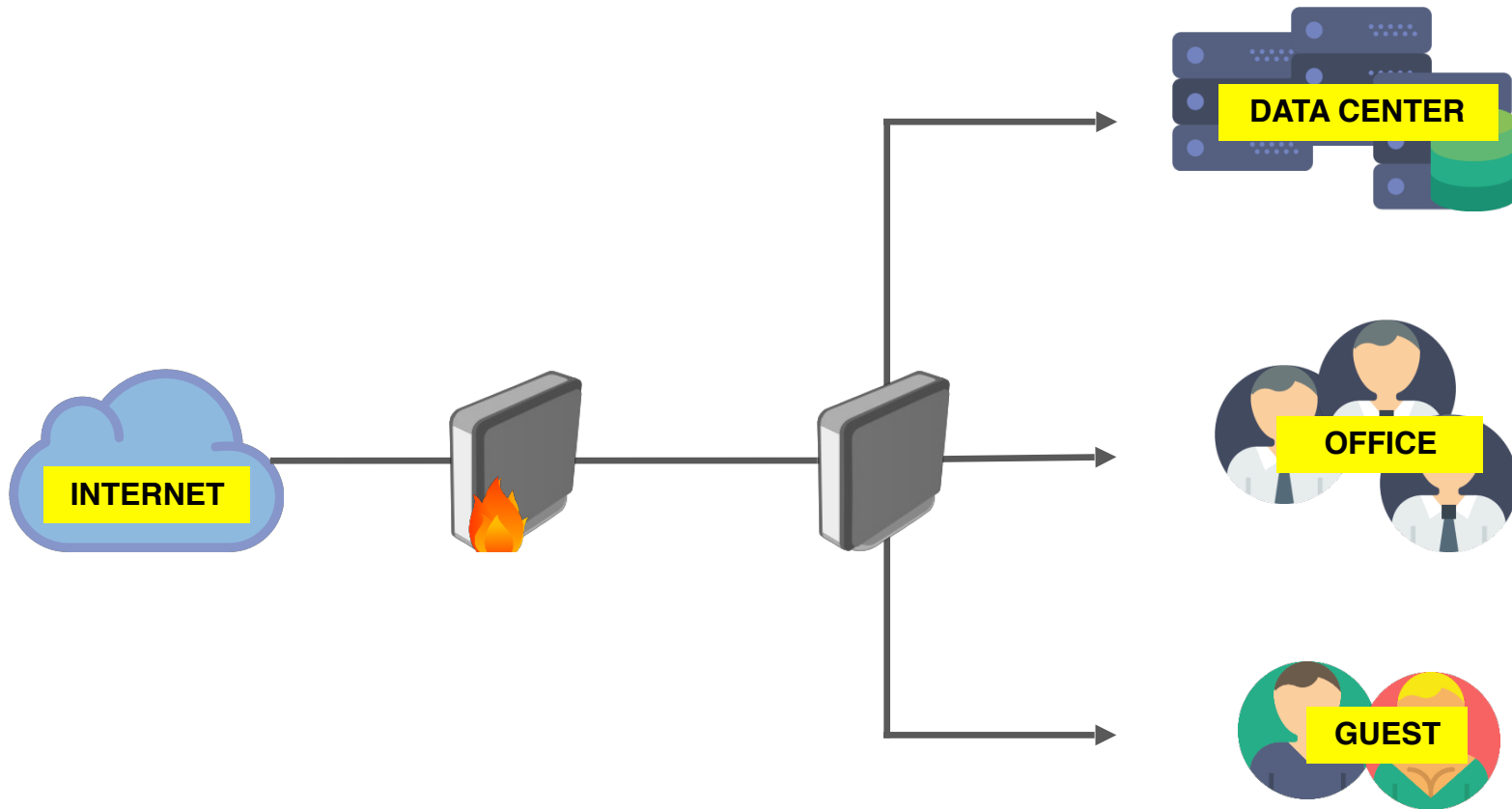
Pro's

- Less resource consumption on each router
- Only focusing security firewall on each network

Con's

- Different network segment, different treatment
- Need to configure firewall differently on each router
- Possible to configure double firewall rules on one another's routers

MikroTik as an IPS



MikroTik as an IPS

Pros

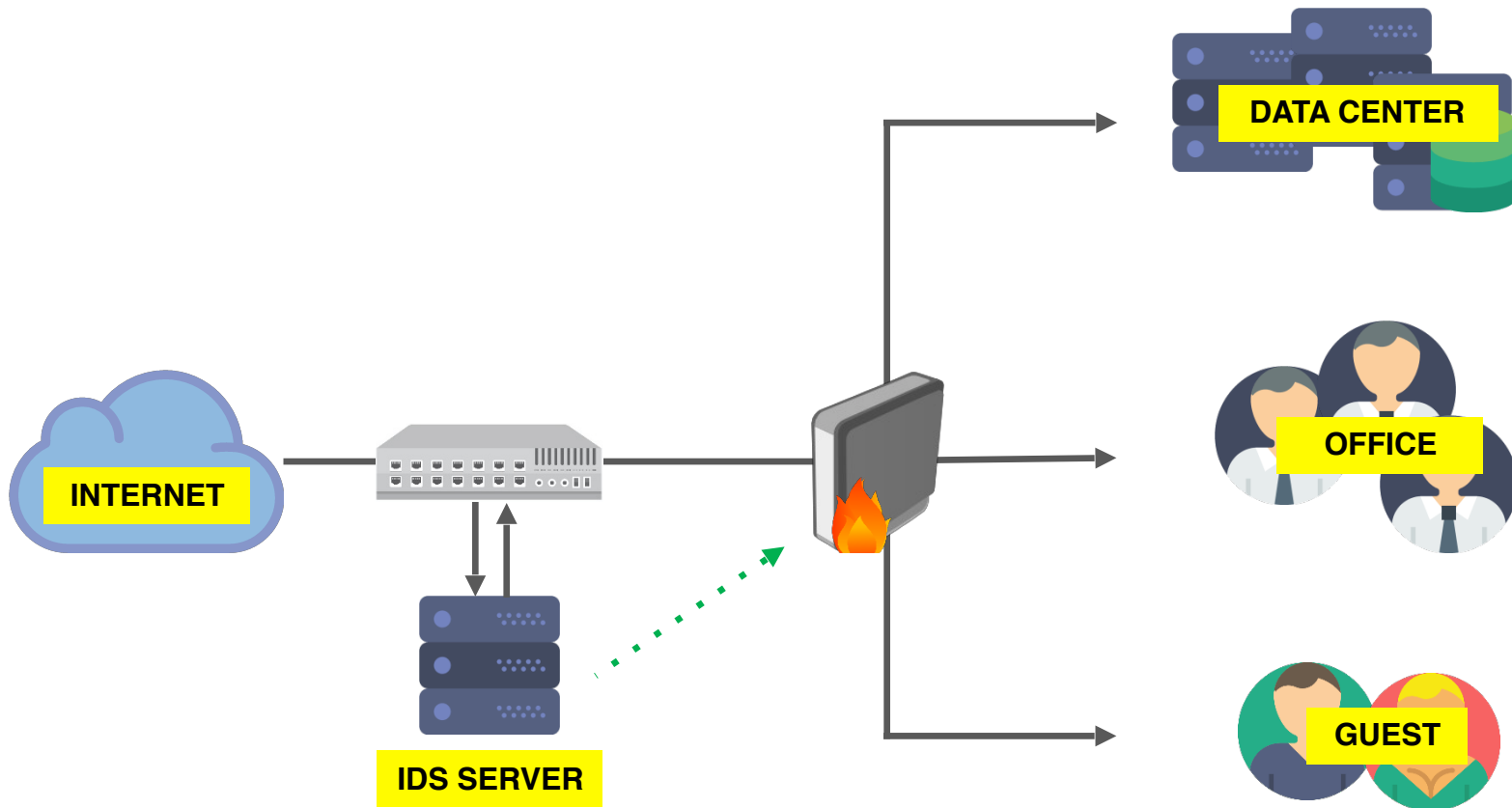
- Clean firewall configuration on router, because all firewall configuration already defined on an IPS** router

Cons

- Need high resource Device on MikroTik as an IPS

**Intrusion Prevention System ??

MikroTik with IDS as a trigger



MikroTik with IDS as a trigger

Pro's

- All firewall rules are made automatically by API from IDS server

Con's

- Need additional device for triggering by bad traffic
- Need powerful device for mirroring all traffic from networks
- Need special scripting for sending information to router
- Expensive

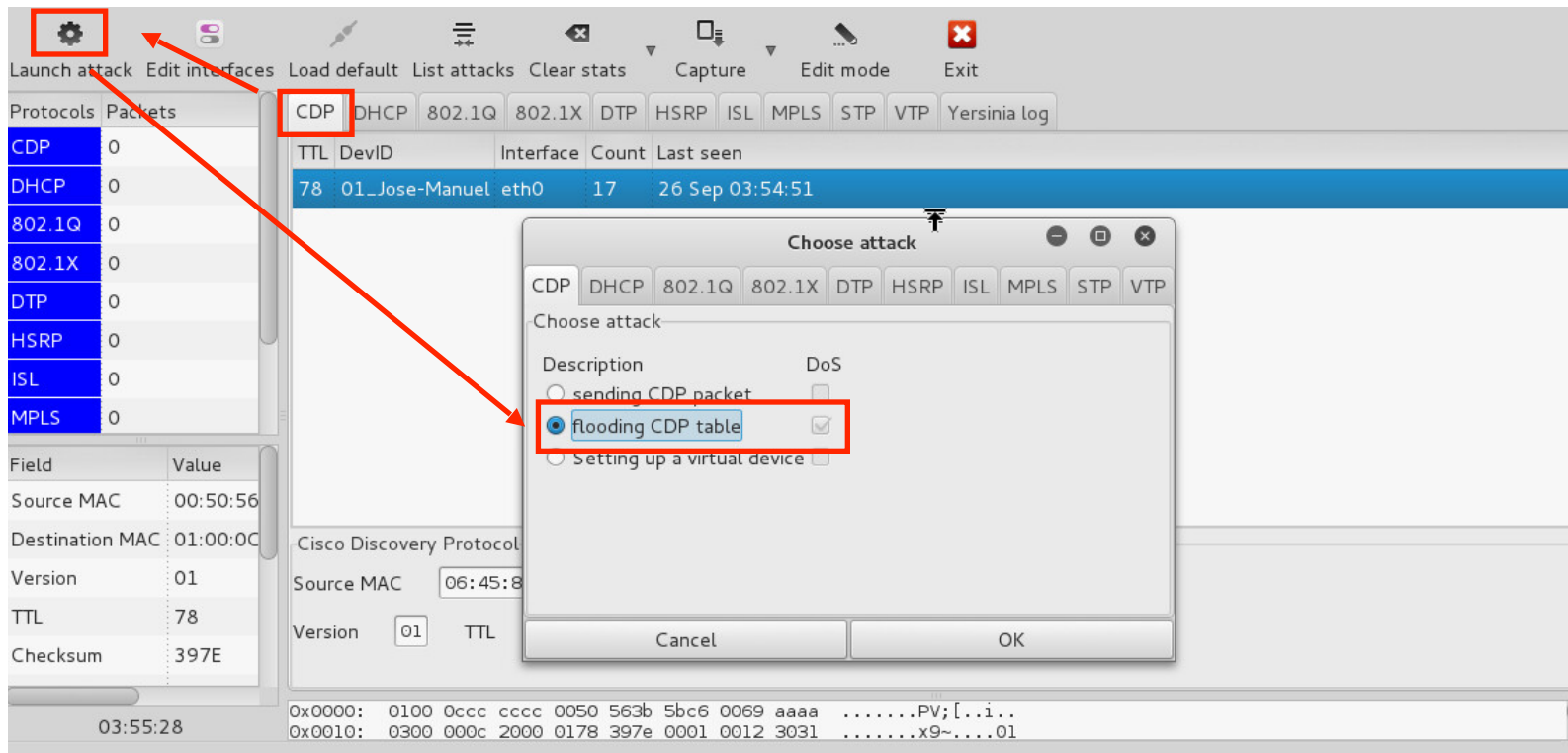
OSI LAYER ATTACKS

MikroTik Neighbor Discovery Protocol

- MikroTik Neighbor Discovery protocol (MNDP) allows to "find" other devices compatible with MNDP or CDP (Cisco Discovery Protocol) or LLDP in Layer2 broadcast domain.
- works on interfaces that support IP protocol and have at least one IP address and on all ethernet-like interfaces even without IP addresses
- is enabled by default for all new Ethernet-like interfaces
- uses UDP protocol port 5678

MNDP Attack

- This tool will be sending a lot of “fake” CDP neighbors to the RouterOS device.



MNDP Attack

- RouterOS is receiving information about thousands of “fake” neighbor devices.

Neighbor List

Discovery Settings Find

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
ether2-UPSTR...	46.154.246.82	E2:0D:AC:05:9E:52	0V00000	yersinia	0.7.3		no	117	00:00:00
ether2-UPSTR...	21.108.167.41	7C:F9:43:4A:09:C8	GXXXXXX	yersinia	0.7.3		no	31	00:00:00
ether2-UPSTR...	3.76.110.72	14:D6:B1:6D:07:0F	7KKKKKK	yersinia	0.7.3		no	20	00:00:00
ether2-UPSTR...	12.2.232.99	38:5E:76:4D:7D:BC	O66666J	yersinia	0.7.3		no	24	00:00:00
ether2-UPSTR...	30.226.179.0	15:B9:1D:06:24:68	ASSSSS6	yersinia	0.7.3		no	44	00:00:00
ether2-UPSTR...	44.197.156.29	A9:D9:27:71:2A:3A	EESSSS	yersinia	0.7.3		no	101	00:00:00
ether2-UPSTR...	13.75.247.115	25:91:9C:12:E4:96	666666J	yersinia	0.7.3		no	25	00:00:00
ether2-UPSTR...	46.230.114.54	0C:A0:1D:06:3B:EF	NNNNNN1	yersinia	0.7.3		no	120	00:00:00
ether2-UPSTR...	3.116.162.36	91:7C:84:38:B3:AC	BBBBBT	yersinia	0.7.3		no	20	00:00:00
ether2-UPSTR...	26.83.20.72	0D:EC:6F:61:2E:0E	CCPPPP	yersinia	0.7.3		no	36	00:00:00
ether2-UPSTR...	45.232.20.20	F3:4E:9D:61:62:88	4KKKKKK	yersinia	0.7.3		no	112	00:00:00
ether2-UPSTR...	27.121.134.114	08:2E:88:6B:42:86	QQQ5555	yersinia	0.7.3		no	38	00:00:00
ether2-UPSTR...	9.1.125.35	94:94:4F:49:29:4C	1HHHHHH	yersinia	0.7.3		no	22	00:00:00
ether2-UPSTR...	2.18.198.24	D3:55:0B:22:BA:65	3GGGGGG	yersinia	0.7.3		no	19	00:00:00
ether2-UPSTR...	8.15.127.111	EF:CE:91:14:4E:F6	1IIIIII	yersinia	0.7.3		no	22	00:00:00

204624 items out of 2490525

MNDP Attack

- It's exhausting the resources of the router and impacting the performance

Profile (Running)

CPU: `cpu0` [Start] [Stop]

`tool profile freeze-frame-interval=1` [New Window]

Name	CPU	Usage
cpu0		100.0
ethernet	0	0.0
management	0	100.0
profiling	0	0.0

Resources

Uptime: 02:16:21 [OK]

Free Memory: 359.1 MiB [PCI]

Total Memory: 1010.9 MiB [USB]

CPU: Intel(R) [CPU]

CPU Count: 1 [IRQ]

CPU Frequency: 2294 MHz [RPS]

CPU Load: 100 % [Hardware]

Free HDD Space: 7.4 MiB

Total HDD Size: 56.5 MiB

Sector Writes Since Reboot: 392

Total Sector Writes: 392

Architecture Name: x86

`system resource cpu print`

Version: 6.42.5 (stable)

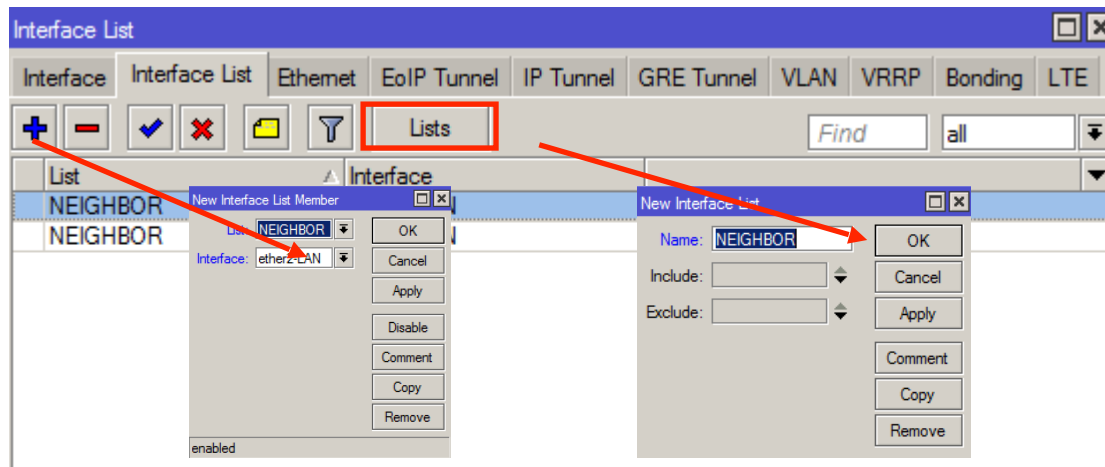
Build Time: Jun/26/2018 12:12:08

Preventing MNDP Attacks

- To prevent such attacks we must select which interfaces can communicate using MNDP/CDP/LLDP.
- Creating “interface-list” and selecting which interfaces to enable neighbor discovery on (MNDP)

MNDP Attack

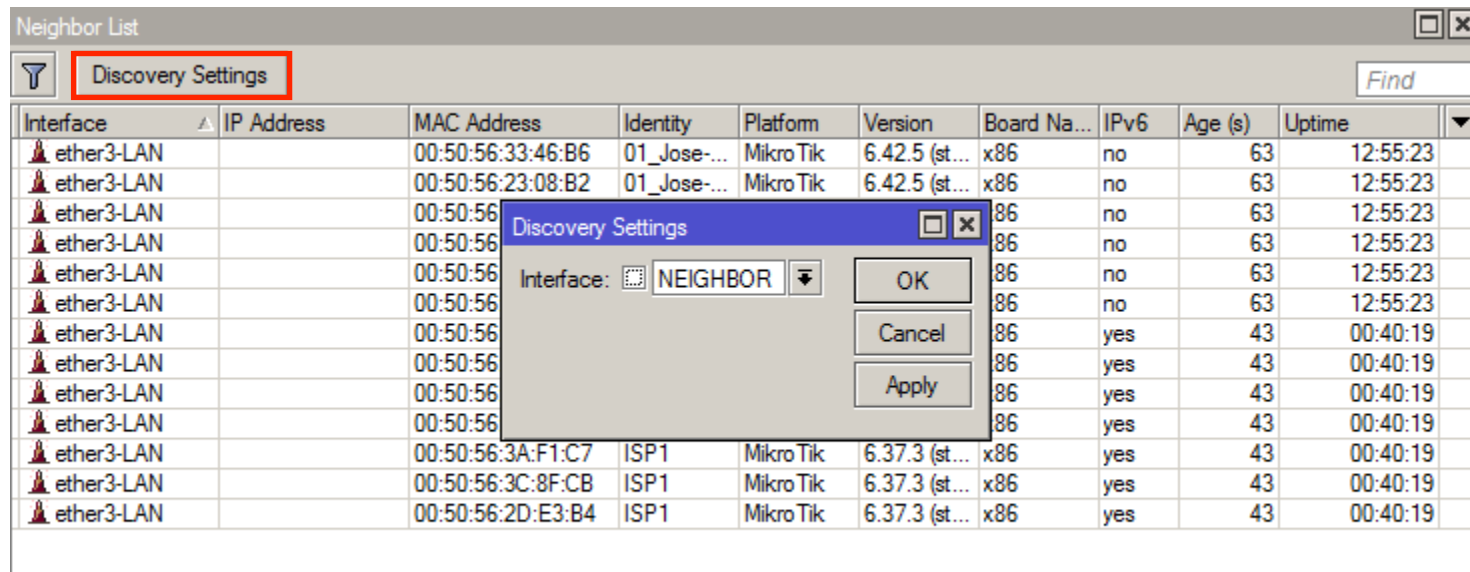
- Creating “interface-list” for accessing MikroTik Neighbor Discovery Protocol



```
/interface list add name=NEIGHBOR  
/interface list member  
add interface=etherX list=NEIGHBOR  
add interface=etherY list=NEIGHBOR
```

MNDP Attack

- IP > Neighbors and set Discovery Settings to previous “interface-list been made.



The screenshot shows the Mikrotik Neighbor List window. The 'Discovery Settings' button is highlighted with a red box. A dialog box titled 'Discovery Settings' is open, showing the 'Interface' dropdown menu set to 'NEIGHBOR'. The dialog has 'OK', 'Cancel', and 'Apply' buttons.

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
ether3-LAN		00:50:56:33:46:B6	01_Jose...	MikroTik	6.42.5 (st...	x86	no	63	12:55:23
ether3-LAN		00:50:56:23:08:B2	01_Jose...	MikroTik	6.42.5 (st...	x86	no	63	12:55:23
ether3-LAN		00:50:56:...				x86	no	63	12:55:23
ether3-LAN		00:50:56:...				x86	no	63	12:55:23
ether3-LAN		00:50:56:...				x86	no	63	12:55:23
ether3-LAN		00:50:56:...				x86	no	63	12:55:23
ether3-LAN		00:50:56:...				x86	no	63	12:55:23
ether3-LAN		00:50:56:...				x86	yes	43	00:40:19
ether3-LAN		00:50:56:...				x86	yes	43	00:40:19
ether3-LAN		00:50:56:...				x86	yes	43	00:40:19
ether3-LAN		00:50:56:...				x86	yes	43	00:40:19
ether3-LAN		00:50:56:3A:F1:C7	ISP1	MikroTik	6.37.3 (st...	x86	yes	43	00:40:19
ether3-LAN		00:50:56:3C:8F:CB	ISP1	MikroTik	6.37.3 (st...	x86	yes	43	00:40:19
ether3-LAN		00:50:56:2D:E3:B4	ISP1	MikroTik	6.37.3 (st...	x86	yes	43	00:40:19

```
/ip neighbor discovery-settings set discover-interface-list=NEIGHBOR
```

DHCP Starvation Attack

- An attack that works by broadcasting DHCP requests with spoofed MAC addresses.
- DHCP starvation attack targets DHCP servers whereby forged DHCP requests are crafted by an attacker with the intent of exhausting all available IP addresses that can be allocated by the DHCP server

DHCP Starvation Attack

- This tool sends multiple “fake” DHCP requests to the router

The screenshot shows a network tool interface with a 'Choose attack' dialog box open. The 'DHCP' tab is selected in the dialog, and the 'sending DISCOVER packet' option is chosen. The main interface shows a table of protocols and packets, with 'DHCP' highlighted. The 'Dynamic Host Configuration' section is visible, showing fields for SIP, Op, Htype, CI, and CH. The 'Flags' field is set to 8000. The interface also includes a menu bar with options like 'Launch attack', 'Edit interfaces', 'Load default', 'List attacks', 'Clear stats', 'Capture', 'Edit mode', and 'Exit'. A gear icon in the top left corner is highlighted with a red box, and a red arrow points from it to the 'DHCP' tab in the 'Choose attack' dialog.

Protocols	Packets
CDP	0
DHCP	0
802.1Q	0
802.1X	0
DTP	0
HSRP	0
ISL	0
MPLS	0

SIP	DIP	MessageType	Interface	Count	Last seen
192.168.1.254	192.168.1.1	03 REQUEST	eth0	1	26 Sep 14:51:52
192.168.1.1	192.168.1.254	05 ACK	eth0	1	26 Sep 14:51:52

Field	Value
Source MAC	00:0C:29
Destination MAC	00:50:56
SIP	192.168.
DIP	192.168.
SPort	68

Dynamic Host Configuration	
Source MAC	02:48:33:
SIP	0.0.0.0
Op	01
Htype	01
CI	0.0.0.0
CH	02:48:33:66:02:51

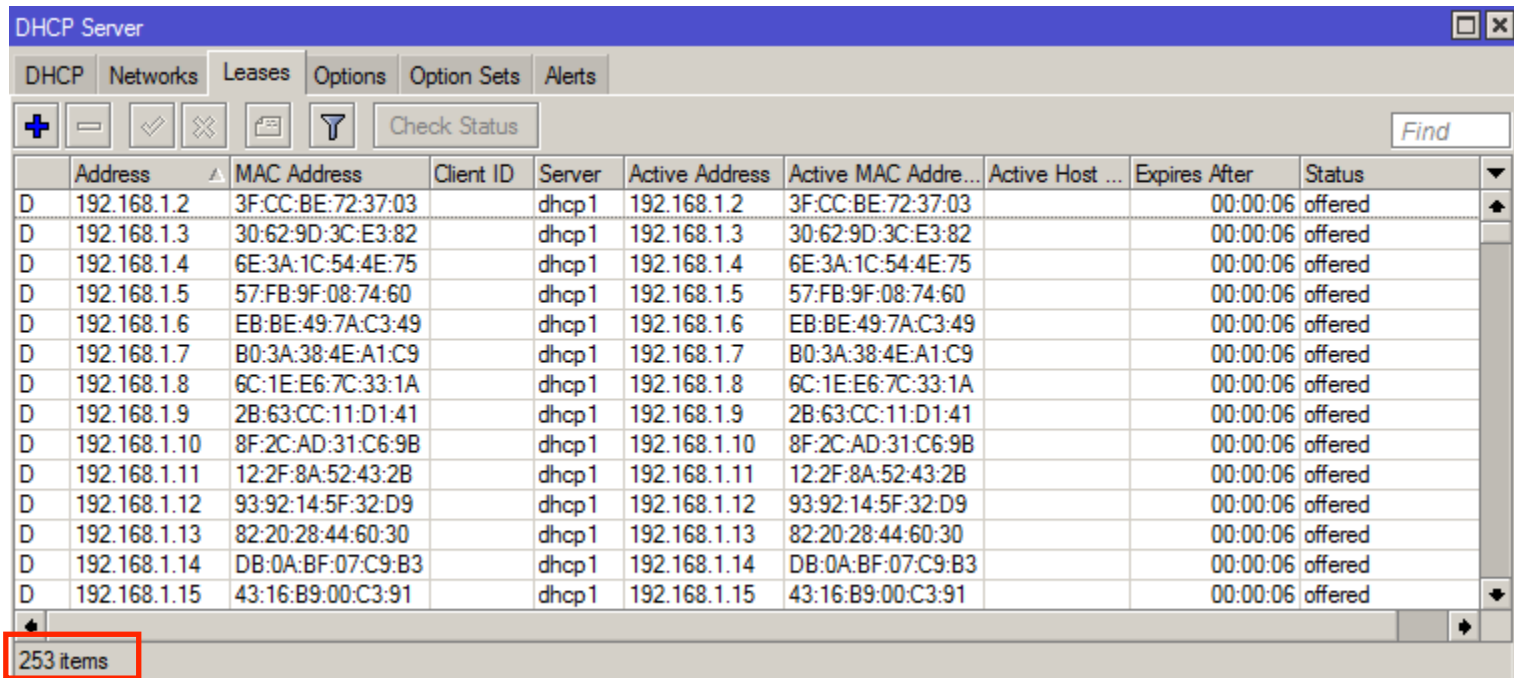
Description	DoS
<input type="radio"/> sending RAW packet	<input type="checkbox"/>
<input checked="" type="radio"/> sending DISCOVER packet	<input checked="" type="checkbox"/>
<input type="radio"/> creating DHCP rogue server	<input type="checkbox"/>
<input type="radio"/> sending RELEASE packet	<input checked="" type="checkbox"/>

Flags: 8000

0x0000: 0050 563b 5bc6 000c 2903 09ce 0800 4500 .PV;[...].....E.
0x0010: 0148 58de 4000 4011 5c77 c0a8 01fe c0a8 .HX.@.@.\w.....

DHCP Starvation Attack

- Attacker exhausts DHCP leases with multiple dhcp-requests to the router.



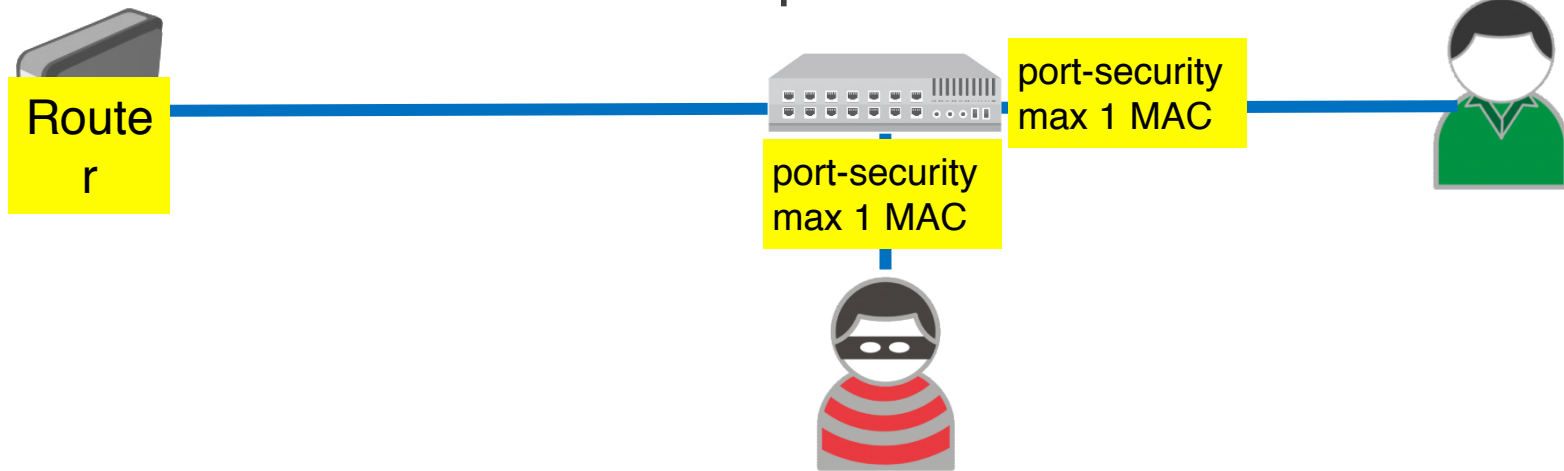
The screenshot shows a DHCP Server interface with a table of leases. The table has the following columns: Address, MAC Address, Client ID, Server, Active Address, Active MAC Address, Active Host, Expires After, and Status. The status for all leases is 'offered'.

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host	Expires After	Status
D	192.168.1.2	3F:CC:BE:72:37:03		dhcp1	192.168.1.2	3F:CC:BE:72:37:03		00:00:06	offered
D	192.168.1.3	30:62:9D:3C:E3:82		dhcp1	192.168.1.3	30:62:9D:3C:E3:82		00:00:06	offered
D	192.168.1.4	6E:3A:1C:54:4E:75		dhcp1	192.168.1.4	6E:3A:1C:54:4E:75		00:00:06	offered
D	192.168.1.5	57:FB:9F:08:74:60		dhcp1	192.168.1.5	57:FB:9F:08:74:60		00:00:06	offered
D	192.168.1.6	EB:BE:49:7A:C3:49		dhcp1	192.168.1.6	EB:BE:49:7A:C3:49		00:00:06	offered
D	192.168.1.7	B0:3A:38:4E:A1:C9		dhcp1	192.168.1.7	B0:3A:38:4E:A1:C9		00:00:06	offered
D	192.168.1.8	6C:1E:E6:7C:33:1A		dhcp1	192.168.1.8	6C:1E:E6:7C:33:1A		00:00:06	offered
D	192.168.1.9	2B:63:CC:11:D1:41		dhcp1	192.168.1.9	2B:63:CC:11:D1:41		00:00:06	offered
D	192.168.1.10	8F:2C:AD:31:C6:9B		dhcp1	192.168.1.10	8F:2C:AD:31:C6:9B		00:00:06	offered
D	192.168.1.11	12:2F:8A:52:43:2B		dhcp1	192.168.1.11	12:2F:8A:52:43:2B		00:00:06	offered
D	192.168.1.12	93:92:14:5F:32:D9		dhcp1	192.168.1.12	93:92:14:5F:32:D9		00:00:06	offered
D	192.168.1.13	82:20:28:44:60:30		dhcp1	192.168.1.13	82:20:28:44:60:30		00:00:06	offered
D	192.168.1.14	DB:0A:BF:07:C9:B3		dhcp1	192.168.1.14	DB:0A:BF:07:C9:B3		00:00:06	offered
D	192.168.1.15	43:16:B9:00:C3:91		dhcp1	192.168.1.15	43:16:B9:00:C3:91		00:00:06	offered

253 items

Preventing DHCP Starvation Attacks

- Attacker uses a new MAC address to request a new DHCP lease
- Restrict the number of MAC addresses on the port of switch.
- Will not be able to lease more IP addresses than MAC addresses allowed on the port



Rogue DHCP server

- A rogue DHCP server is a DHCP server on a network which is not under the administrative control.
- It is set up on a network by an attacker, for taking advantage from clients.

Rogue DHCP server

The screenshot shows a network security tool interface with a 'Launch attack' menu item highlighted by a red box. A red arrow points from this menu item to a 'DHCP' tab in a 'Choose attack' dialog box. In the dialog box, the 'creating DHCP rogue server' option is selected and highlighted with a red box. The background interface shows a table of protocols and packets, with 'DHCP' selected. The table has columns for Protocol, Packets, SIP, DIP, MessageType, Interface, Count, and Last seen. The DHCP entry shows 0 packets and a '03 REQUEST' message type on the 'eth0' interface.

Protocols	Packets	SIP	DIP	MessageType	Interface	Count	Last seen
CDP	0	192.168.1.254	192.168.1.1	03 REQUEST	eth0	1	26 Sep 15:59:27
DHCP	0	192.168.1.1	192.168.1.254				
802.1Q	0	192.168.1.254	192.168.1.1				
802.1X	0	192.168.1.254	192.168.1.1				
DTP	0	192.168.1.254	192.168.1.1				
HSRP	0	192.168.1.1	192.168.1.254				
ISL	0	192.168.1.254	192.168.1.1				
MPLS	0	192.168.1.254	192.168.1.1				

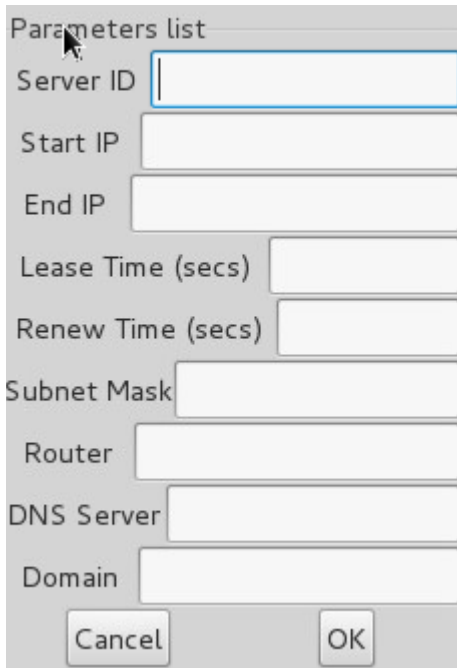
Field Value

Source MAC	00:0C:29:00:00:00
Destination MAC	00:50:56:00:00:00
SIP	192.168.1.1
DIP	192.168.1.254
SPort	68

16:34:04

0x0000: 0050 563b 5bc6 000c 2903 09ce 0800 4500 .PV;[...].E.
0x0010: 0148 93b0 4000 4011 21a5 c0a8 01fe c0a8 .H..@.@.1.....

Rogue DHCP server



Parameters list

Server ID

Start IP

End IP

Lease Time (secs)

Renew Time (secs)

Subnet Mask

Router

DNS Server

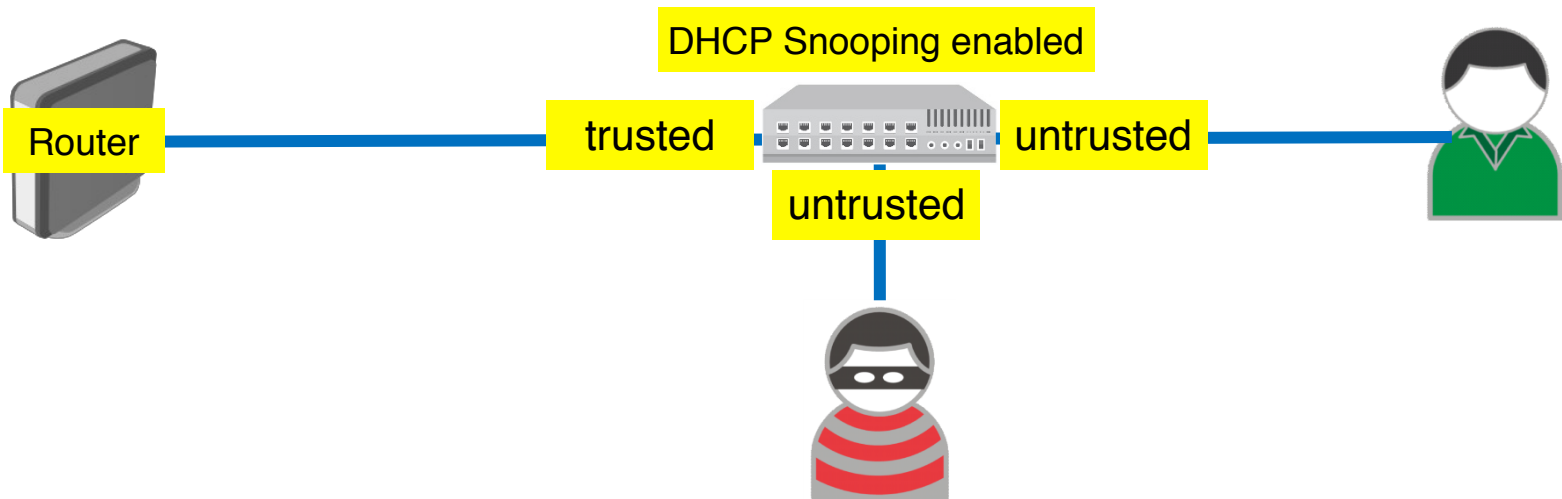
Domain

Cancel OK

- **Server IP** – the IP server, the name of which will send the answer the DHCP (*xxx.xxx.xxx.xxx*);
- **Start IP** – initial IP, issued to customers -address address range (*xxx.xxx.xxx.xxx*);
- **End IP** – IP, issued to customers -address address range (*xxx.xxx.xxx.xxx*);
- **Time The Lease (secs)** – The time in seconds for which the address is given
- **Time The Renew (secs)** – The time in seconds how many clients must renew the address lease
- **Subnet Mask** – Subnet mask for the clients (*xxx.xxx.xxx.xxx*);
- **Router** – router address issued to clients (*xxx.xxx.xxx.xxx*, *the address of a fake router*);
- **DNS Server** – DNS server provided to clients (*xxx.xxx.xxx.xxx*, *the address of a fake DNS server*);
- **The Domain** – a domain name in the local area network (*abc.def*);

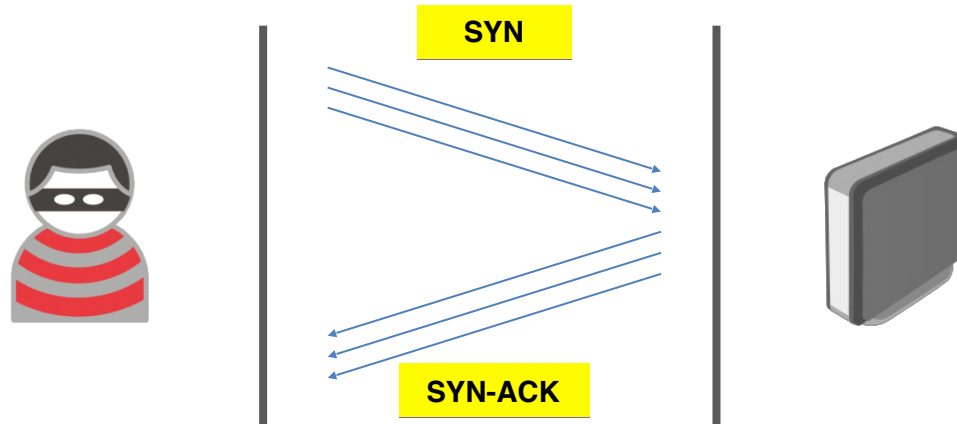
Preventing Rogue DHCP

- Enable DHCP Snooping on the switch
- Make port facing router as DHCP Snooping Trusted
- Binding Address and MAC for known clients
- RouterOS DHCP alert is ONLY sending information, not stopping or preventing an attack.



https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#DHCP_Snooping_and_DHCP_Option_82

TCP SYN Attack



- This type of attack takes advantage of the three-way handshake to establish communication
- In SYN flooding, the attacker send the target a large number of TCP/SYN packets.
- These packets have a source address, and the target computer replies (TCP/SYN-ACK packet) back to the source IP, trying to establish a TCP connection

TCP SYN Attack

- Scanning available port on target, normal target usually port 80/http service

```
root@kali:~# nmap 192.168.1.1

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-09-26 04:33 WIB
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
179/tcp   open  bgp
443/tcp   open  https
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: 00:50:56:3B:5B:C6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```

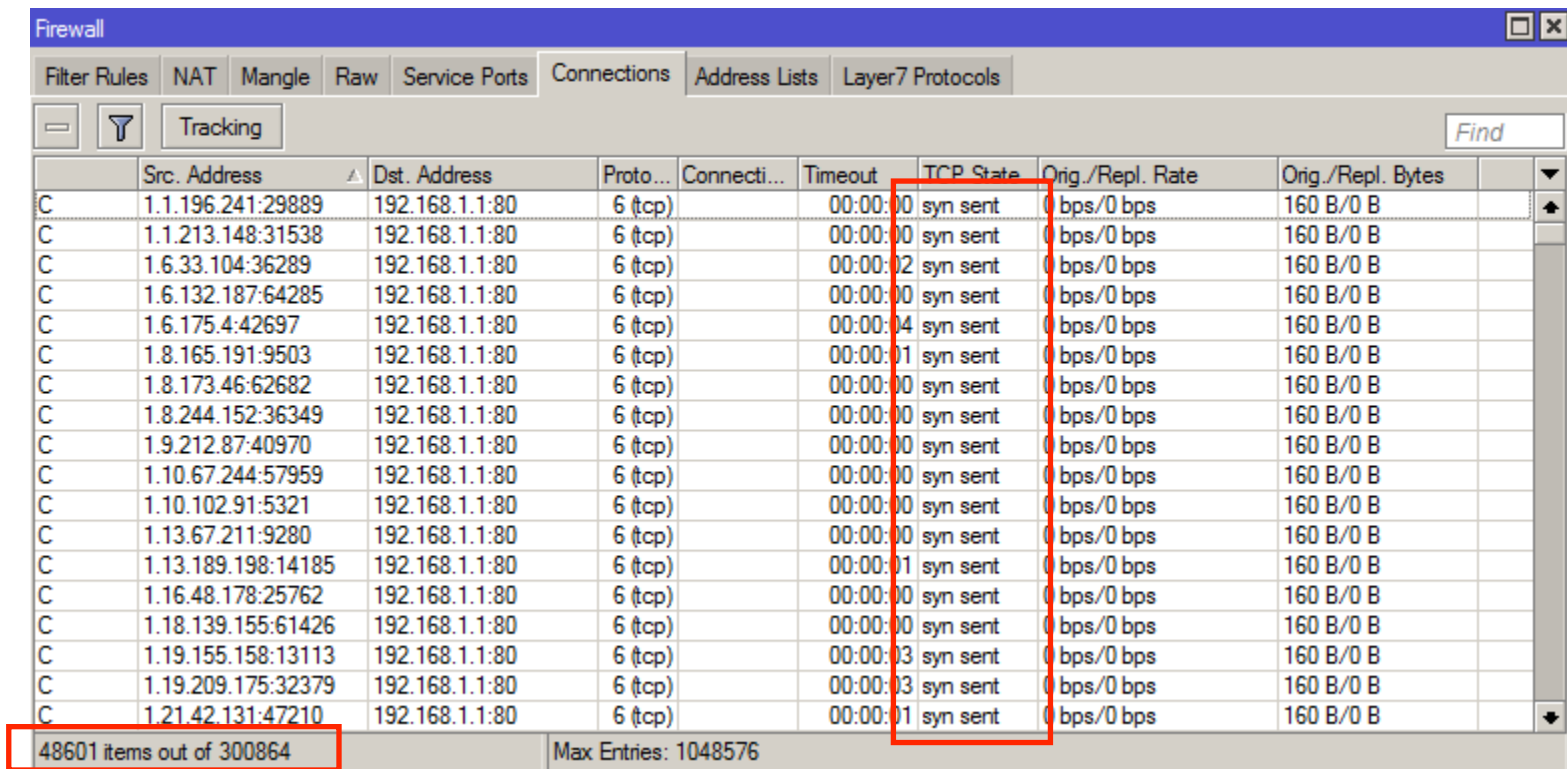
TCP SYN Attack

- Download and install “hping3” and run command bellow

```
root@kali:~# hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

TCP SYN Attack

- “IP > Firewall > Connections” please observe the “syn sent” from random source addresses



The screenshot shows the Mikrotik WinBox Firewall Connections tab. The table displays a list of connections, all in the 'syn sent' state, indicating a SYN flood attack. The source addresses are random, and the destination is 192.168.1.1:80. A red box highlights the 'TCP State' column, and another red box highlights the status bar at the bottom showing 48601 items out of 300864.

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	1.1.196.241:29889	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.1.213.148:31538	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.6.33.104:36289	192.168.1.1:80	6 (tcp)		00:00:02	syn sent	0 bps/0 bps	160 B/0 B
C	1.6.132.187:64285	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.6.175.4:42697	192.168.1.1:80	6 (tcp)		00:00:04	syn sent	0 bps/0 bps	160 B/0 B
C	1.8.165.191:9503	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps	160 B/0 B
C	1.8.173.46:62682	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.8.244.152:36349	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.9.212.87:40970	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.10.67.244:57959	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.10.102.91:5321	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.13.67.211:9280	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.13.189.198:14185	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps	160 B/0 B
C	1.16.48.178:25762	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.18.139.155:61426	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.19.155.158:13113	192.168.1.1:80	6 (tcp)		00:00:03	syn sent	0 bps/0 bps	160 B/0 B
C	1.19.209.175:32379	192.168.1.1:80	6 (tcp)		00:00:03	syn sent	0 bps/0 bps	160 B/0 B
C	1.21.42.131:47210	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps	160 B/0 B

48601 items out of 300864 Max Entries: 1048576

TCP SYN Attack

- Torch interface traffic

The screenshot shows the Torch application interface with the following configuration and data:

Basic: Interface: ether2-UPSTREAM, Entry Timeout: 00:00:03 s

Collect: Src. Address, Dst. Address, MAC Protocol, Protocol, DSCP, Src. Address6, Dst. Address6, Port, VLAN Id

Filters: Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0, Src. Address6: ::/0, Dst. Address6: ::/0, MAC Protocol: all, Protocol: any, Port: any, VLAN Id: any, DSCP: any

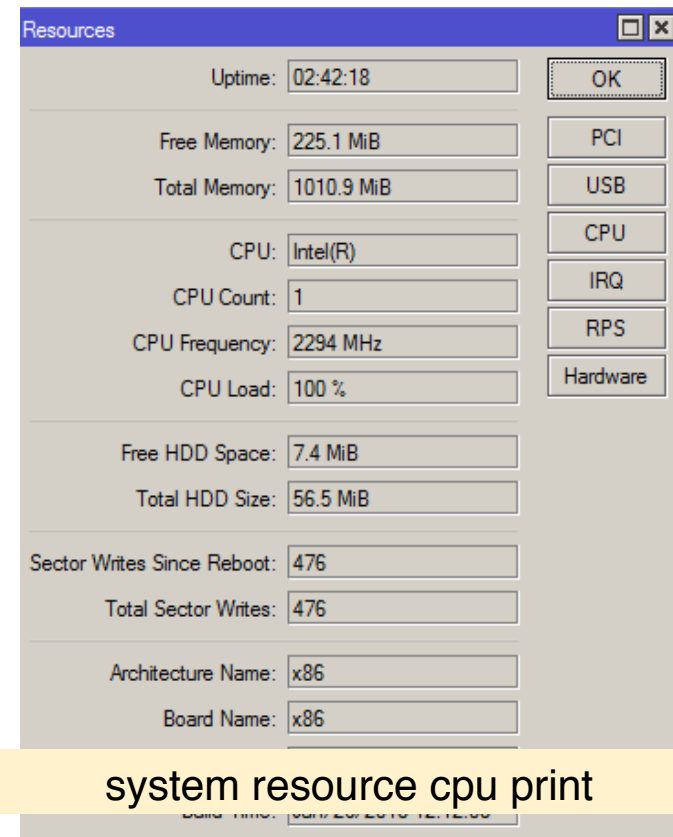
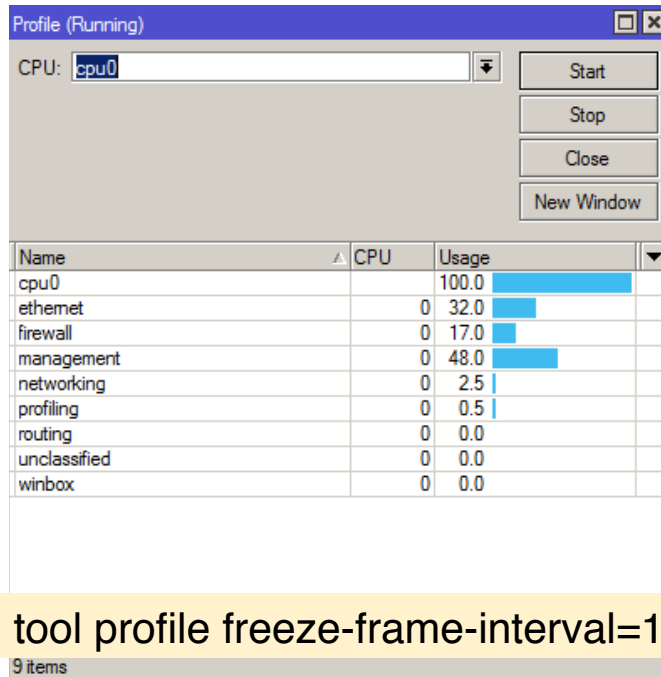
Buttons: Start, Stop, Close, New Window

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pa
800 (ip)	6 (tcp)	1.250.82.222:2059	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.246.185.126:2069	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.6.189.216:2149	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.171.180.16:2161	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.55.102.115:2429	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	4.4.55.160:2464	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.251.194.197:2657	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.63.96.213:2820	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.100.185.79:2878	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.219.212.187:2897	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	4.26.6.116:3019	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.150.129.7:3101	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.184.139.122:3135	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.219.251.220:3280	192.168.1.1:80 (http)			0 bps	1392 bps	0	

Summary: 13320 items, Total Tx: 0 bps, Total Rx: 38.5 Mbps, Total Tx Packet: 0, Total Rx Packet: 27 691

TCP SYN Attack

- The attack is exhausting the resources of the router and impacting the performance

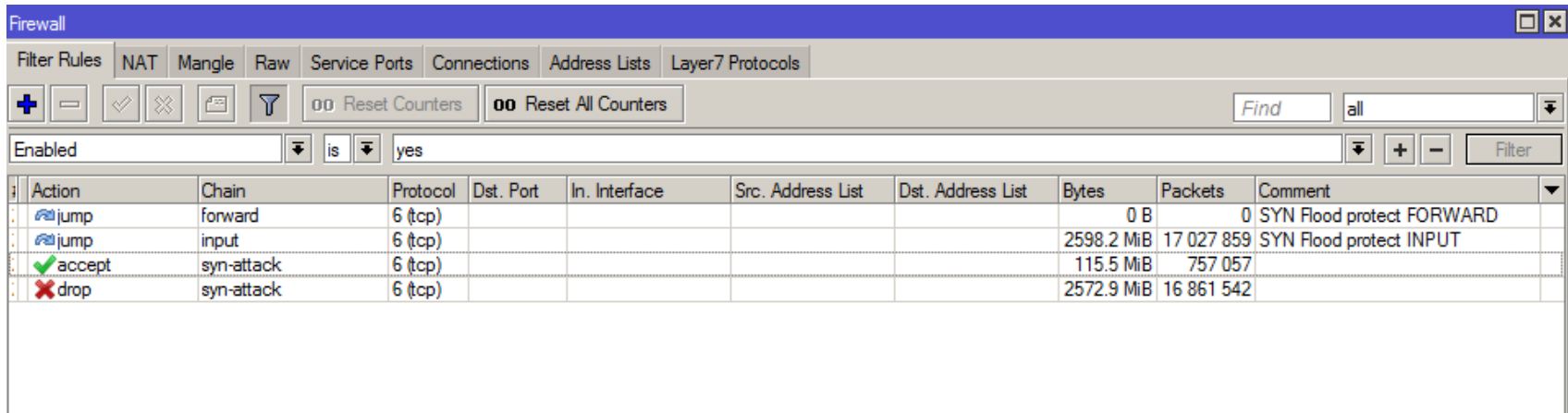


Preventing TCP SYN Attack

- Rate-limiting for each new tcp connection
- Reduce syn-received timer
- And setup tcp syn-cookies

Preventing TCP SYN Attack

- Creating firewall for preventing tcp SYN flood



The screenshot shows the Mikrotik WinBox Firewall Filter configuration window. The window title is "Firewall". The tabs include Filter Rules, NAT, Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7 Protocols. The "Filter Rules" tab is active. The window shows a list of four firewall rules:

Action	Chain	Protocol	Dst. Port	In. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
jump	forward	6 (tcp)					0 B	0	SYN Flood protect FORWARD
jump	input	6 (tcp)					2598.2 MiB	17 027 859	SYN Flood protect INPUT
accept	syn-attack	6 (tcp)					115.5 MiB	757 057	
drop	syn-attack	6 (tcp)					2572.9 MiB	16 861 542	

/ip firewall filter

```
add action=jump chain=forward comment="SYN Flood protect FORWARD" connection-state=new  
jump-target=syn-attack protocol=tcp tcp-flags=syn
```

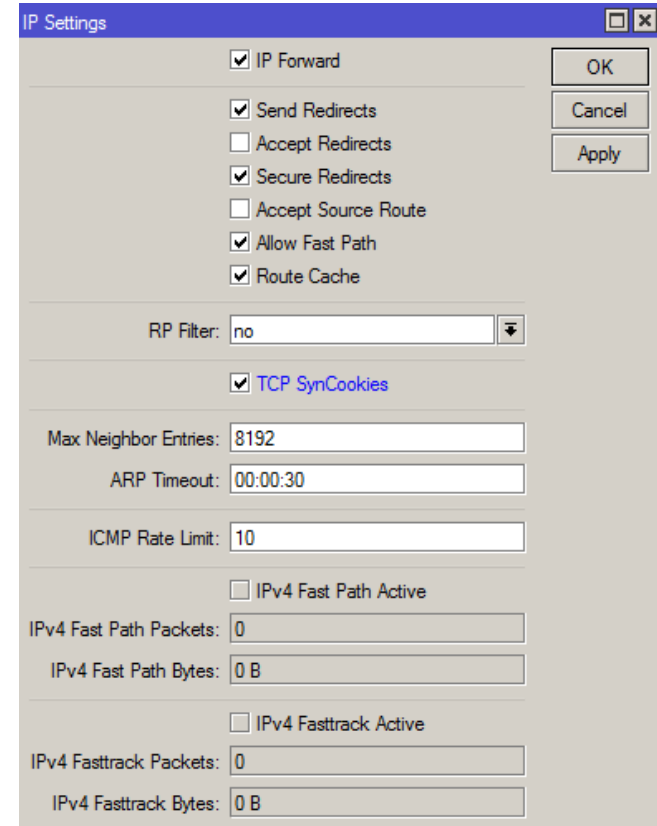
```
add action=jump chain=input comment="SYN Flood protect INPUT" connection-state=new jump-  
target=syn-attack protocol=tcp tcp-flags=syn
```

```
add action=accept chain=syn-attack connection-state=new limit=400,5:packet protocol=tcp tcp-  
flags=syn
```

```
add action=drop chain=syn-attack connection-state=new protocol=tcp tcp-flags=syn
```

Preventing TCP SYN Attack

- IP > Settings and enable “TCP SynCookies”



```
/ip settings set tcp-syncookies=yes
```

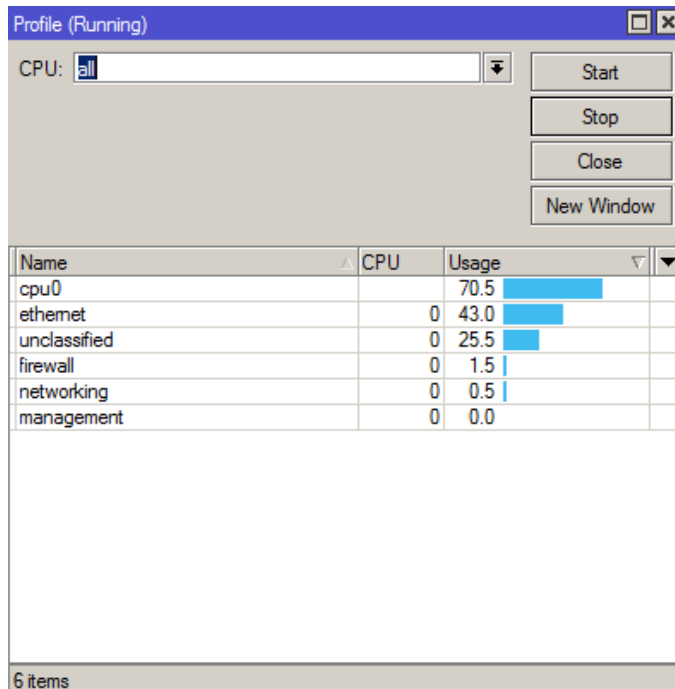
TCP SYN Attack

- Run hping3 again

```
root@kali:~# hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Preventing TCP SYN Attack

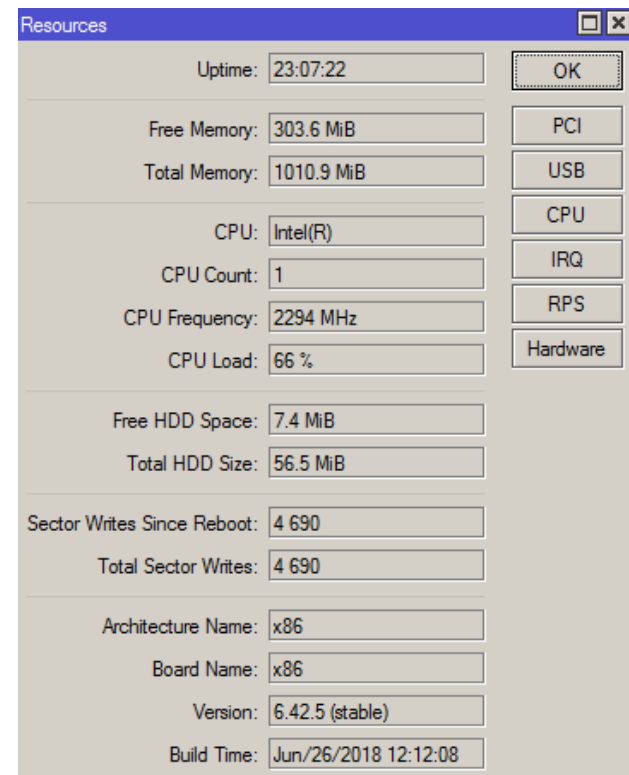
- These rules are stopping the tcp SYN attack, but still affecting the CPU resources. *(need more powerful router for preventing)*



The screenshot shows a window titled 'Profile (Running)' with a 'CPU:' field set to 'all'. Below the field are buttons for 'Start', 'Stop', 'Close', and 'New Window'. A table displays the following data:

Name	CPU	Usage
cpu0		70.5
ethemet	0	43.0
unclassified	0	25.5
firewall	0	1.5
networking	0	0.5
management	0	0.0

6 items



The screenshot shows a window titled 'Resources' with the following system statistics:

Uptime:	23:07:22
Free Memory:	303.6 MiB
Total Memory:	1010.9 MiB
CPU:	Intel(R)
CPU Count:	1
CPU Frequency:	2294 MHz
CPU Load:	66 %
Free HDD Space:	7.4 MiB
Total HDD Size:	56.5 MiB
Sector Writes Since Reboot:	4 690
Total Sector Writes:	4 690
Architecture Name:	x86
Board Name:	x86
Version:	6.42.5 (stable)
Build Time:	Jun/26/2018 12:12:08

UDP Flood Attack

- An UDP flood does not exploit any vulnerability.
- The aim of UDP floods is creating and sending large amount of UDP datagrams from spoofed IP's to the target server.
- When a server receives this type of traffic, it is unable to process every request and it consumes its bandwidth with sending ICMP “destination unreachable” packets.

UDP Flood Attack

- Scanning available port on target, normal target usually port 53/dns service

```
root@kali:~# nmap 192.168.1.1
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-09-26 04:33 WIB
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
179/tcp   open  bgp
443/tcp   open  https
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: 00:50:56:3B:5B:C6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```

UDP Flood Attack

- Start attacking UDP protocol port 53(dns) with hping3

```
root@kali:~# hping3 --flood --rand-source --udp -p 53 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

UDP Flood Attack

- “IP > Firewall > Connections” please observe “udp” protocol from random source addresses

Firewall

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

Tracking Find

	Src. Address	Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	1.1.124.145:16274	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.1.152.193:4070	192.168.1.1:53	17 (udp)		00:00:09		0 bps/0 bps	28 B/0 B
C	1.1.210.234:39613	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B
C	1.1.232.251:7299	192.168.1.1:53	17 (udp)		00:00:07		0 bps/0 bps	28 B/0 B
C	1.2.43.209:20491	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.2.63.154:53419	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.2.124.175:15303	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.2.124.227:24114	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.2.166.33:39602	192.168.1.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	1.2.170.109:56965	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B
C	1.2.201.185:55335	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.2.243.99:16763	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.2.252.77:55178	192.168.1.1:53	17 (udp)		00:00:08		0 bps/0 bps	28 B/0 B
C	1.2.252.134:42559	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B
C	1.3.179.240:49331	192.168.1.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	1.4.3.78:28758	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.4.15.108:36180	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.4.35.49:12614	192.168.1.1:53	17 (udp)		00:00:08		0 bps/0 bps	28 B/0 B

177065 items out of 335494 Max Entries: 1048576

UDP Flood Attack

- Torch interface traffic

Basic configuration:
Interface: ether2-UPSTREAM
Entry Timeout: 00:00:03 s

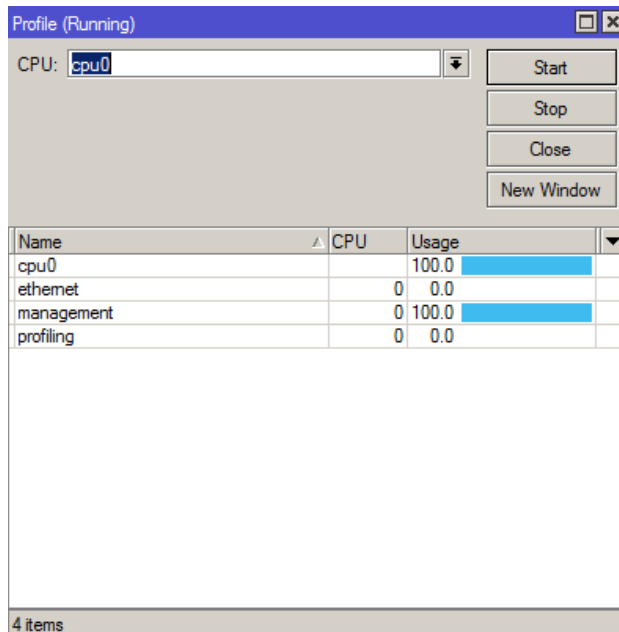
Collect options:
 Src. Address
 Dst. Address
 MAC Protocol
 Protocol
 DSCP
 Src. Address6
 Dst. Address6
 Port
 VLAN Id

Filters:
Src. Address: 0.0.0.0/0
Dst. Address: 0.0.0.0/0
Src. Address6: ::/0
Dst. Address6: ::/0
MAC Protocol: all
Protocol: any
Port: any
VLAN Id: any
DSCP: any

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	17 (udp)	64.247.124.230:16074	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	74.246.215.130:16101	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	66.6.136.152:16125	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	68.223.155.223:17278	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	72.124.173.35:17304	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	66.185.185.215:17322	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	74.187.215.252:17323	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	73.61.251.35:17333	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	65.59.239.81:17370	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	64.166.36.152:17405	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	72.129.35.53:17425	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	68.121.62.13:17437	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	64.239.142.236:17441	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	68.134.201.114:17457	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (ip)	17 (udp)	68.94.142.199:17517	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
6200 items		Total Tx: 0 bps	Total Rx: 9.1 Mbps	Total Tx Packet: 0	Total Rx Packet: 19 119		

UDP Flood Attack

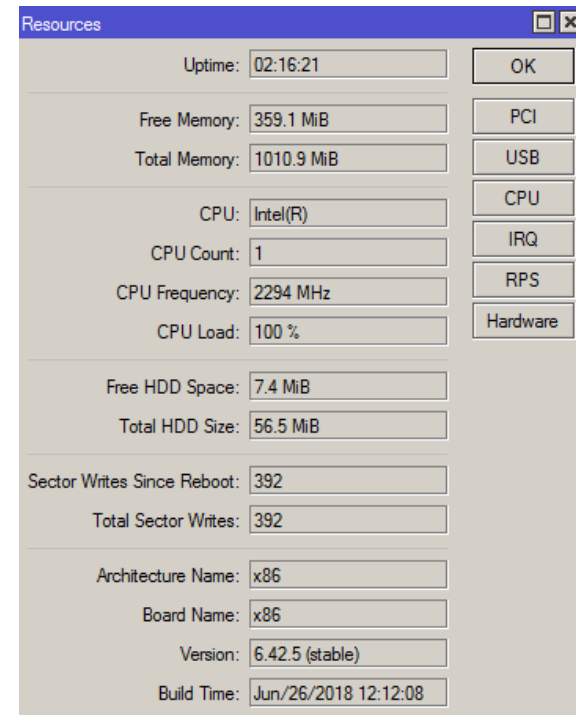
- The attack is exhausting the resources of the router and impacting the performance



The screenshot shows a window titled 'Profile (Running)'. At the top, there is a dropdown menu for 'CPU' set to 'cpu0' and buttons for 'Start', 'Stop', 'Close', and 'New Window'. Below this is a table with columns 'Name', 'CPU', and 'Usage'. The table shows the following data:

Name	CPU	Usage
cpu0		100.0
ethernet	0	0.0
management	0	100.0
profiling	0	0.0

At the bottom of the window, it says '4 items'.



The screenshot shows a window titled 'Resources' with various system statistics and hardware information:

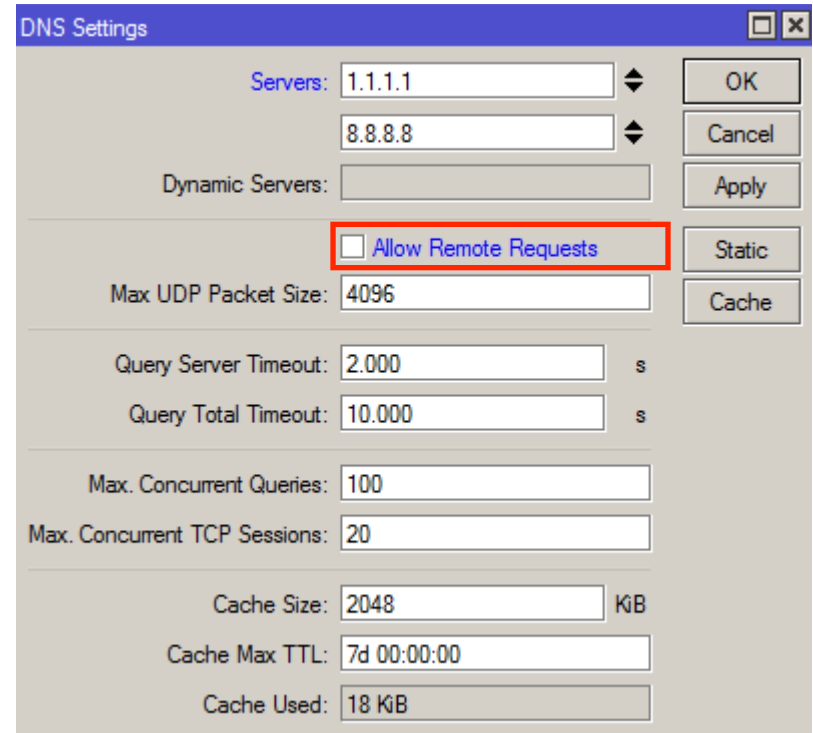
- Uptime: 02:16:21
- Free Memory: 359.1 MiB
- Total Memory: 1010.9 MiB
- CPU: Intel(R)
- CPU Count: 1
- CPU Frequency: 2294 MHz
- CPU Load: 100 %
- Free HDD Space: 7.4 MiB
- Total HDD Size: 56.5 MiB
- Sector Writes Since Reboot: 392
- Total Sector Writes: 392
- Architecture Name: x86
- Board Name: x86
- Version: 6.42.5 (stable)
- Build Time: Jun/26/2018 12:12:08

Preventing UDP Flood Attack

- Disable DNS forwarder on MikroTik if not required.
- If “IP -> DNS” – *Allow remote request* is enabled, make sure appropriate filter rule is set to prevent incoming DNS attacks.
- Rate-limiting for each new udp connection.

Preventing UDP Flood Attack

- Uncheck *Allow Remote Requests* on router



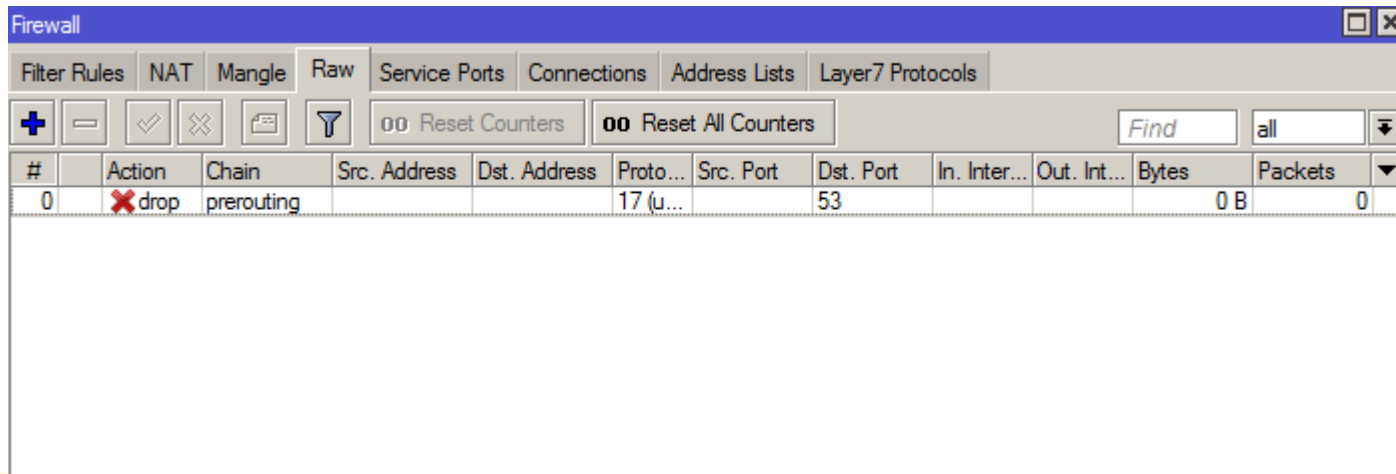
The screenshot shows a 'DNS Settings' window with the following configuration:

Field	Value
Servers	1.1.1.1 8.8.8.8
Dynamic Servers	
Max UDP Packet Size	4096
Query Server Timeout	2.000 s
Query Total Timeout	10.000 s
Max. Concurrent Queries	100
Max. Concurrent TCP Sessions	20
Cache Size	2048 KB
Cache Max TTL	7d 00:00:00
Cache Used	18 KB

The 'Allow Remote Requests' checkbox is highlighted with a red box and is currently unchecked.

Preventing UDP Flood Attack

- Block dns request “udp/53” traffic from outside



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is active, and a rule is configured to drop traffic. The rule is named '0' and is located in the 'prerouting' chain. It targets traffic with protocol '17 (udp)' and destination port '53' coming from the 'OUTSIDE' interface. The action is set to 'drop'.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✖ drop	prerouting			17 (u...		53			0 B	0

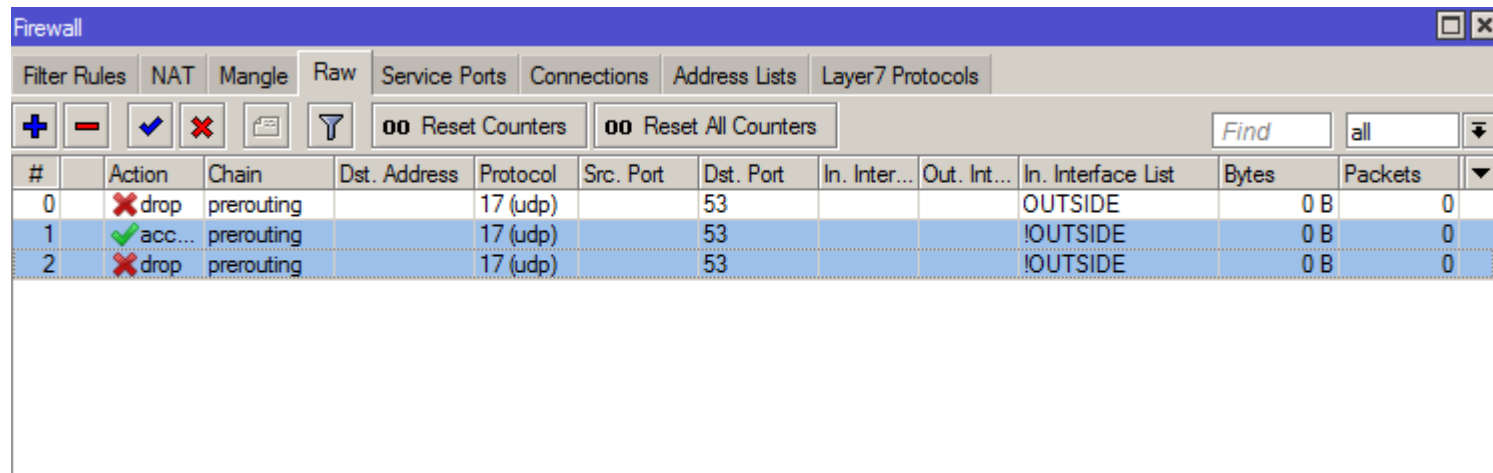
```
/interface list add name=OUTSIDE
```

```
/interface list member add interface=ether3-internet list=OUTSIDE
```

```
/ip firewall raw add action=drop chain=prerouting dst-port=53 in-interface-list=OUTSIDE  
protocol=udp
```


Preventing UDP Flood Attack

- Rate-limiting every udp/53 packet requests



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Raw' tab is selected. The table below shows the configuration of three firewall rules:

#	Action	Chain	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Interface List	Bytes	Packets
0	✗ drop	prerouting		17 (udp)		53			OUTSIDE	0 B	0
1	✓ acc...	prerouting		17 (udp)		53			!OUTSIDE	0 B	0
2	✗ drop	prerouting		17 (udp)		53			!OUTSIDE	0 B	0

```
/ip firewall raw
add action=accept chain=prerouting dst-port=53 in-interface-list=!OUTSIDE limit=100,5:packet
protocol=udp
add action=drop chain=prerouting dst-port=53 in-interface-list=!OUTSIDE protocol=udp
```

ICMP Smurf Attack

- This type of attack uses large amount of Internet Control Message Protocol (ICMP) ping traffic targeted at an Internet Broadcast Address e.g 192.168.1.255.
- The reply IP address is spoofed to that of the intended victim e.g 1.2.3.4
- All the replies are sent to the victim instead of the IP used for the pings.
- Since a single Internet Broadcast Address can support a maximum of 255 hosts, a smurf attack amplifies a single ping 255 times.

ICMP Smurf Attack

- Start attacking ICMP smurf with random source

```
root@kali:~# hping3 --icmp --flood --rand-source -c 20000 --spooof 192.168.1.1 192.168.1.255
HPING 192.168.1.255 (eth0 192.168.1.255): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
█
```

ICMP Smurf Attack

The screenshot shows the Torch application interface. The 'Basic' tab is selected, showing the interface as 'ether2-LAN' and an entry timeout of '00:00:03'. The 'Collect' tab has several checkboxes: 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Address6', 'Dst. Address6', 'Port', and 'VLAN Id'. The 'Filters' tab shows various filter settings. The traffic table below shows a list of ICMP packets. The destination address column is highlighted with a red box, showing that all packets are sent to 192.168.1.255.

Et...	Protocol	Src.	Dst.	Tx Rate	Fx Rate	Tx Pack...	Fx Pack...
800 (ip)	1 (icmp)	3.165.35.24	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	2.157.113.252	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.20.180.198	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.143.233.131	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.143.18.248	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.136.185.167	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.180.181.187	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.155.172.83	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	2.63.28.173	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.173.237.250	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.247.136.135	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.148.60.101	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	3.132.197.139	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	2.129.76.69	192.168.1.255	0 bps	480 bps	0	1
800 (ip)	1 (icmp)	2.8.10.2	192.168.1.255	0 bps	480 bps	0	1

6091 items | Total Tx: 0 bps | Total Fx: 8.0 Mbps | Total Tx Packet: 0 | Total Fx Packet: 16 754

- All of attacker's traffic as a destination address has the broadcast address of the network

ICMP Smurf Attack

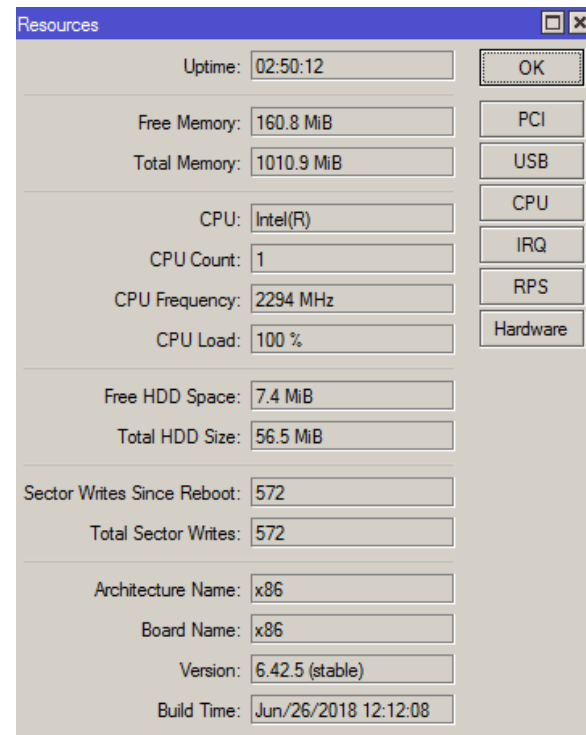
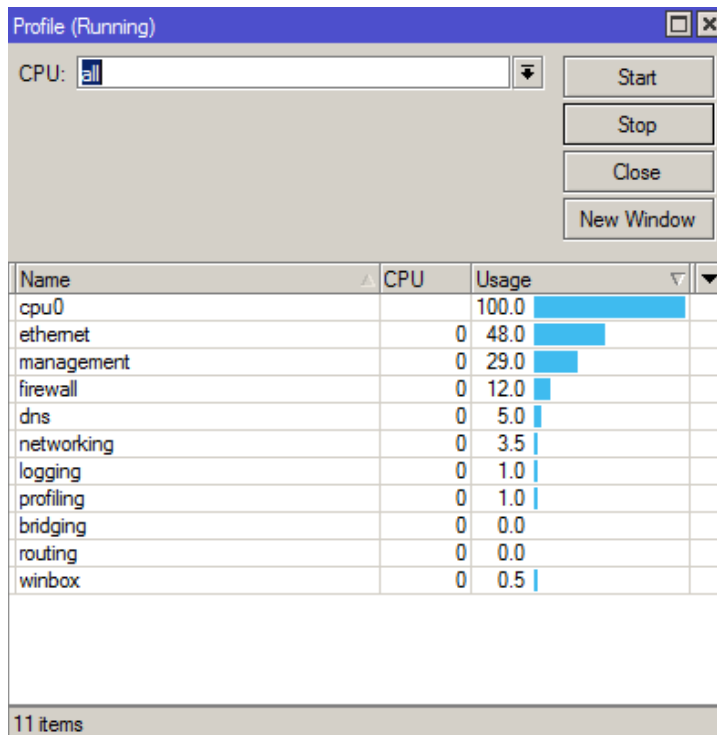
The screenshot shows the Mikrotik WinBox Firewall Connections tab. The table displays a list of connections, with a red box highlighting the destination IP address 192.168.1.255 for multiple entries, indicating an ICMP smurf attack. The first entry shows a connection to 255.255.255.255:5678 via UDP. The subsequent entries show connections to 192.168.1.255 via ICMP.

	Src. Address	△ Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes	
C	0.0.0.0:5678	255.255.255.255:5678	17 (udp)		00:00:00		0 bps/0 bps	13.3 KiB/0 B	▼
C	2.2.18.173	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	▲
C	2.3.18.227	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	2.3.21.3	192.168.1.255	1 (icmp)		00:00:08		0 bps/0 bps	28 B/0 B	
C	2.3.78.119	192.168.1.255	1 (icmp)		00:00:03		0 bps/0 bps	28 B/0 B	
C	2.3.198.86	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	2.5.66.248	192.168.1.255	1 (icmp)		00:00:01		0 bps/0 bps	28 B/0 B	
C	2.5.111.10	192.168.1.255	1 (icmp)		00:00:01		0 bps/0 bps	28 B/0 B	
C	2.5.120.238	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	2.5.181.227	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	2.5.212.63	192.168.1.255	1 (icmp)		00:00:08		0 bps/0 bps	28 B/0 B	
C	2.7.106.3	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	2.7.203.180	192.168.1.255	1 (icmp)		00:00:02		0 bps/0 bps	28 B/0 B	
C	2.7.222.246	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	2.8.28.151	192.168.1.255	1 (icmp)		00:00:02		0 bps/0 bps	28 B/0 B	
C	2.8.48.78	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	2.8.97.214	192.168.1.255	1 (icmp)		00:00:02		0 bps/0 bps	28 B/0 B	
C	2.8.103.111	192.168.1.255	1 (icmp)		00:00:00		0 bps/0 bps	28 B/0 B	▼

174701 items out of 340160 | Max Entries: 1048576

ICMP Smurf Attack

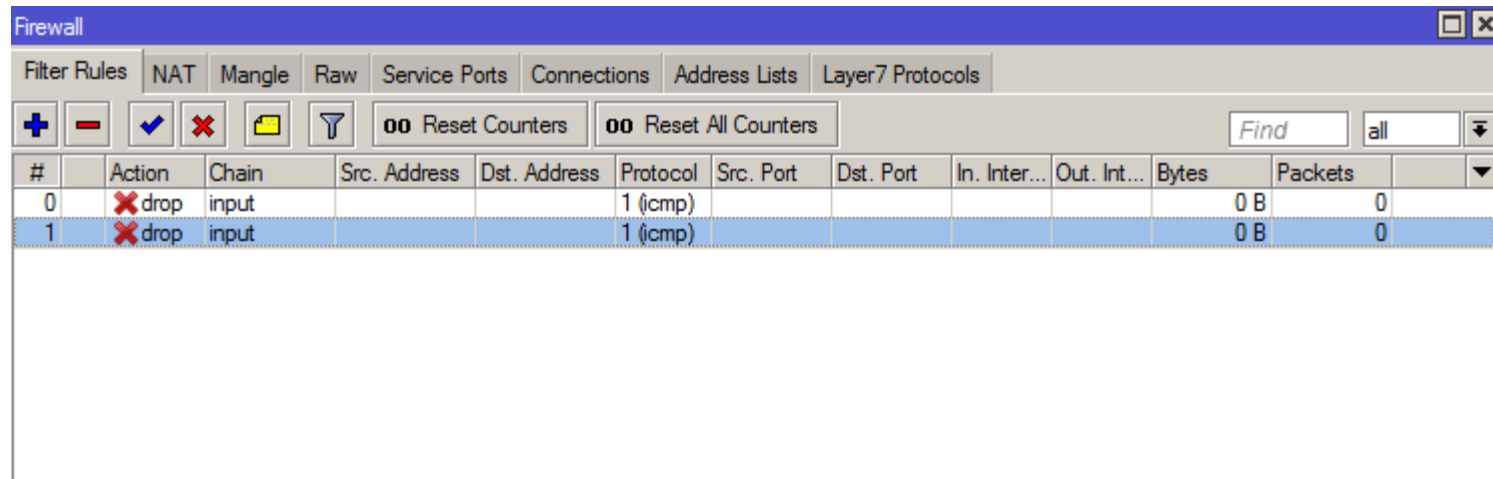
- The attack is exhausting the resources of the router and impacting the performance



Preventing ICMP Smurf Attack

- Configure routers not to forward or accept packets directed to broadcast addresses.
- Configure individual hosts or routers to not respond to ping requests from outside

Preventing ICMP Smurf Attack



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active. The table below shows two rules, both with the action 'drop' and protocol 'icmp'.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✗ drop	input			1 (icmp)					0 B	0
1	✗ drop	input			1 (icmp)					0 B	0

```
/ip firewall filter
```

```
add action=drop chain=input dst-address-type=broadcast icmp-options=0:0-255 protocol=icmp
```

```
add action=drop chain=input in-interface-list=OUTSIDE protocol=icmp
```


Password Brute Force Attack

- A brute force attack is a trial-and-error method used to obtain information such as a users password or any other credential information.
- In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

Password Brute Force Attack

- Router under SSH Brute Force Attack

The screenshot shows the Torch (Running) application interface. The configuration is as follows:

- Interface: ether2-LAN
- Entry Timeout: 00:00:03 s
- Filters:
 - Src. Address: 0.0.0.0/0
 - Dst. Address: 0.0.0.0/0
 - Src. Address6: ::/0
 - Dst. Address6: ::/0
 - MAC Protocol: all
 - Protocol: any
 - Port: any
 - VLAN Id: any
 - DSCP: any

The table below shows the active connections:

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.1.254:39202	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:45605	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:38707	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:40363	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:57012	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:51584	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:40917	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:59630	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:42983	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:56839	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:42752	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:58035	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:34975	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:52383	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:57142	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0

Summary statistics at the bottom:

- 70 items
- Total Tx: 0 bps
- Total Rx: 0 bps
- Total Tx Packet: 0
- Total Rx Packet: 0

Password Brute Force Attack

- Router under Telnet Brute Force Attack

The screenshot shows the Torch (Running) application interface. The configuration is as follows:

- Interface: ether2-LAN
- Entry Timeout: 00:00:03 s
- Collect: Src. Address, Dst. Address, Protocol, Src. Address6, Dst. Address6, Port, MAC Protocol, DSCP, VLAN Id
- Filters: Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0, Src. Address6: ::/0, Dst. Address6: ::/0, MAC Protocol: all, Protocol: any, Port: any, VLAN Id: any, DSCP: any

The results table shows the following data:

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.1.254:40876	192.168.1.1:23 (telnet)	592 bps	1120 bps	1	2
800 (ip)	6 (tcp)	192.168.1.254:57657	192.168.1.1:23 (telnet)	968 bps	1056 bps	1	2
800 (ip)	6 (tcp)	192.168.1.254:44580	192.168.1.1:23 (telnet)	2.2 kbps	528 bps	1	1
800 (ip)	6 (tcp)	192.168.1.254:53595	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:45764	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:51001	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0

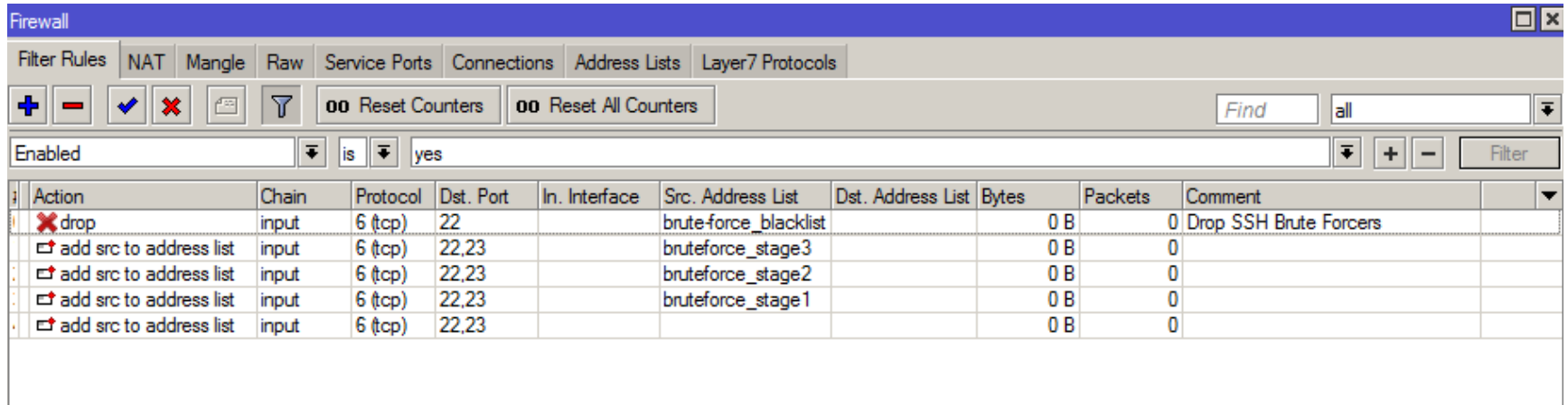
Summary statistics at the bottom:

- 6 items
- Total Tx: 3.8 kbps
- Total Rx: 2.7 kbps
- Total Tx Packet: 3
- Total Rx Packet: 5

Preventing Brute Force Attack

- Limiting the number of times a user can unsuccessfully attempt to log in
- Temporarily locking out users who exceed the specified maximum number of failed login attempts
- Requiring users to create complex passwords
- Periodically changing a password

Preventing Brute Force Attack



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is active. The rule is named 'Drop SSH Brute Forcers' and is currently disabled. The configuration is as follows:

Action	Chain	Protocol	Dst. Port	In. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
<input checked="" type="checkbox"/> drop	input	6 (tcp)	22		brute-force_blacklist		0 B	0	Drop SSH Brute Forcers
<input checked="" type="checkbox"/> add src to address list	input	6 (tcp)	22,23		brute-force_stage3		0 B	0	
<input checked="" type="checkbox"/> add src to address list	input	6 (tcp)	22,23		brute-force_stage2		0 B	0	
<input checked="" type="checkbox"/> add src to address list	input	6 (tcp)	22,23		brute-force_stage1		0 B	0	
<input checked="" type="checkbox"/> add src to address list	input	6 (tcp)	22,23				0 B	0	

Preventing Brute Force Attack

```
/ip firewall filter
add action=drop chain=input comment="Drop SSH Brute Forcers" dst-port=22 protocol=tcp \
  src-address-list=brute-force_blacklist
add action=add-src-to-address-list address-list=brute-force_blacklist address-list-timeout=1d
chain=input \
  connection-state=new dst-port=22,23 protocol=tcp src-address-list=bruteforce_stage3
add action=add-src-to-address-list address-list=bruteforce_stage3 address-list-timeout=30s
chain=input \
  connection-state=new dst-port=22,23 protocol=tcp src-address-list=bruteforce_stage2
add action=add-src-to-address-list address-list=bruteforce_stage2 address-list-timeout=30s
chain=input \
  connection-state=new dst-port=22,23 protocol=tcp src-address-list=bruteforce_stage1
add action=add-src-to-address-list address-list=bruteforce_stage1 address-list-timeout=1m
chain=input \
  connection-state=new dst-port=22,23 protocol=tcp
```

Port Scanner Detection

- A port scan is a method for determining which ports on a network are open or available.
- Running a port scan on a network or server reveals which ports are open and listening (*receiving information*)
- Port Scan tools (like NMAP) can detect what version of an application is running on a port
- Port scanning is the “gate” for starting an attack or penetration to your networks

Port Scanner Detection

- Scanning available ports on the target

```
root@kali:~# nmap 192.168.1.1
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-09-26 04:33 WIB
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
179/tcp   open  bgp
443/tcp   open  https
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: 00:50:56:3B:5B:C6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```


Preventing Port Scanner

- Create Port Scanner Detection on router and block the address

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✗ drop	input			1 (icmp)					0 B	0
1	✗ drop	input			1 (icmp)					0 B	0
2	✗ drop	input								0 B	0
::: Port scanners to list											
3	➡ add...	input			6 (tcp)					0 B	0
::: NMAP FIN Stealth scan											
4	➡ add...	input			6 (tcp)					0 B	0
::: SYN/FIN scan											
5	➡ add...	input			6 (tcp)					0 B	0
::: SYN/RST scan											
6	➡ add...	input			6 (tcp)					0 B	0
::: FIN/PSH/URG scan											
7	➡ add...	input			6 (tcp)					0 B	0
::: ALL/ALL scan											
8	➡ add...	input			6 (tcp)					0 B	0
::: NMAP NULL scan											
9	➡ add...	input			6 (tcp)					0 B	0

Preventing Port Scanner

```
/ip firewall filter
```

```
add action=drop chain=input src-address-list="port scanners"
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input
comment="Port scanners to list " protocol=tcp psd=21,3s,3,1
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input
comment="NMAP FIN Stealth scan" protocol=tcp tcp-flags=\
    fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input
comment="SYN/FIN scan" protocol=tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input
comment="SYN/RST scan" protocol=tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input
comment="FIN/PSH/URG scan" protocol=tcp tcp-flags=\
    fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input
comment="ALL/ALL scan" protocol=tcp tcp-flags=\
    fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input
comment="NMAP NULL scan" protocol=tcp tcp-flags=\
    !fin,!syn,!rst,!psh,!ack,!urg
```

SECURING THE ROUTER

PORT KNOCKING

What is Port Knocking

- Port knocking is a method that enables access to the router only after receiving a sequenced connection attempts on a set of “pre-specified” open ports.
- Once the correct sequence of the connection attempts is received, the RouterOS dynamically adds a host source IP to the allowed address list and you will be able to connect to your router.
- You can use some online available port-knock clients, or manually connect router IP address with defined ports.
- The port "knock" itself is similar to a secret handshake and can consist of any number of TCP, UDP, or ICMP or other protocol packets to numbered ports on the destination machine

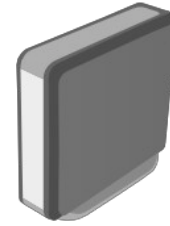
How the Port Knocking works



Host trying to make a connection to first “knocking-port”



RouterOS dynamically adds a host source IP to the allowed address-list



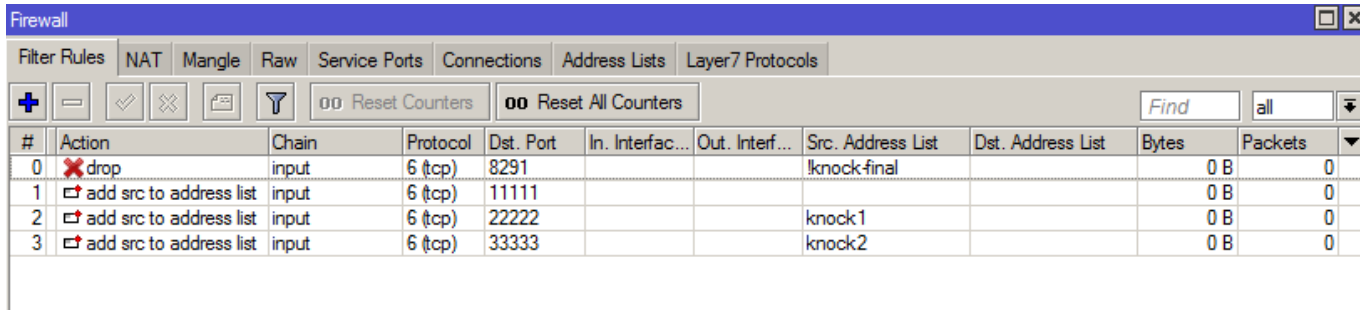
Host trying to make a second attempt “knocking-port”



RouterOS will check if IP coming from the same first connection on allowed address-list

If the IP is the same and the time between first attempt and seconds within a specified time then the host IP will be allowed to access the router

How the Port Knocking works



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active. The table below shows the configured rules:

#	Action	Chain	Protocol	Dst. Port	In. Interfac...	Out. Interf...	Src. Address List	Dst. Address List	Bytes	Packets
0	drop	input	6 (tcp)	8291			!knock-final		0 B	0
1	add src to address list	input	6 (tcp)	11111			knock1		0 B	0
2	add src to address list	input	6 (tcp)	22222			knock2		0 B	0
3	add src to address list	input	6 (tcp)	33333			knock2		0 B	0

```
/ip firewall filter
```

```
add action=drop chain=input dst-port=8291 protocol=tcp src-address-list=!knock-final
```

```
add action=add-src-to-address-list address-list=knock1 address-list-timeout=10s chain=input dst-port=11111 \
```

```
    protocol=tcp
```

```
add action=add-src-to-address-list address-list=knock2 address-list-timeout=10s chain=input dst-port=22222 \
```

```
    protocol=tcp src-address-list=knock1
```

```
add action=add-src-to-address-list address-list=knock-final address-list-timeout=1d chain=input \  
    dst-port=33333 protocol=tcp src-address-list=knock2
```

How the Port Knocking works

```
D:\Saya\Apps\knock>dir
Volume in drive D has no label.
Volume Serial Number is F258-BA8D

Directory of D:\Saya\Apps\knock

09/09/2018  12:40 PM    <DIR>          .
09/09/2018  12:40 PM    <DIR>          ..
07/03/2005  02:30 AM             1,295,582  cygwin1.dll
08/10/2005  02:52 PM             15,238   knock.exe
           2 File(s)         1,310,820 bytes
           2 Dir(s)      127,842,557,952 bytes free

D:\Saya\Apps\knock>knock.exe
usage: knock [options] <host> <port[:proto]> [port[:proto]] ...
options:
  -u, --udp           make all ports hits use UDP (default is TCP)
  -v, --verbose       be verbose
  -V, --version       display version
  -h, --help         this help

example:  knock myserver.example.com 123:tcp 456:udp 789:tcp

D:\Saya\Apps\knock>knock your.mikrotik.ip-or-domain 12345:tcp 54321:udp
```

Port Knocking for Windows

Port Knocking for Linux

```
apt-get install knockd or yum install knockd
knock your.mikrotik.ip-address-or-domain 12345:tcp 54321:udp
```


SECURE CONNECTIONS

What is a Secure Connection

- A connection that is encrypted by one or more security protocols to ensure the security of data flowing between two or more nodes.
- When a connection is not encrypted, it can be easily listened to by anyone with the knowledge on how to do it.
- Protect the data being transferred from one computer to another

Self-signed Certificate

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar menu with options like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, System, Queues, Files, Log, Radius, Tools, New Terminal, Make Supout.rif, Manual, New WinBox, and Exit. The main window displays the 'IP Service List' dialog, which contains a table of services. The 'www-ssl' service is selected. A smaller dialog titled 'IP Service <www-ssl>' is open over it, showing configuration fields for Name, Port, Available From, and Certificate. The Certificate dropdown menu is open, showing options: enabled, CA, certificate.crt_0, none, and www.

Name	Port	Available From	Certificate
X api	8728		
X api-ssl	8729		none
X ftp	21		
ssh	22		
X telnet	23		
winbox	8291		
X www	80		
www-ssl	443		www

```
ip service set www-ssl certificate=www
```

Self-signed Certificate

Insecure Connection x +

https://webfix.mafiasoleh.info

Your connection is not secure

The owner of webfix.mafiasoleh.info has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

[Go Back](#) [Advanced](#)

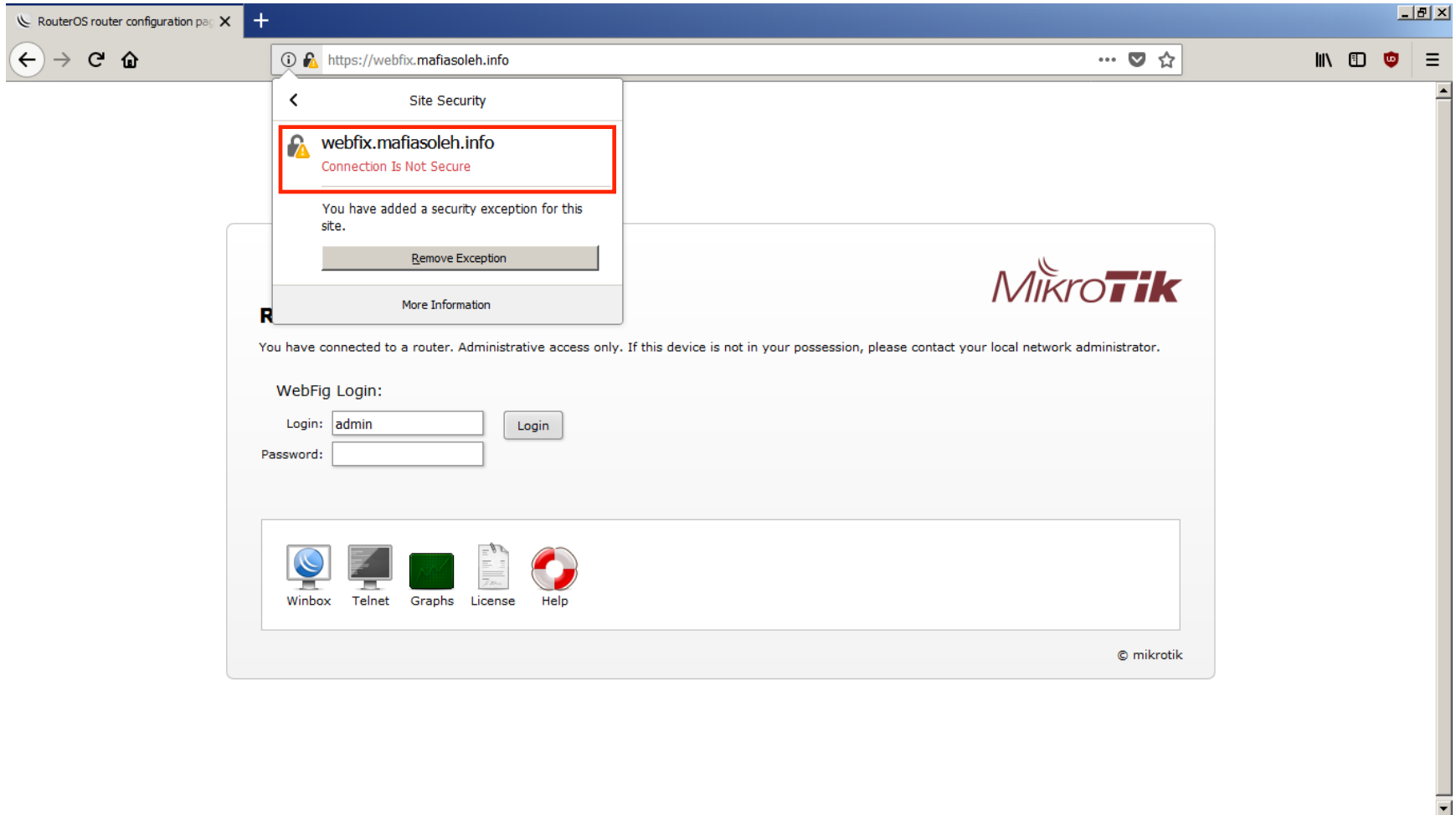
webfix.mafiasoleh.info uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

[Add Exception...](#)

Self-signed Certificate



Free of Charge Valid Certificate

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with various system settings. The main window shows the 'IP Service List' dialog, which contains a table of services. The 'www-ssl' service is selected and highlighted in blue. An 'IP Service <www-ssl>' configuration dialog is overlaid on top, showing the following fields:

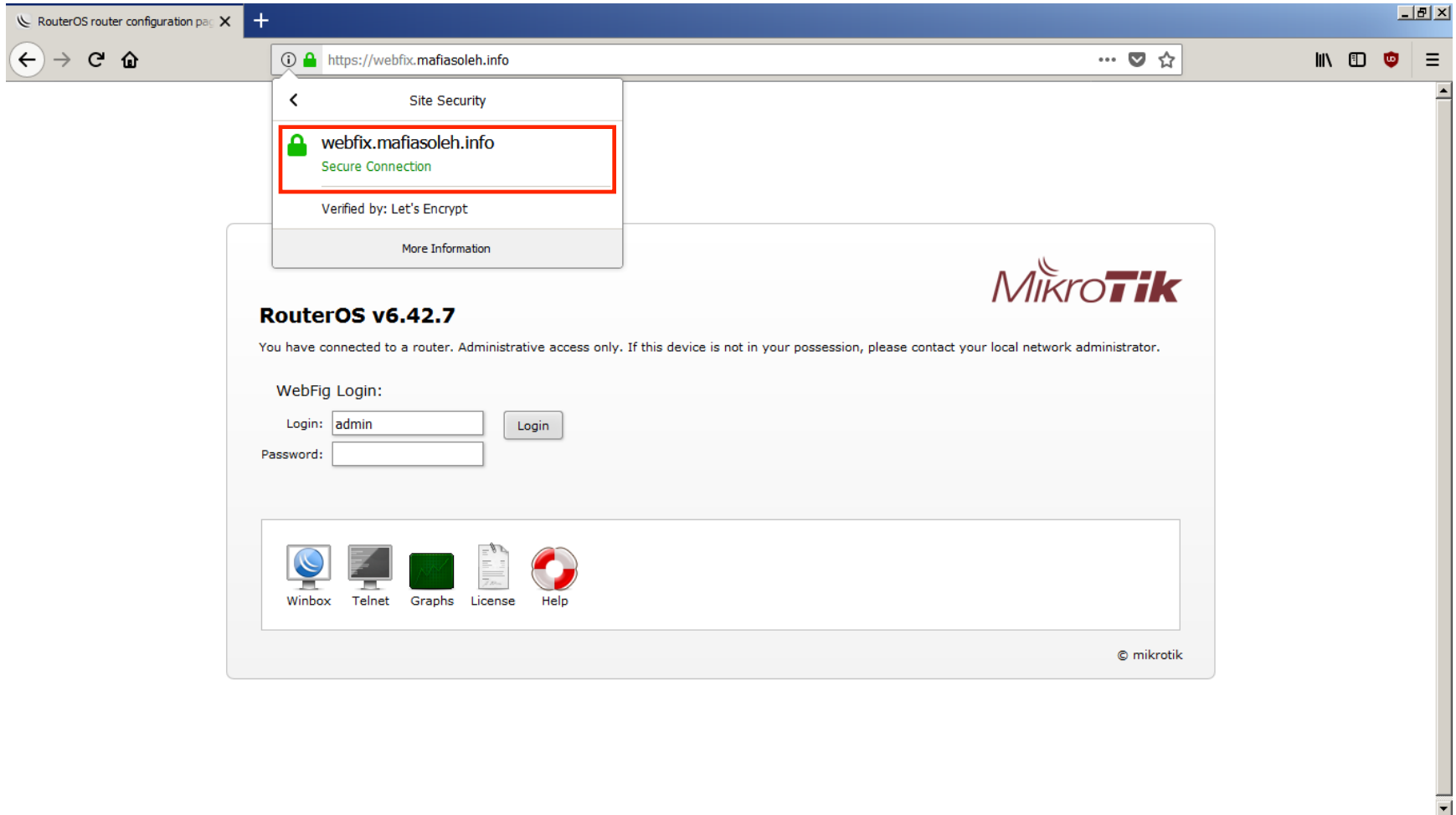
- Name: www-ssl
- Port: 443
- Available From: (empty)
- Certificate: certificate.crt_0

Buttons for 'OK', 'Cancel', 'Apply', and 'Disable' are visible on the right side of the configuration dialog. The status 'enabled' is shown at the bottom of the configuration dialog.

Name	Port	Available From	Certificate
X api	8728		
X api-ssl	8729		none
X ftp	21		
ssh	22		
X telnet	23		
winbox	8291		
X www	80		
www-ssl	443		

```
ip service set www-ssl certificate=certificate.crt_0
```

Free of Charge Valid Certificate

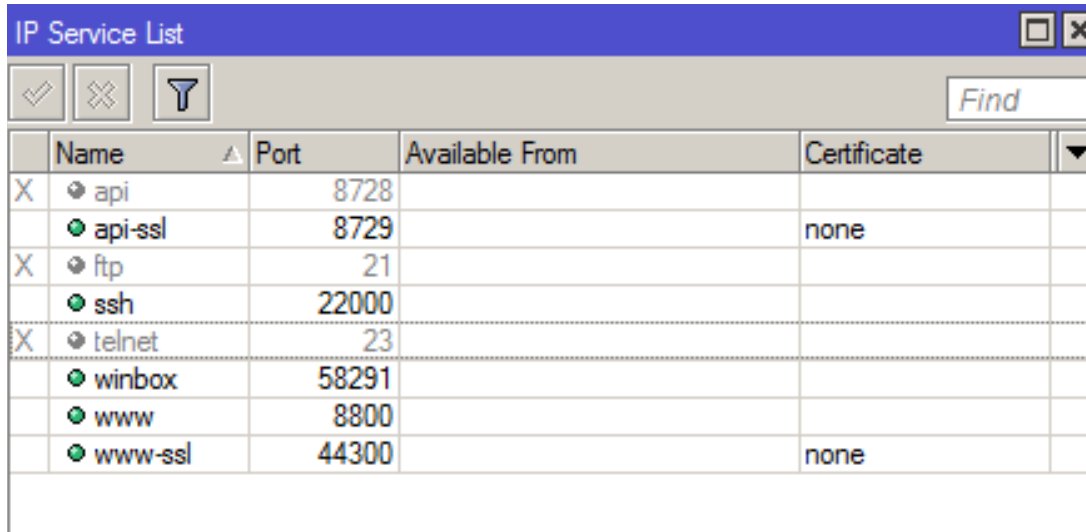


DEFAULT PORTS FOR THE SERVICES

Default Ports for the Services

- In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network.
- The port number identifies what type of port it is, and what kind of service those port is serving
- Some ports have numbers that are assigned to them by the IANA, and these are called the "well-known ports" which are specified in RFC1700.
- Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and designated as well-known ports.

Default Ports for the Services



The screenshot shows a window titled "IP Service List" with a search bar and a table of services. The table has columns for Name, Port, Available From, and Certificate. The services listed are: api (8728), api-ssl (8729), ftp (21), ssh (22000), telnet (23), winbox (58291), www (8800), and www-ssl (44300). The telnet service is marked as disabled with an 'X' in the first column.

	Name	Port	Available From	Certificate
X	api	8728		
	api-ssl	8729		none
X	ftp	21		
	ssh	22000		
X	telnet	23		
	winbox	58291		
	www	8800		
	www-ssl	44300		none

```
/ip service set telnet disabled=yes  
/ip service set ftp disabled=yes  
/ip service set www port=8800  
/ip service set ssh port=22000  
/ip service set www-ssl disabled=no port=44300  
/ip service set api disabled=yes  
/ip service set winbox port=58291
```

NB: Obscurity is not security - you should also use firewall rules

TUNNELING THROUGH SSH

What is an SSH Tunnel

- An SSH tunnel consists of an encrypted tunnel created using the SSH protocol connection
- The SSH tunnel can be used to encapsulate unencrypted traffic and transmit it via an encrypted channel.

How SSH Works



Host connects to RouterOS using ssh with local-port forwarding parameter



RouterOS accepted ssh connections from host



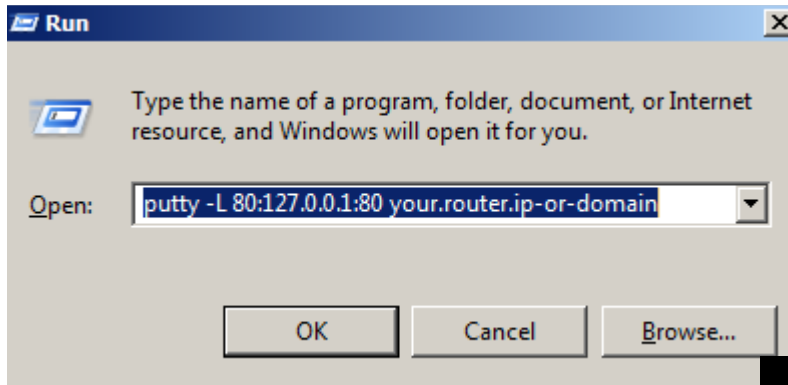
Host trying to open unencrypted port (80) from ssh tunnel via local-port forwarding ip



RouterOS sending http request from host via ssh tunnel



Configuring the SSH tunnel



SSH Local-Forwarding for Windows

SSH Local-Forwarding for Linux

```
ssh -L 80:127.0.0.1:80 your.router.ip-or-domain
```

```
MikroTik RouterOS 6.42.5 (c) 1999-2018      http://www.mikrotik.com/

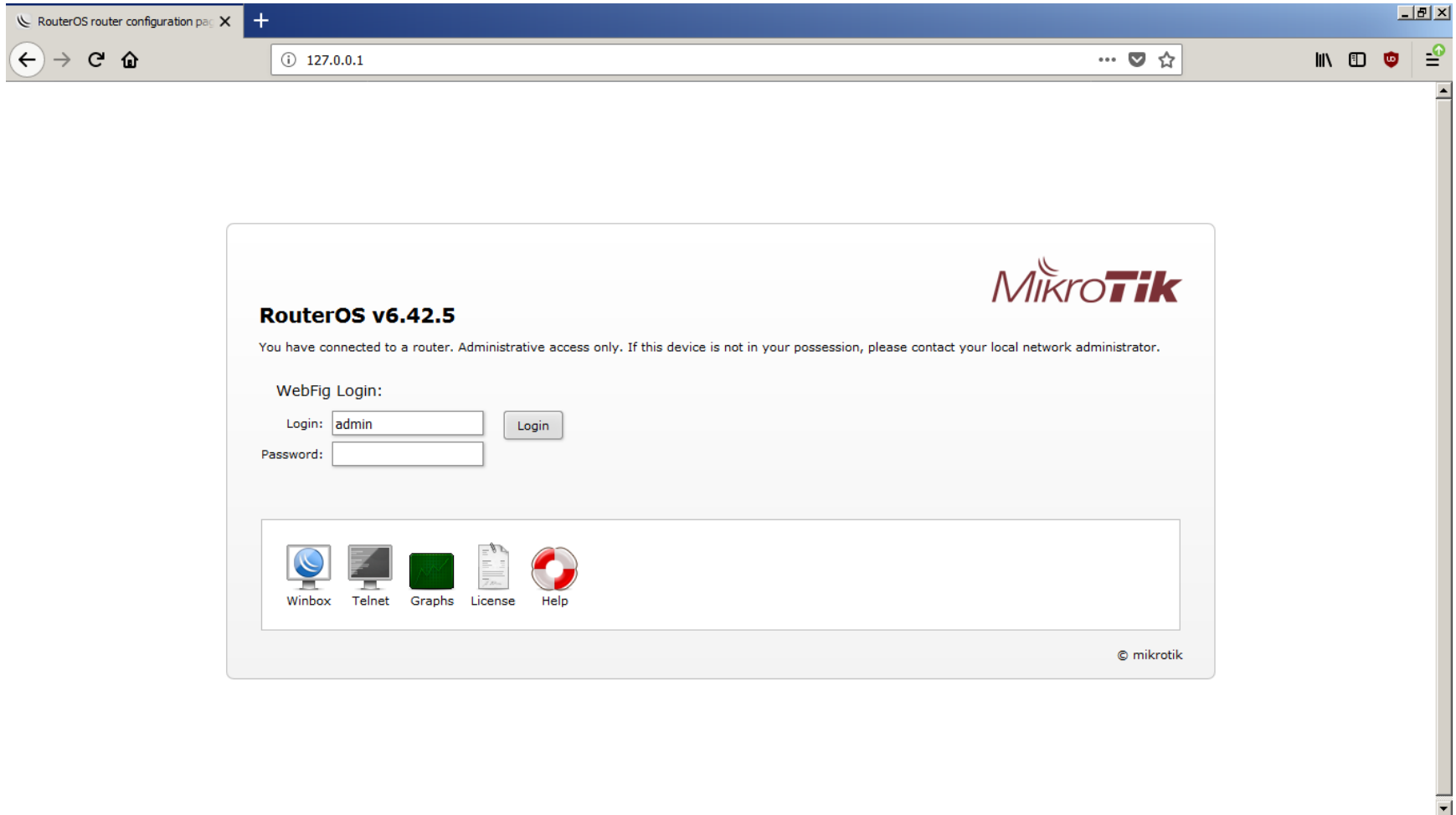
[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..          Move up one level
/command     Use command at the base level

[admin@01_Jose-Manuel] > █
```

Configuring the SSH tunnel



STATEFUL FIREWAL

RouterOS implements a stateful firewall. A stateful-firewall is a firewall capable of tracking ICMP, UDP, and TCP connections.

This means that the firewall is able to identify if a packet is related to previous packet.

Firewall can track operating state.

Connection tracking

The screenshot shows the Mikrotik WinBox interface for session 192.168.6.250. The 'Connections' tab is active, displaying a table with one entry:

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rat
SAC	192.168.6.250:8291	192.168.6.254:59183	6 (tcp)		23:59:59	established	7.8 kbps/320 bps

A 'Connection Tracking' dialog box is open, showing the following settings:

- Enabled: yes
- TCP Syn Sent Timeout: 00:00:05
- TCP Syn Received Timeout: 00:00:05
- TCP Established Timeout: 1d 00:00:00
- TCP Fin Wait Timeout: 00:00:10
- TCP Close Wait Timeout: 00:00:10
- TCP Last Ack Timeout: 00:00:10
- TCP Time Wait: 00:00:10
- TCP Close: 00:00:10
- TCP Max Retransmit Timeout: 00:05:00
- TCP Unacked Timeout: 00:05:00
- UDP Timeout: 00:00:10
- UDP Stream Timeout: 00:03:00

Connection tracking

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.6.250 (MikroTik) - WinBox v6.43.12 on CHR (x86_64)". The "Session" tab is active, showing "Safe Mode" and "Session: 192.168.6.250". The "Firewall" section is selected, with the "Tracking" tab highlighted. A "Connection Tracking" dialog box is open, showing the following configuration:

Parameter	Value
Enabled	yes
TCP Syn Sent Timeout	00:00:05
TCP Syn Received Timeout	00:00:05
TCP Established Timeout	1d 00:00:00
TCP Fin Wait Timeout	00:00:10
TCP Close Wait Timeout	00:00:10
TCP Last Ack Timeout	00:00:10
TCP Time Wait	00:00:10
TCP Close	00:00:10
TCP Max Retransmit Timeout	00:05:00
TCP Unacked Timeout	00:05:00
UDP Timeout	00:00:10
UDP Stream Timeout	00:03:00
ICMP Timeout	00:00:10
Generic Timeout	00:10:00

The background shows a Firewall rule named "SAC" with "Src. Address" set to "192.168.6.250/32". The "Tracking" tab is highlighted in the Firewall configuration area. The status bar at the bottom indicates "1 item" and "Max Entries: 1048576".

Connection tracking



Lab. ICMP tracking

```
/interface ethernet
set [ find default-name=ether1 ] comment="To Internet" name=ether1-
internet
set [ find default-name=ether2 ] comment="To Lan" name=ether2-Lan

/ip pool
add name=dhcp_pool0 ranges=192.168.11.2-192.168.11.254

/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=ether2-Lan
name=dhcp1
```

Lab. ICMP tracking

```
/ip address
add address=192.168.11.1/24 interface=ether2-Lan network=192.168.11.0

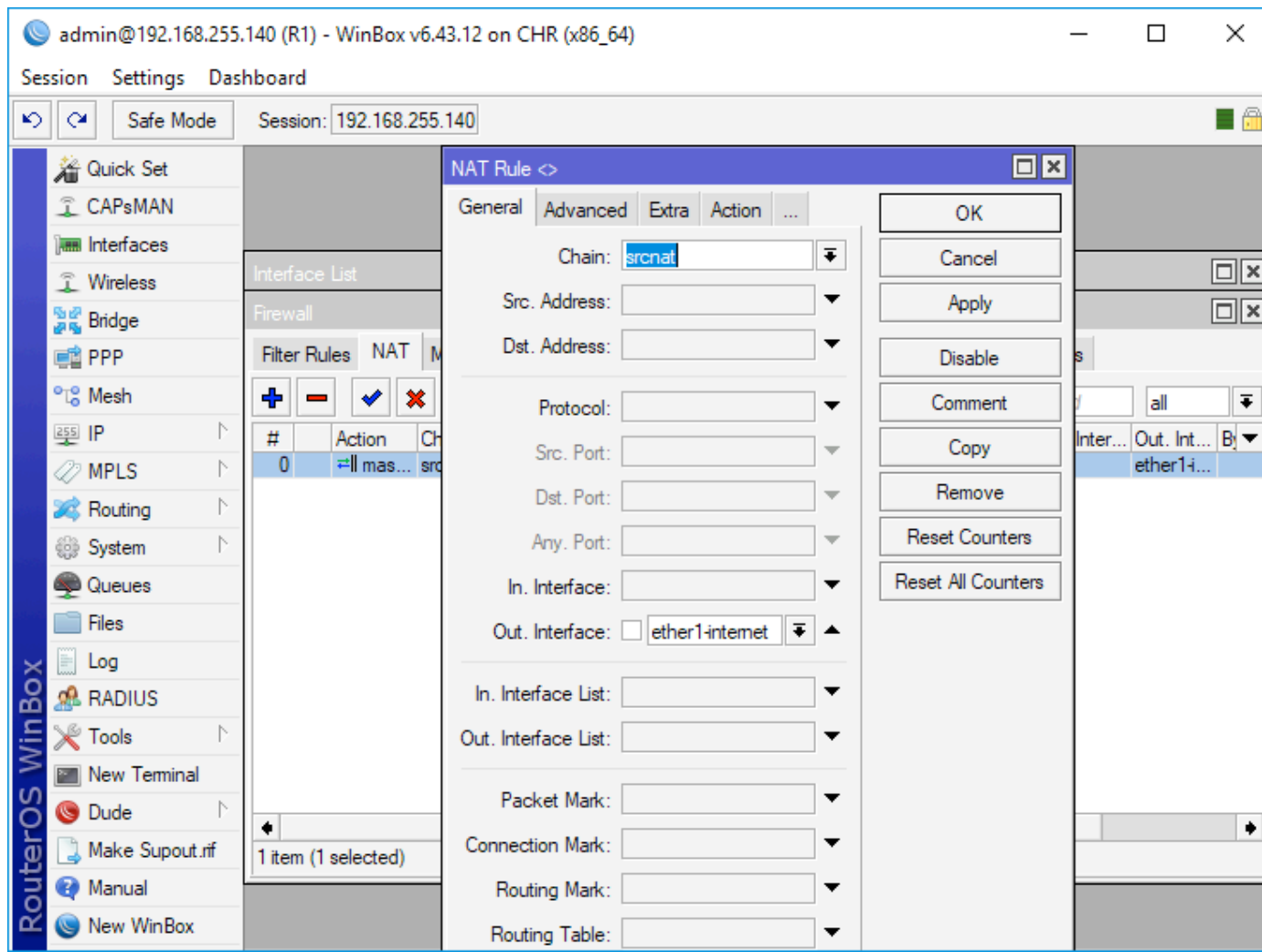
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=ether1-
internet

/ip dhcp-server network
add address=192.168.11.0/24 gateway=192.168.11.1

/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1-internet

/system identity
set name=R1
```

Lab. ICMP tracking



The screenshot shows the WinBox interface for configuring a NAT rule. The window title is "admin@192.168.255.140 (R1) - WinBox v6.43.12 on CHR (x86_64)". The main menu includes "Session", "Settings", and "Dashboard". The "NAT Rule" configuration window is open, showing the "General" tab. The "Chain" is set to "srcnat". The "Out. Interface" is set to "ether1-internet". The "In. Interface List" and "Out. Interface List" are empty. The "Packet Mark", "Connection Mark", "Routing Mark", and "Routing Table" are also empty. The "Action" tab is visible but not selected. The "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Reset Counters", and "Reset All Counters" buttons are present. The background shows the RouterOS WinBox sidebar with various configuration options like "Quick Set", "CAPsMAN", "Interfaces", "Wireless", "Bridge", "PPP", "Mesh", "IP", "MPLS", "Routing", "System", "Queues", "Files", "Log", "RADIUS", "Tools", "New Terminal", "Dude", "Make Supout.rif", "Manual", and "New WinBox".

Lab. ICMP tracking

admin@192.168.255.140 (R1) - WinBox v6.43.12 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 192.168.255.140

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dude
Make Supout.tif
Manual
New WinBox

Interface List

Firewall

#	Action	Chain
0	masquerade	srcnat

1 item (1 selected)

NAT Rule <>

Advanced Extra Action Statistics ...

Action: masquerade

Log

Log Prefix: [empty]

To Ports: [empty]

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Lab. ICMP tracking

```
/ip firewall mangle
add action=mark-connection chain=forward dst-address=8.8.8.8 new-
connection-mark=icmp passthrough=yes protocol=icmp
add action=mark-packet chain=forward connection-mark=icmp new-packet-
mark=icmpout out-interface=ether1-internet passthrough=yes
add action=mark-packet chain=forward connection-mark=icmp new-packet-
mark=icmpin out-interface=ether2-Lan passthrough=yes
```

Lab. ICMP tracking

```
/ip firewall mangle  
add action=mark-connection chain=forward dst-address=8.8.8.8  
new-connection-mark=icmp passthrough=yes protocol=icmp
```

Lab. ICMP tracking

The screenshot shows the WinBox interface for a Mikrotik router. The main window is titled "Firewall" and is displaying the "Tracking" tab. The tracking table shows several entries, with one entry for ICMP traffic highlighted by a blue box.

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Ra
SAC	192.168.11.1:58013	192.168.11.254:22	6 (tcp)		23:46:29	established	0 bps/0 bps
SCs	192.168.11.254	8.8.8.8	1 (icmp)	icmp	00:00:09		1344 bps/1344 bps
C	192.168.11.254:68	192.168.11.1:67	17 (u...		00:00:00		0 bps/0 bps
SAC	192.168.255.1:49188	192.168.255.140:22	6 (tcp)		23:46:29	established	0 bps/0 bps
SAC	192.168.255.1:49190	192.168.255.140:22	6 (tcp)		23:45:46	established	0 bps/0 bps
SAC	192.168.255.1:65527	192.168.255.140:8291	6 (tcp)		00:04:59	established	3.6 kbps/19.0 kb
C	192.168.255.240:137	192.168.255.255:137	17 (u...		00:00:09		0 bps/0 bps

The terminal window at the bottom shows the command prompt: `[admin@R1] >`

Lab. ICMP tracking

The screenshot shows the WinBox interface for configuring Firewall Filter Rules. The 'Filter Rules' tab is active, and the 'Filter Rules' list is displayed. The table below shows the configuration for three filter rules, with the 'Bytes' and 'Packets' columns highlighted by a blue box.

#	Action	Chain	Sr...	Dst. Address	Proto...	S.. D..	Out. Interface	Bytes	Packets
0	mark conne...	forward		8.8.8.8	1 (c...			672 B	8
1	mark packet	forward					ether1-internet	672 B	8
2	mark packet	forward					ether2-Lan	672 B	8

Below the table, the status of the filter rules is shown: 3 items, 0 items, 2 items, and enabled.

Lab. ICMP tracking

```
/ip firewall mangle  
add action=mark-packet chain=forward connection-mark=icmp new-packet-  
mark=icmpout out-interface=ether1-internet passthrough=yes
```

Lab. ICMP tracking

The screenshot shows the WinBox interface for RouterOS configuration. The main window is titled "Mangle Rule <>" and is divided into several tabs: General, Advanced, Extra, Action, and Statistics. The "General" tab is active, and the following settings are visible:

- Chain:** forward (highlighted with a blue box and the number 1)
- Out. Interface:** ether1-internet (highlighted with a blue box and the number 2)
- Connection Mark:** icmp (highlighted with a blue box and the number 3)
- Action:** mark packet (highlighted with a blue box and the number 4)
- New Packet Mark:** icmpout
- Passthrough:** checked

The left sidebar shows the RouterOS menu with various configuration options like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, RADIUS, Tools, New Terminal, Dude, Make Supout.nf, Manual, and New WinBox.

Lab. ICMP tracking

```
/ip firewall mangle  
add action=mark-packet chain=forward connection-mark=icmp new-packet-  
mark=icmpin out-interface=ether2-Lan passthrough=yes
```

Lab. ICMP tracking

The screenshot shows the WinBox interface for configuring a Mangle Rule. The window title is "admin@192.168.255.140 (R1) - WinBox v6.43.12 on CHR (x86_64)". The interface includes a sidebar with navigation options like "Quick Set", "CAPsMAN", "Interfaces", "Wireless", "Bridge", "PPP", "Mesh", "IP", "MPLS", "Routing", "System", "Queues", "Files", "Log", "RADIUS", "Tools", "New Terminal", "Dude", "Make Supout.tif", "Manual", and "New WinBox".

The main configuration area is divided into two panes, both titled "Mangle Rule <>". The left pane shows the "General" tab with the following settings:

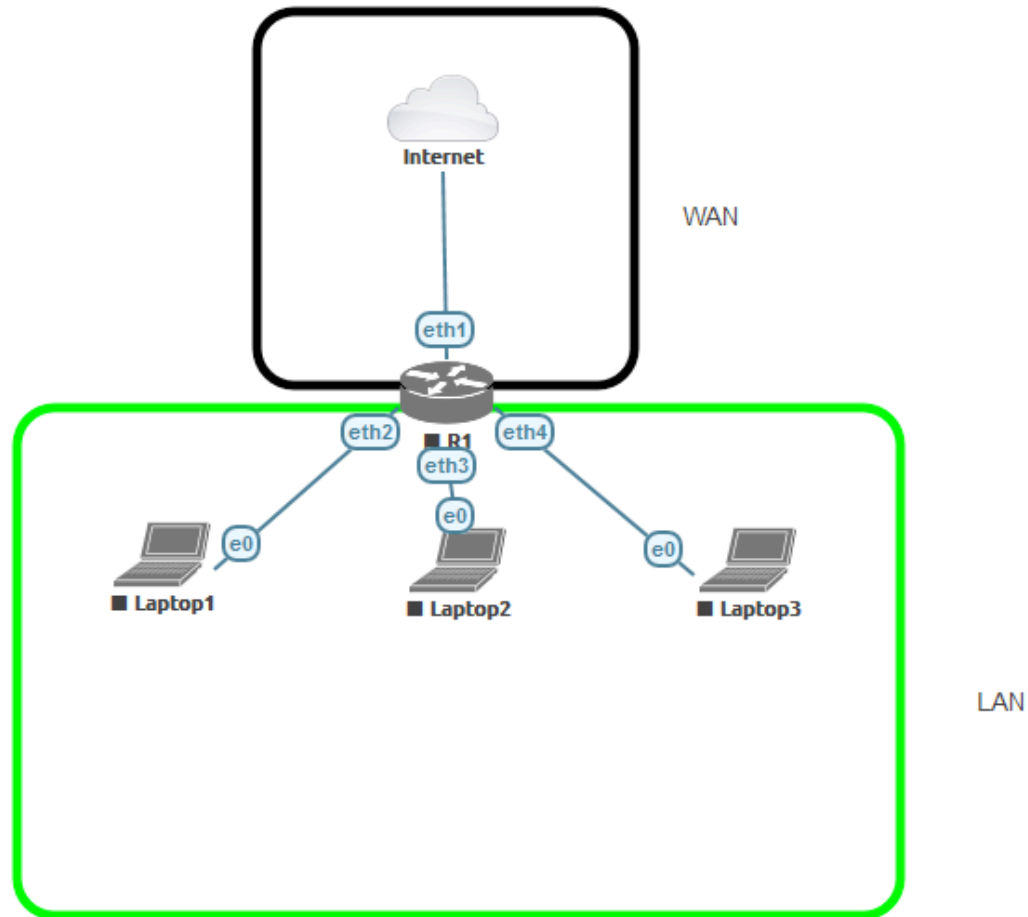
- Chain: forward
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)
- Out. Interface: ether2-Lan
- In. Interface List: (empty)
- Out. Interface List: (empty)
- Packet Mark: (empty)
- Connection Mark: icmp
- Routing Mark: (empty)
- Routing Table: (empty)

The right pane shows the "Action" tab with the following settings:

- Action: mark packet
- Log
- Log Prefix: (empty)
- New Packet Mark: icmpin
- Passthrough

Large blue numbers "1" and "2" are overlaid on the interface. Number "1" is positioned next to the "Out. Interface" dropdown menu, and number "2" is positioned next to the "Action" dropdown menu.

Lab. Securing areas



Lab. Securing areas

```
/interface bridge
add fast-forward=no name=Lan

/interface ethernet
set [ find default-name=ether1 ] name=E1-ToInternet

/interface list
add name=WAN
add name=LAN
```

Lab. Securing areas

```
/ip pool
add name=dhcp_pool0 ranges=192.168.188.2-192.168.188.254

/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=Lan name=dhcp1

/interface bridge port
add bridge=Lan interface=ether2
add bridge=Lan interface=ether3
add bridge=Lan interface=ether4

/interface list member
add interface=E1-ToInternet list=WAN
add interface=Lan list=LAN
```

Lab. Securing areas

```
/ip address
add address=192.168.188.1/24 interface=Lan network=192.168.188.0

/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=E1-
ToInternet

/ip dhcp-server network
add address=192.168.188.0/24 gateway=192.168.188.1

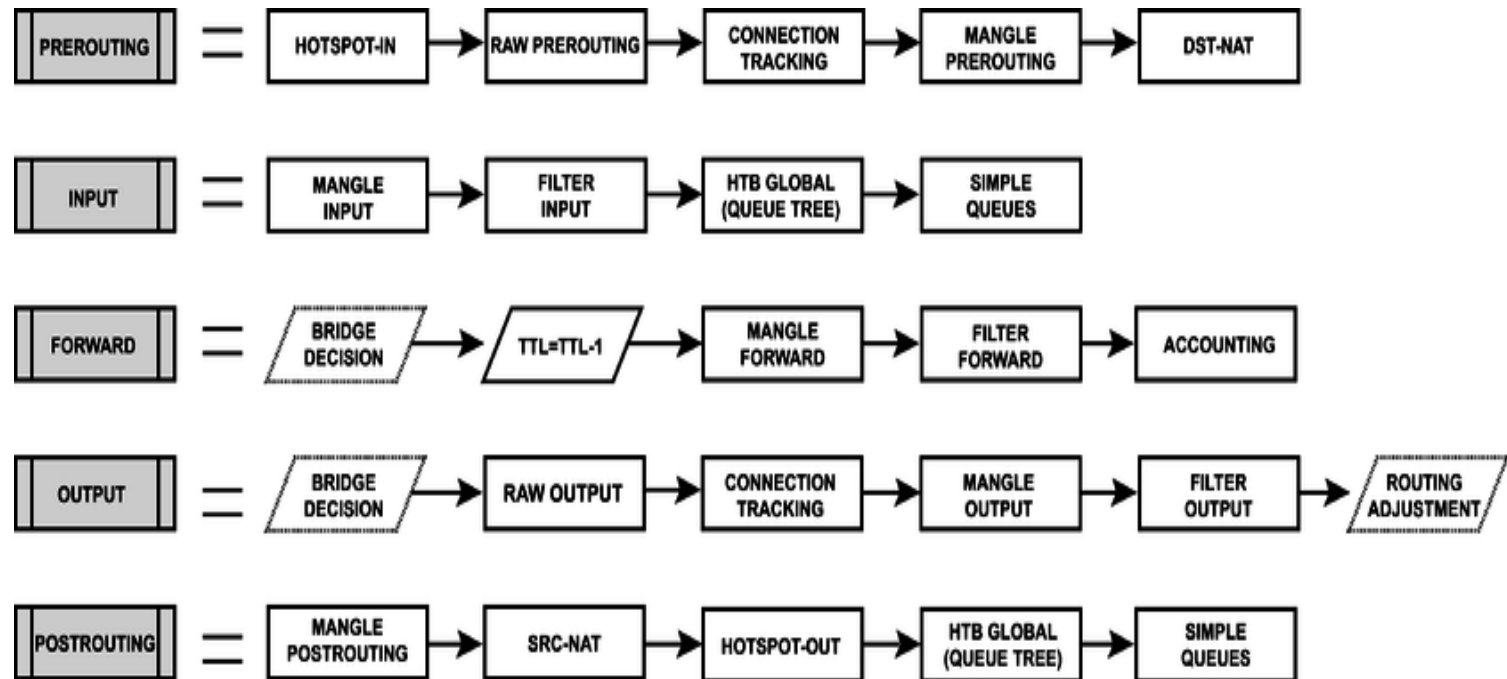
/ip firewall filter
add action=drop chain=forward comment="Drop external traffic"
connection-state=new in-interface-list=WAN

/ip firewall nat
add action=masquerade chain=srcnat out-interface-list=WAN

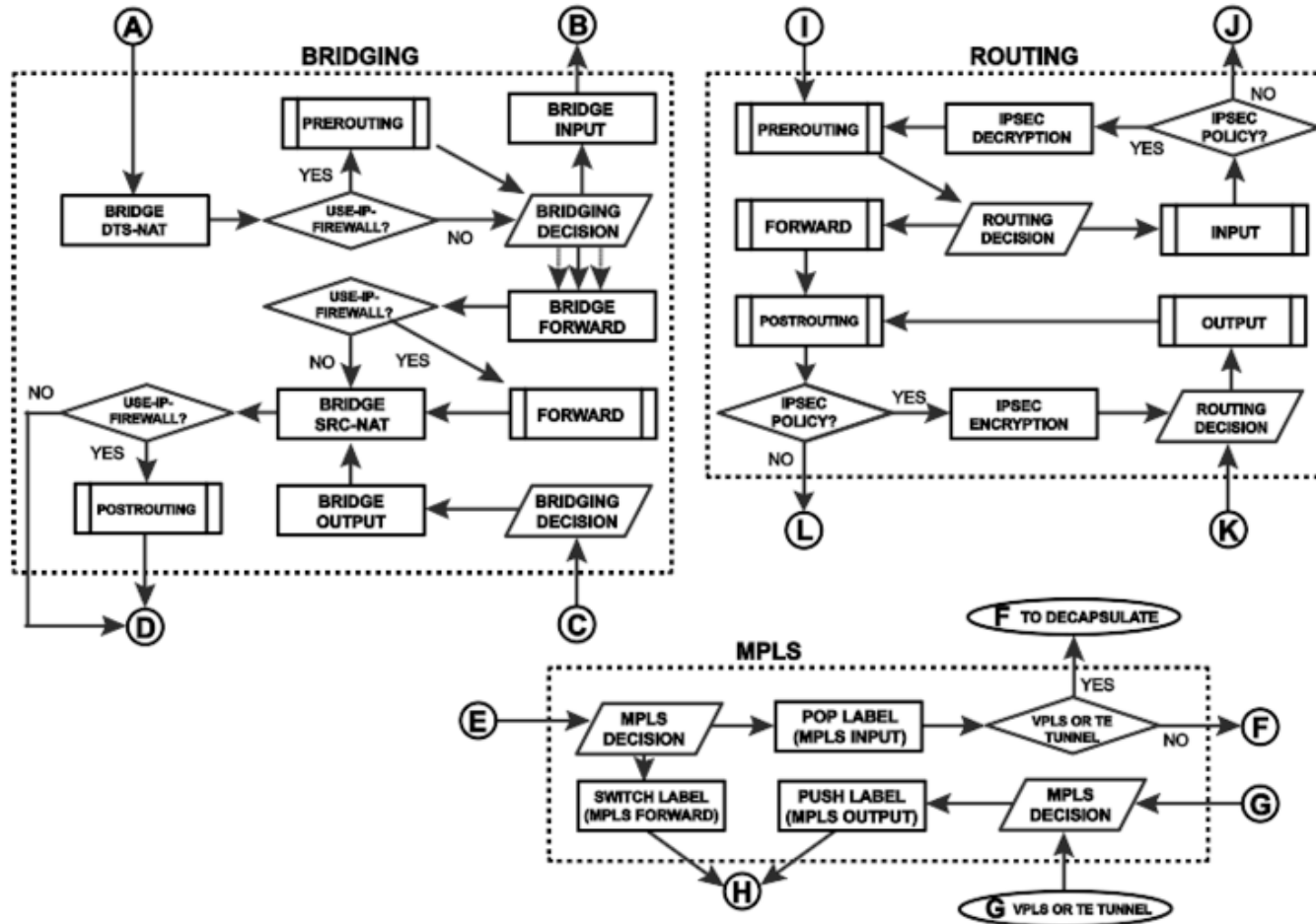
/system identity
set name=R1
```

PACKET FLOW

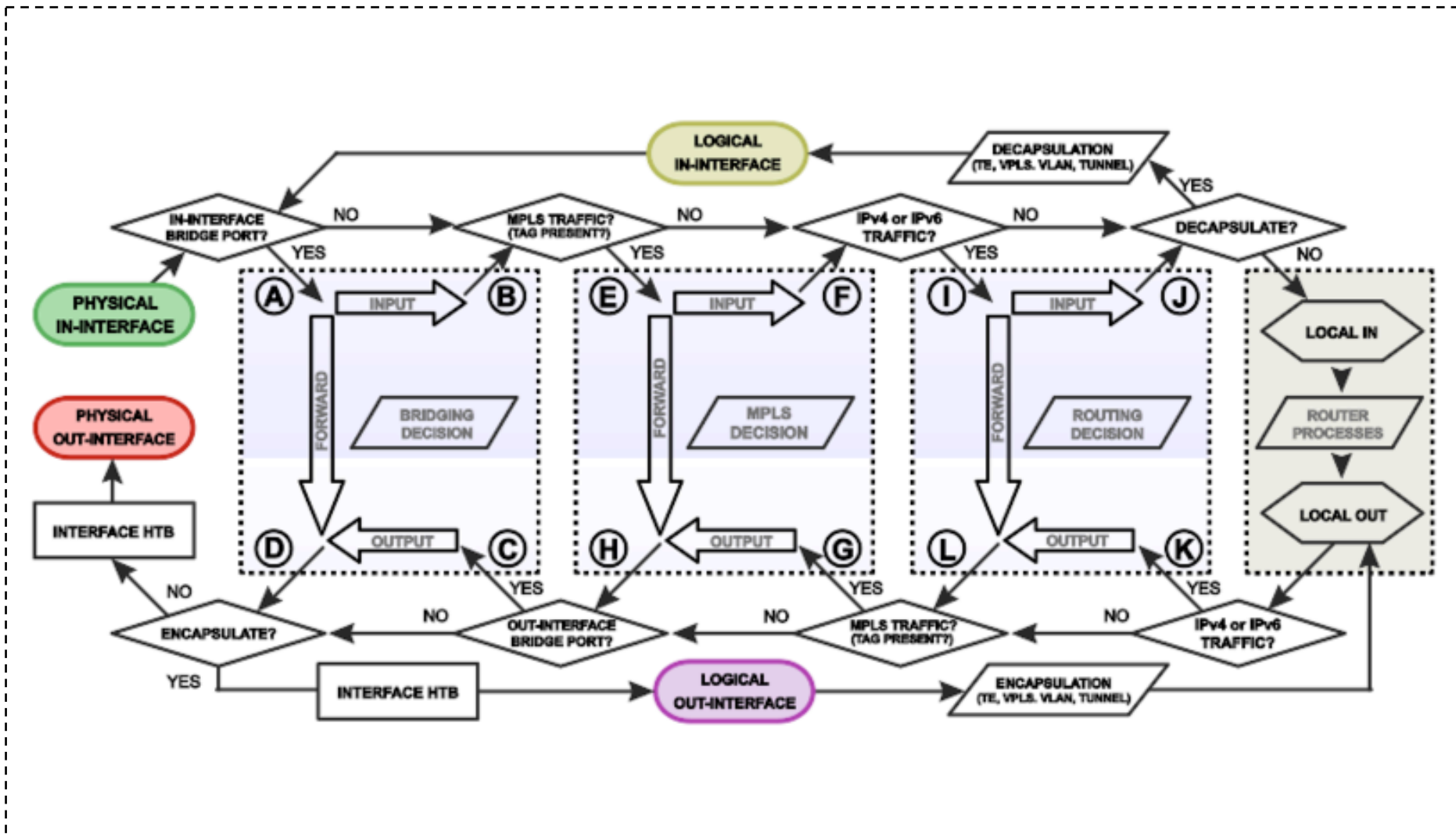
Packet flow



Packet flow



Packet flow

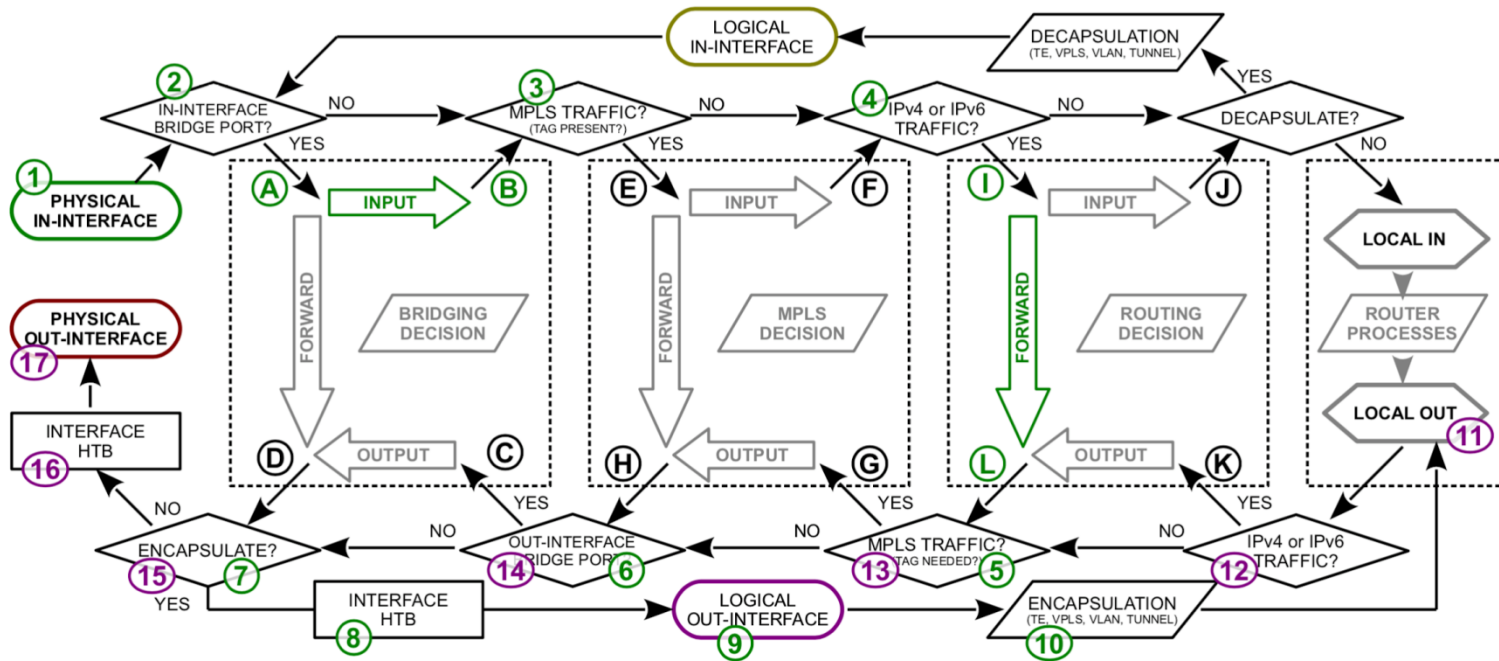


Packet flow

Packet Flow Scenario:

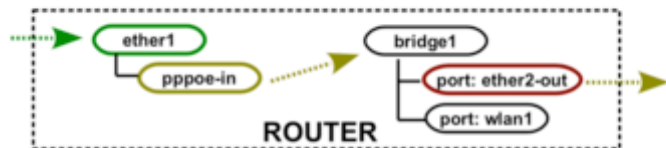


This Scenario in Packet Flow Diagram:

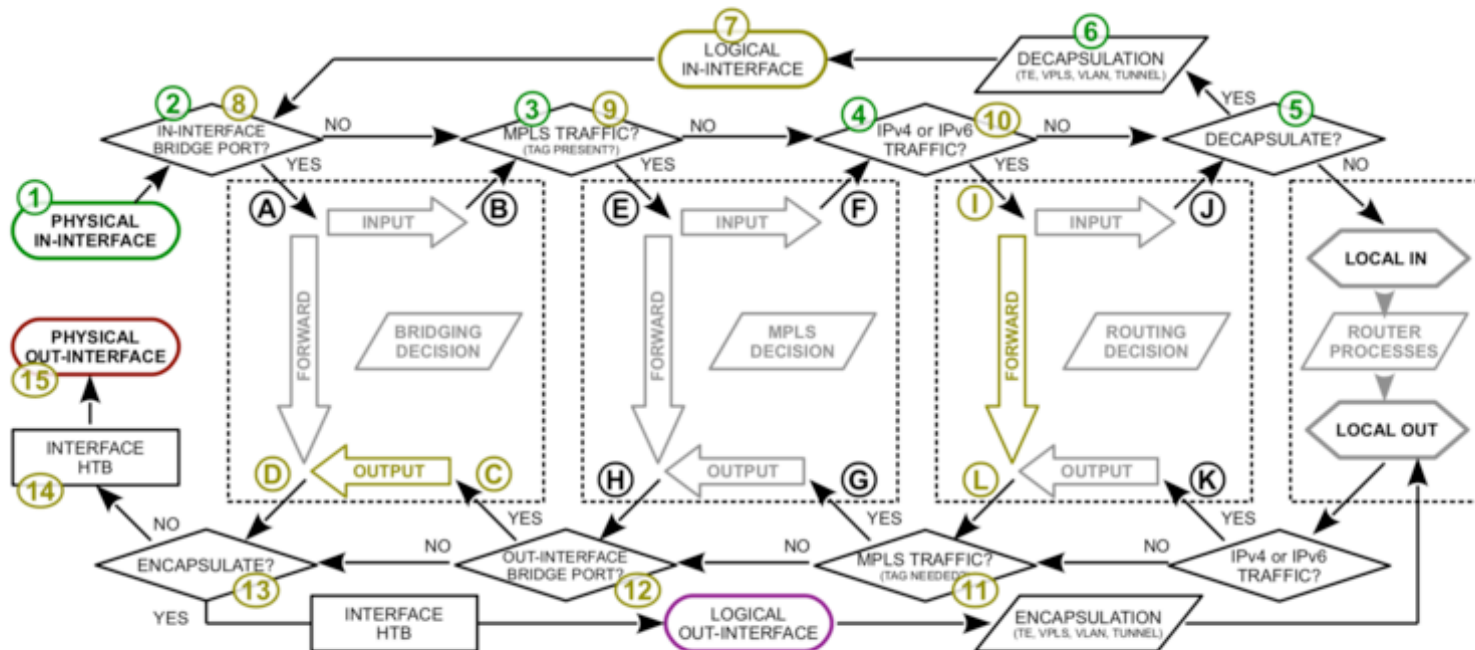


Packet flow

Packet Flow Scenario:



This Scenario in Packet Flow Diagram:

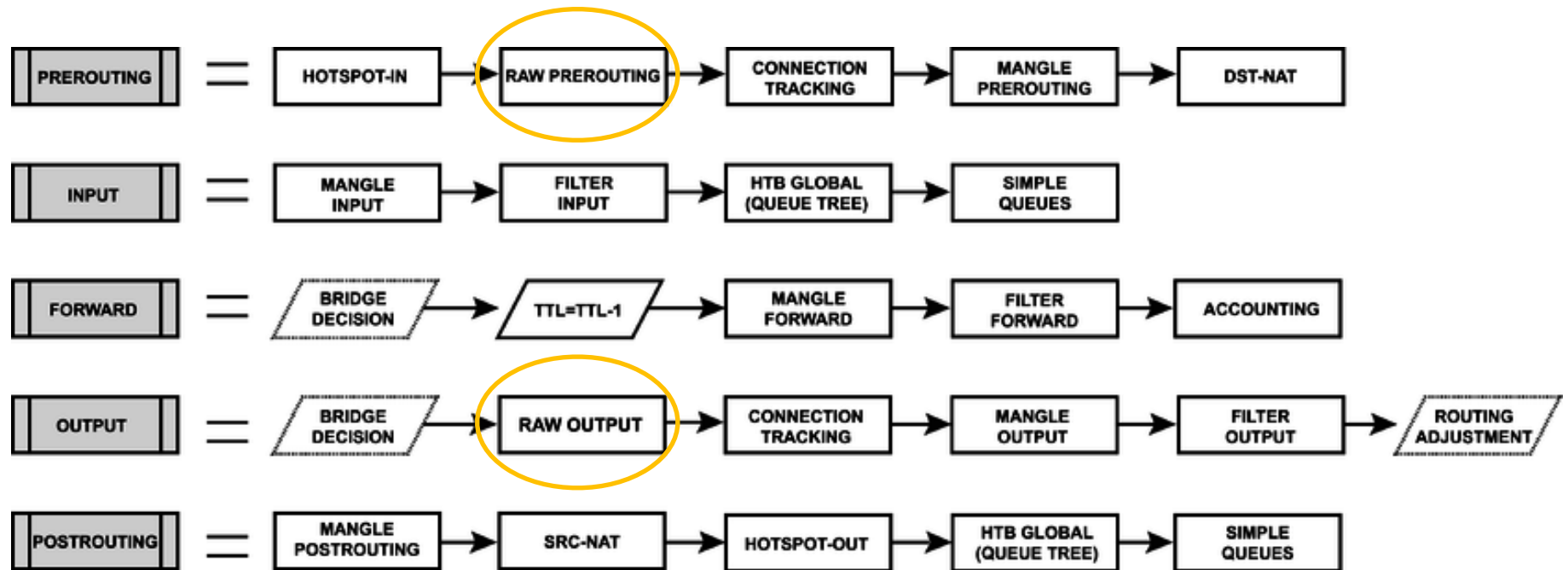


RAW TABLE

Raw table

- Raw table offer two chains - prerouting and output.
- The function of the raw table is to process the packets before the conntrack process.
- This is much more efficient.

Raw table chains



Raw table

The screenshot shows the WinBox interface for configuring a Firewall rule. The 'New Raw Rule' dialog box is open, showing the 'General' tab. The 'Chain' dropdown is set to 'prerouting', and the 'Src. Address' dropdown is set to 'prerouting'. The 'Dst. Address' dropdown is empty. The 'Protocol' dropdown is empty. The 'Src. Port', 'Dst. Port', and 'Any. Port' dropdowns are empty. The 'In. Interface' and 'Out. Interface' dropdowns are empty. The 'In. Interface List' and 'Out. Interface List' dropdowns are empty. The 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters' buttons are visible on the right side of the dialog box.

admin@192.168.255.140 (R1) - WinBox v6.42.4 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 192.168.255.140

Firewall

Filter Rules NAT Mangle Raw Service

#	Action	Chain	Src. Address
0 items			

New Raw Rule

General Advanced Extra Action ...

Chain: prerouting

Src. Address: prerouting

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Raw table. Drop packets

The screenshot shows the WinBox interface for a Mikrotik router. The main window is titled "admin@192.168.255.140 (R1) - WinBox v6.42.4 on CHR (x86_64)". The "New Raw Rule" dialog box is open, showing the following configuration:

- Chain: prerouting
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: udp
- Src. Port: (empty)
- Dst. Port: 53
- Any. Port: (empty)
- In. Interface: ether1-Internet
- Out. Interface: (empty)
- In. Interface List: (empty)
- Out. Interface List: (empty)

The dialog box has buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters. The background shows the WinBox sidebar with various menu items like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, Dude, Make Supout.rif, Manual, and New WinBox. The main window also shows a "Layer7 Protocols" table with columns for Port, Dst. Port, In. Inter..., Out. Int..., and Byt.

Raw table. Drop packets

The screenshot shows the WinBox v6.42.4 interface. The main window title is "admin@192.168.255.140 (R1) - WinBox v6.42.4 on CHR (x86_64)". The interface includes a top navigation bar with "Session", "Settings", and "Dashboard" tabs. Below this is a "Safe Mode" button and a "Session: 192.168.255.140" field. A left sidebar contains a tree view of system components: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, Dude, Make Supout.rif, Manual, and New WinBox. The main area displays the "New Raw Rule" dialog box, which has tabs for "Advanced", "Extra", "Action", and "Statistics". The "Action" tab is active, showing "Action: drop" in a dropdown menu, an unchecked "Log" checkbox, and a "Log Prefix:" field. On the right side of the dialog, there are buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Reset Counters", and "Reset All Counters". In the background, a table titled "Layer7 Protocols" is visible, with columns for "Port", "Dst. Port", "In. Inter...", "Out. Int...", and "By".

Raw table. Synflood attack

```
/ip firewall filter
add action=drop chain=input protocol=tcp tcp-flags=syn in-
interface=E1-ToInternet
```

Raw table. Synflood attack

The screenshot shows the WinBox v6.42.4 interface on a CHR (x86_64) device. The session is identified as 'admin@192.168.255.140 (R1)'. The left sidebar contains a menu with options: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, Dude, Make Supout.nf, Manual, New WinBox, and Exit. The main area displays a 'Resources' window with the following data:

Resource	Value
Uptime	00:08:12
Free Memory	1171.5 MiB
Total Memory	1203.2 MiB
CPU	QEMU
CPU Count	1
CPU Frequency	2299 MHz
CPU Load	100 %
Free HDD Space	69.3 MiB
Total HDD Size	95.3 MiB
Sector Writes Since Reboot	1 456
Total Sector Writes	1 457
Architecture Name	x86_64
Board Name	CHR
Version	6.42.4 (stable)
Build Time	Jun/15/2018 14:14:17

Raw table. Synflood attack

```
/ip firewall raw
chain=input action=drop tcp-flags=syn protocol=tcp in-interface=E1-
ToInternet
```

Raw table. Synflood attack

admin@192.168.255.140 (R1) - WinBox v6.42.4 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 192.168.255.140 CPU: 35%

Firewall

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

+ - ✓ ✗ [Filter Icon] 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✗ drop	prerouting			6 (tcp)			ether1		10.9 MiB	286 767

Raw table. Synflood attack

Test it on your
router!

DEFAULT CONFIGURATION

MikroTik Default Configuration

- All RouterBOARDS from factory come with a default configuration. There are several different configurations depending on the board type:
 - CPE router
 - LTE CPE AP router
 - AP router (single or dual band)
 - PTP Bridge (AP or CPE)
 - WISP Bridge (AP in ap_bridge mode)
 - Switch
 - IP only
 - CAP (Controlled Access Point)
- When should you remove the default-configuration and set up the router from scratch?

CPE Router

- In this type of configurations router is configured as wireless client device.
- WAN interface is Wireless interface.
- WAN port has configured DHCP client, is protected by IP firewall and MAC discovery/connection is disabled.

CPE Router

- List of routers using this type of configuration:
 - RB711, 911, 912, 921, 922 - with Level3 (CPE) license
 - SXT
 - QRT
 - SEXTANT
 - LHG
 - LDF
 - DISC
 - Groove
 - Metal

LTE CPE AP router

- This configuration type is applied to routers that have both an LTE and a wireless interface.
- The LTE interface is considered as a WAN port protected by the firewall and MAC discovery/connection disabled.
- IP address on the WAN port is acquired automatically. Wireless is configured as an access point and bridged with all available Ethernet ports.
- List of routers using this type of configuration:
 - wAP LTE kit
 - LtAP mini kit

AP Router (single or dual band)

- This type of configuration is applied to home access point routers to be used straight out of the box without additional configuration (except router and wireless passwords)
- First Ethernet port is configured as a WAN port (protected by firewall, with a DHCP client and disabled MAC connection/discovery)
- Other Ethernet ports and wireless interfaces are added to local LAN bridge with an IP 192.168.88.1/24 and a DHCP server
- In case of dual band routers, one wireless is configured as 5 GHz access point and the other as 2.4 GHz access point.
- List of routers using this type of configuration:
 - RB450, 751, 850, 951, 953, 2011, 3011, 4011
 - mAP, wAP, hAP, OmniTIK

PTP Bridge (AP or CPE)

- Bridged ethernet with wireless interface
- Default IP address 192.168.88.1/24 is set on the bridge interface
- There are two possible options - as CPE and as AP
 - For CPE wireless interface is set in "station-bridge" mode.
 - For AP "bridge" mode is used.
- List of routers using this type of configuration:
 - DynaDish - as CPE

WISP Bridge

- Configuration is the same as PTP Bridge in AP mode, except that wireless mode is set to ap_bridge for PTMP setups.
- Router can be accessed directly using MAC address.
- If device is connected to the network with enabled DHCP server, configured DHCP client configured on the bridge interface will get the IP address, that can be used to access the router.
- List of routers using this type of configuration:
 - RB 911,912,921,922 - with Level4 license
 - cAP, Groove A, Metal A, RB711 A
 - BaseBox, NetBox
 - mANTBox, NetMetal

Switch

- This configuration utilises switch chip features to configure dumb switch.
- All ethernet ports are added to switch group and default IP address 192.168.88.1/24 is set on master port.
- RoS 6.41 onwards uses Hardware Offload and places all ports into a Bridge instead.
- List of routers using this type of configuration:
 - FiberBox
 - CRS without wireless interface

IP Only

- When no specific configuration is found, IP address 192.168.88.1/24 is set on ether1, or combo1, or sfp1.
- List of routers using this type of configuration:
 - RB 411,433,435,493,800,M11,M33,1100
 - CCR

CAP

- This type of configuration is used when device is to be used as a wireless access point which is controlled by the CAPsMAN
- When CAP default configuration is loaded, ether1 is considered as a management port with a DHCP client
- All other Ethernet interfaces are bridged and all wireless interfaces are set to be managed by the CAPsMAN
- None of the current boards come with the CAP mode enabled from the factory. The above mentioned configuration is applied to all boards with at least one wireless interfaces when set to the CAP mode

IPv6

- Note. The IPv6 package by default is disabled on RouterOS v6. When enabled, after the first reboot, default configuration will be applied to the IPv6 firewall as well.

Print the factory default-configuration

- `/system default-configuration print`

IP firewall to a router

- Work with new connections to decrease load on a router;
- Create address-list for IP addresses that are allowed to access your router;
- Enable ICMP access (optionally);
- Drop everything else, log=yes might be added to log packets that hit the specific rule;

IP firewall for clients

- Established/related packets are added to fasttrack** for faster data throughput
 - firewall will work with new connections only;
- Drop invalid connection and log them with prefix invalid;
- Drop attempts to reach non public addresses from your local network (rfc1918) (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
 - drop forward dst-address-list=not_in_internet
 - bridge1 is local network interface
 - log attempts with prefix="!public_from_LAN";

** note Fasttrack limitations for Queues etc

IP firewall for clients

- Drop incoming packets that are not NATed,
 - ether1 is public interface, log attempts with !NAT prefix;
- Drop incoming packets from Internet, which are not public IP addresses (rfc1918),
 - ether1 is public interface,
 - log attempts with prefix="!public";
- Drop packets from LAN that does not have LAN IP,
 - 192.168.88.0/24 is local network used subnet;

MANAGEMENT ACCESS

RouterOS services

- `/ip service disable telnet,ftp,www,api,api-ssl`

Change default ports

- `/ip service set ssh port=2200`

Restrict access by ip

- /ip service set winbox address=192.168.88.0/24

Mac-server

RouterOS has built-in options for easy management access to network devices even without IP configuration. On production networks the particular services should be set to restricted access (e.g. only internal interfaces) or disable entirely!

```
/tool mac-server set allowed-interface-list=none
```

```
/tool mac-server mac-winbox set allowed-interface-list=none
```

```
/tool mac-server ping set enabled=no
```

Bandwidth Test

Bandwidth test server is used to test throughput between two MikroTik routers. It is recommended to disable it on a production environment.

```
/tool bandwidth-server set enabled=no
```

DNS Cache

DNS cache facility can be used to provide domain name resolution for the router itself as well as for the clients connected to it.

In case the DNS cache is not required on your router or if another router is used for such purposes, DNS cache should be disabled:

```
/ip dns set allow-remote-requests=no
```

If DNS cache is left enabled be sure to protect UDP/53 on the input chain with firewall rules

Other Client Services

```
/ip proxy set enabled=no
```

```
/ip socks set enabled=no
```

```
/ip upnp set enabled=no
```

```
/ip cloud set ddns-enabled=no update-time=no
```

More Secure SSH - Strong-Crypto=Yes

Introduces following changes in the SSH configuration:

- Prefer 256 and 192 bit encryption instead of 128 bits
- Disable null encryption
- Prefer sha256 for hashing instead of sha1
- Disable md5
- Use 2048bit prime for Diffie Hellman exchange instead of 1024bit

```
/ip ssh set strong-crypto=yes
```

Unused interfaces

In order to protect from unauthorised access, it is considered good practice to disable all unused interfaces on the router

BRIDGE FIREWALL

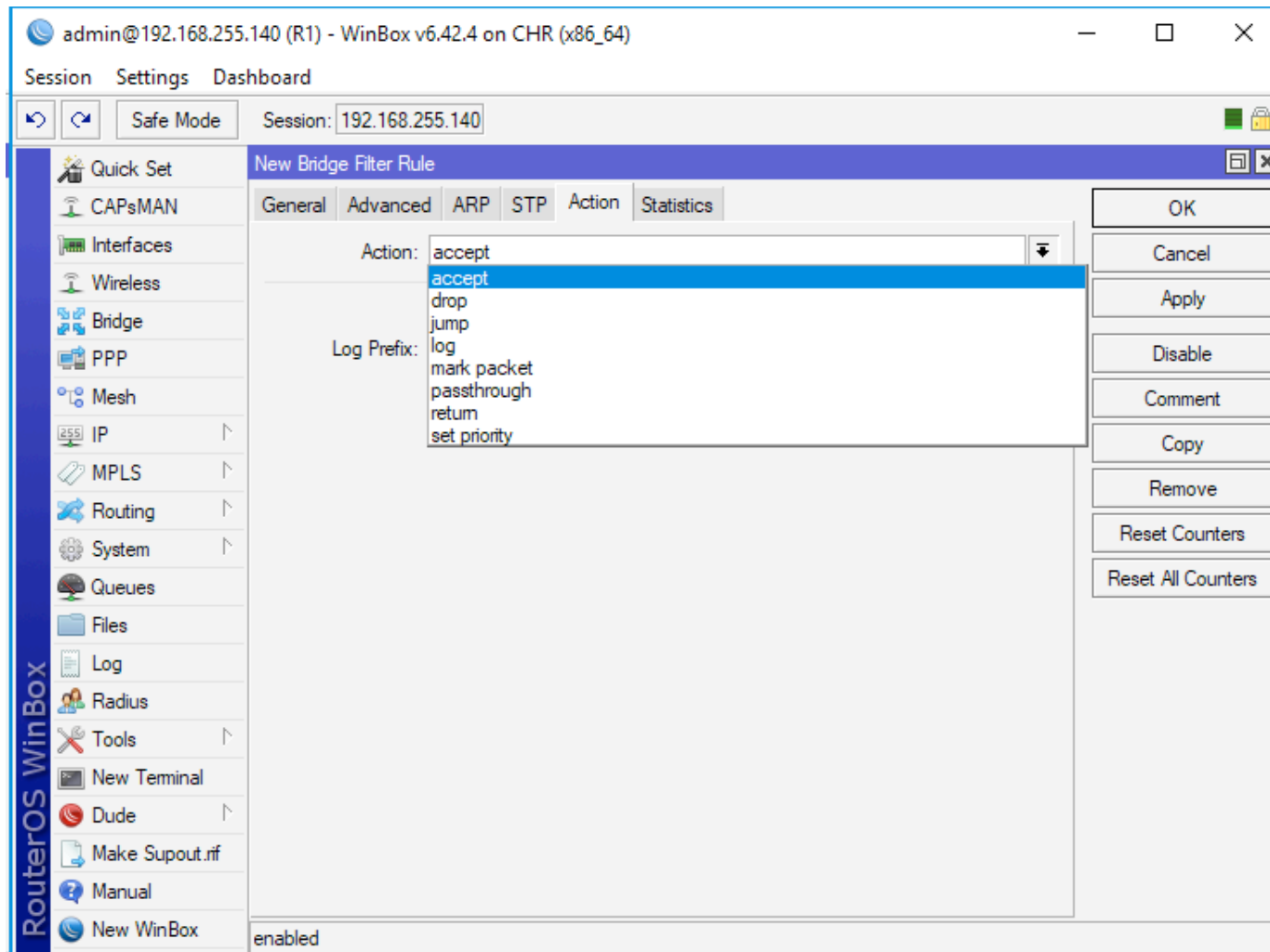
Bridge Firewall

The bridge firewall implements packet filtering and thereby provides security functions that are used to manage data flow to, from and through bridge.

Bridge Firewall

The screenshot displays the RouterOS WinBox interface. The top bar shows the user 'admin@192.168.255.140 (R1)' and the version 'WinBox v6.42.4 on CHR (x86_64)'. The main menu includes 'Session', 'Settings', and 'Dashboard'. The left sidebar lists various configuration categories: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, Dude, Make Supout.rif, Manual, and New WinBox. The main window is titled 'Firewall' and contains tabs for 'Filter Rules', 'NAT', 'Mangle', 'Raw', 'Service Ports', 'Connections', 'Address Lists', and 'Layer7 Protocols'. A table with columns '#', 'Action', 'Chain', 'Src. Address', 'Dst. Address', 'Proto...', 'Src. Port', 'Dst. Port', 'In. Inter...', 'Out. Int...', and 'Byt...' is visible. A 'New Bridge Filter Rule' dialog box is open, showing the 'General' tab. The 'Chain' dropdown is set to 'forward', and a list of options (input, forward, output) is displayed. The dialog also includes fields for 'Interfaces', 'Bridges', 'Src. MAC Address', 'Dst. MAC Address', 'MAC Protocol', 'IP', 'Packet Mark', and 'Ingress Priority'. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters' are present. The status 'enabled' is shown at the bottom of the dialog.

Bridge Firewall



Lab. Only PPPoE Traffic



Lab. Only PPPoE Traffic

R1 Setup (PPPoE Server)

```
                /interface ethernet
set [ find default-name=ether1 ] name=E1-ToBridge

/ip address
add address=192.168.100.1/30 interface=E1-ToBridge
network=192.168.100.0
```

Lab. Only PPPoE Traffic

```
/interface pppoe-server server  
add disabled=no interface=E1-ToBridge
```

```
/ppp secret  
add local-address=10.100.100.1 name=test password=test \  
remote-address=10.200.200.2 service=pppoe
```

```
/system identity  
set name=R1
```

Lab. Only PPPoE Traffic

R3 Setup (PPPoE Client)

```
/interface ethernet
set [ find default-name=ether1 ] name=E1-ToBridge

/interface pppoe-client
add disabled=no interface=E1-ToBridge name=test password=test \
user=test

/ip address
add address=192.168.100.2/30 interface=E1-ToBridge \
network=192.168.100.0

/system identity set name=R3
```

Lab. Only PPPoE Traffic

Bridge Setup

```
/interface bridge  
add name=bridge1
```

```
/interface ethernet  
set [ find default-name=ether2 ] name=E2-ToR1  
set [ find default-name=ether3 ] name=E3-ToR3
```

```
/interface bridge filter  
add action=accept chain=forward mac-protocol=pppoe  
add action=accept chain=forward mac-protocol=pppoe-discovery  
add action=drop chain=forward
```


Lab. Only PPPoE Traffic

```
/interface bridge port  
add bridge=bridge1 interface=E2-ToR1  
add bridge=bridge1 interface=E3-ToR3
```

```
/system identity  
set name=Bridge
```

ICMP FILTERING

What is ICMP Filtering

- ICMP helps networks to cope with communication problems
- No authentication method; can be used by hackers to crash computers on the network
- Firewall/packet filter must be able to determine, based on its message type, whether an ICMP packet should be allowed to pass

ICMPv4 FILTERING

Table Filtering Recommendations

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-unreach-net	Rate-Limit	Rate-Limit	Rate-Limit
ICMPv4-unreach-host	Rate-Limit	Rate-Limit	Rate-Limit
ICMPv4-unreach-proto	Rate-Limit	Deny	Rate-Limit
ICMPv4-unreach-port	Rate-Limit	Deny	Rate-Limit
ICMPv4-unreach-frag-needed	Send	Permit	Rate-Limit
ICMPv4-unreach-src-route	Rate-Limit	Deny	Rate-Limit
ICMPv4-unreach-net-unknown (<i>Depr</i>)	Deny	Deny	Deny
ICMPv4-unreach-host-unknown	Rate-Limit	Deny	Ignore
ICMPv4-unreach-host-isolated (<i>Depr</i>)	Deny	Deny	Deny
ICMPv4-unreach-net-tos	Rate-Limit	Deny	Rate-Limit

Recommendations for

ICMPv4

Table Filtering Recommendations

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-unreach-host-tos	Rate-Limit	Deny	Rate-Limit
ICMPv4-unreach-admin	Rate-Limit	Rate-Limit	Rate-Limit
ICMPv4-unreach-prec-violation	Rate-Limit	Deny	Rate-Limit
ICMPv4-unreach-prec-cutoff	Rate-Limit	Deny	Rate-Limit
ICMPv4-quench	Deny	Deny	Deny
ICMPv4-redirect-net	Rate-Limit	Deny	Rate-Limit
ICMPv4-redirect-host	Rate-Limit	Deny	Rate-Limit
ICMPv4-redirect-tos-net	Rate-Limit	Deny	Rate-Limit
ICMPv4-redirect-tos-host	Rate-Limit	Permit	Rate-Limit
ICMPv4-timed-ttl	Rate-Limit	Permit	Rate-Limit

Recommendations for

ICMPv4

Table Filtering Recommendations

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-timed-reass	Rate-Limit	Permit	Rate-Limit
ICMPv4-parameter-pointer	Rate-Limit	Deny	Rate-Limit
ICMPv4-option-missing	Rate-Limit	Deny	Rate-Limit
ICMPv4-req-echo-message	Rate-Limit	Permit	Rate-Limit
ICMPv4-req-echo-reply	Rate-Limit	Permit	Rate-Limit
ICMPv4-req-router-sol	Rate-Limit	Deny	Rate-Limit
ICMPv4-req-router-adv	Rate-Limit	Deny	Rate-Limit
ICMPv4-req-timestamp-message	Rate-Limit	Deny	Rate-Limit
ICMPv4-req-timestamp-reply	Rate-Limit	Deny	Rate-Limit
ICMPv4-info-message (<i>Depr</i>)	Deny	Deny	Deny

Recommendations for
ICMPv4

Table Filtering Recommendations

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-info-reply (Depr)	Deny	Deny	Deny
ICMPv4-mask-request	Rate-Limit	Deny	Rate-Limit
ICMPv4-mask-reply	Rate-Limit	Deny	Rate-Limit

Recommendations for
ICMPv4

ICMPv4 Error Messages

- Echo Reply (Type 0, Code 0)
- Destination Unreachable (Type 3)
 - Net Unreachable (Code 0)
 - Host Unreachable (Code 1)
 - Protocol Unreachable (Code 2)
 - Port Unreachable (Code 3)
 - Fragmentation Needed and DF Set (Code 4)
 - Source Route Failed (Code 5)
 - Destination Network Unknown (Code 6) (Deprecated)
 - Destination Host Unknown (Code 7)
 - Source Host Isolated (Code 8) (Deprecated)
 - Communication with Destination Network Administratively Prohibited (Code 9) (Deprecated)

ICMPv4 Error Messages

- Destination Unreachable (Type 3)
 - Communication with Destination Host Administratively Prohibited (Code 10) (Deprecated)
 - Network Unreachable for Type of Service (Code 11)
 - Host Unreachable for Type of Service (Code 12)
 - Communication Administratively Prohibited (Code 13)
 - Host Precedence Violation (Code 14)
 - Precedence Cutoff in Effect (Code 15)

ICMPv4 Error Messages

- Source Quench (Type 4, Code 0)
- Redirect (Type 5)
 - Redirect Datagrams for the Network (Code 0)
 - Redirect Datagrams for the Host (Code 1)
 - Redirect datagrams for the Type of Service and Network (Code 2)
 - Redirect Datagrams for the Type of Service and Host (Code 3)
- Time Exceeded (Type 11)
 - Time to Live Exceeded in Transit (Code 0)
 - Fragment Reassembly Time Exceeded (Code 1)

ICMPv4 Error Messages

- Parameter Problem (Type 12)
 - Pointer Indicates the Error (Code 0)
 - Required Option is Missing (Code 1)

ICMPv4 Informational Messages

- Echo or Echo Reply Message
 - Echo Message (Type 8, Code 0)
 - Echo Reply Message (Type 0, Code 0)
- Router Solicitation or Router Advertisement message
 - Router Solicitation Message (Type 10, Code 0)
 - Router Advertisement Message (Type 9, Code 0)
- Timestamp or Timestamp Reply Message
 - Timestamp Message (Type 13, Code 0)
 - Timestamp Reply Message (Type 14, Code 0)

ICMPv4 Informational Messages

- Information Request or Information Reply Message (Deprecated)
 - Information Request Message (Type 15, Code 0)
 - Information Reply Message (Type 16, Code 0)
- Address Mask Request or Address Mask Reply
 - Address Mask Request (Type 17, Code 0)
 - Address Mask Reply (Type 18, Code 0)

How the ICMP Filtering Works

#	Action	Chain	Src. Address	Dst. Address	Protocol	ICMP Options/ICMP Type	IC...	Bytes	Packets
0	jump	forward						0 B	0
::: echo reply									
1	✓ accept	icmp			1 (icmp)	0 (echo reply)	0	0 B	0
::: net unreachable									
2	✓ accept	icmp			1 (icmp)	3 (destination unreachable)	0	0 B	0
::: host unreachable									
3	✓ accept	icmp			1 (icmp)	3 (destination unreachable)	1	0 B	0
::: host unreachable fragmentation required									
4	✓ accept	icmp			1 (icmp)	3 (destination unreachable)	4	0 B	0
::: allow source quench									
5	✓ accept	icmp			1 (icmp)	4 (source quench)	0	0 B	0
::: allow echo request									
6	✓ accept	icmp			1 (icmp)	8 (echo request)	0	0 B	0
::: allow time exceed									
7	✓ accept	icmp			1 (icmp)	11 (time exceeded)	0	0 B	0
8	✓ accept	icmp			1 (icmp)	12 (parameter problem)	0	0 B	0
::: deny all other types									
9	✗ drop	icmp						0 B	0

10 items

How the ICMP Filtering Works

```
/ip firewall filter
add action=jump chain=forward jump-target=icmp
add action=accept chain=icmp comment="echo reply" icmp-options=0:0 protocol=icmp
add action=accept chain=icmp comment="net unreachable" icmp-options=3:0 protocol=icmp
add action=accept chain=icmp comment="host unreachable" icmp-options=3:1 protocol=icmp
add action=accept chain=icmp comment="host unreachable fragmentation required" \
    icmp-options=3:4 protocol=icmp
add action=accept chain=icmp comment="allow source quench" icmp-options=4:0 protocol=icmp
add action=accept chain=icmp comment="allow echo request" icmp-options=8:0 protocol=icmp
add action=accept chain=icmp comment="allow time exceed" icmp-options=11:0 protocol=icmp
add action=accept chain=icmp comment="allow parameter bad" icmp-options=12:0 protocol=icmp
add action=drop chain=icmp comment="deny all other types"
```


ENCRYPTED TUNNELS ON ROUTEROS

L2TP/IPsec

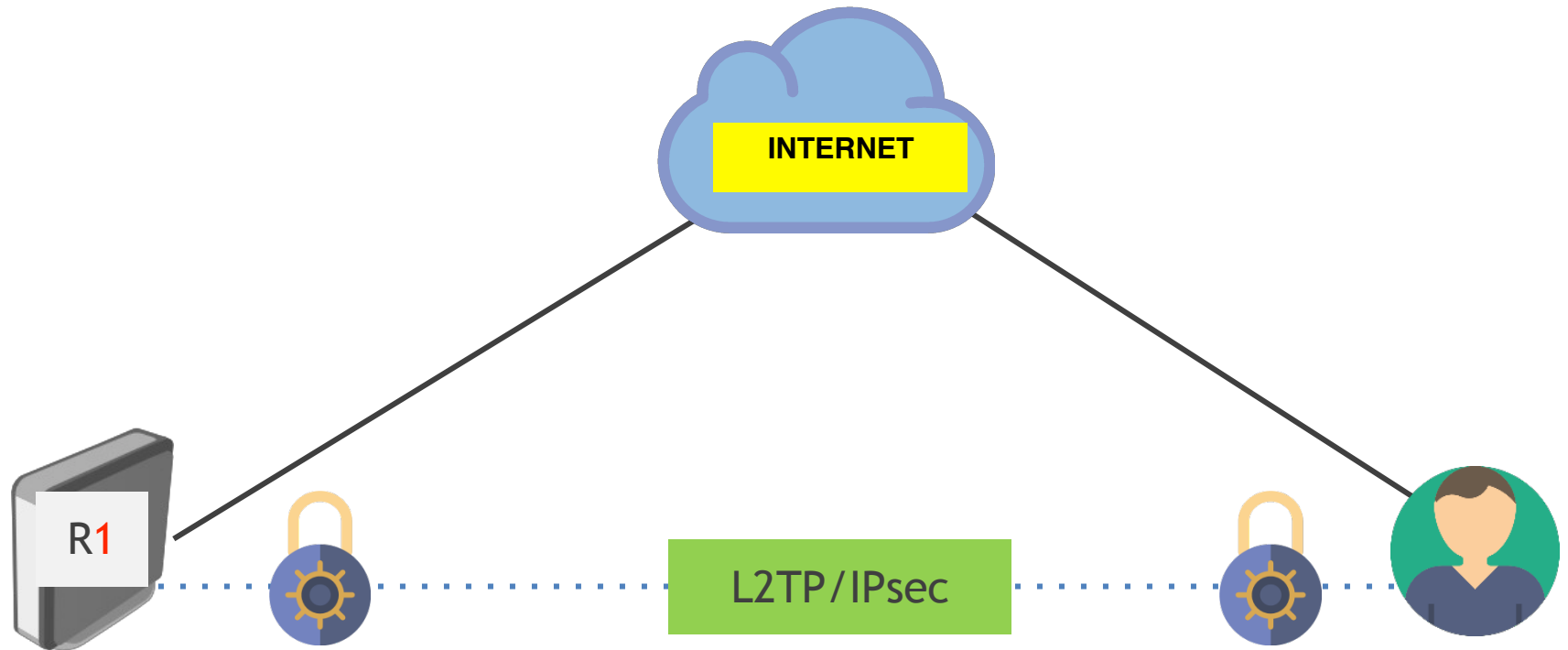
What is L2TP/IPsec

- L2TP stands for Layer 2 Tunnelling Protocol. L2TP was first proposed in 1999 as an upgrade to both L2F (Layer 2 Forwarding Protocol) and PPTP (Point-to-Point Tunnelling Protocol)
- Because L2TP does not provide strong encryption or authentication by itself, another protocol called IPsec is most often used in conjunction with L2TP
- Used together, L2TP and IPsec is much more secure than PPTP (Point-to-Point Tunnelling Protocol), but also slightly slower

What is L2TP/IPsec

- L2TP/IPSec offers high speeds, and high levels of security for transmitting data
- It generally makes use of AES ciphers for encryption
- L2TP sometimes has problems traversing firewalls due to its use of UDP port 500 which some firewalls have been known to block by default

Lab Setup



Setup L2TP/IPsec Server

The screenshot shows a network configuration interface with the following details:

- Interface:** PPPoE Servers, Secrets, Profiles, Active Connections, L2TP Secrets
- Buttons:** +, -, ✓, ✗, [Folder Icon], [Filter Icon], PPP Scanner, PPTP Server, SSTP Server, L2TP Server, OVPN Server, PPPoE Scan, Find
- Table Headers:** Name, Type, Actual MTU, L2 MTU, Tx, Rx
- L2TP Server Configuration Window:**
 - Enabled
 - Max MTU: 1450
 - Max MRU: 1450
 - MRRU: [Dropdown]
 - Keepalive Timeout: 30
 - Default Profile: default-encryption
 - Max Sessions: [Dropdown]
 - Authentication: mschap2, mschap1, chap, pap
 - Use IPsec: yes
 - IPsec Secret: fibercli.com
 - Caller ID Type: ip address
 - One Session Per Host
 - Allow Fast Path

```
/interface l2tp-server server set authentication=mschap1,mschap2 \
enabled=yes ipsec-secret=84GsvZAtUQnE use-ipsec=yes
```

Setup L2TP/IPsec Server

The screenshot shows a network configuration window titled 'PPP' with a 'New PPP Secret' dialog box open. The dialog box has the following fields and values:

- Name: demo
- Password: demo
- Service: l2tp
- Caller ID: (empty)
- Profile: default-encryption
- Local Address: 10.0.0.1
- Remote Address: 10.0.0.11
- Routes: (empty)
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)
- Last Logged Out: (empty)

The status at the bottom of the dialog is 'enabled'.

```
/ppp secret add name=demo password=demo local-address=10.0.0.1 \  
remote-address=10.0.0.11 profile=default-encryption service=l2tp
```

Setup L2TP/IPsec Client

Connect to a Workplace

← **Connect to a Workplace**

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

Next Cancel

Setup L2TP/IPsec Client

Connect to a Workplace

← **Connect to a Workplace**

Type your user name and password

User name: demo

Password: demo

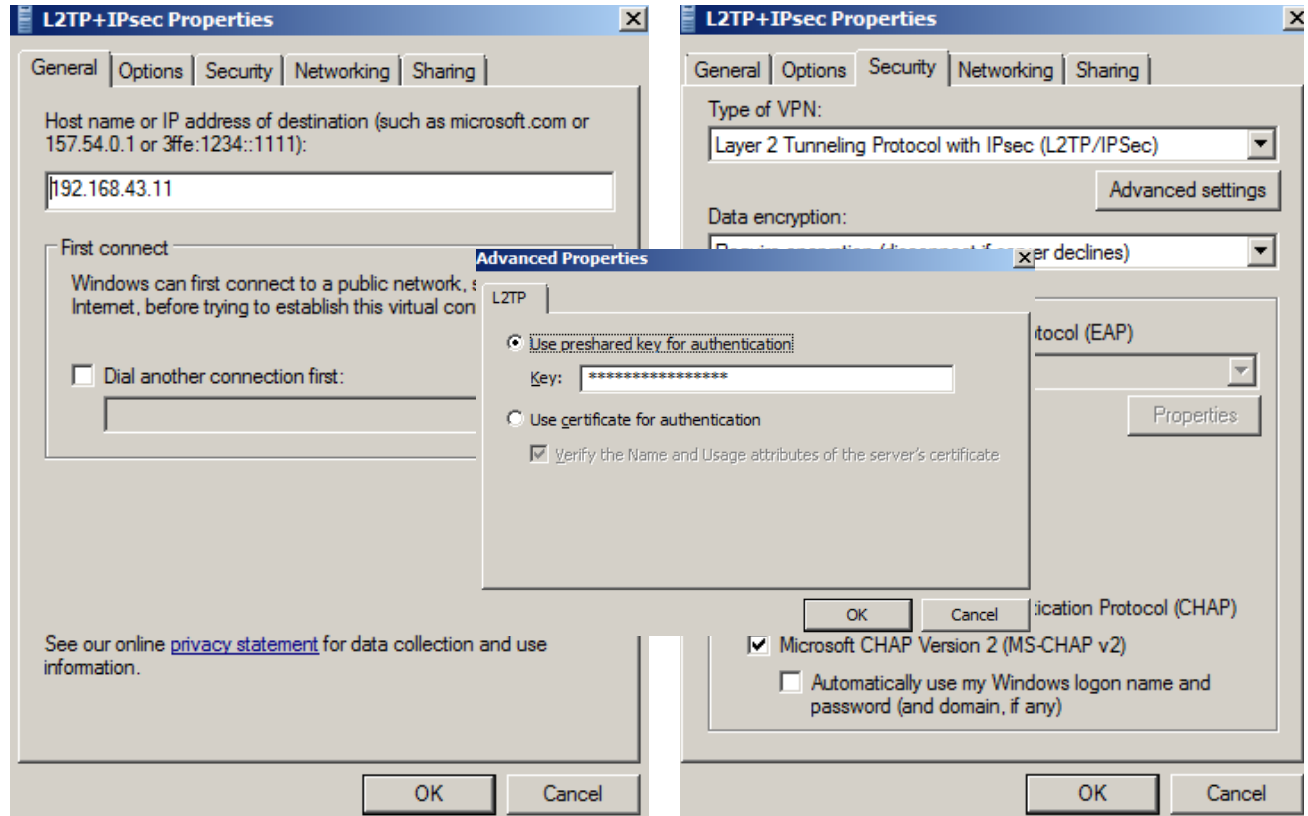
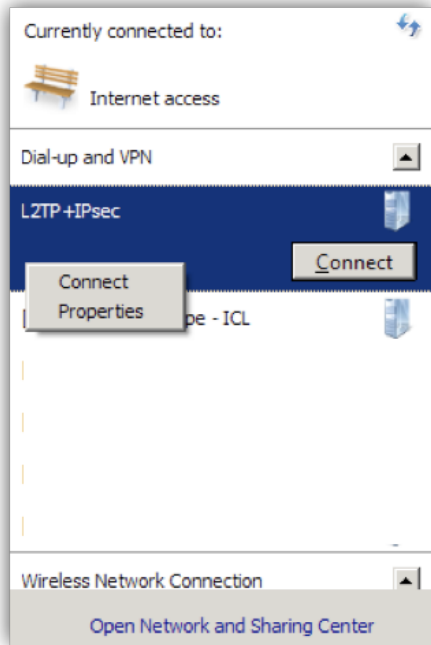
Show characters

Remember this password

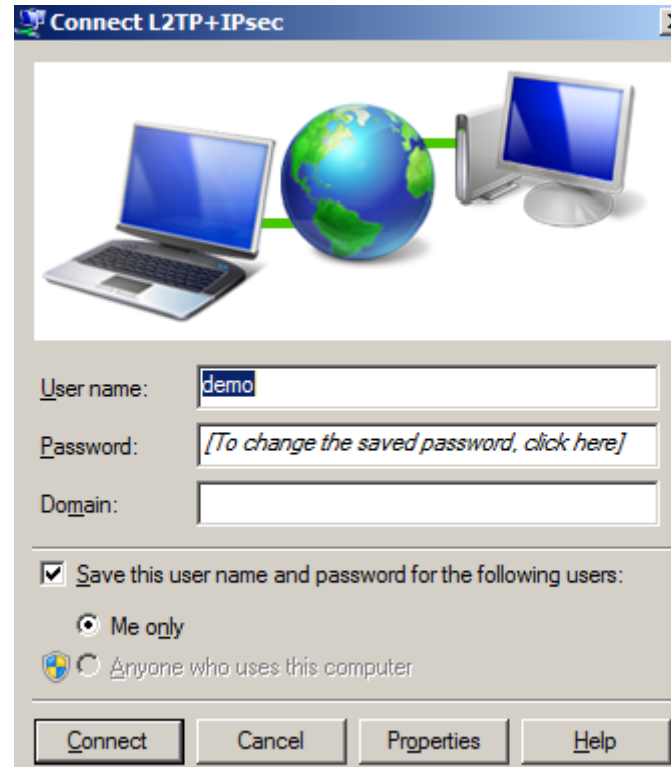
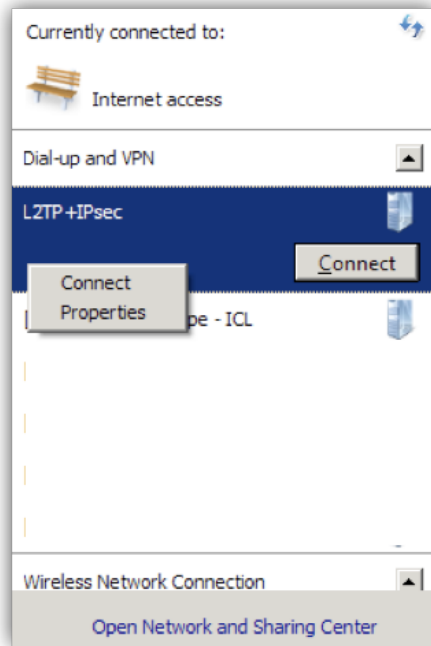
Domain (optional):

Connect **Cancel**

Setup L2TP/IPsec Client



Setup L2TP/IPsec Client



Setup L2TP/IPsec Client

The image shows a network configuration interface for PPP. The main window, titled "PPP", has tabs for "Interface", "PPPoE Servers", "Secrets", "Profiles", "Active Connections", and "L2TP Secrets". The "L2TP Secrets" tab is active, displaying a table of active users.

Name	Service	Caller ID	Encoding	Address	Uptime
L demo	l2tp	192.168.43.252	cbc(aes) + hmac(sha1)	10.0.0.11	00:01:15

An "Active User" dialog box is open, showing details for the selected user "demo".

PPP Active User <demo>

General

Name: demo

Service: l2tp

Caller ID: 192.168.43.252

Encoding: cbc(aes) + hmac(sha1)

Address: 10.0.0.11

Uptime: 00:01:29

Session ID: 81700001 hex

Limit Bytes In: []

Limit Bytes Out: []

local

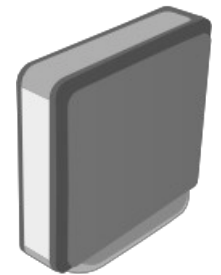
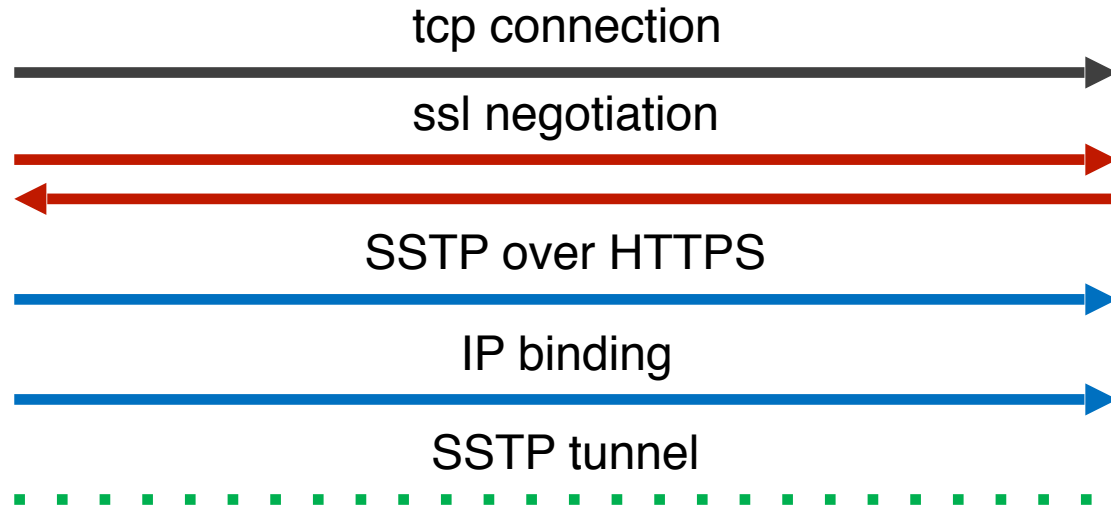
Buttons: OK, Remove, Ping

SSTP

What is SSTP

- Microsoft introduced Secure Socket Tunneling Protocol (SSTP) in Windows Vista and it is still considered to be a Windows-only platform even though it is available on a number of other operating systems.
- It has very similar advantages as OpenVPN as SSTP uses SSLv3 and it has greater stability as it is included with Windows which also makes it simpler to use.
- It uses the same port used by SSL connections; port 443.
- It uses 2048 bit encryption and authentication certificates.
- SSTP uses SSL transmissions instead of IPsec because SSL supports roaming instead of just site-to-site transmissions.
- RouterOS has both the SSTP server and client implementation

How the SSTP works



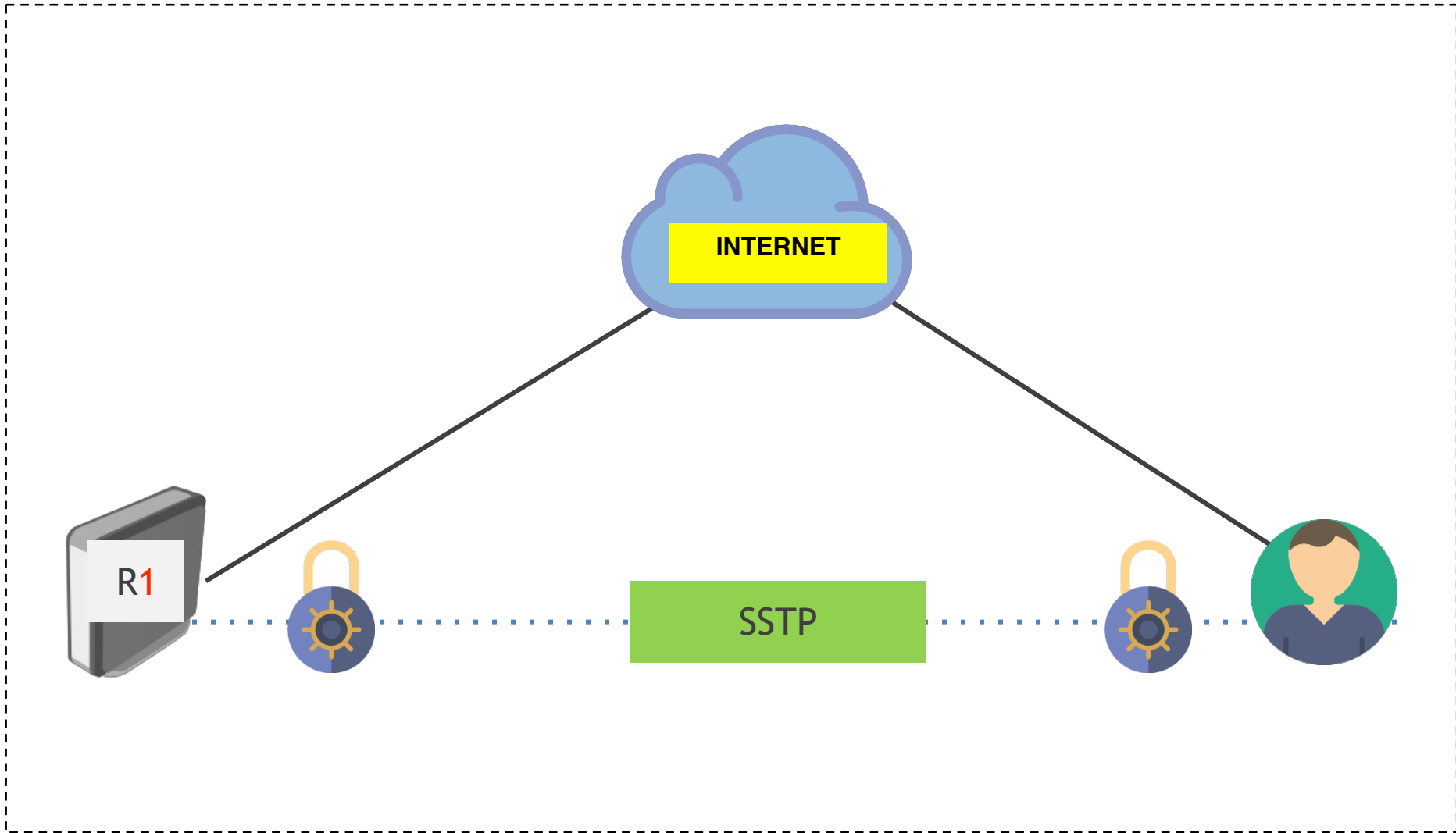
How the SSTP works

- TCP connection is established from client to server (by default on port 443)
- SSL validates server certificate. If certificate is valid connection is established otherwise connection is torn down. (But see note below)
- The client sends SSTP control packets within the HTTPS session which establishes the SSTP state machine on both sides

How the SSTP works

- PPP negotiation over SSTP. Client authenticates to the server and binds IP addresses to SSTP interface
- SSTP tunnel is now established and packet encapsulation can begin.
- Note: Two RouterOS devices can establish an SSTP tunnel even without the use of certificates (not in accordance with Microsoft standard)
- It is recommended to use the certificates at all times!

Lab Setup



Self-signed Certificate

General Key Usage Status

Name: sstp

Issuer:

Country: ES

State: Toledo

Locality: Illescas

Organization: IT

Unit: IT

Common Name: sstp.example.com

Subject Alt. Name: DNS: sstp.example.com

Key Size: 2048

Days Valid: 365

OK Cancel Apply Copy Remove Sign Sign via SCEP Import Card Reinstall Card Verify Set CA Passphrase Export Revoke

General Key Usage Status

Key Usage:

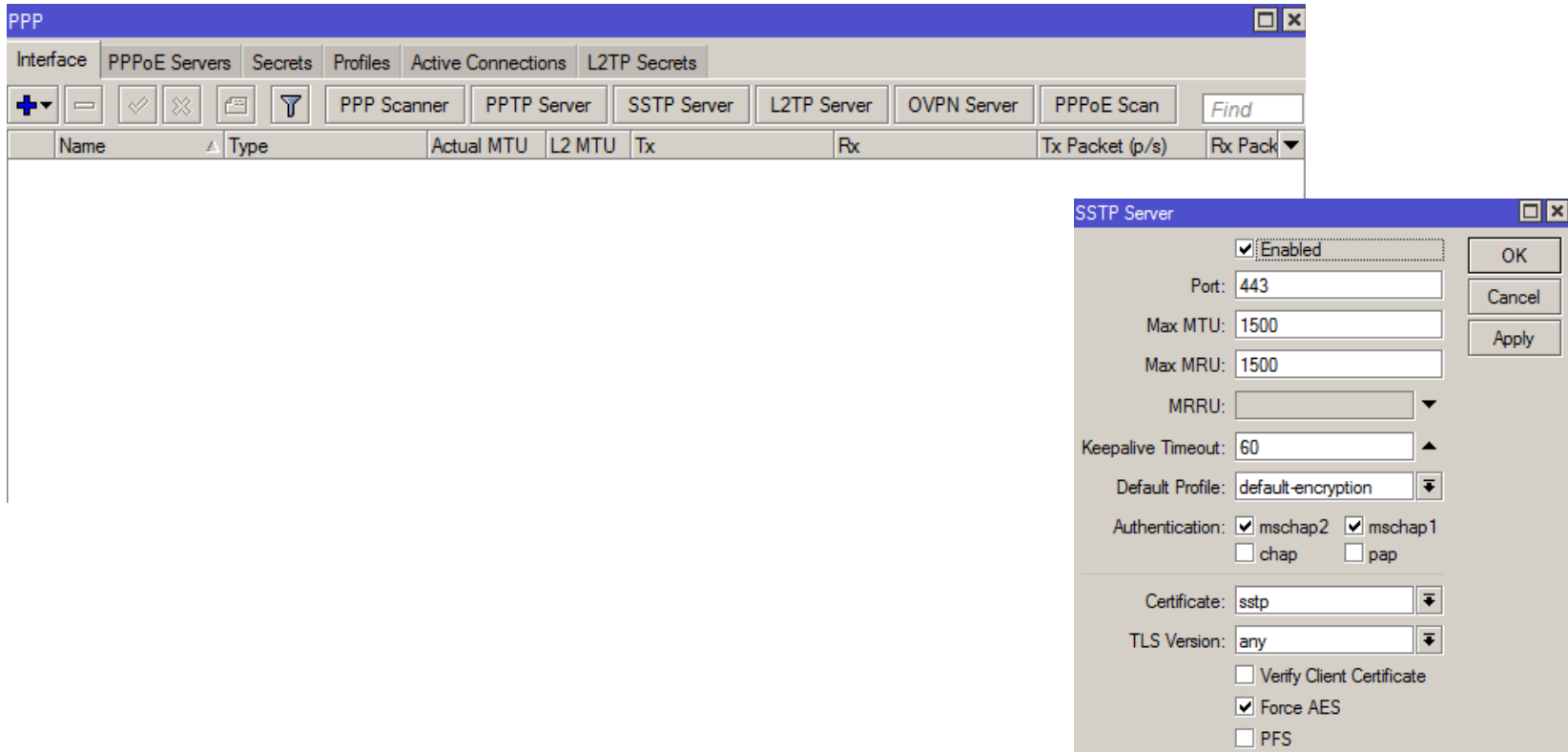
- digital signature
- key encipherment
- key agreement
- crl sign
- decipher only
- server gated crypto
- timestamp
- ipsec tunnel
- email protect
- tls client
- content commitment
- data encipherment
- key cert. sign
- encipher only
- dvcs
- ocsip sign
- ipsec user
- ipsec end system
- code sign
- tls server

OK Cancel Apply Copy Remove Sign Sign via SCEP Import Card Reinstall Card Verify Set CA Passphrase Export Revoke

```
certificate add name=sstp country=ES state=Toledo locality=Illescas organization=IT unit=IT \
common-name=ssstp.example.com subject-alt-name=DNS:ssstp.example.com key-size=2048 days-valid=365 \
key-usage=digital-signature,key-encipherment,tls-client,tls-server
```

```
/ certificate sign sstp name=sstp ca=CA
/ certificate set sstp trusted=yes
```

Lab Setup



```
/interface sstp-server server set authentication=mschap1,mschap2 certificate=sstp default-profile=default-encryption \
enabled=yes force-aes=yes
```

Setup SSTP Server

The screenshot shows a network configuration window titled 'PPP' with several tabs: 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. The 'Secrets' tab is active, displaying a table with columns: Name, Password, Service, Caller ID, Profile, Local Address, Remote Address, and Last Logged Out. A 'Find' search box is located to the right of the table. Overlaid on the right side is a 'New PPP Secret' dialog box with the following fields and values:

- Name: demo
- Password: demo
- Service: sstp
- Caller ID: (empty)
- Profile: default-encryption
- Local Address: 10.0.0.1
- Remote Address: 10.0.0.11
- Routes: (empty)
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)
- Last Logged Out: (empty)

Buttons on the right side of the dialog include OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The 'enabled' checkbox at the bottom is checked.

```
/ppp secret add name=demo password=demo local-address=10.0.0.1 remote-address=10.0.0.11 \  
profile=default-encryption service=sstp
```

Setup SSTP Server

Connect to a Workplace

← **Connect to a Workplace**

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

Next **Cancel**

Setup SSTP Client

Connect to a Workplace

← **Connect to a Workplace**

Type your user name and password

User name: demo

Password: demo

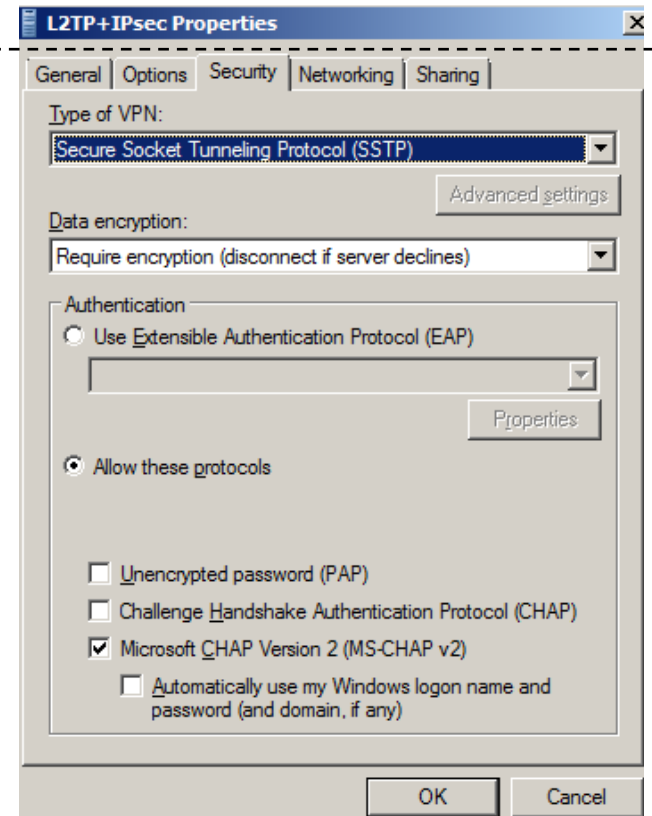
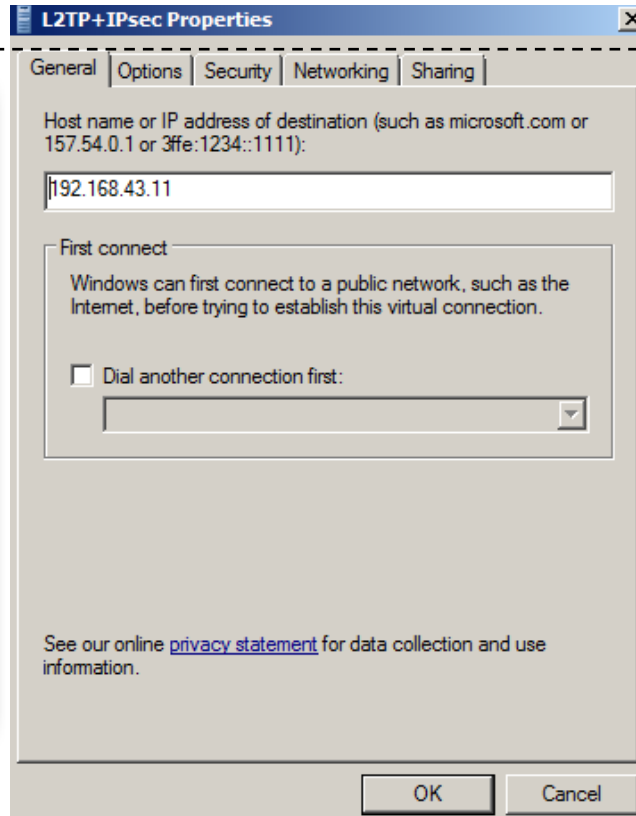
Show characters

Remember this password

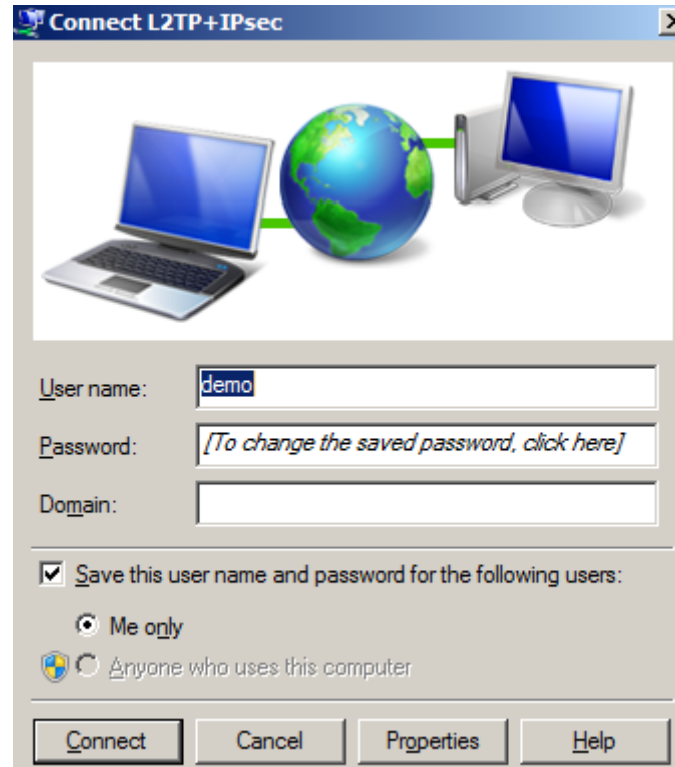
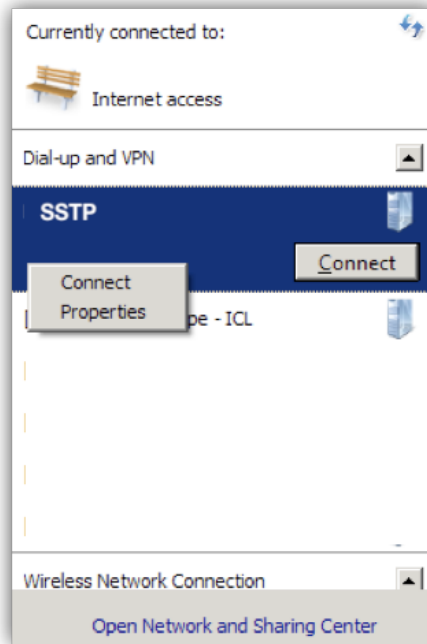
Domain (optional):

Connect Cancel

Setup SSTP Client



Setup SSTP Client



IPsec

What is IPsec

Internet Protocol Security (IPsec) is a set of protocols defined by the Internet Engineering Task Force (IETF) to secure packet exchange over unprotected IPv4 or IPv6 networks such as Internet. Provides Layer 3 security (RFC 2401)

IPsec Combines different components :

- Security associations (SA)
- Authentication headers (AH)
- Encapsulating security payload (ESP)
- Internet Key Exchange (IKE)

What is IPsec

IPsec standardisation defined in :

- RFC 4301 Defines the original IPsec architecture and elements common to both AH and ESP
- RFC 4302 Defines authentication headers (AH)
- RFC 4303 Defines the Encapsulating Security Payload (ESP)
- RFC 2408 ISAKMP
- RFC 5996 IKE v2 (Sept 2010)
- RFC 4835 Cryptographic algorithm implementation for ESP and AH

The Benefits of IPsec

Confidentiality

- By encrypting data

Integrity

- Routers at each end of a tunnel calculate the checksum or hash value of the data

Authentication

- Signatures and certificates
- All these while still maintaining the ability to route through existing IP Networks

The Benefits of IPsec

Data integrity and source authentication

- Data “signed” by sender and “signature” is verified by the recipient
- Modification of data can be detected by signature “verification”
- Because “signature” is based on a shared secret, it gives source authentication

Anti-replay protection

- Optional; the sender must provide it but the recipient may ignore

The Benefits of IPsec

Key management

- IKE – session negotiation and establishment
- Sessions are rekeyed or deleted automatically
- Secret keys are securely established and authenticated
- Remote peer is authenticated through varying options

IPsec Modes

Transport Mode

- IPsec header is inserted into the IP packet
- No new packet is created
- Works well in networks where increasing a packet's size could cause an issue
- Frequently used for remote-access VPNs



normal traffic without IPsec



traffic with transport mode IPsec

IPsec Modes

Tunnel Mode

- Entire IP packet is encrypted and becomes the data component of a new (and larger) IP packet.
- Frequently used in an IPsec site-to-site VPN

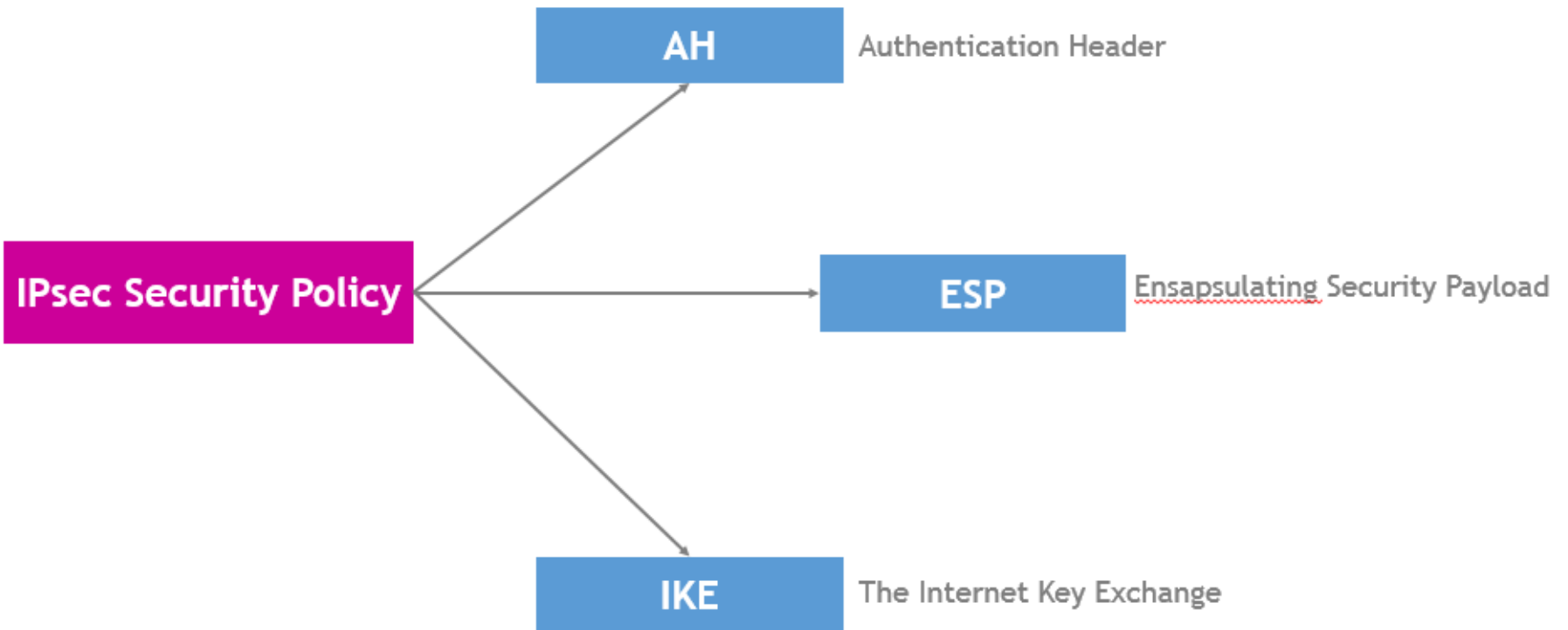


normal traffic without IPsec



traffic with tunnel mode IPsec

IPsec Architecture



Authentication Header (AH)

AH is a protocol that provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram.

What parts of the datagram are used for the calculation, and the placement of the header, depends whether tunnel or transport mode is used.

- Provides source authentication and data integrity
 - Protection against source spoofing and replay attacks
- Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out

Authentication Header (AH)

- Operates on top of IP using protocol 51
- In IPv4, AH protects the payload and all header fields except mutable fields and IP options (such as IPsec option)

MikroTik RouterOS supports the following authentication algorithms for AH:

- SHA1
- MD5

Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) uses shared key encryption to provide data privacy. ESP also supports its own authentication scheme like that used in AH, or can be used in conjunction with AH.

ESP packages its fields in a very different way than AH. Instead of having just a header, it divides its fields into three components:

- ESP Header** : Comes before the encrypted data and its placement depends on : whether ESP is used in transport mode or tunnel mode.
- ESP Trailer** : This section is placed after the encrypted data. It : contains padding that is used to align the encrypted data.
- ESP Auth Data** : This field contains an Integrity Check Value (ICV), computed : in a manner similar to how the AH protocol works, for : when ESP's optional authentication feature is used.

Encapsulating Security Payload (ESP)

- Uses IP protocol 50
- Provides all that is offered by AH, plus data confidentiality
 - It uses symmetric key encryption
- Must encrypt and/or authenticate in each packet
 - Encryption occurs before authentication
- Authentication is applied to data in the IPsec header as well as the data contained as payload

Encapsulating Security Payload (ESP)

RouterOS ESP supports various encryption and authentication algorithms.

Authentication : SHA1, MD5

Encryption :

DES : 56-bit DES-CBC encryption algorithm;

3DES : 168-bit DES encryption algorithm;

AES : 128, 192 and 256-bit key AES-CBC encryption algorithm;

Blowfish : added since v4.5

Twofish : added since v4.5

Camellia : 128, 192 and 256-bit key Camellia encryption algorithm

: added since v4.5

Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) is a protocol that provides authenticated keying material for Internet Security Association and Key Management Protocol (ISAKMP) framework. There are other key exchange schemes that work with ISAKMP, but IKE is the most widely used one. Together they provide means for authentication of hosts and automatic management of security associations (SA).

- “An IPsec component used for performing mutual authentication and establishing and maintaining Security Associations.” (RFC 5996)
- Typically used for establishing IPsec sessions
- A key exchange mechanism
- Five variations of an IKE negotiation:
 - Two modes (aggressive and main modes)
 - Three authentication methods (pre-shared, public key encryption, and public key signature)
- Uses UDP port 500

IKE Mode

Mode	Descriptions
Main Mode	<ul style="list-style-type: none">• Three exchanges of information between IPsec peers. Initiator sends one or more proposals to the other peer (responder)• Responder selects a proposal
Aggressive Mode	<ul style="list-style-type: none">• Achieves same result as main mode using only 3 packets First packet sent by initiator containing all info to establish SA• Second packet by responder with all security parameters selected• Third packet finalizes authentication of the ISAKMP session
Quick Mode	<ul style="list-style-type: none">• Negotiates the parameters for the IPsec session.• Entire negotiation occurs within the protection of ISAKMP session

Internet Key Exchange (IKE)

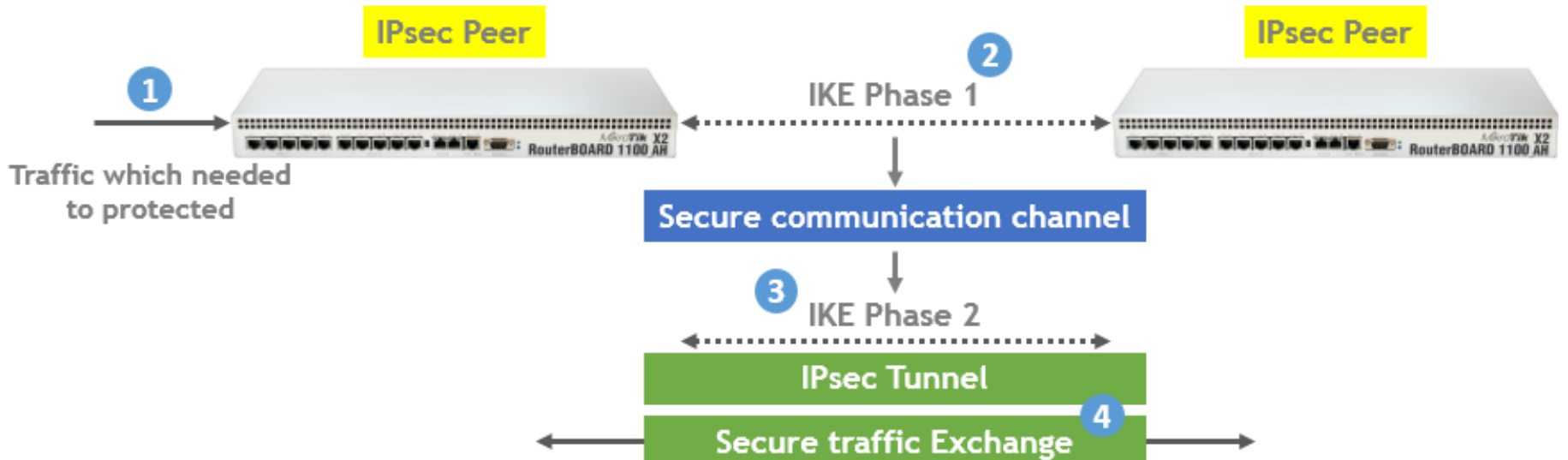
Phase I

- Establish a secure channel (ISAKMP SA)
- Using either main mode or aggressive mode
- Authenticate computer identity using certificates or pre-shared secret

Phase II

- Establishes a secure channel between computers intended for the transmission of data (IPsec SA)
- Using quick mode

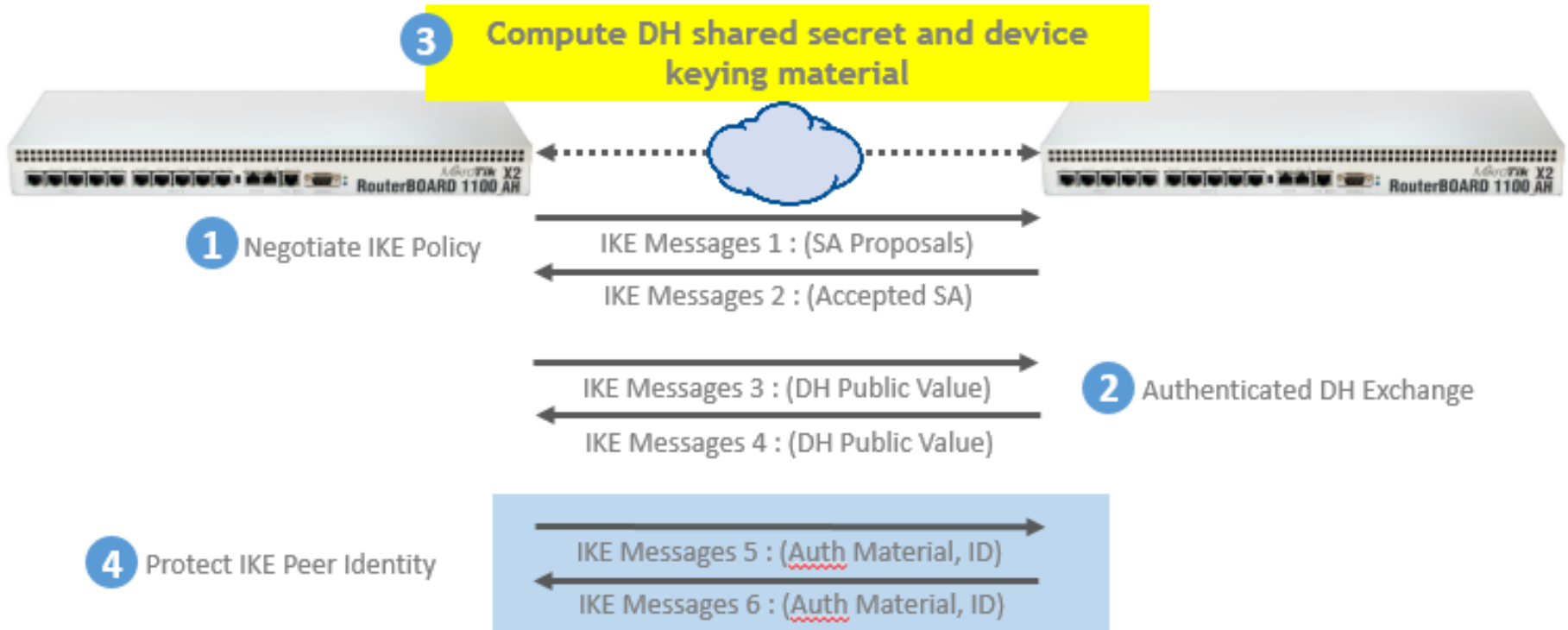
Internet Key Exchanger (IKE)



IKE Phase 1 (Main Mode)

- Main mode negotiates an ISAKMP SA which will be used to create IPsec SAs.
- Three steps
 - SA negotiation (encryption algorithm, hash algorithm, authentication method, which DF group to use)
 - Do a Diffie-Hellman exchange
 - Provide authentication information
 - Authenticate the peer

IKE Phase 1 (Main Mode)



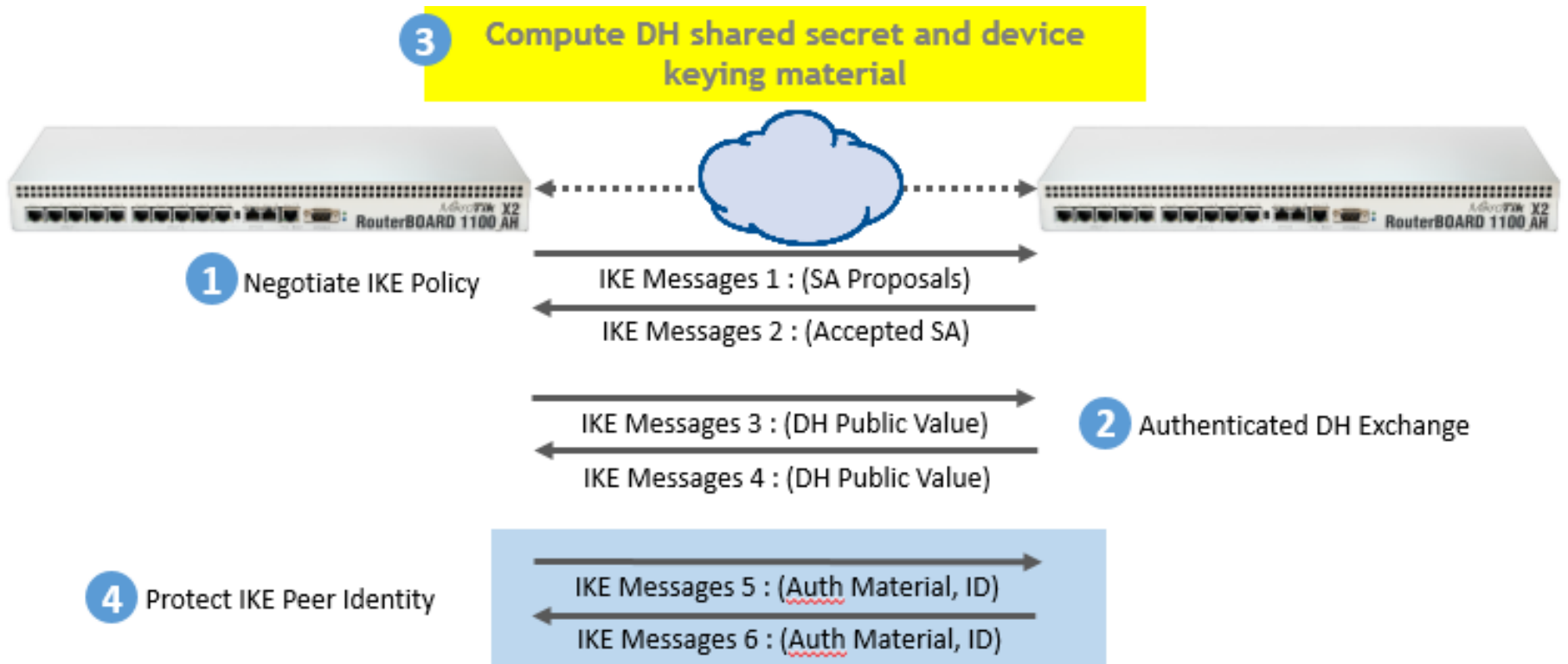
IKE Phase 1 (Aggressive Mode)

- Uses 3 (vs 6) messages to establish IKE SA
- No denial of service protection
- Does not have identity protection
- Optional exchange and not widely implemented

IKE Phase 2 (Quick Mode)

- All traffic is encrypted using the ISAKMP Security Association
- Creates/refreshes keys
- Each quick mode negotiation results in two IPsec Security Associations (one inbound, one outbound)

IKE Phase 2 (Quick Mode)



IKEv2

- Internet Key Exchange Version 2 (IKEv2) is the second-generation standard for a secure key exchange between connected devices.
- IKEv2 works by using an IPsec-based tunnelling protocol to establish a secure connection.
- One of the single most important benefits of IKEv2 is its ability to reconnect very quickly in the event that your VPN connection gets disrupted.
- Quick reconnections and strong encryption IKEv2 makes an excellent candidate to use

Lab Setup

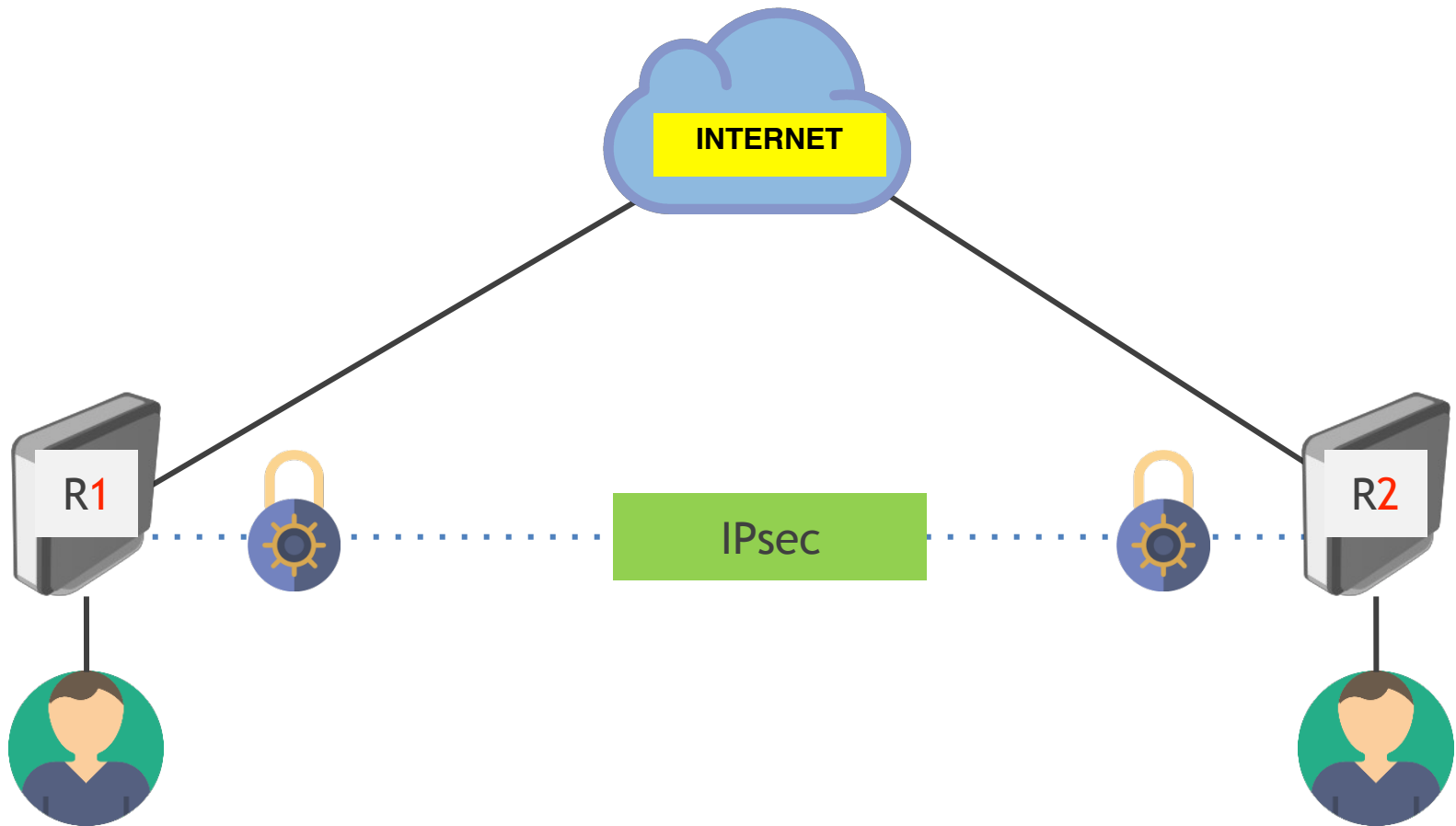
R1

- Public Address :
11.11.11.2/24
- Local Address: 192.168.1.0/24

R2

- Public Address :
22.22.22.2/24
- Local Address: 192.168.2.0/24

Lab Setup



Setup IPsec R1

The screenshot displays two windows from a network configuration tool. The 'Interface List' window shows a table of interfaces:

Name	Type	MTU	L2 MTU
R ether1-to-internet	Ethernet	1500	
R ether2-to-local	Ethernet	1500	
R ether10-Management	Ethernet	1500	

The 'Address List' window shows a table of IP addresses:

Address	Network	Interface
11.11.11.2/24	11.11.11.0	ether1-to-internet
192.168.1.1/24	192.168.1.0	ether2-to-local
192.168.111.11/24	192.168.111.0	ether10-Manag...

/ip address

add address=11.11.11.2/24 interface=ether1-to-internet network=11.11.11.0

add address=192.168.1.1/24 interface=ether2-to-local network=192.168.1.0

Setup IPsec R1

The screenshot displays a network configuration window titled "Route List". It features a table with columns for "Dst. Address", "Gateway", "Distance", "Routing Mark", and "Pref. Source". The table lists several routes, including a default route (0.0.0.0/0) with a distance of 1 and gateway 11.11.11.1. Below the table, a detailed view for the route <0.0.0.0/0> is shown, with fields for "Dst. Address" (0.0.0.0/0), "Gateway" (11.11.11.1), "Check Gateway", "Type" (unicast), "Distance" (1), and "Scope" (30). The interface includes various control buttons like "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", and "Remove".

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	11.11.11.1 reachable ether1-to-internet	1		
DAC	11.11.11.0/24	ether1-to-internet reachable	0		11.11.11.2
DAC	192.168.1.0/24	ether2-to-local reachable	0		192.168.1.1
DAC	192.168.111.0...	ether10-Management reachable	0		192.168.111.11

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 11.11.11.1 reachable ether1-to-internet

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

OK
Cancel
Apply
Disable
Comment
Copy
Remove

```
/ip route add distance=1 gateway=11.11.11.1
```

Setup IPsec R1

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📄 🏠 00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port
0	masquerade	srcnat				

NAT Rule <>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ether1-to-internet

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

New NAT Rule

Advanced Extra Action Statistics ...

Action: masquerade

Log

Log Prefix:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

```
/ip firewall nat add action=masquerade chain=srcnat out-interface=ether1-to-internet
```

Setup IPsec R1

Address	Port	Propos...	Has
22.22.22.2	500	obey	sha

1 item (1 selected)

IPsec Peer <22.22.22.2>

Address: 22.22.22.2

Port: 500

Local Address: ::

Auth. Method: pre shared key

Passive

Secret: ipsec-lab

Policy Template Group: default

Exchange Mode: main

Send Initial Contact

NAT Traversal

My ID: auto

Proposal Check: obey

Hash Algorithm: sha1

Encryption Algorithm:

des 3des aes-128

aes-192 aes-256 blowfish

camellia-128 camellia-192 camellia-256

Mode Configuration:

DH Group: modp1024

Generate Policy: no

Lifetime: 1d 00:00:00

Lifeytes:

DPD Interval: 120 s

DPD Maximum Failures: 5

```
/ip ipsec peer add address=22.22.22.2/32 nat-traversal=no secret=ipsec-lab
```

Setup IPsec R1-NEW

The screenshot shows the Mikrotik WinBox interface for configuring IPsec. The left sidebar has 'Tools' > 'IPsec' selected (1). The main window shows the 'IPsec' configuration page with the 'Peers' tab active (2). A table lists the peers:

#	Name	Address
0	peer-R2	22.22.22

The configuration dialog for 'peer-R2' (4) is open, showing the following settings:

- Name: peer-R2
- Address: 22.22.22.2
- Port: (empty)
- Local Address: 11.11.11.2
- Profile: default
- Exchange Mode: main
- Passive
- Send INITIAL_CONTACT

Buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove are visible. The status bar shows 'enabled' and 'responder'.

```
/ip ipsec peer add address=22.22.22.2/32 local-address=11.11.11.2 name=peer-R2
```

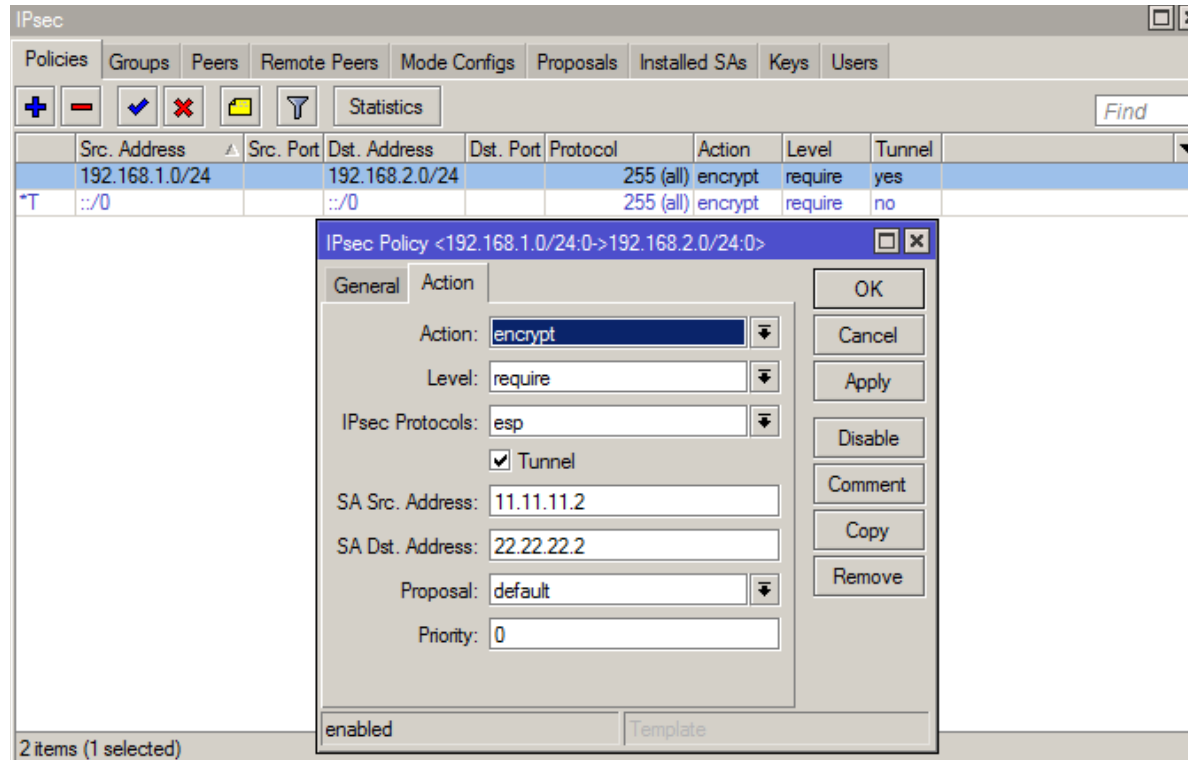

Setup IPsec R1-NEW

The screenshot shows the IPsec configuration interface. On the left, the 'Identities' tab is selected, and a table lists the identity 'peer-R2' with a pre-shared key. A red circle '1' highlights the 'Identities' tab, and a red circle '2' highlights the '+' button. On the right, the 'IPsec Identity <peer-R2>' dialog is open, showing configuration options for the selected identity. A red circle '3' highlights the dialog title. The dialog fields are as follows:

Field	Value
Peer	peer-R2
Auth. Method	pre shared key
Secret
Policy Template Group	default
Notrack Chain	
My ID Type	auto
Remote ID Type	auto
Match By	remote id
Mode Configuration	
Generate Policy	no

```
/ip ipsec identity add peer=peer-R2 secret=myIPSecLABsecret
```

Setup IPsec R1



```
/ip ipsec policy  
add dst-address=192.168.2.0/24 tunnel=yes sa-dst-address=22.22.22.2 \  
sa-src-address=11.11.11.2 src-address=192.168.1.0/24
```

Setup IPsec R1

The screenshot displays the Mikrotik WinBox Firewall configuration interface. The main window shows a table of firewall rules with the following data:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	accept	srcnat	192.168.1.0/24	192.168.2.0/24						0 B	0
1	masquerade	srcnat							ether1+	7.5 KB	48

Two configuration dialog boxes are overlaid on the main window:

- NAT Rule <192.168.1.0/24->192.168.2.0/24> (General tab):** Chain: srcnat, Src. Address: 192.168.1.0/24, Dst. Address: 192.168.2.0/24.
- NAT Rule <192.168.1.0/24->192.168.2.0/24> (Action tab):** Action: accept, Log: .

```
/ip firewall nat add chain=srcnat dst-address=192.168.2.0/24 src-address=192.168.1.0/24 place-before=0
```

Setup IPsec R2

The screenshot displays two network configuration windows. The 'Interface List' window shows a table of interfaces:

Name	Type	MTU	L2 MTU	Tx
R ether1-to-internet	Ethernet	1500		
R ether2-to-local	Ethernet	1500		
R ether10-Management	Ethernet	1500		

The 'Address List' window shows a table of IP addresses:

Address	Network	Interface
22.22.22.2/24	22.22.22.0	ether1-to-internet
192.168.2.1/24	192.168.2.0	ether2-to-local
192.168.111.1...	192.168.111.0	ether10-Management

/ip address

add address=22.22.22.2/24 interface=ether1-to-internet network=22.22.22.0

add address=192.168.2.1/24 interface=ether2-to-local network=192.168.2.0

Setup IPsec R2

The screenshot shows a network configuration interface with two windows. The top window, titled "Route List", displays a table of routes. The bottom window, titled "Route <0.0.0.0/0>", shows the configuration details for the selected route.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	22.22.22.1 reachable ether1-to-intemet	1		
DAC	22.22.22.0/24	ether1-to-intemet reachable	0		22.22.22.2
DAC	192.168.2.0/24	ether2-to-local reachable	0		192.168.2.1
DAC	192.168.111.0...	ether10-Management reachable	0		192.168.111.12

The "Route <0.0.0.0/0>" window shows the following configuration:

- General tab selected
- Dst. Address: 0.0.0.0/0
- Gateway: 22.22.22.1 (dropdown menu shows "reachable ether1-to-intemet")
- Check Gateway: (dropdown menu)
- Type: unicast (dropdown menu)
- Distance: 1
- Scope: 30

Buttons on the right side of the "Route <0.0.0.0/0>" window include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

```
/ip route add distance=1 gateway=22.22.22.1
```

Setup IPsec R2

The screenshot displays the Mikrotik WinBox Firewall configuration interface. The main window shows a table with one rule:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port
0	masquerade	srcnat				

Two configuration windows are open:

- NAT Rule <**: Shows Chain: srcnat, Out. Interface: ether1-to-internet.
- New NAT Rule**: Shows Action: masquerade, Log: unchecked, Log Prefix: empty.

```
/ip firewall nat add action=masquerade chain=srcnat out-interface=ether1-to-internet
```

Setup IPsec R2-OLD

The screenshot shows the IPsec configuration interface. On the left, a table lists the configured peers:

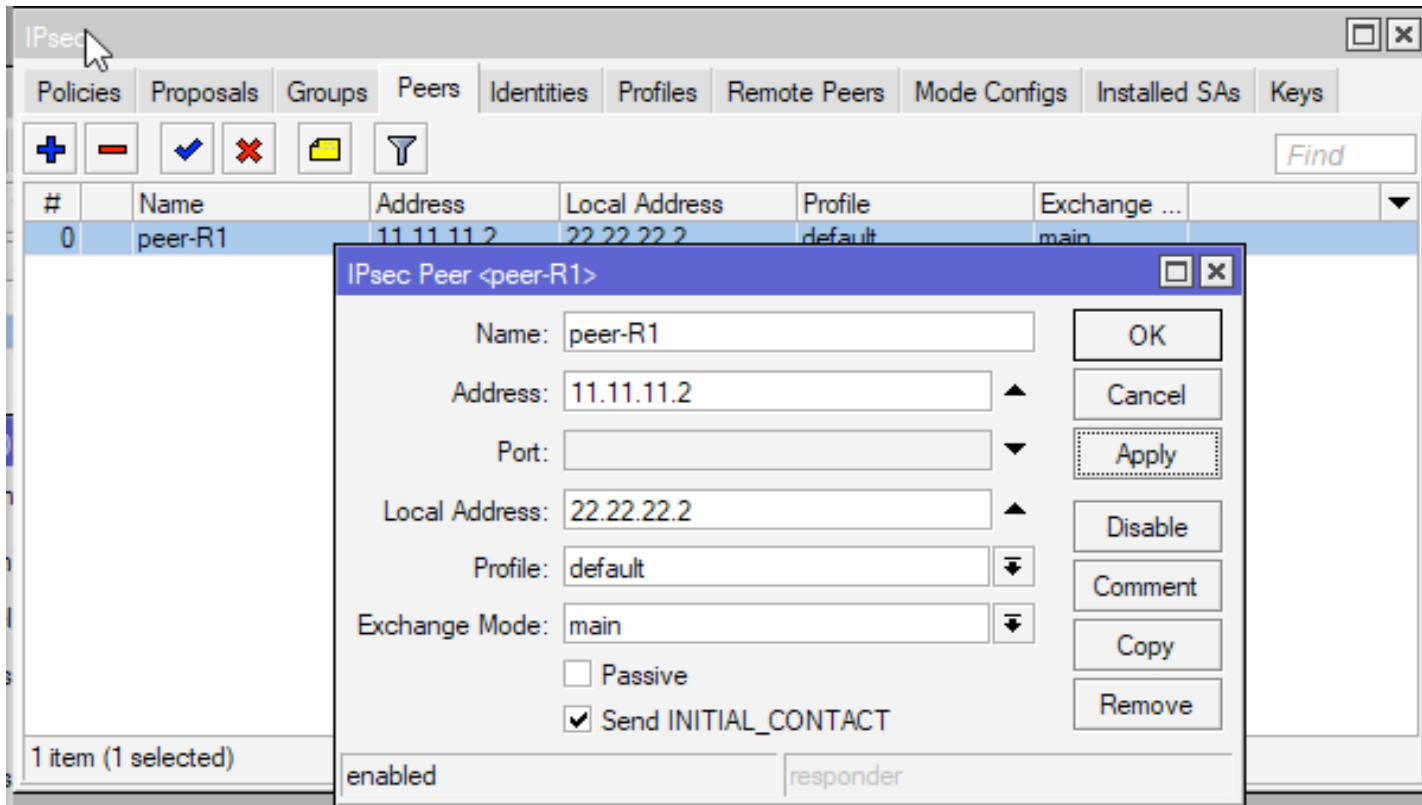
Address	Port	Propos...	Hash Al...	Encrypt...
11.11.11.2	500	obey	sha1	3des a...

Below the table, it indicates "1 item". On the right, the "IPsec Peer <11.11.11.2>" configuration window is open, showing the following settings:

- Address: 11.11.11.2
- Port: 500
- Local Address: ::
- Auth. Method: pre shared key
- Passive
- Secret: *****
- Policy Template Group: default
- Exchange Mode: main
- Send Initial Contact
- NAT Traversal
- My ID: auto
- Proposal Check: obey
- Hash Algorithm: sha1
- Encryption Algorithm: des, 3des, aes-128, aes-192, aes-256, blowfish, camellia-128, camellia-192, camellia-256
- Mode Configuration: [dropdown]
- DH Group: modp1024
- Generate Policy: no
- Lifetime: 1d 00:00:00
- Lifeytes: [dropdown]
- DPD Interval: 120 s
- DPD Maximum Failures: 5

```
/ip ipsec peer add address=11.11.11.2/32 nat-traversal=no secret=ipsec-lab
```

Setup IPsec R2-NEW



```
/ip ipsec peer add address=11.11.11.2/32 local-address=22.22.22.2 name=peer-R1
```


Setup IPsec R2-NEW

The screenshot shows the IPsec configuration interface. On the left, a table lists the configured peers:

#	Peer	Auth. Method	XAuth
0	peer-R1	pre shared key	

Below the table, it indicates "1 item (1 selected)".

The main window, titled "IPsec Identity <peer-R1>", shows the configuration for the selected peer:

- Peer: peer-R1
- Auth. Method: pre shared key
- Secret: [Redacted]
- Policy Template Group: default
- Notrack Chain: [Empty]
- My ID Type: auto
- Remote ID Type: auto
- Match By: remote id
- Mode Configuration: [Empty]
- Generate Policy: no

Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The status "enabled" is shown at the bottom.

```
/ip ipsec identity add peer=peer-R1 secret=myIPSecLABsecret
```

Lab Setup

The screenshot shows the IPsec configuration interface. At the top, there are tabs for Policies, Groups, Peers, Remote Peers, Mode Configs, Proposals, Installed SAs, Keys, and Users. Below the tabs is a toolbar with icons for adding, deleting, and filtering policies, along with a 'Statistics' button and a 'Find' search box. A table lists the configured policies:

	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
	192.168.2.0/24		192.168.1.0/24		255 (...)	encrypt	require	yes
*T	::/0		::/0		255 (...)	encrypt	require	no

An 'IPsec Policy <192.168.2.0/24->192.168.1.0/24:0>' dialog box is open, showing the configuration for the selected policy. The 'General' tab is active, and the 'Action' section is expanded. The configuration includes:

- Action: encrypt
- Level: require
- IPsec Protocols: esp
- Tunnel
- SA Src. Address: 22.22.22.2
- SA Dst. Address: 11.11.11.2
- Proposal: default
- Priority: 0

Buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove are visible on the right side of the dialog.

```
/ip ipsec policy  
add dst-address=192.168.1.0/24 tunnel=yes sa-dst-address=11.11.11.2 \  
sa-src-address=22.22.22.2 src-address=192.168.2.0/24
```

Lab Setup

The screenshot displays the Mikrotik WinBox Firewall configuration interface. At the top, there are tabs for Filter Rules, NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocols. Below the tabs is a toolbar with icons for adding, deleting, and applying rules, along with buttons for 'Reset Counters' and 'Reset All Counters'. A table lists the firewall rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✓ accept	srcnat	192.168.2.0/24	192.168.1.0/24						60 B	1
1	≡ masquerade	srcnat							ether1t...	17.4 KB	113

Two configuration dialog boxes are overlaid on the main window. The left dialog is titled 'NAT Rule <192.168.2.0/24->192.168.1.0/24>' and shows the 'General' tab. The 'Chain' is set to 'srcnat', 'Src. Address' is '192.168.2.0/24', and 'Dst. Address' is '192.168.1.0/24'. The right dialog is titled 'NAT Rule <192.168.2.0/24->192.168.1.0/24>' and shows the 'Action' tab. The 'Action' is set to 'accept', and the 'Log' checkbox is unchecked. Both dialogs have buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

```
ip firewall nat add chain=srcnat dst-address=192.168.1.0/24 src-address=192.168.2.0/24 place-before=0
```

Lab Setup

```
CA Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\fajar>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.2.2
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.2.1

C:\Documents and Settings\fajar>
```

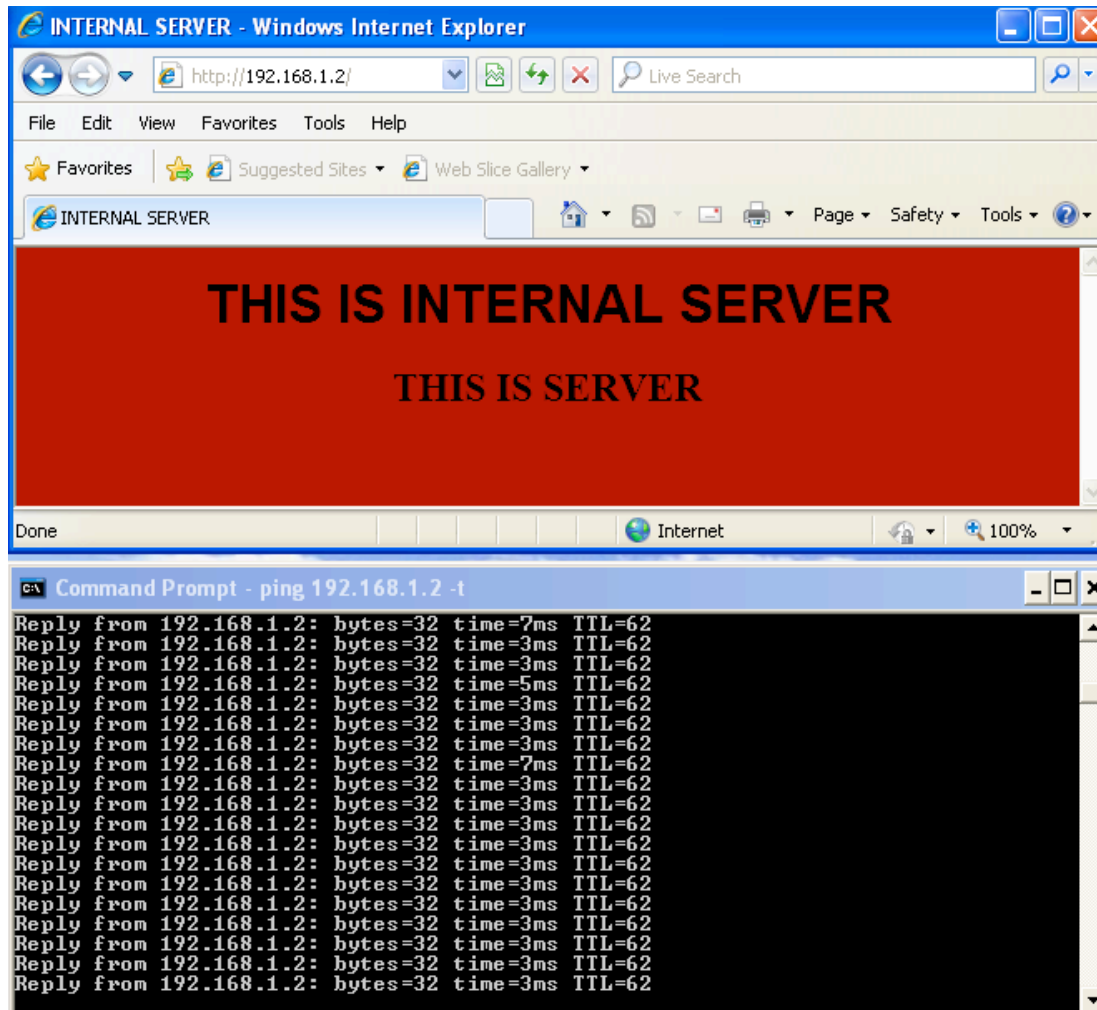
```
CA Command Prompt - ping 192.168.1.2 -t
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\fajar>ping 192.168.1.2 -t

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=4ms TTL=62
Reply from 192.168.1.2: bytes=32 time=3ms TTL=62
Reply from 192.168.1.2: bytes=32 time=3ms TTL=62
Reply from 192.168.1.2: bytes=32 time=3ms TTL=62
Reply from 192.168.1.2: bytes=32 time=3ms TTL=62
Reply from 192.168.1.2: bytes=32 time=3ms TTL=62
Reply from 192.168.1.2: bytes=32 time=3ms TTL=62
Reply from 192.168.1.2: bytes=32 time=3ms TTL=62
```

Lab Setup



MTCSE SUMMARY

Certification Test

- If needed reset router configuration and restore from a backup
- Make sure that you have an access to the www.mikrotik.com training portal
- Login with your account
- Choose **my training sessions**
- Good luck!