

# MikroTik IPSec ike2 VPN server

Easy and clear step-by-step guide

# Nikita Tarikin

Certified network engineer  
MikroTik PRO, Russia



# Nikita Tarikin

Certified network engineer  
MikroTik PRO, Russia

Since 2016

MTCNA 90%

MTCRE 93%

MTCWE 84%

MTCTCE 76%

MTCUME 90%



# MikroTik network engineering for your business

1. Designing enterprise class network infrastructure
2. Building high-performance, reliable, protected networks
3. Security and performance audit of existing network configurations
4. Monitoring and maintaining critical infrastructure
5. Troubleshooting and consulting
6. Remote support 24 / 7 / 365
7. Advanced MikroTik certified trainings in Asia  
*(coming soon)*

MTCNA 90%

MTCRE 93%

MTCWE 84%

MTCTCE 76%

MTCUME 90%



Please  
contact me

**E-mail me your ideas:**

nikita@tarikin.com

**Add me to your Facebook:**

Nikita Tarikin

**Follow me on Instagram:**

@tarikin

**Start private conversation:**

 **Telegram** [t.me/tarikin](https://t.me/tarikin)

 **Messenger** Nikita Tarikin



Please  
contact me

**Nikita Tarikin**

`nikita@tarikin.com`



# Why IKE2?

# Compare VPN types (RouterOS)

	L2TP	L2TP/IPSEC + psk	OpenVPN	PPTP	SSTP	IPSec IKE2
Protocol	UDP	UDP over UDP/ESP	TCP	GRE	TCP	UDP, ESP
Performance	Fast	Medium	Slow	Fast	Slow	Very fast
Connection establishment	Medium	Slow	Slow	Medium	Medium	Very fast
Requires strong CPU for encryption	No	Yes	Yes	No	Yes	Yes
Multicore CPU load balance	Yes	Yes	No	Yes	Yes	Yes
Security	Low	Strong	Strong	Low	Strong	Very strong
Push routes	No	No	Yes	No	No	Yes
Bypass NAT	Yes	Yes	Yes	Yes	Yes	Yes
Has interface	Yes	Yes	Yes	Yes	Yes	No
OS popularity	High	Very high	High	Very high	Low	High



# Why IKE2?

1. Blazing fast throughput performance
2. Instant connection establishment
3. Military grade security standards
4. Supported by most modern OS's
5. Can push routes to clients
6. Bypasses any NAT
7. Mobile friendly



# Network diagram

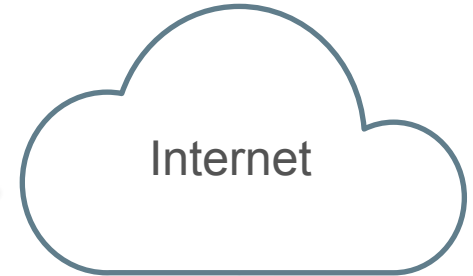


My laptop

# Networking for dummies 😊



Magic



Internet

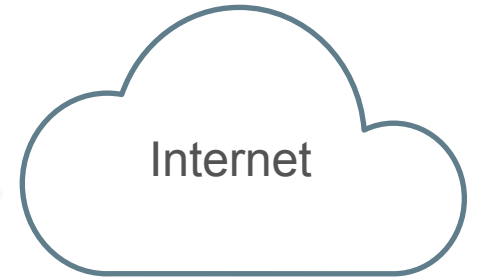


My laptop

## Networking for advanced users 🧐



My router



Internet





LAN



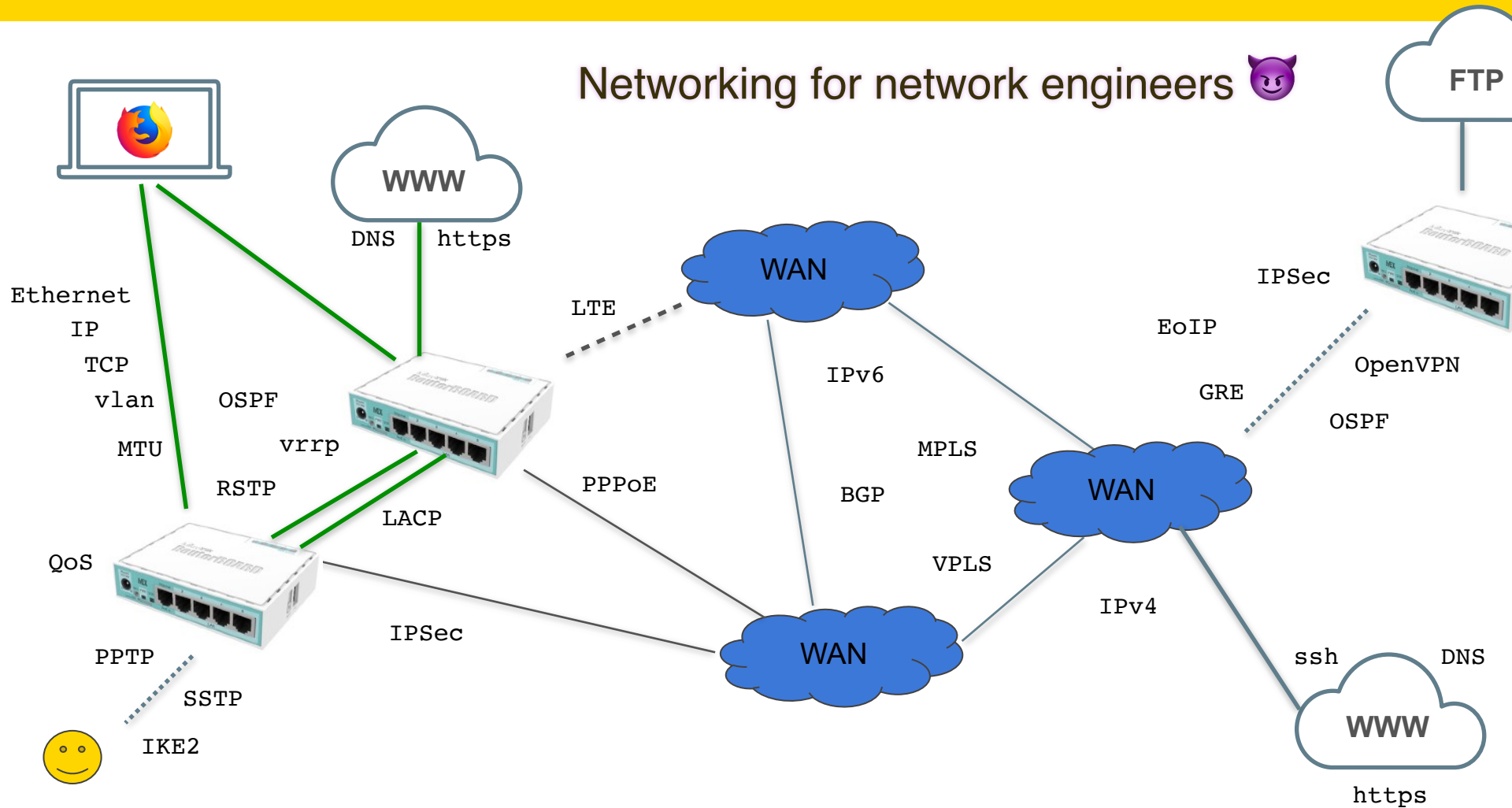
MikroTik  
Router

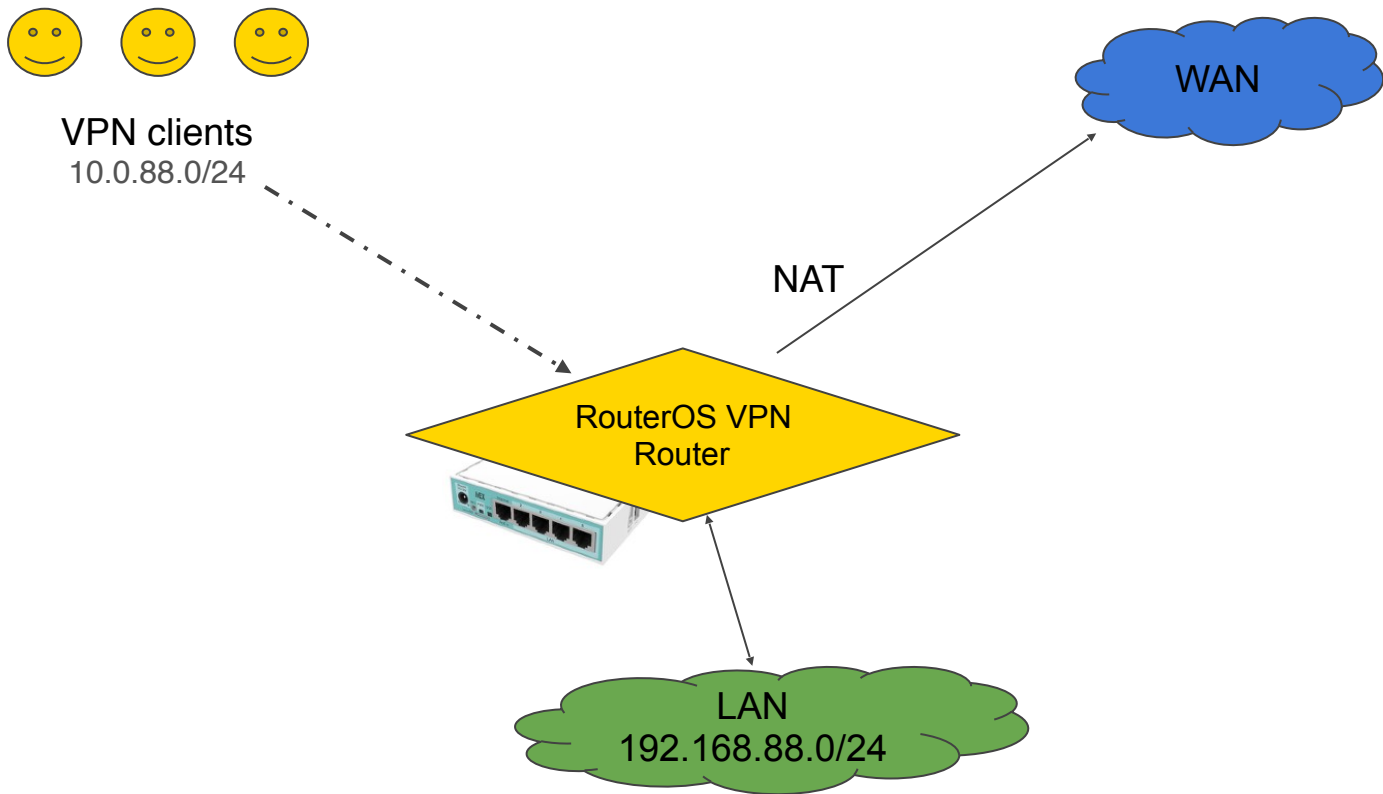
WAN



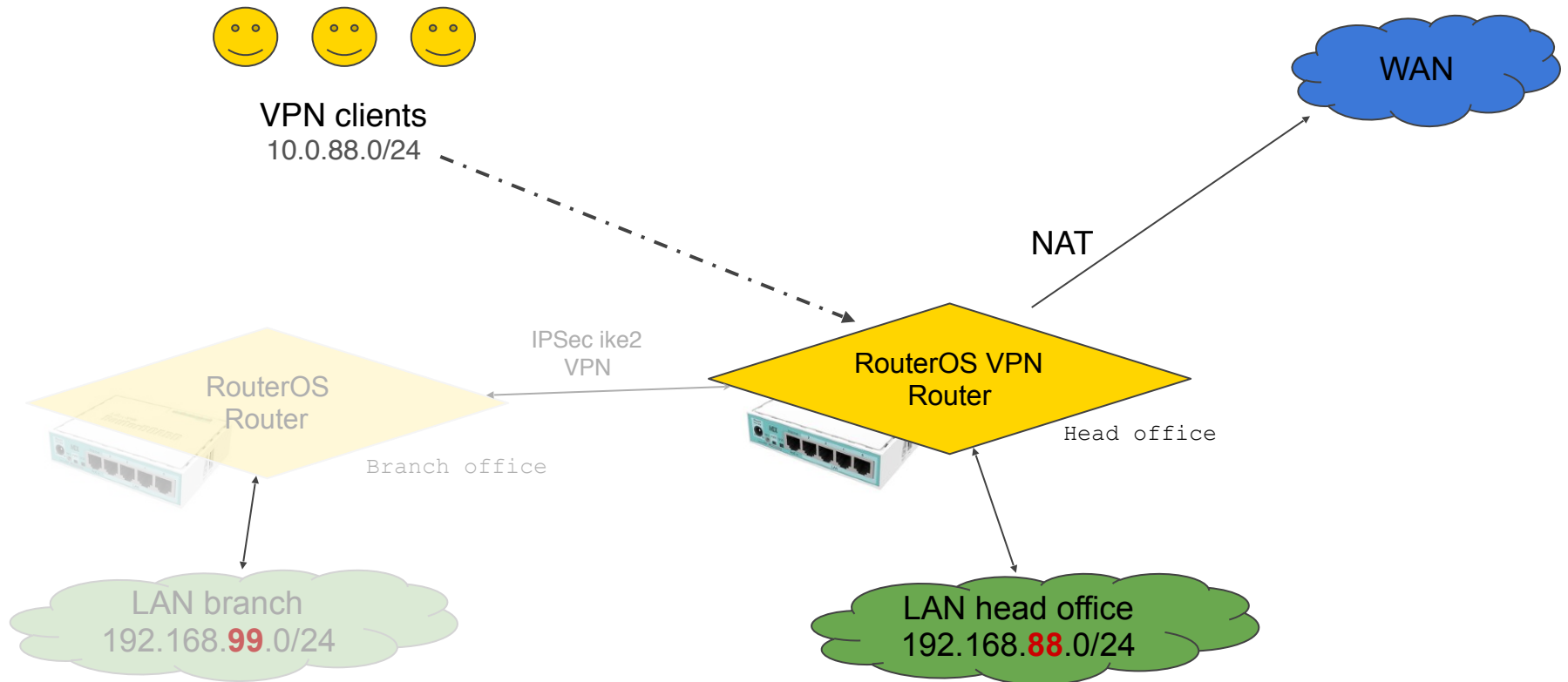
## Networking for IT juniors 🧑🔧

# Networking for network engineers 🤪





Network diagram



Network diagram

# Configure RouterOS

# Configure RouterOS

1. Before you start
2. General system settings
3. Generate SSL certificates
4. Setting up IPSec
5. Setting up Firewall
6. Setting up NAT
7. Setting up MTU/MSS



# Before you start

Checklist for your demo lab

1. MTCNA knowledge (recommended)
2. RouterOS 6.44 or newer
3. Lab environment (recommended)
4. Default configuration 6.41+
5. Aware of IPSec changes since 6.43



# Upgrade RouterOS to 6.44+

The image illustrates the process of upgrading RouterOS. It shows the MikroTik website where the 6.44.3 (Stable) package for MIPSBE is downloaded. The WinBox interface shows the package being uploaded to the router's file system. Finally, a reboot dialog box is shown, indicating the next step in the upgrade process.

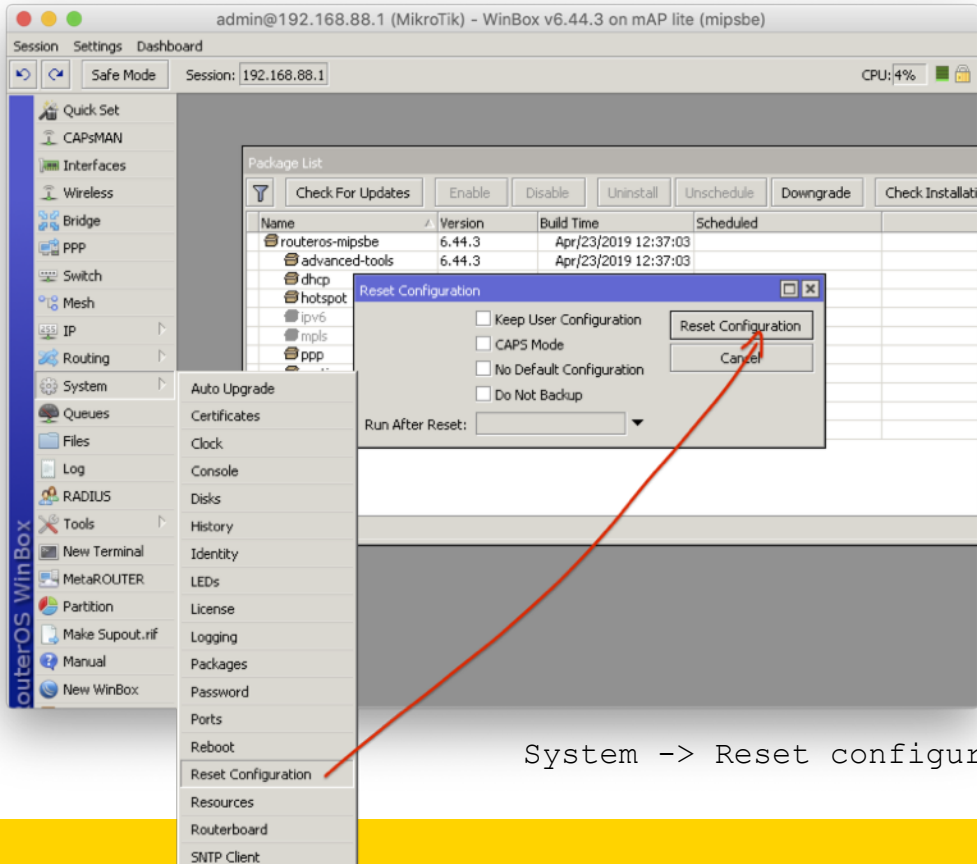
1. Download package from  
[www.mikrotik.com/download](http://www.mikrotik.com/download)

2. Upload package to / of  
your RouterBoard

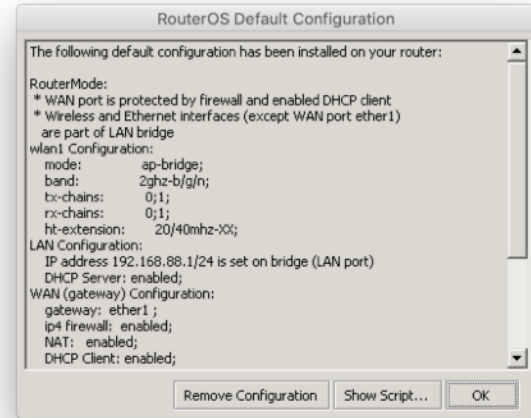
3. System -> Reboot



# Reset RouterBoard to default v6.44+ configuration



This will apply new default firewall rules, interface lists, basic security settings etc..



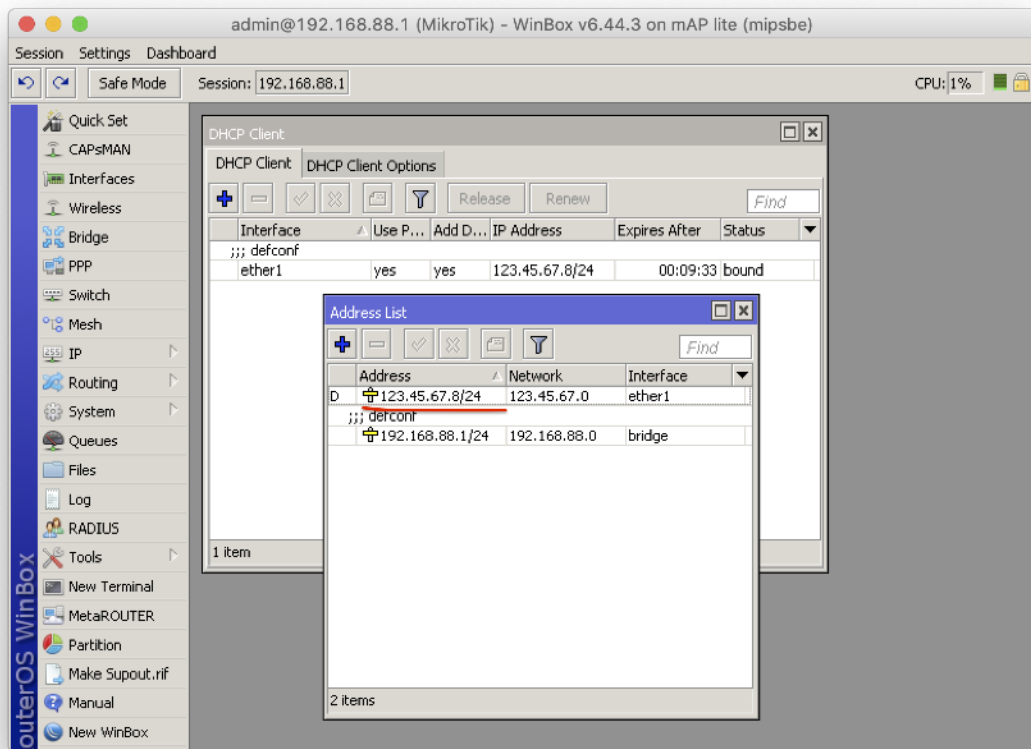
# General system settings

Agenda for next slides:

1. WAN IP/DNS addresses
2. Timezone
3. NTP
4. Loopback bridge
5. IP pool

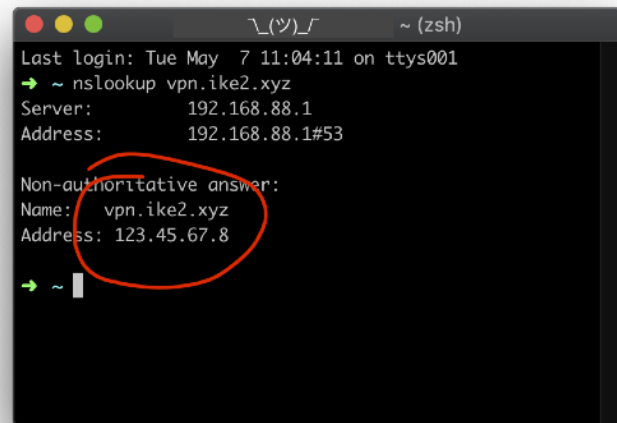


# WAN IP and DNS addresses for IKE2 VPN server



123.45.67.8 is on WAN interface

Check DNS records:  
Name: **vpn.ike2.xyz**  
Address: **123.45.67.8**

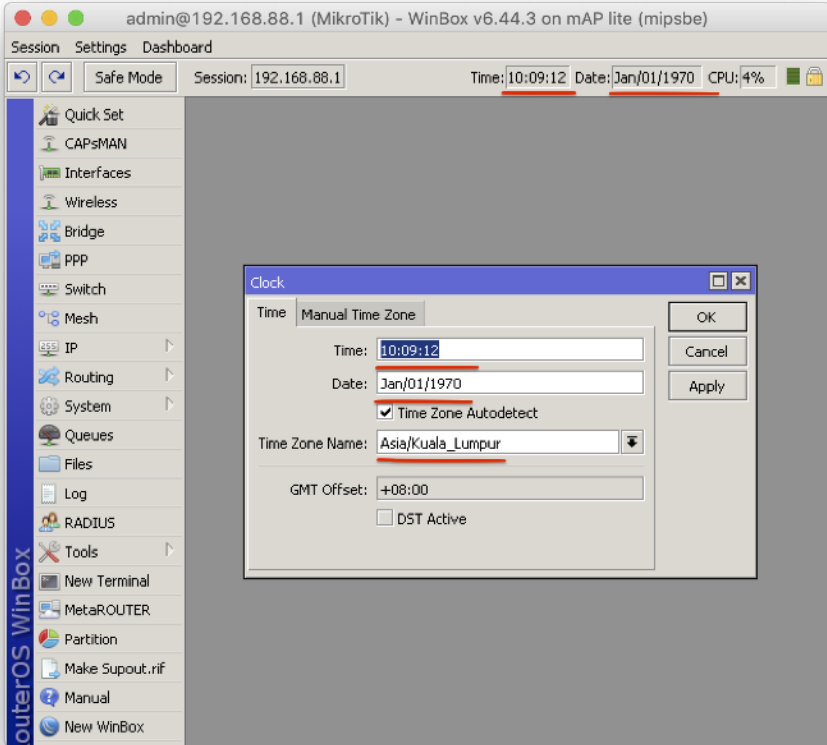


\* Set DNS records with your domain name registrar control panel



# Setup correct timezone

Important



System -> Clock

```
/system clock set time-zone-name=Asia/  
Kuala_Lumpur
```



# Setup auto date/time

Important

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1 Time: 12:36:41 Date: May/08/2019 CPU: 2%

outerOS WinBox

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
  - Auto Upgrade
  - Certificates
  - Clock
  - Console
  - Disks
  - History
  - Identity
  - LEDs
  - License
  - Logging
  - Packages
  - Password
  - Ports
  - Reboot
  - Reset Configuration
  - Resources
  - Routerboard
  - SNTP Client**
  - Scheduler
  - Scripts
  - Shutdown
- Routing
- System
  - Queues
  - Files
  - Log
  - RADILUS
  - Tools
    - New Terminal
    - MetaROUTER
    - Partition
    - Make Spoutout.nif
    - Manual
    - New WinBox

SNTP Client

Enabled

Mode: unicast

Primary NTP Server: 0.0.0.0

Secondary NTP Server: 0.0.0.0

Server DNS Names: 0.asia.pool.ntp.org

1.asia.pool.ntp.org

2.asia.pool.ntp.org

Dynamic Servers:

Poll Interval: 32 s

Active Server: 119.28.183.184

Last Update From: 119.28.183.184

Last Update: 00:00:09 ago

Last Adjustment: 3 442 us

Last Bad Packet From:

Last Bad Packet:

Last Bad Packet Reason:

OK

Cancel

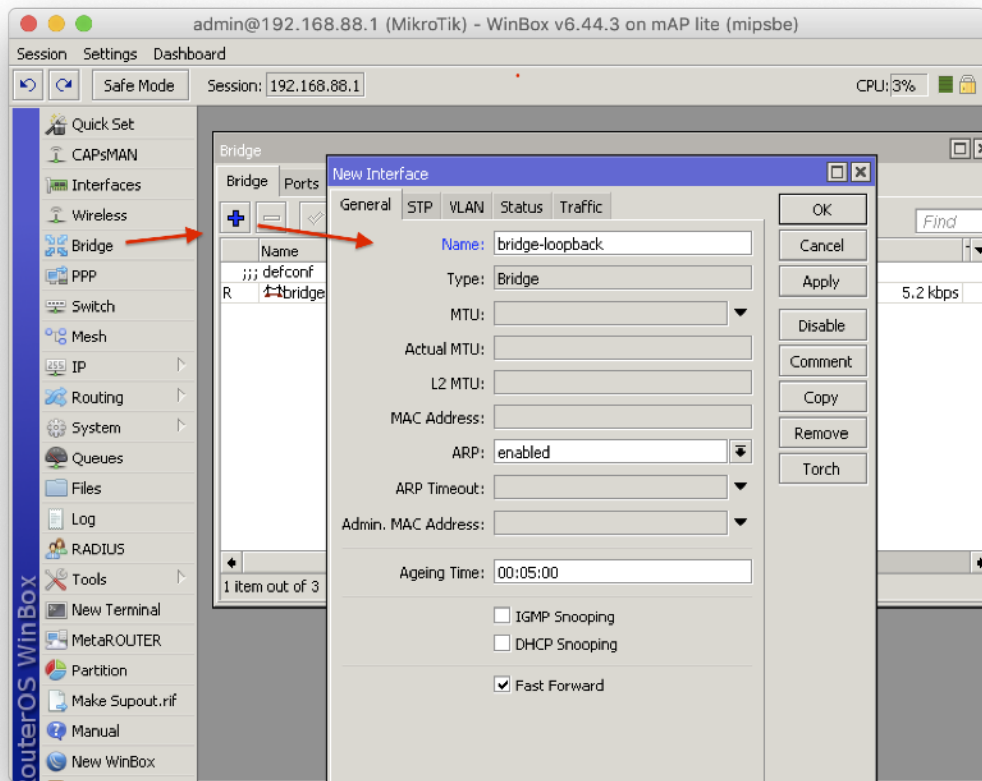
Apply

Activate NTP client

```
/system ntp client set enabled=yes  
server-dns-names=0.asia.pool.ntp.org,  
1.asia.pool.ntp.org,2.asia.pool.ntp.org
```



# Add new loopback bridge



```
/interface bridge add  
name=bridge-loopback
```



# Set loopback bridge IP address

The screenshot shows the Mikrotik WinBox interface. The main window is titled "Bridge" and displays a table of bridge configurations. A "New Address" dialog box is open, showing the configuration for a new address. The "Address" field is set to "10.0.88.0/24", the "Network" field is set to "10.0.88.0", and the "Interface" field is set to "bridge-loopback". The "Address List" dialog box is also open, showing a table of existing addresses.

Address	Network	Interface
123.45.67.8/24	123.45.67.0	ether1
192.168.88.1/24	192.168.88.0	bridge

The "New Address" dialog box contains the following fields:

- Address: 10.0.88.0/24
- Network: 10.0.88.0
- Interface: bridge-loopback

The "Address List" dialog box contains the following table:

Address	Network	Interface
123.45.67.8/24	123.45.67.0	ether1
192.168.88.1/24	192.168.88.0	bridge

```
/ip address add  
address=10.0.88.1/24  
interface=bridge-loopback  
network=10.0.88.0
```

```
U6CMOIK=10*0*88*0
```



# Add new IP Pool for ike2 VPN clients

The screenshot shows the Mikrotik WinBox interface. The left sidebar contains a menu with items like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, Routing, System, Queues, Files, Log, RADIUS, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rif, Manual, and New WinBox. The main window displays the 'IP Pool' configuration dialog. The 'New IP Pool' sub-dialog is open, showing the following fields:

- Name: pool vpn.ike2.xyz
- Addresses: 10.0.88.2-10.0.88.254
- Next Pool: none

The background shows the 'Address List' table with the following data:

Address	Network	Interface
10.0.88.0/24	10.0.88.0	bridge-loopback
123.45.67.8/24	123.45.67.0	ether1

```
/ip pool add name="pool  
vpn.ike2.xyz"  
ranges=10.0.88.2-10.0.88.254
```

```
ranges=10.0.88.2-10.0.88.254
```



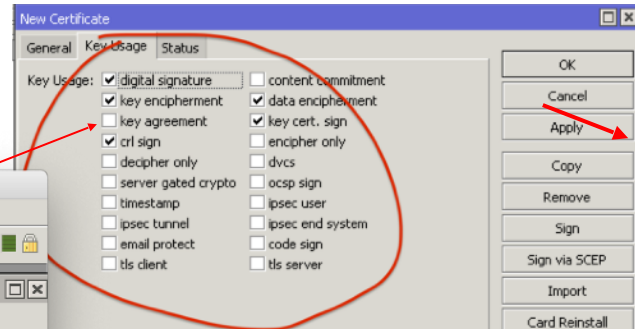
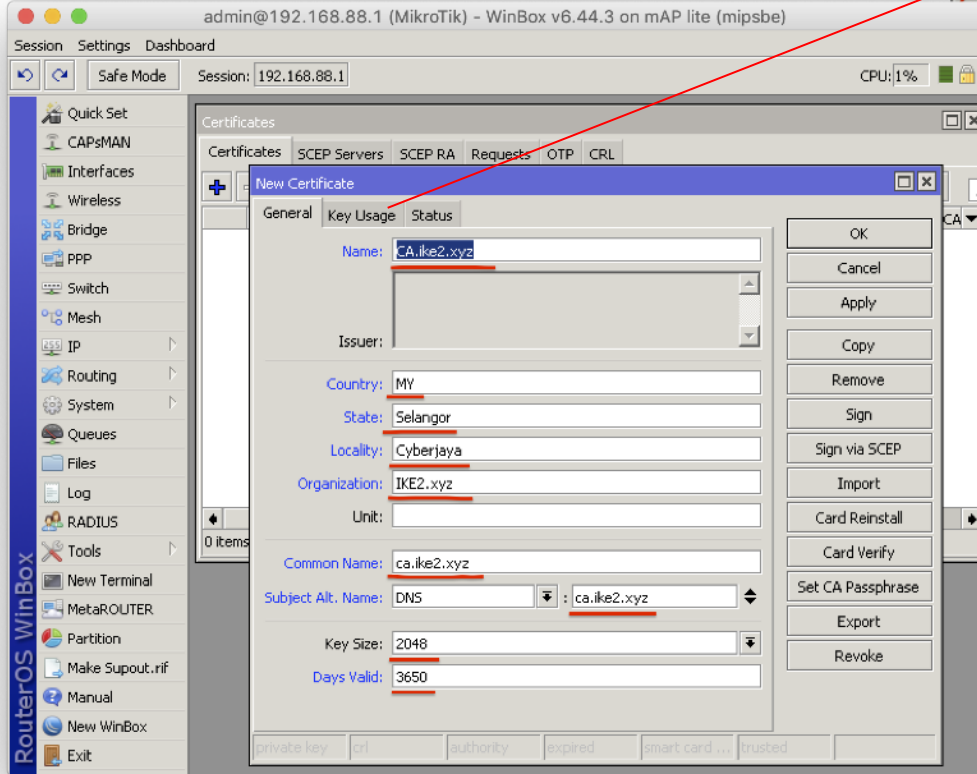
# Generate SSL certificates

Agenda for next slides

1. Generate CA
2. Generate server SSL
3. Generate client SSL
4. Export client SSL

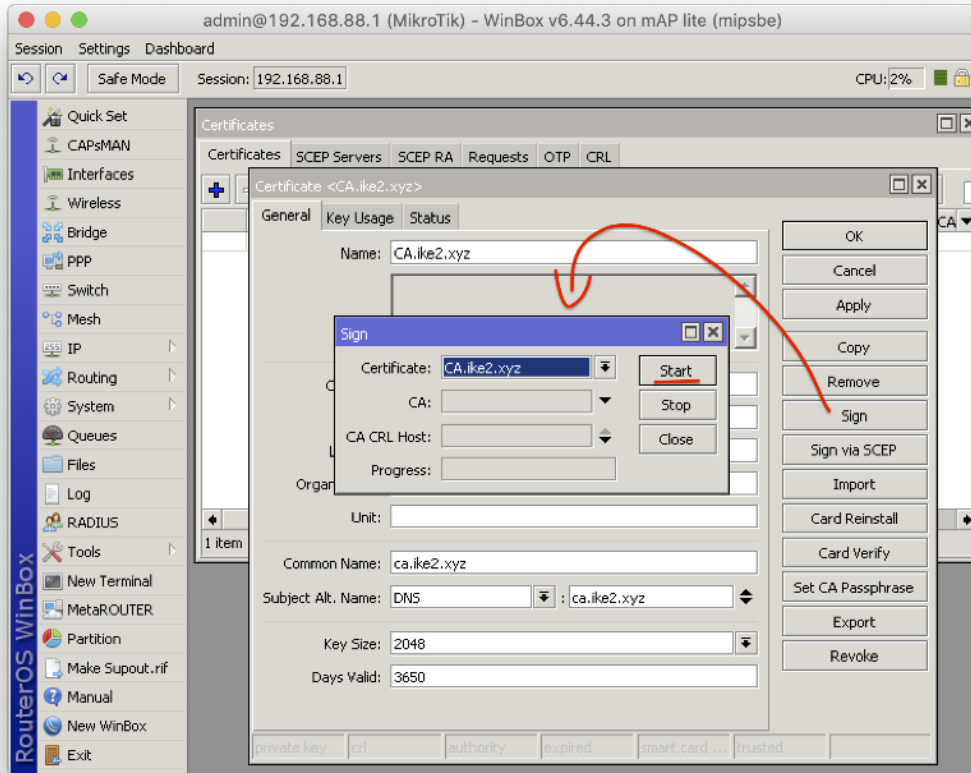


# Generate CA SSL certificate



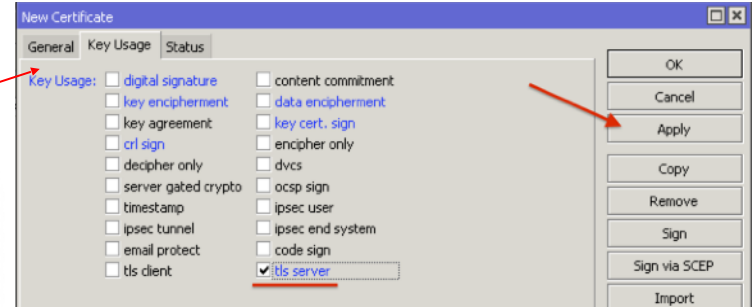
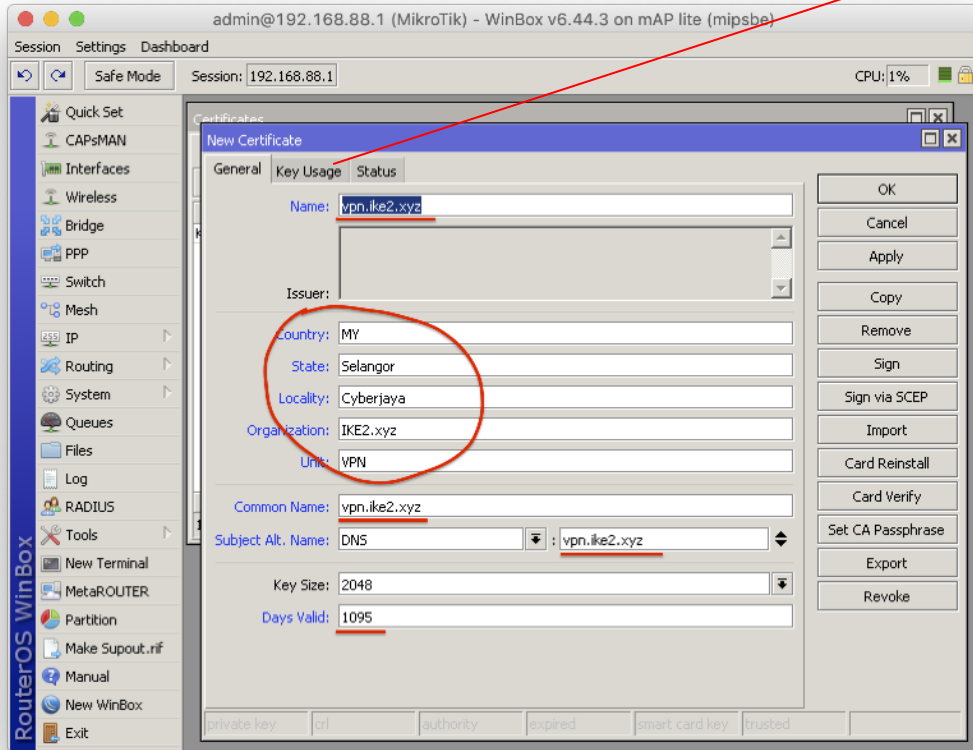
```
/certificate add name=CA.ike2.xyz  
country=MY state=Selangor  
locality=Cyberjaya  
organization=IKE2.xyz common-  
name=ca.ike2.xyz subject-alt-  
name=DNS:ca.ike2.xyz key-size=2048  
days-valid=3650 trusted=yes key-  
usage=digital-signature,key-  
encipherment,data-encipherment,key-  
cert-sign,crl-sign
```

# Self-sign CA SSL certificate (*Certificate Authority*)



```
/certificate sign CA.ike2.xyz
```

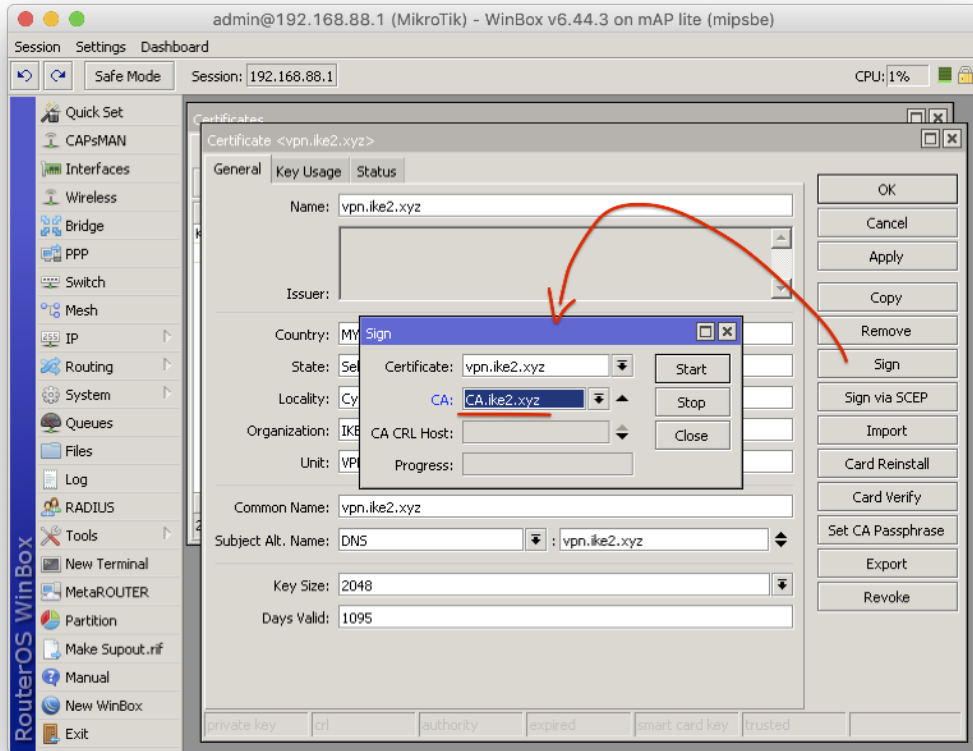
# Generate server SSL certificate



```
/certificate add name=vpn.ike2.xyz  
country=MY state=Selangor  
locality=Cyberjaya  
organization=IKE2.xyz unit=VPN  
common-name=vpn.ike2.xyz subject-  
alt-name=DNS:vpn.ike2.xyz key-  
size=2048 days-valid=1095  
trusted=yes key-usage=tls-server
```

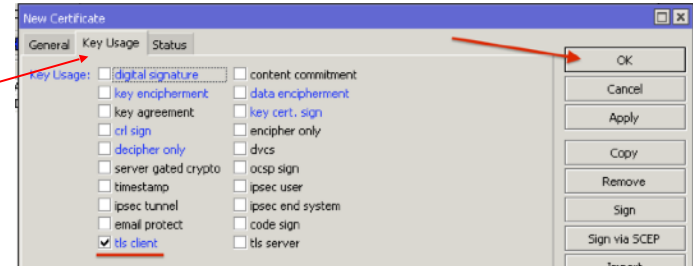
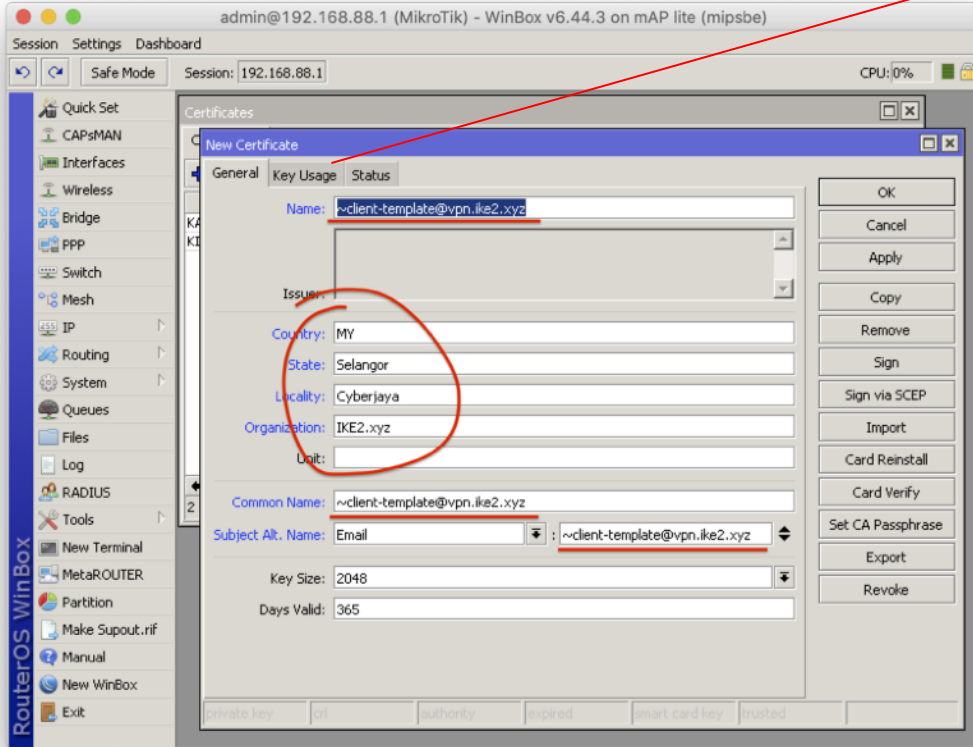


# Sign server SSL certificate with CA.ike2.xyz authority



```
/certificate sign vpn.ike2.xyz  
ca=CA.ike2.xyz
```

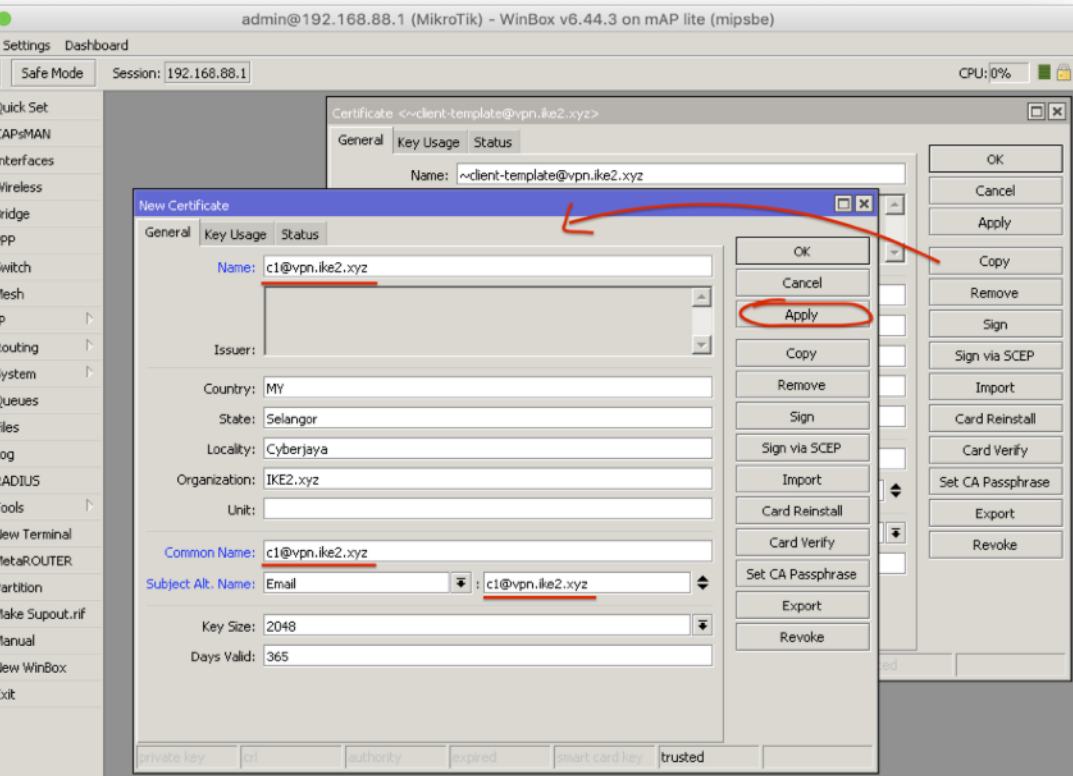
# Client certificate template



```
/certificate add name=~client-  
template@vpn.ike2.xyz country=MY  
state=Selangor locality=Cyberjaya  
organization=IKE2.xyz common-  
name=~client-template@vpn.ike2.xyz  
subject-alt-name=email::~client-  
template@vpn.ike2.xyz key-size=2048  
days-valid=365 trusted=yes key-  
usage=tls-client
```

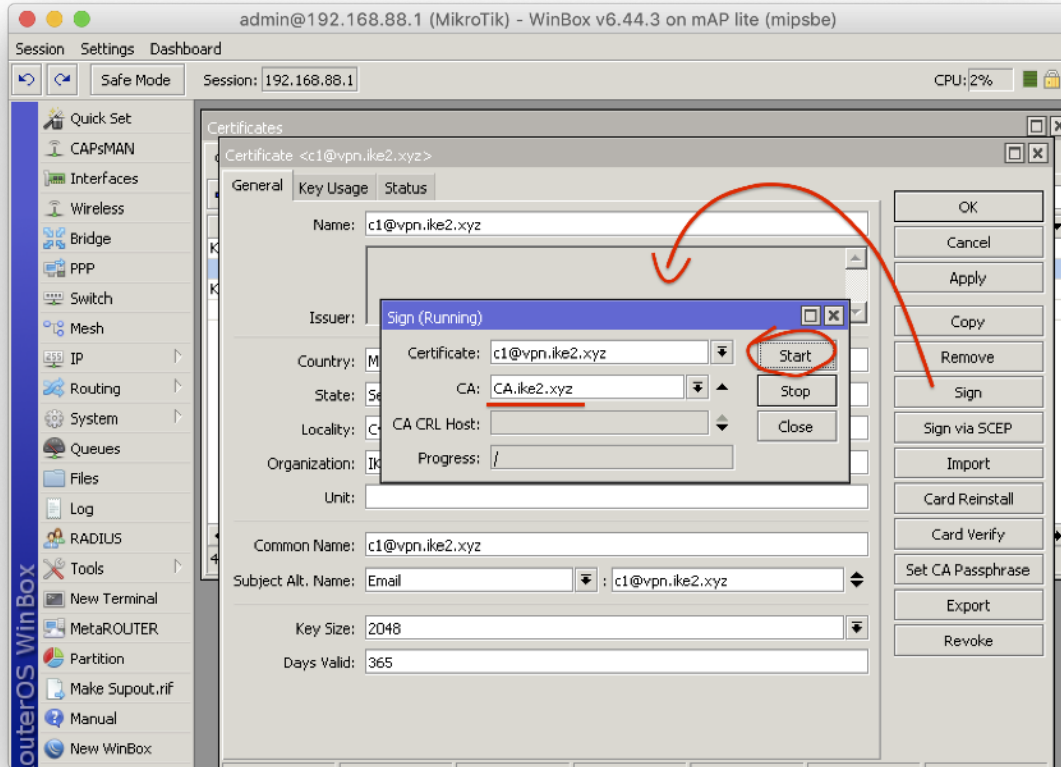


# Generate client SSL certificate from template



```
/certificate add copy-from=~client-  
template@vpn.ike2.xyz  
name=c1@vpn.ike2.xyz common-  
name=c1@vpn.ike2.xyz subject-alt-  
name=email:c1@vpn.ike2.xyz
```

# Sign client SSL certificate with CA.ike2.xyz authority

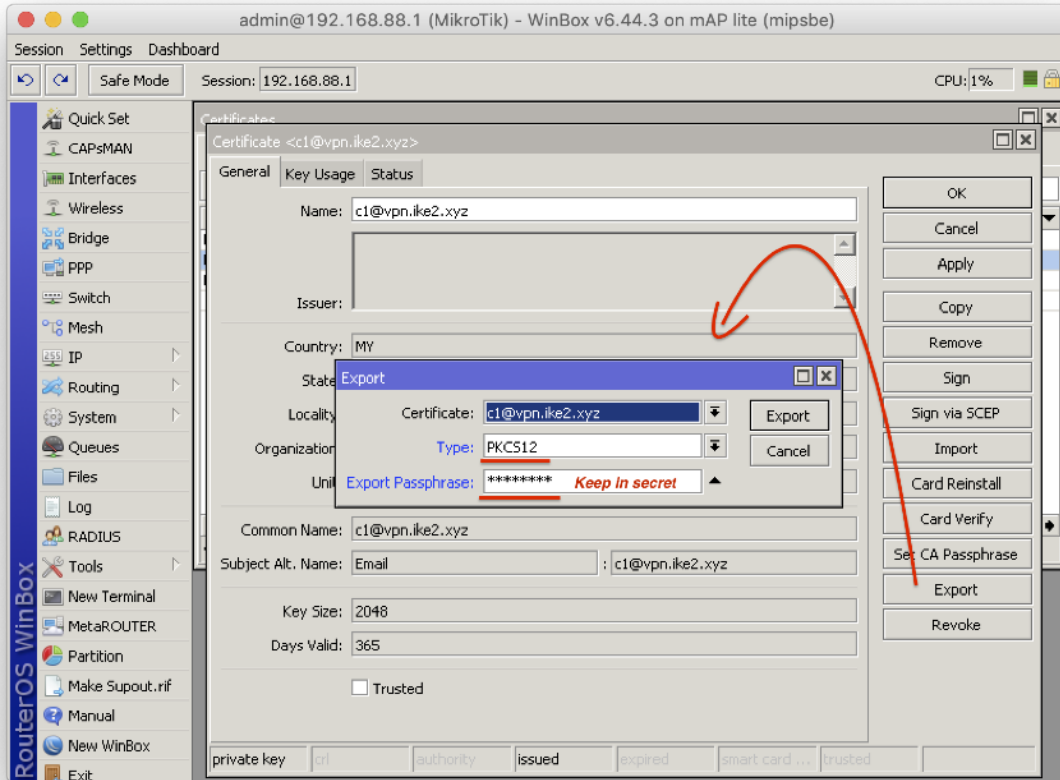


```
/certificate sign  
c1@vpn.ike2.xyz ca=CA.ike2.xyz
```





# Export client SSL certificate + private key to .p12 file

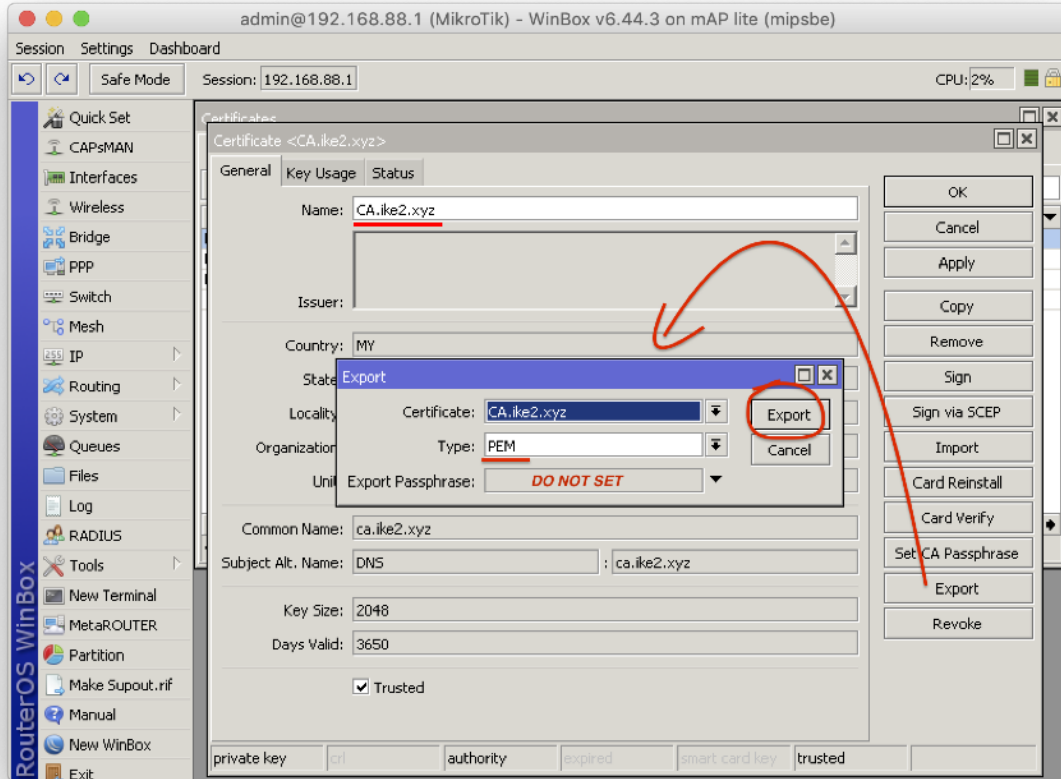


```
/certificate export-certificate  
c1@vpn.ike2.xyz type=pkcs12  
export-passphrase=keepinsecret
```

```
export-passphrase=keepinsecret
```



# Export CA SSL certificate .crt file



```
/certificate  
export-certificate CA.ike2.xyz
```



# Download exported SSL certificates

---

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)". The "Certificates" section is active, displaying a table of certificates. A "File List" dialog box is open, showing a list of files in the "Files" directory. A red circle highlights the two certificate files: "cert\_export\_CA.ike2.xyz.crt" and "cert\_export\_c1@vpn.ike2.xyz.p12". A red arrow points from the "Files" menu item in the left sidebar to the dialog box.

Name	Common Name	Subject Alt. Name	Key Size	Days Valid	Trusted	CA
KAT CA.ike2.xyz	ca.ike2.xyz	DNS:ca.ike2.xyz	2048	3650	yes	
KI c1@vpn.ike2.xyz	c1@vpn.ike2.xyz	DNS:c1@vpn.ike2.xyz	2048	3650	yes	CA.ike2.xyz
KI vpn.ike2.xyz	vpn.ike2.xyz	DNS:vpn.ike2.xyz	2048	3650	yes	CA.ike2.xyz

File Name	Type	Size	Creation Time
cert_export_CA.ike2.xyz.crt	.crt file	1359 B	May/08/2019 11:00:00
cert_export_c1@vpn.ike2.xyz.p12	.p12 file	3688 B	May/08/2019 11:00:00
Flash	disk		Jan/01/1970 00:00:00
flash/pub	directory		May/24/2017 00:00:00
flashy/skins	directory		Jan/01/1970 00:00:00

# Setting up IPSec

## Agenda for next slides

1. Setup Mode Configs
2. Setup Peer Profiles
3. Setup Proposals
4. Setup Peers
5. Setup Policy Groups
6. Setup Policies
7. Setup Identities



# IPSec mode config

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1 CPU: 2%

IPsec

Policies Proposals Groups Peers Identities Profiles Remote Peers Mode Configs Installed SAs Keys

Name	Resp...	Address Pool	Address	Address Prefi...	Split Include	System DNS
request-only	no					

New IPsec Mode Config

Name: modeconf vpn.ike2.xyz

Responder

Address Pool: pool vpn.ike2.xyz

Address:

Address Prefix Length: 32

Split Include: 0.0.0.0/0

System DNS

Static DNS: 10.0.88.1

IPsec Mode Config <modeconf vpn.ike2.xyz>

Name: modeconf vpn.ike2.xyz

Responder

Address Pool: pool vpn.ike2.xyz

Address:

Address Prefix Length: 32

Split Include: 192.168.88.0/24

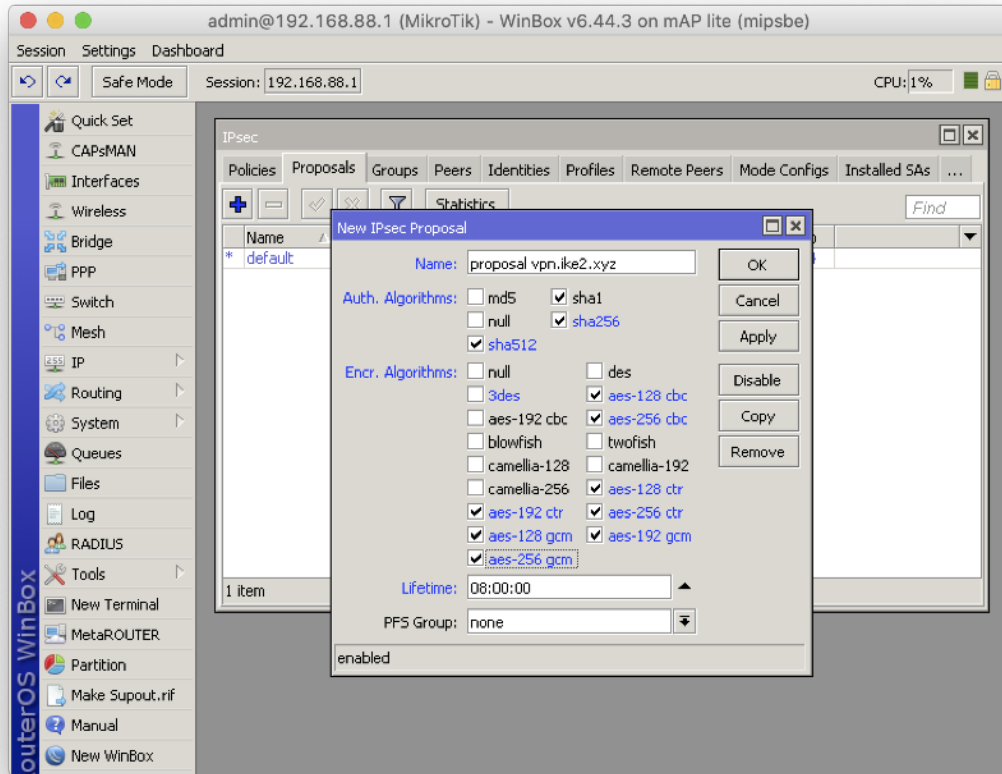
System DNS

Static DNS: 10.0.88.1

```
/ip ipsec mode-config
add address-pool="pool
vpn.ike2.xyz" address-prefix-
length=32 name="modeconf
vpn.ike2.xyz" split-
include=0.0.0.0/0 static-
dns=10.0.88.1 system-dns=no
```



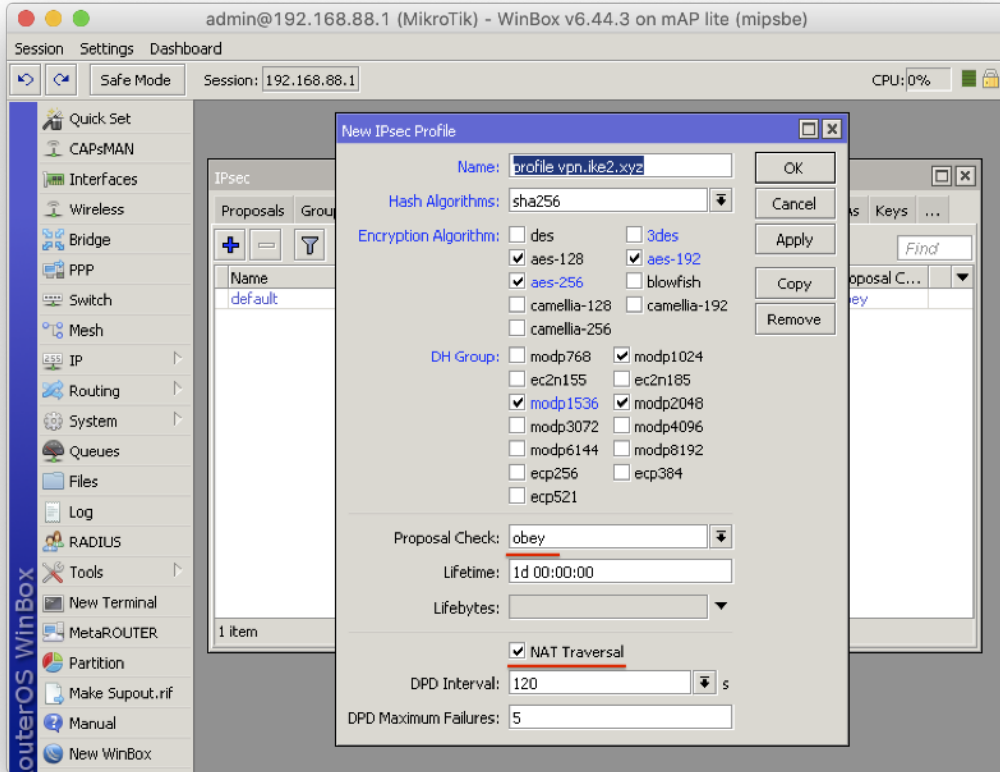
# IPSec proposal (phase 2)



```
/ip ipsec proposaladd auth-  
algorithms=sha512,sha256,sha1  
enc-algorithms=aes-256-  
cbc,aes-256-ctr,aes-256-  
gcm,aes-192-ctr,aes-192-  
gcm,aes-128-cbc,aes-128-  
ctr,aes-128-gcm lifetime=8h  
name="proposal vpn.ike2.xyz"  
pfs-group=none
```



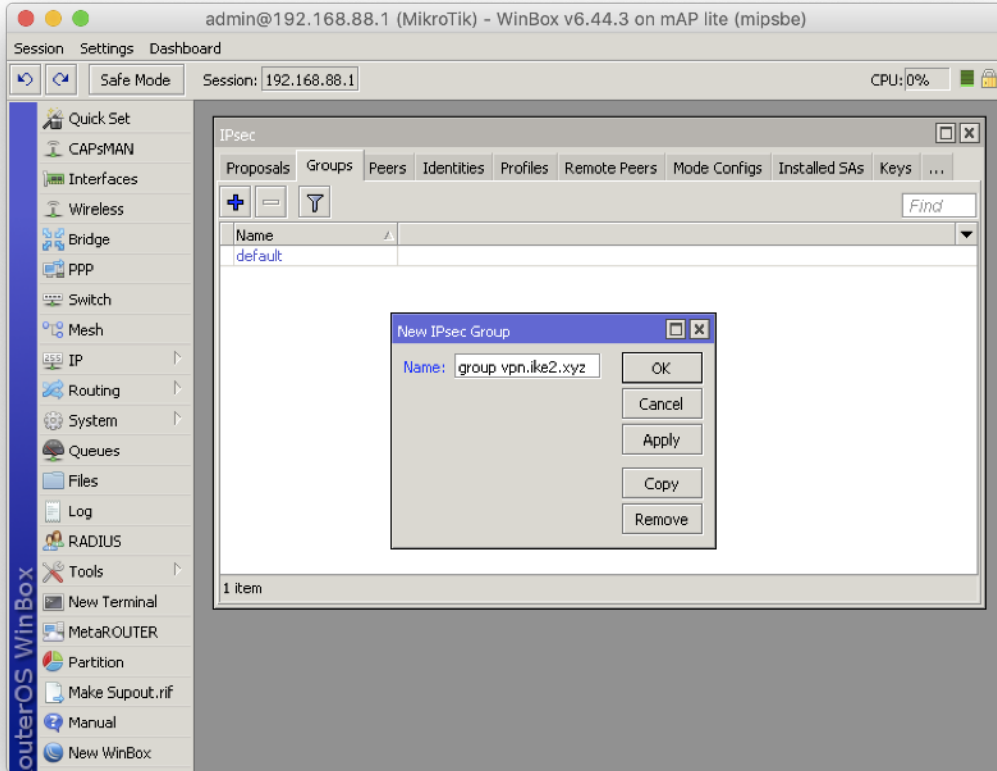
# IPSec peer profile



```
/ip ipsec profile add dh-  
group=modp2048,modp1536,modp102  
4 enc-  
algorithm=aes-256,aes-192,aes-1  
28 hash-algorithm=sha256  
name="profile.vpn.ike2.xyz"  
nat-traversal=yes proposal-  
check=obey
```



# IPSec policy group



```
/ip ipsec policy group  
add name="group vpn.ike2.xyz"
```



# IPSec policy template

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1 CPU: 1%

IPsec

#	Src. Address	Src. P...	Dst. Address	Dst. P...	Prot...	Action	Level
0 *T	:::0		:::0		255 ...	encrypt	

New IPsec Policy

General Action Status

Src. Address: 0.0.0.0

Src. Port:

Dst. Address: 10.0.88.0/24

Dst. Port:

Protocol: 255 (all)

Template

Group: group vpn.ike2.xyz

enabled Template Active

New IPsec Policy

General Action Status

Action: encrypt

IPsec Protocols: esp

SA Src. Address: 0.0.0.0

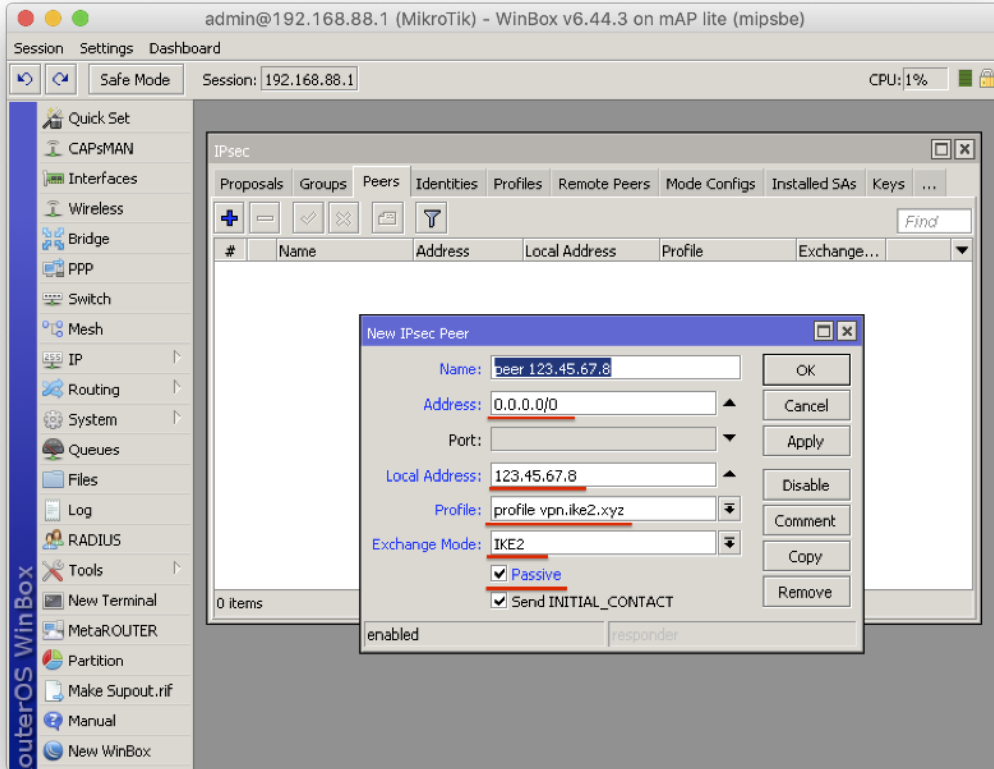
SA Dst. Address: 0.0.0.0

Proposal: proposal vpn.ike2.xyz

enabled Template Active

```
/ip ipsec policy add dst-  
address=10.0.88.0/24 group="group  
vpn.ike2.xyz" proposal="proposal  
vpn.ike2.xyz" src-address=0.0.0.0/  
template=yes sa-src-address=0.0.0.0  
sa-dst-address=0.0.0.0 ipsec-  
protocols=esp level=require  
protocol=all action=encrypt
```

# IPSec peer



```
/ip ipsec peer add exchange-  
mode=ike2 address=0.0.0.0/0  
local-address=123.45.67.8  
name="peer 123.45.67.8"  
passive=yes send-initial-  
contact=yes profile="profile  
vpn.ike2.xyz"
```

# IPSec identities (RouterOS 6.44)

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU:1%

### New IPsec Identity

Peer: peer 123.45.67.8

Auth. Method: rsa signature

Certificate: vpn.ike2.xyz

Remote Certificate: c1@vpn.ike2.xyz

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: c1@vpn.ike2.xyz

Match By: certificate

Mode Configuration: modeconf vpn.ike2.xyz

Generate Policy: port strict

enabled

### New IPsec Identity

Peer: peer 123.45.67.8

Auth. Method: rsa signature

Certificate: vpn.ike2.xyz

Remote Certificate: c2@vpn.ike2.xyz

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: c2@vpn.ike2.xyz

Match By: certificate

Mode Configuration: modeconf vpn.ike2.xyz

Generate Policy: port strict

enabled

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove

```
/ip ipsec identity add auth-method=rsa-signature
certificate=vpn.ike2.xyz remote-
certificate=c1@vpn.ike2.xyz generate-
policy=port-strict match-by=certificate mode-
config="modeconf vpn.ike2.xyz" peer="peer
123.45.67.8" policy-template-group="group
vpn.ike2.xyz" remote-id=user-fqdn:c1@vpn.ike2.xyz
```

```
/ip ipsec identity add auth-method=rsa-signature
certificate=vpn.ike2.xyz remote-
certificate=c2@vpn.ike2.xyz generate-
policy=port-strict match-by=certificate mode-
config="modeconf vpn.ike2.xyz" peer="peer
123.45.67.8" policy-template-group="group
vpn.ike2.xyz" remote-id=user-fqdn:c2@vpn.ike2.xyz
```

# IPSec identities (RouterOS 6.45+)

admin@192.168.88.1 (MikroTik) - WinBox v6.45beta54 on mAP lite (mipsbe)

Dashboard

Session: 192.168.88.1 Time: 13:33:44 Date: Jun/07/2019 CPU: 2%

IPsec

Policies Proposals Groups Peers Identities

#	Peer	Auth. Method	Remote ID
0	peer 123.45.67.8	digital signature	c1@vpn.ike2.xyz
1	peer 123.45.67.8	digital signature	c1@vpn.ike2.xyz
2	peer 123.45.67.8	digital signature	c1@vpn.ike2.xyz
3	peer 123.45.67.8	digital signature	c1@vpn.ike2.xyz
4	peer 123.45.67.8	digital signature	c1@vpn.ike2.xyz
5	peer 123.45.67.8	digital signature	c1@vpn.ike2.xyz
6	peer 123.45.67.8	digital signature	c1@vpn.ike2.xyz

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: c1@vpn.ike2.xyz

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: c1@vpn.ike2.xyz

Match By: certificate

Mode Configuration: modeconf vpn.ike2.xyz

Generate Policy: port strict

enabled

What's new in 6.45

\*) ipsec - renamed "rsa-signature" authentication method to "**digital-signature**";

```
/ip ipsec identity
add auth-method=digital-signature
certificate=vpn.ike2.xyz remote-
certificate=c1@vpn.ike2.xyz generate-
policy=port-strict match-by=certificate mode-
config="modeconf vpn.ike2.xyz" peer="peer
123.45.67.8" policy-template-group="group
vpn.ike2.xyz" remote-id=user-fqdn:c1@vpn.ike2.xyz
```



# Setting up Firewall

## Agenda for next slides

1. Default firewall overview
2. IPSec traffic rules
3. VPN traffic rules



# Setting up Firewall

Understanding the default firewall filter

# RouterOS 6.41+ default configuration firewall overview

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1 CPU: 1%

### Firewall

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

+ - [check] [x] [lock] [filter] [reset] [reset all] Find: all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
;;; special dummy rule to show fasttrack counters															
0	D	pas...	forward											124.1 MIB	211 598
;;; defconf: accept established,related,untracked															
1	✓ acc...	input												6.5 MIB	76 964
;;; defconf: drop invalid															
2	✗ drop	input												3145 B	34
;;; defconf: accept ICMP															
3	✓ acc...	input			1 (icmp)									0 B	0
;;; defconf: drop all not coming from LAN															
4	✗ drop	input							!LAN					33.5 KIB	133
;;; defconf: accept in ipsec policy															
5	✓ acc...	forward												0 B	0
;;; defconf: accept out ipsec policy															
6	✓ acc...	forward												0 B	0
;;; defconf: fasttrack															
7	▶ fas...	forward												6.2 MIB	42 281
;;; defconf: accept established,related, untracked															
8	✓ acc...	forward												6.2 MIB	42 281
;;; defconf: drop invalid															
9	✗ drop	forward												1076 B	23
;;; defconf: drop all from WAN not DSTNATed															
10	✗ drop	forward								WAN				0 B	0

11 items

outerOS WinBox

NETICA Gdansk / NETICA@Gdansk.COM

```
#Input Chain Rules
/ip firewall filter
add action=accept chain=input connection-state=established,related,untracked comment="DEFAULT:
Accept established, related, and untracked traffic."
add action=drop chain=input connection-state=invalid comment="DEFAULT: Drop invalid traffic."
add action=accept chain=input protocol=icmp comment="DEFAULT: Accept ICMP traffic."
add action=drop chain=input in-interface-list=!LAN comment="DEFAULT: Drop all other traffic not
coming from LAN."

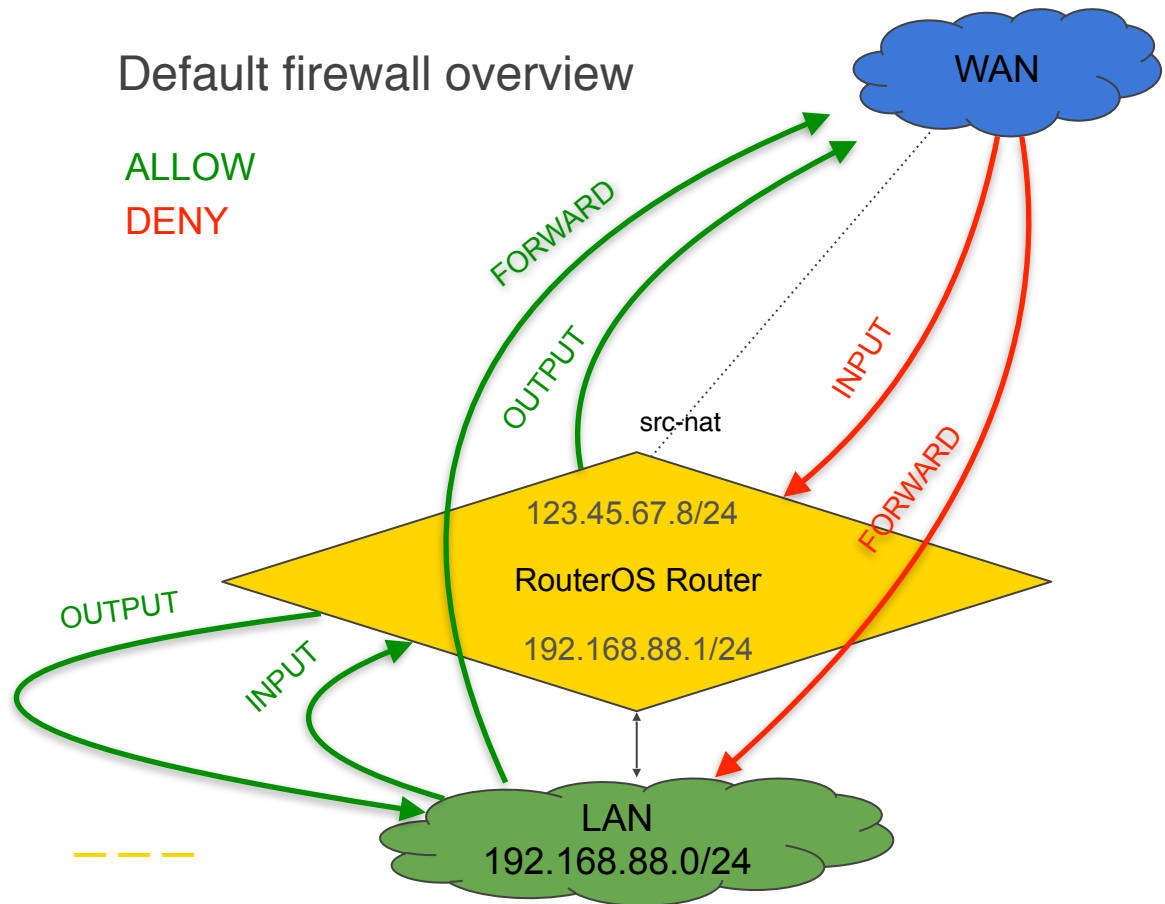
#Forward Chain Rules
/ip firewall filter
add action=accept chain=forward ipsec-policy=in,ipsec comment="DEFAULT: Accept In IPsec policy."
add action=accept chain=forward ipsec-policy=out,ipsec comment="DEFAULT: Accept Out IPsec policy."
add action=accept chain=forward connection-state=established,related,untracked comment="DEFAULT:
Accept established, related, and untracked traffic."
add action=drop chain=forward connection-state=invalid comment="DEFAULT: Drop invalid traffic."
add action=drop chain=forward connection-nat-state=!dstnat connection-state=new in-interface-
list=WAN comment="DEFAULT: Drop all other traffic from WAN that is not DSTNATED."

#Output (defconf: empty filter)
```



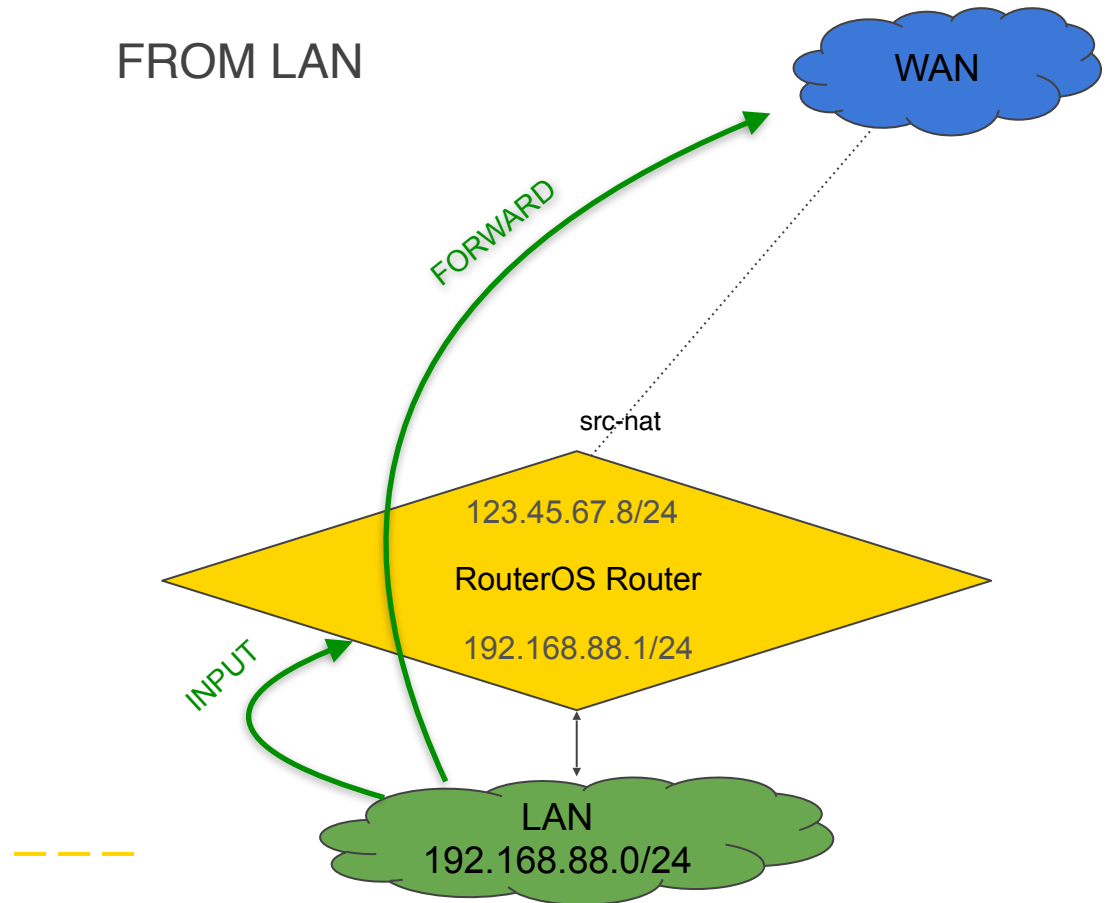
# Setting up Firewall

1. Default firewall overview
2. IPSec traffic rules
3. VPN traffic rules
4. Testing



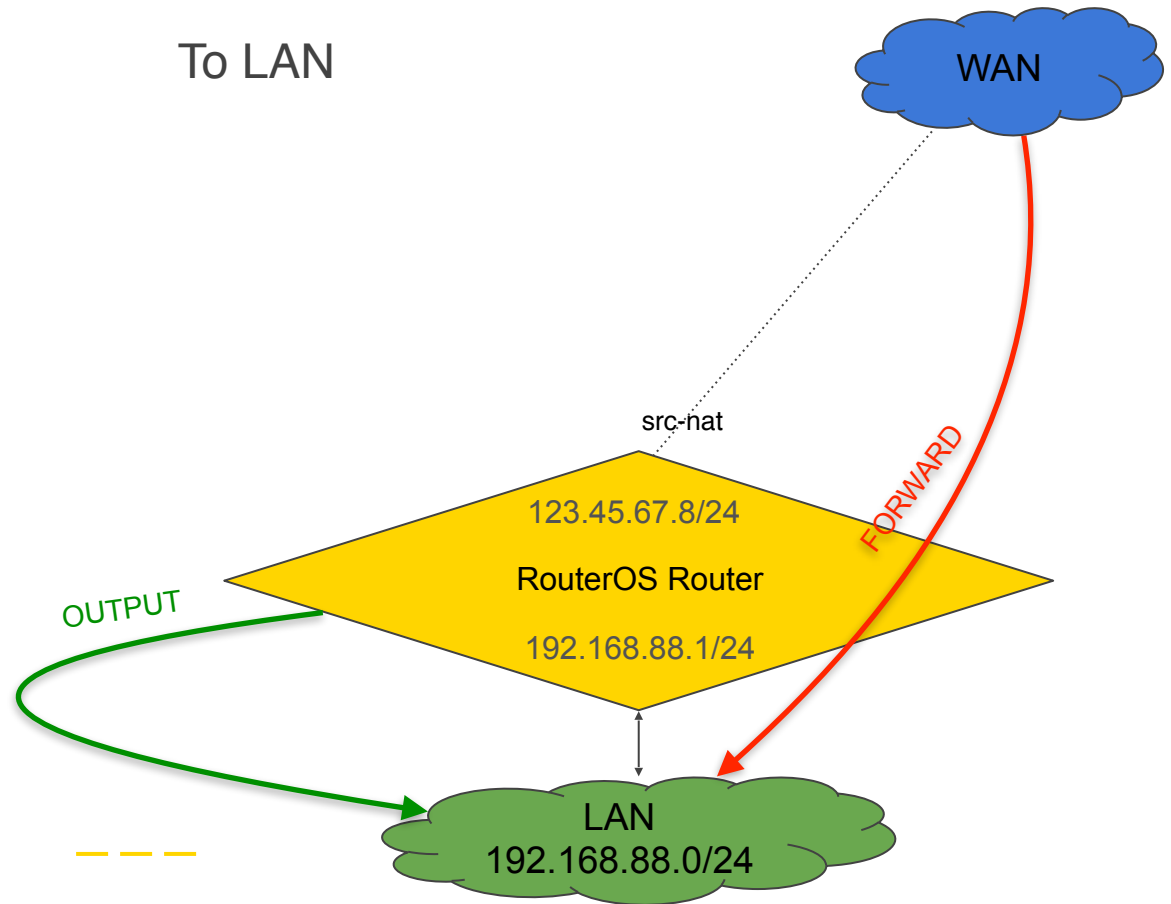
# Default Firewall overview

- a. From LAN
- b. To LAN
- c. From RouterOS
- d. To RouterOS
- e. From WAN
- f. To WAN



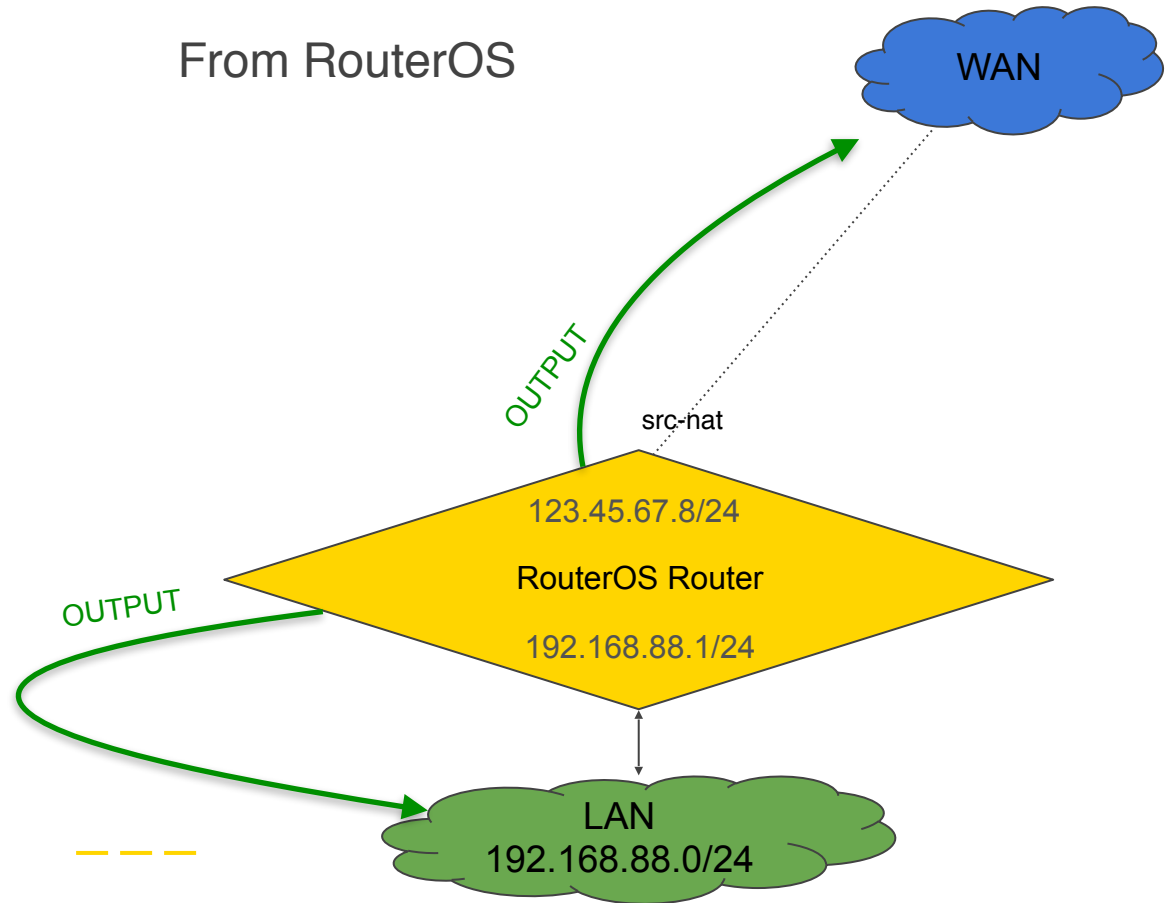
# Default Firewall overview

- a. From LAN
- b. To LAN**
- c. From RouterOS
- d. To RouterOS
- e. From WAN
- f. To WAN



# Default Firewall overview

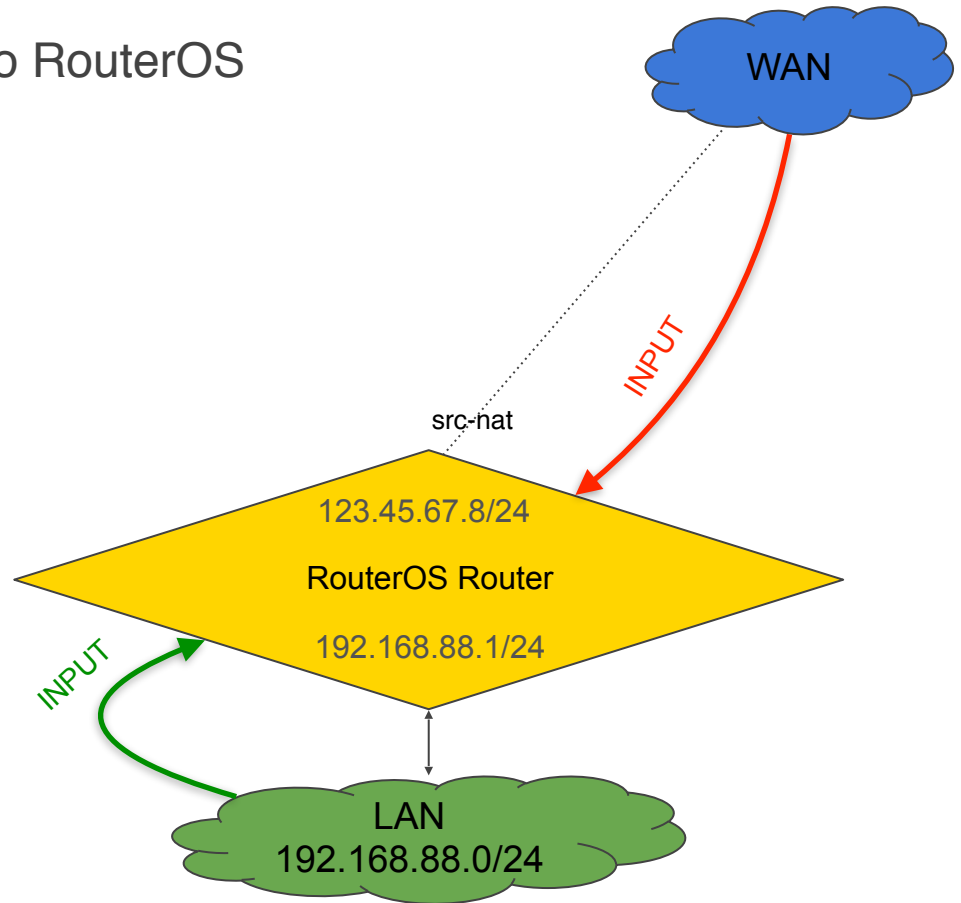
- a. From LAN
- b. To LAN
- c. **From RouterOS**
- d. To RouterOS
- e. From WAN
- f. To WAN



# Default Firewall overview

- a. From LAN
- b. To LAN
- c. From RouterOS
- d. To RouterOS**
- e. From WAN
- f. To WAN

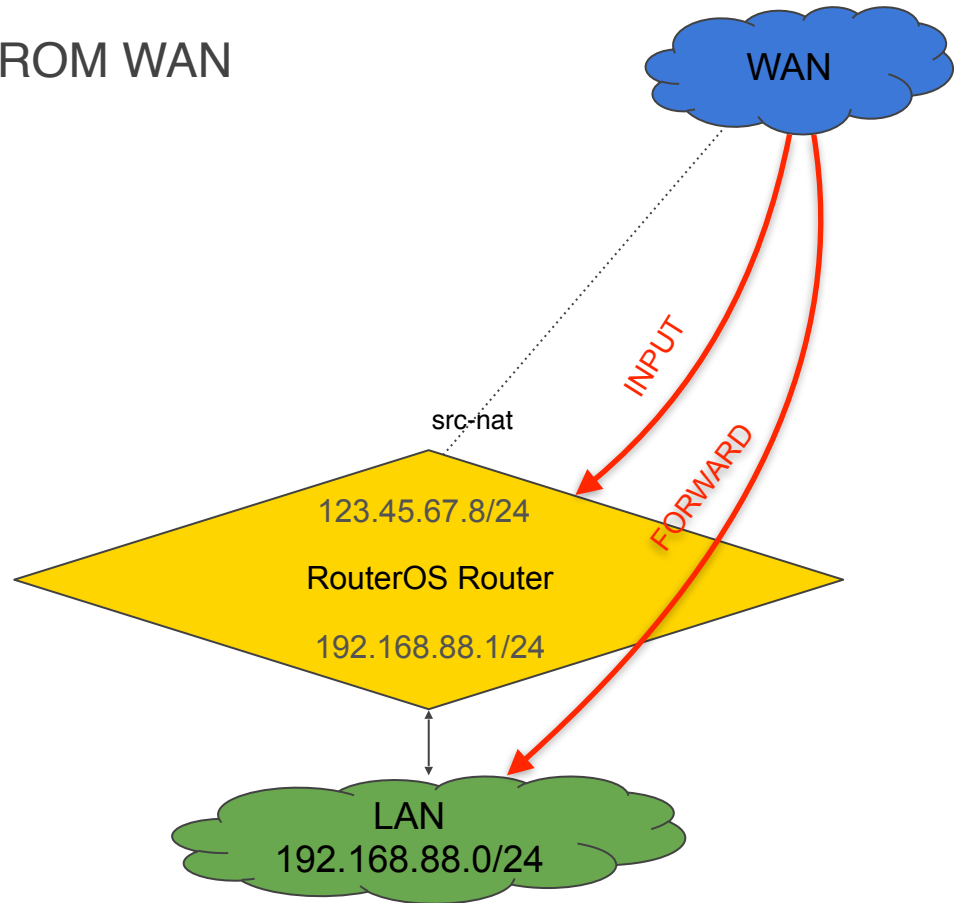
To RouterOS



# Default Firewall overview

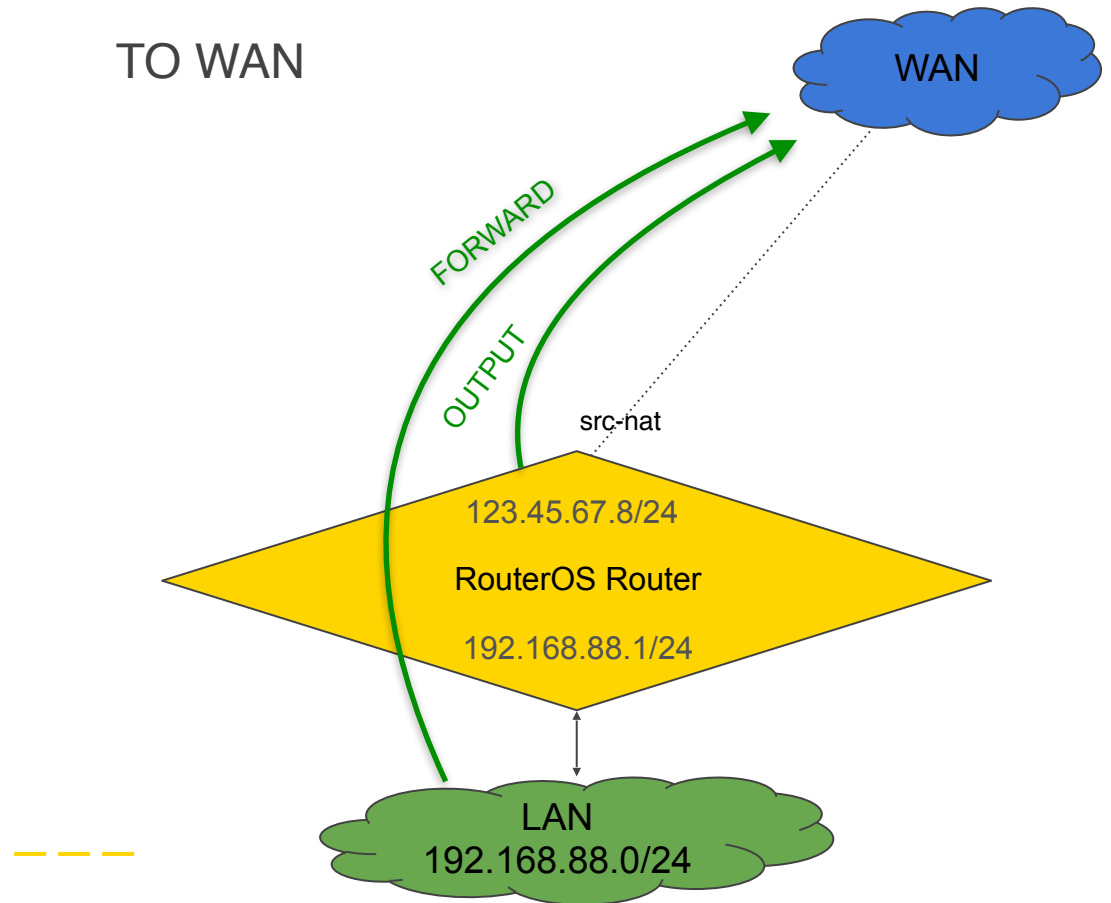
- a. From LAN
- b. To LAN
- c. From RouterOS
- d. To RouterOS
- e. **From WAN**
- f. To WAN

FROM WAN



# Default Firewall overview

- a. From LAN
- b. To LAN
- c. From RouterOS
- d. To RouterOS
- e. From WAN
- f. **To WAN**



# RouterOS 6.41+ default configuration firewall overview

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1 CPU: 1%

### Firewall

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

+ - [check] [x] [info] [filter] [00] Reset Counters [00] Reset All Counters Find

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
;;; special dummy rule to show fasttrack counters															
0	D	pas...	forward											124.1 MIB	211 598
;;; defconf: accept established,related,untracked															
1	✓ acc...	input												6.5 MIB	76 964
;;; defconf: drop invalid															
2	✗ drop	input												3145 B	34
;;; defconf: accept ICMP															
3	✓ acc...	input			1 (icmp)									0 B	0
;;; defconf: drop all not coming from LAN															
4	✗ drop	input							!LAN					33.5 KIB	133
;;; defconf: accept in ipsec policy															
5	✓ acc...	forward												0 B	0
;;; defconf: accept out ipsec policy															
6	✓ acc...	forward												0 B	0
;;; defconf: fasttrack															
7	▶ fas...	forward												6.2 MIB	42 281
;;; defconf: accept established,related, untracked															
8	✓ acc...	forward												6.2 MIB	42 281
;;; defconf: drop invalid															
9	✗ drop	forward												1076 B	23
;;; defconf: drop all from WAN not DSTNATED															
10	✗ drop	forward								WAN				0 B	0

11 items

outerOS WinBox

NETICA © 2017 / NETICA@GMAIL.COM



# Default configuration firewall: **INPUT** chain

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU:0%

**Interface List**

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
;;;	defconf								
LAN	bridge								
;;;	defconf								
WAN	ether1								

2 items

**Firewall**

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

Reset Counters Reset All Counters Find input

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
;;;	defconf:	accept	established,related,untracked												
1	✓ acc...	input												6.8 MB	79 640
;;;	defconf:	drop	invalid											3145 B	34
2	✗ drop	input													
;;;	defconf:	accept	ICMP											0 B	0
3	✓ acc...	input			1 (icmp)										
;;;	defconf:	drop	all not coming from LAN											34.1 KB	135
4	✗ drop	input													

4 items out of 11

## Short summary

1. **Accept ALL** input packets for **established** connections
2. **Accept ALL** input **ICMP** packets
3. **DROP ALL** input packets (except LAN)
4. **Allow everything else**

**DROP ALL !LAN** = **Accept** only LAN

# Default Firewall overview

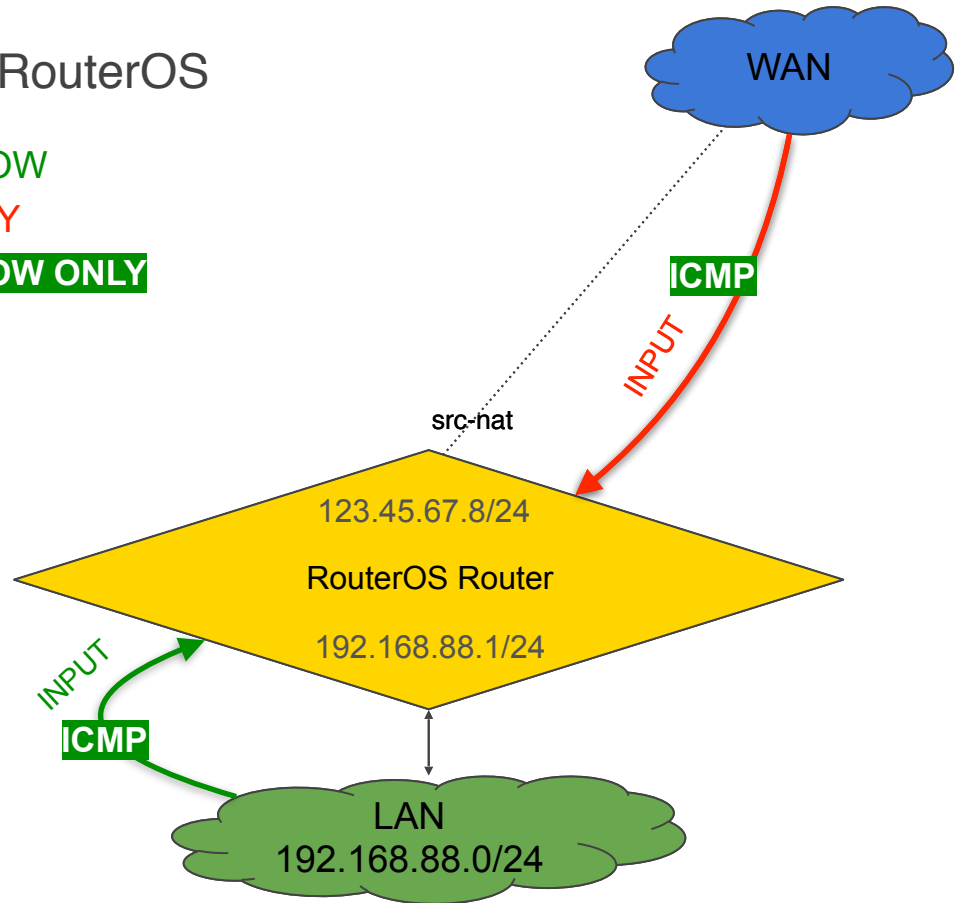
- From LAN
- To LAN
- From RouterOS
- To RouterOS**
- From WAN
- To WAN

TO RouterOS

ALLOW

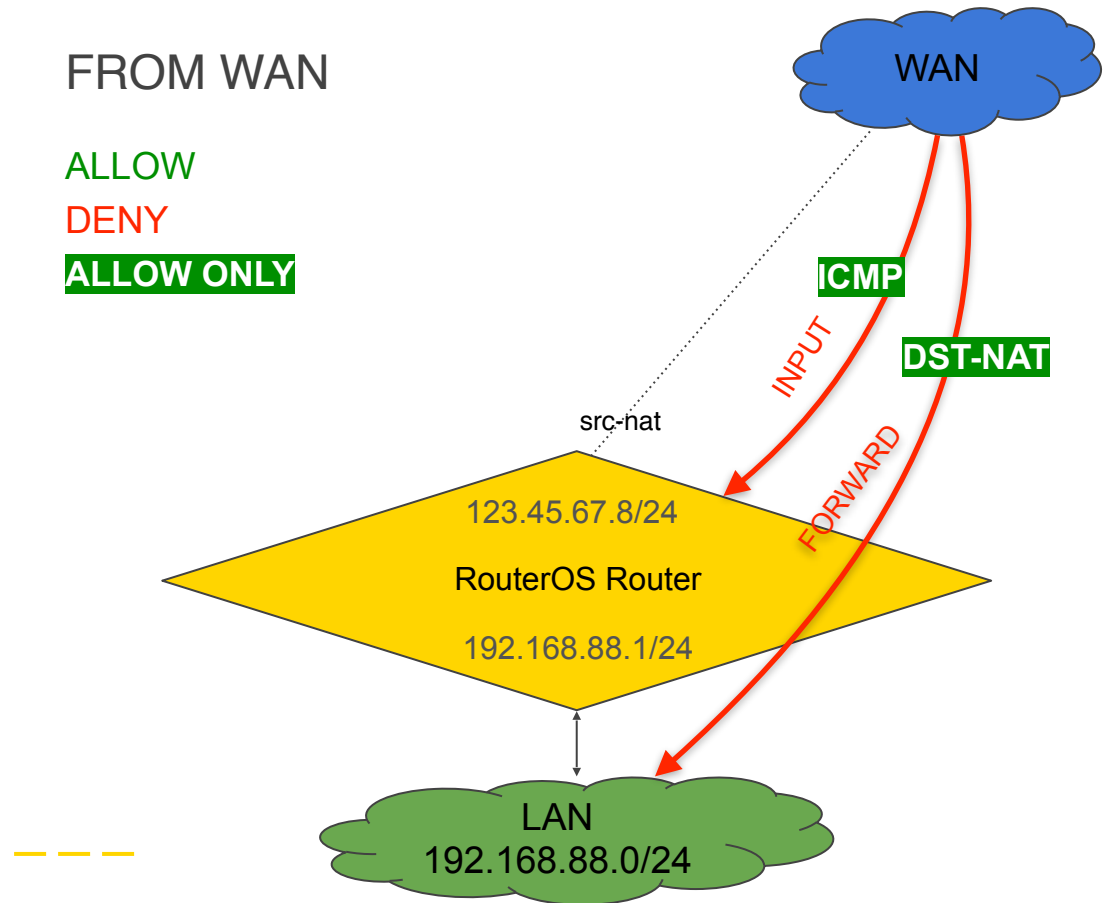
DENY

ALLOW ONLY



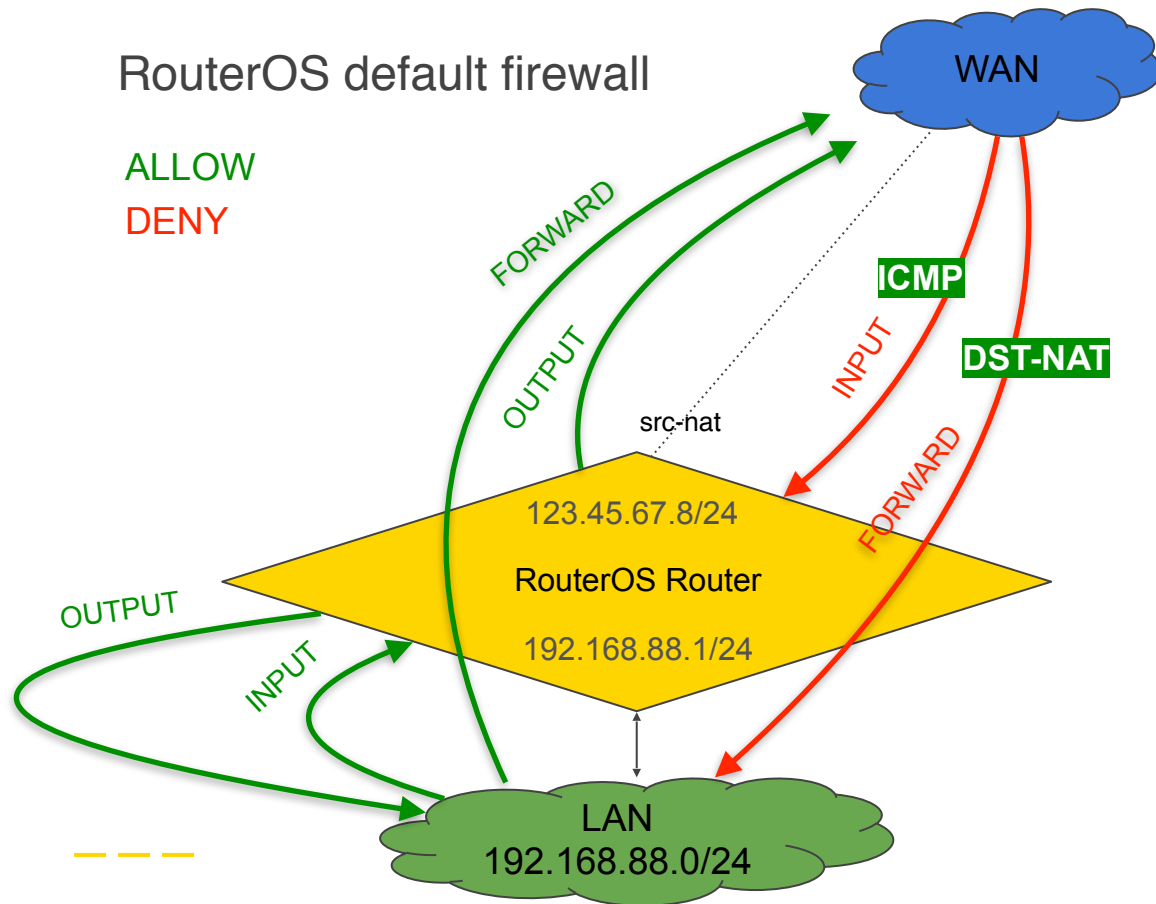
# Default Firewall overview

- a. From LAN
- b. To LAN
- c. From RouterOS
- d. To RouterOS
- e. **From WAN**
- f. To WAN



# Setting up Firewall

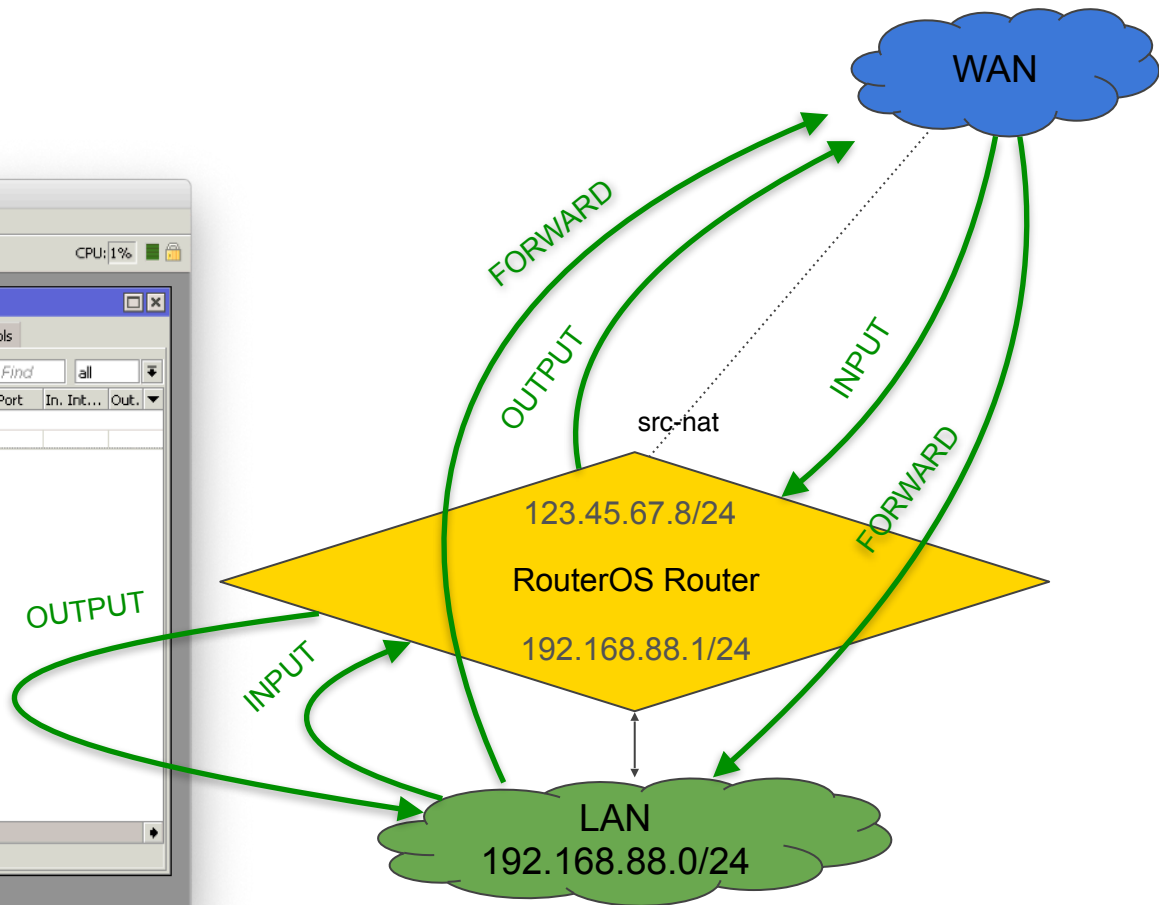
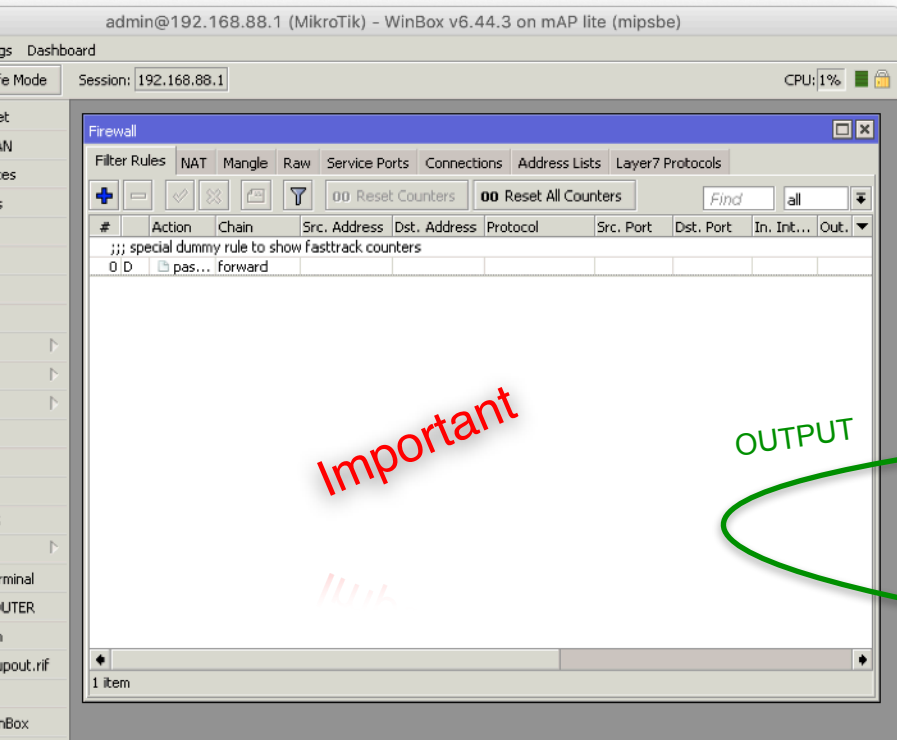
1. Default firewall overview
2. IPSec traffic rules
3. VPN traffic rules
4. Testing



# Empty FIREWALL

ALLOW

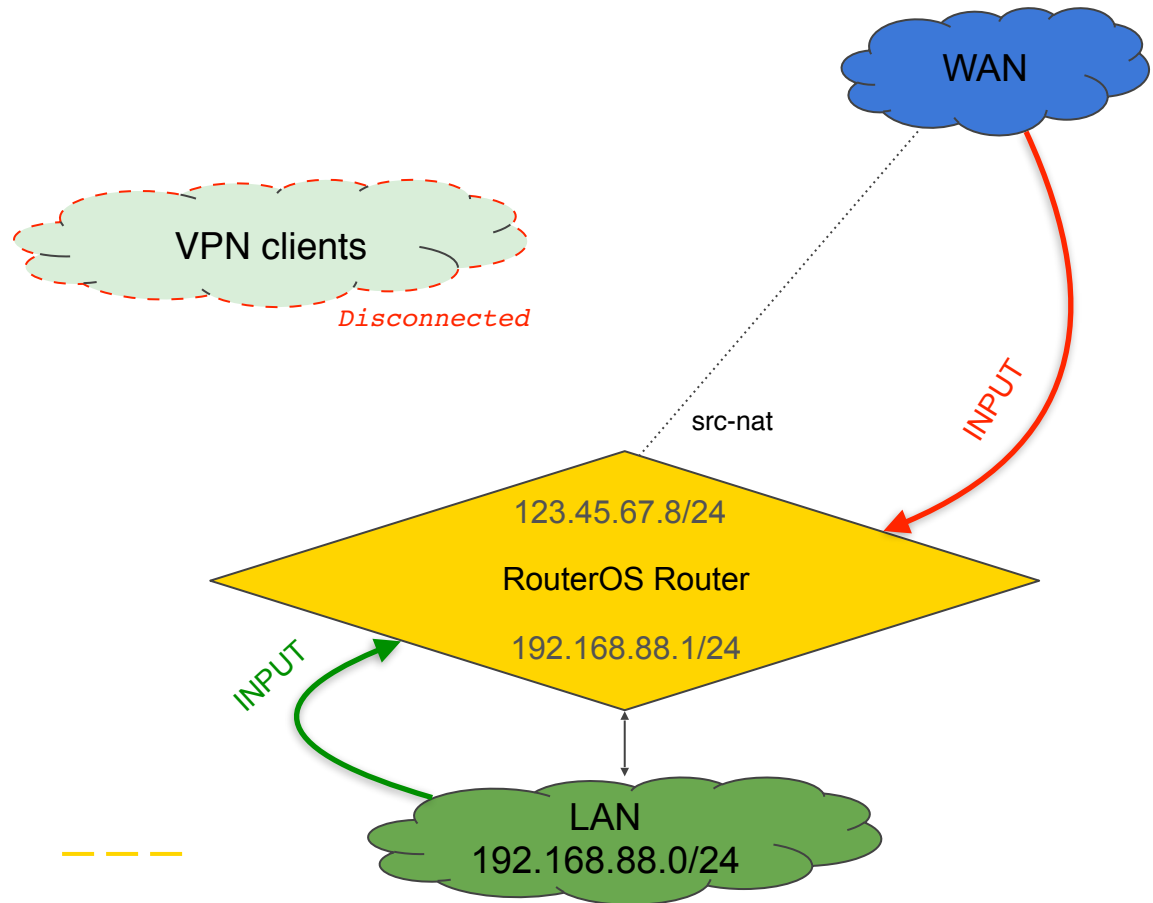
DENY



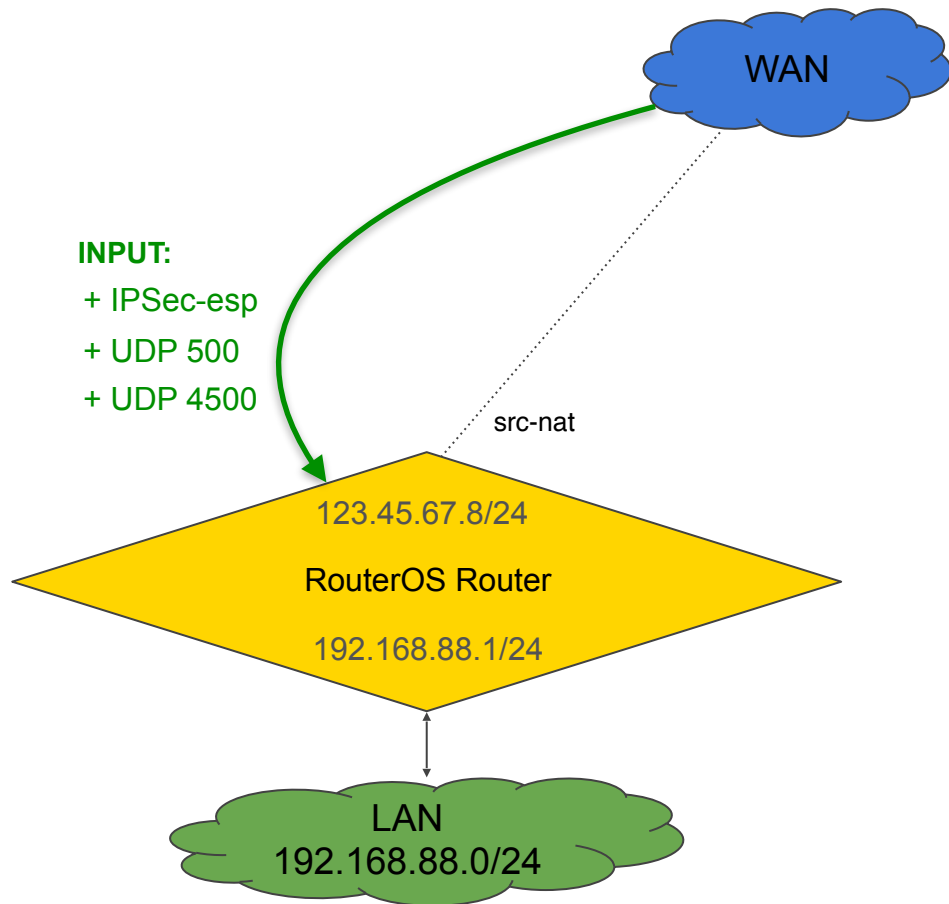
# Setting up Firewall

IPSec traffic rules

# IPSec traffic rules



# IPSec traffic rules





# Firewall filter rules for IPSec ike2 packets (defconf)

INPUT chain

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU: 0%

Firewall

Filter Rules NAT Mar

#	Action	Chain
1	acc...	input
2	drop	input
3	acc...	input
4	drop	input

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address: 123.45.67.8

Protocol: udp

Src. Port:

Dst. Port: 500,4500

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

Comment for New Firewall Rule

Allow UDP 500,4500 IPSec for 123.45.67.8

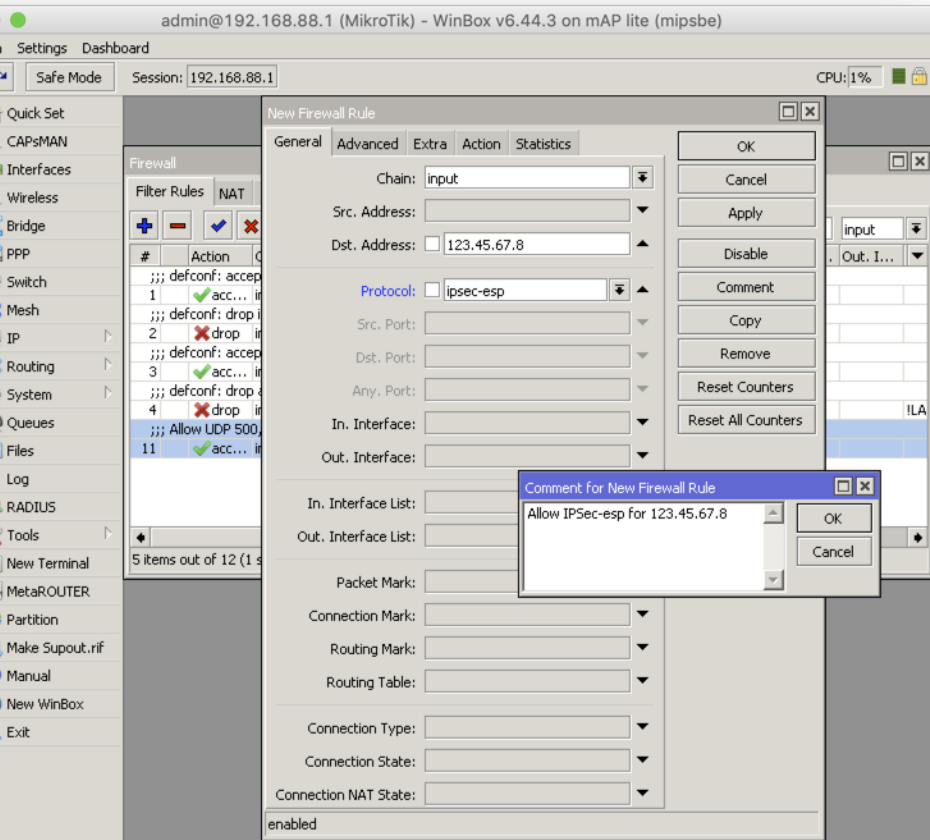
+ UDP 500  
+ UDP 4500

```
/ip firewall filter add place-  
before=[ find where comment~"defconf:  
drop all not coming from LAN" ]  
protocol=udp dst-port=500,4500 dst-  
address=123.45.67.8 action=accept  
chain=input comment="Allow UDP 500,4500  
IPSec for 123.45.67.8"
```



# Firewall filter rules for IPSec ike2 packets (defconf)

INPUT chain



+ IPSec-esp

```
/ip firewall filter add place-  
before=[ find where comment~"defconf:  
drop all not coming from LAN" ]  
protocol=ipsec-esp dst-  
address=123.45.67.8 action=accept  
chain=input comment="Allow IPSec-esp  
for 123.45.67.8"
```



# Firewall filter rules for IPSec ike2 packets (defconf)

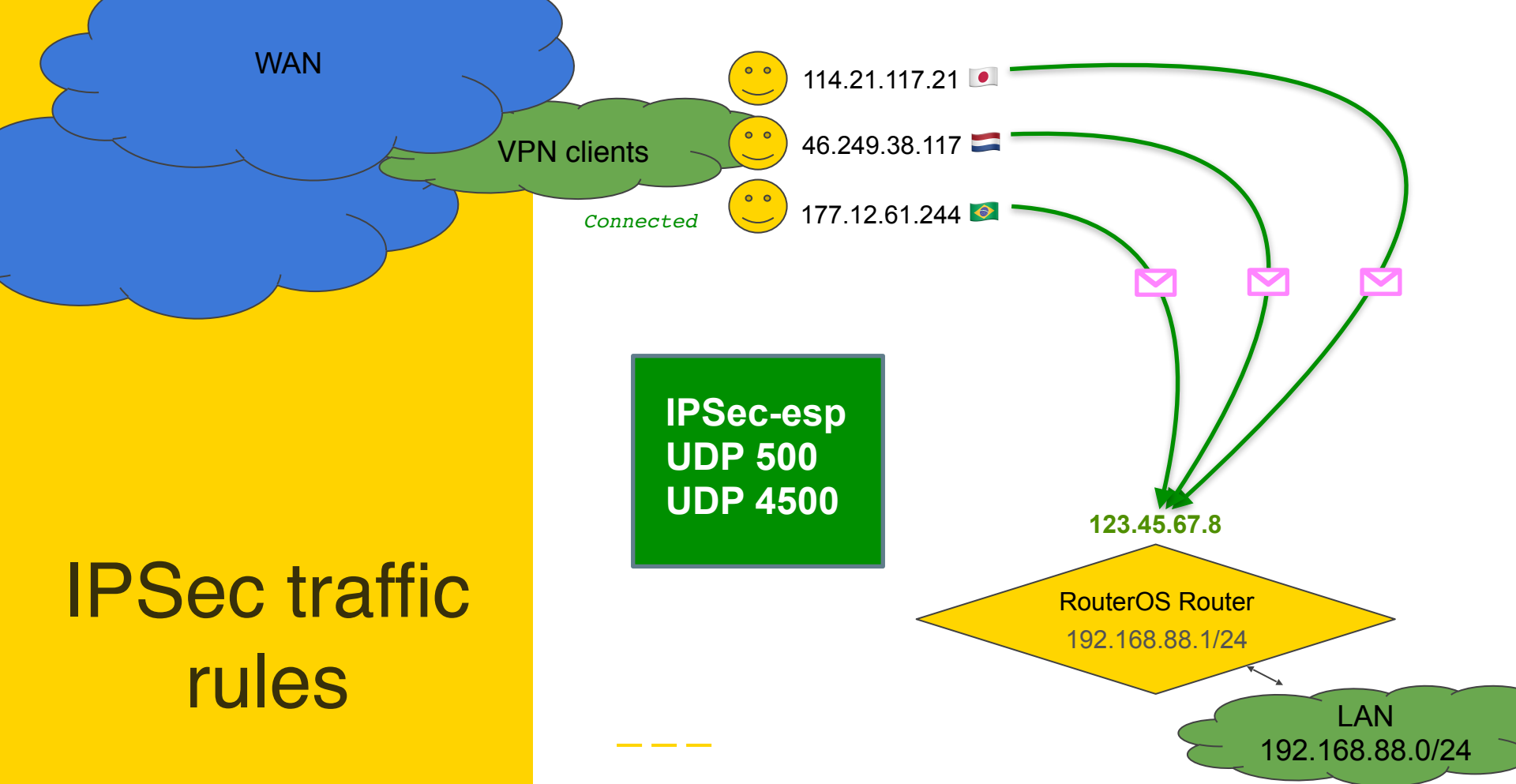
INPUT chain

Move **allow** rules before **drop**

The screenshot displays the Mikrotik WinBox interface with the Firewall Filter Rules configuration window open. The rules are listed in the following order:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...
;;; defconf: accept established,related,untracked									
1	✓ acc...	input							
;;; defconf: drop invalid									
2	✗ drop	input							
;;; defconf: accept ICMP									
3	✓ acc...	input			1 (icmp)				
;;; Allow UDP 500,4500 IPSec for 123.45.67.8									
4	✓ acc...	input	123.45.67.8	123.45.67.8	17 (udp)	500,4500			
;;; Allow IPSec-esp for 123.45.67.8									
5	✓ acc...	input	123.45.67.8	123.45.67.8	50 (ipsec-esp)				
;;; defconf: drop all not coming from LAN									
6	✗ drop	input							!LAN

A green arrow points to rule 11, which is highlighted in blue. The interface also shows a sidebar with various system tools and a top status bar indicating the session and CPU usage.



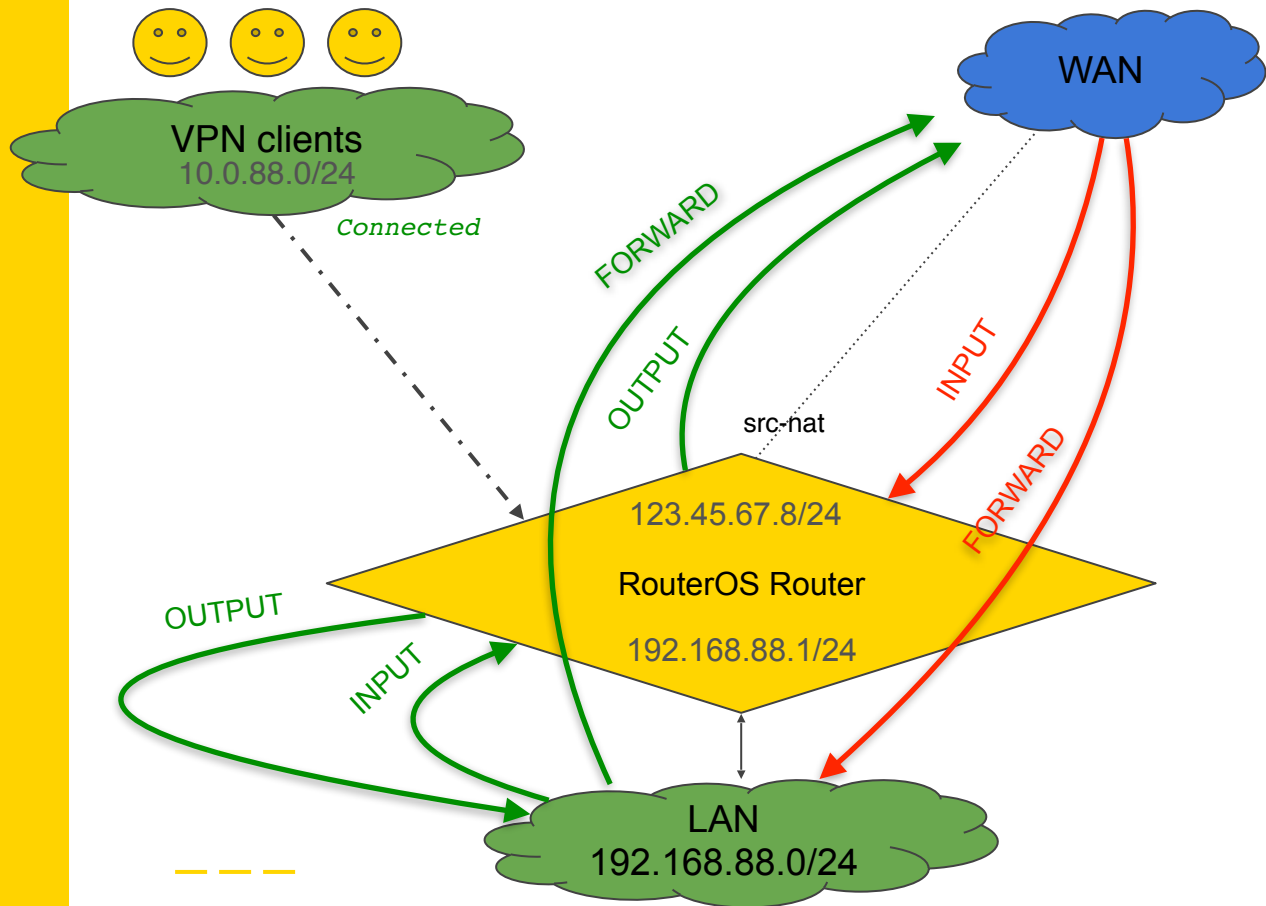
# IPSec traffic rules

# Setting up Firewall

VPN traffic rules

# Setting up Firewall

1. Default firewall overview
2. IPSec traffic rules
3. **VPN traffic rules**
4. Testing



# Default ipsec rules (defconf)

FORWARD chain

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU:0%

Firewall

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

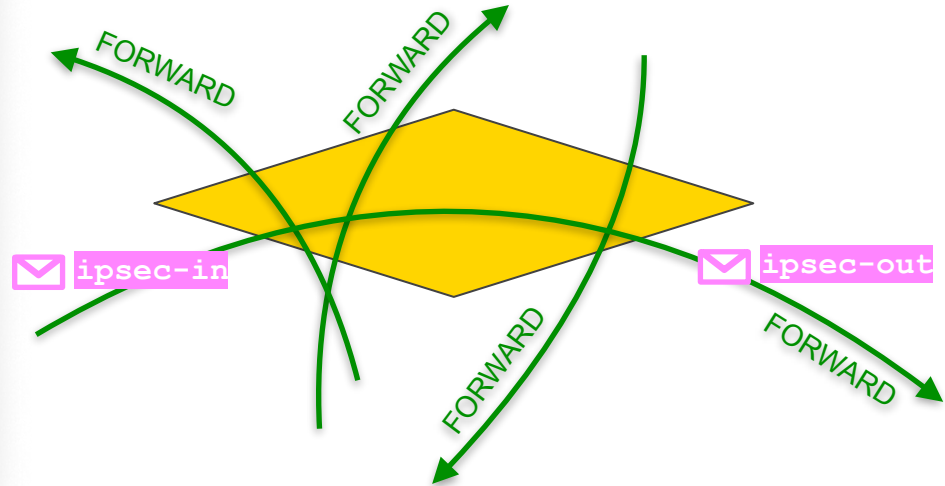
00 Reset Counters 00 Reset All Counters Find forward

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out.
;;; special dummy rule to show fasttrack counters									
0	D	pas...							forward
;;; defconf: accept in ipsec policy									
7	✓ acc...	forward							
;;; defconf: accept out ipsec policy									
8	✓ acc...	forward							
;;; defconf: fasttrack									
9	fas...	forward							
;;; defconf: accept established,related, untracked									
10	✓ acc...	forward							
;;; defconf: drop invalid									
11	✗ drop	forward							
;;; defconf: drop all from WAN not DSTNATed									
12	✗ drop	forward							

7 items out of 13 (2 selected)

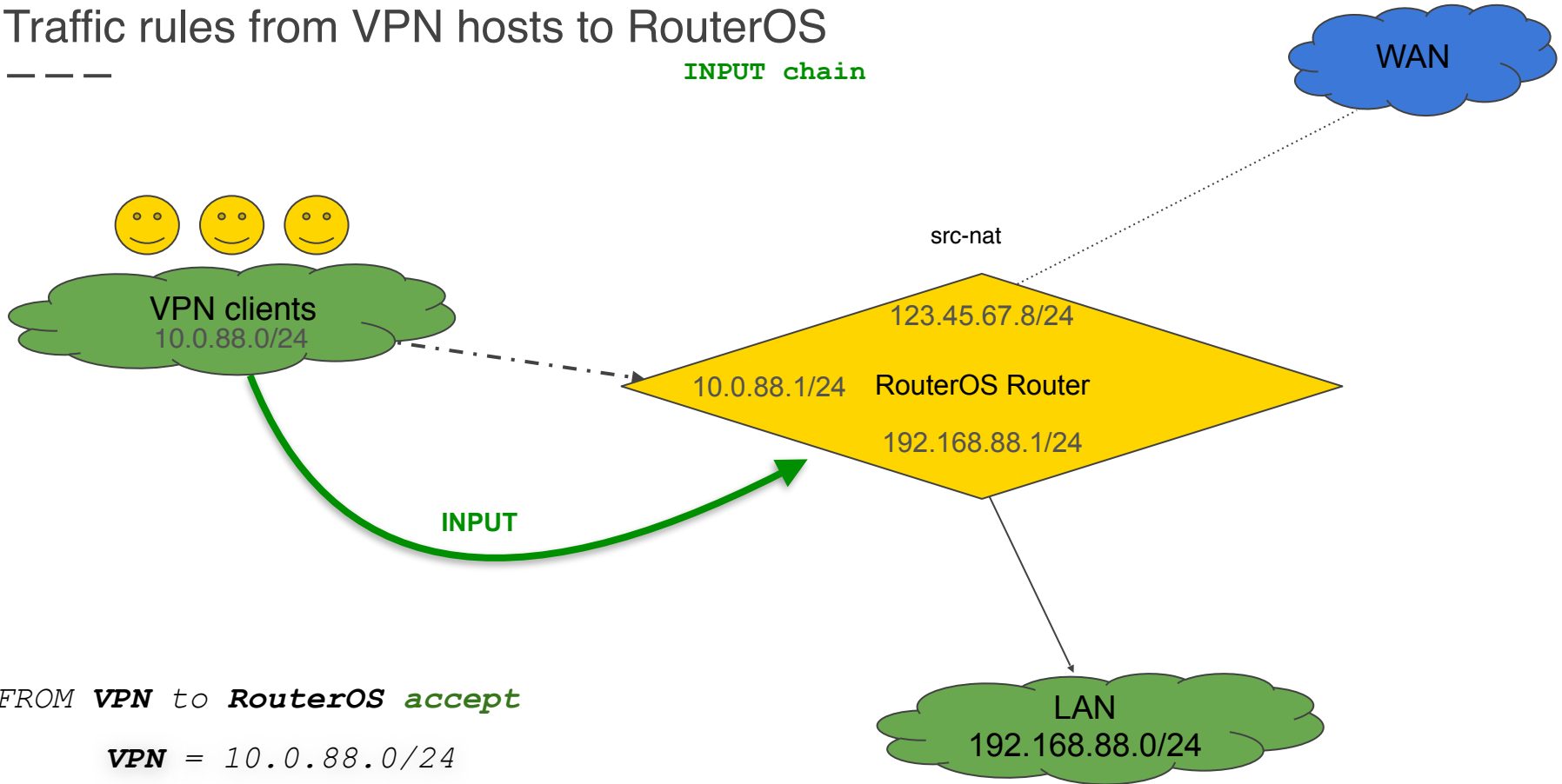
FROM ANY to ANY ipsec-in accept

FROM ANY to ANY ipsec-out accept



# Traffic rules from VPN hosts to RouterOS

INPUT chain



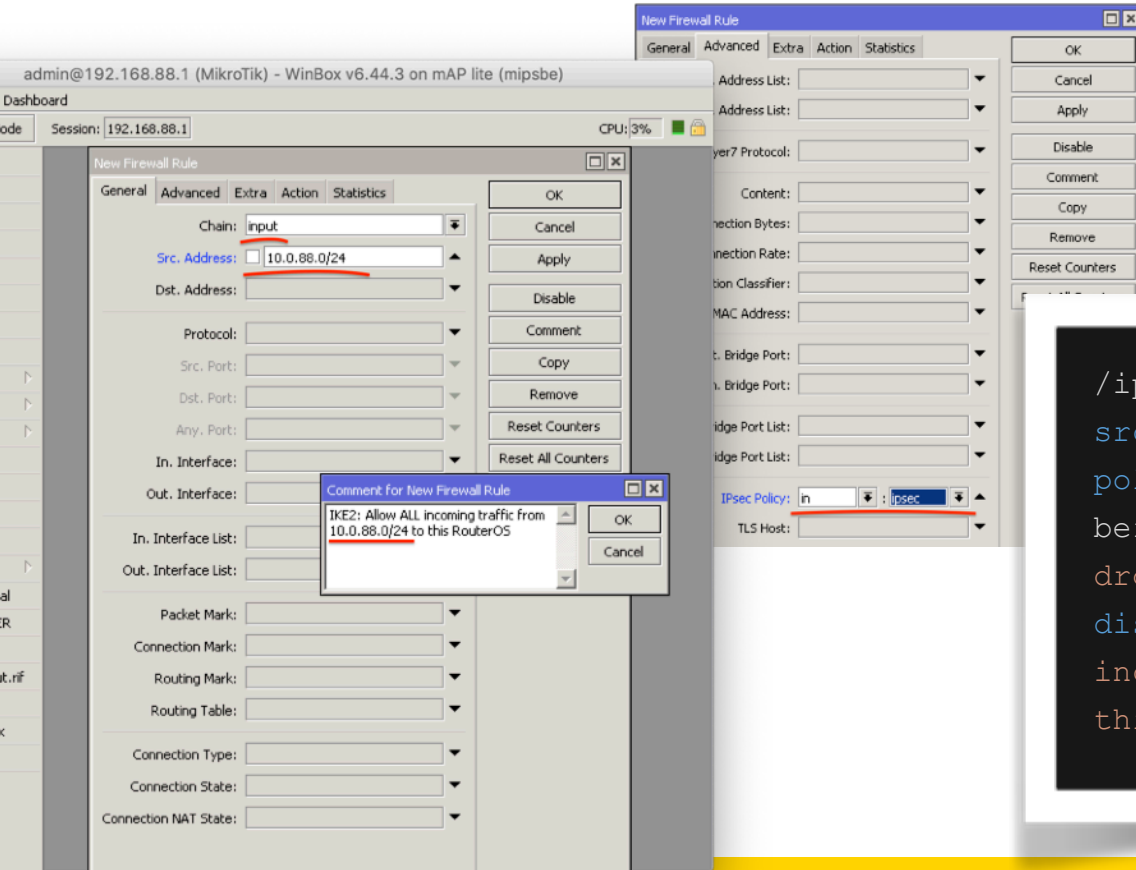
FROM **VPN** to **RouterOS** **accept**

**VPN** = 10.0.88.0/24



# Traffic rules from VPN hosts to RouterOS

INPUT chain



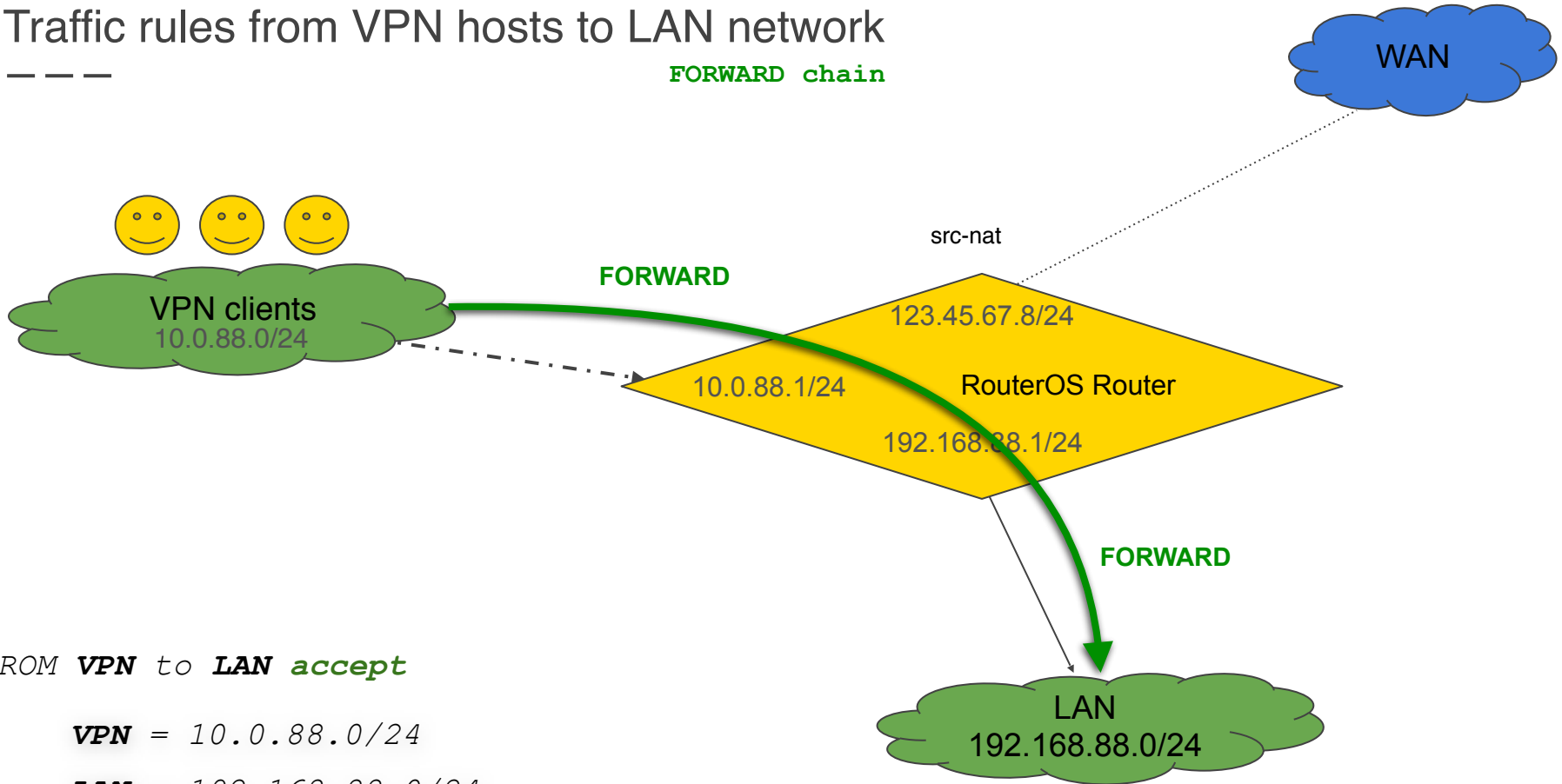
FROM VPN to RouterOS accept

VPN = 10.0.88.0/24

```
/ip firewall filter add chain=input
src-address=10.0.88.0/24 ipsec-
policy=in,ipsec action=accept place-
before=[ find where comment~"defconf:
drop all not coming from LAN" ]
disabled=no comment="IKE2: Allow ALL
incoming traffic from 10.0.88.0/24 to
this RouterOS"
```

# Traffic rules from VPN hosts to LAN network

FORWARD chain



FROM **VPN** to **LAN** *accept*

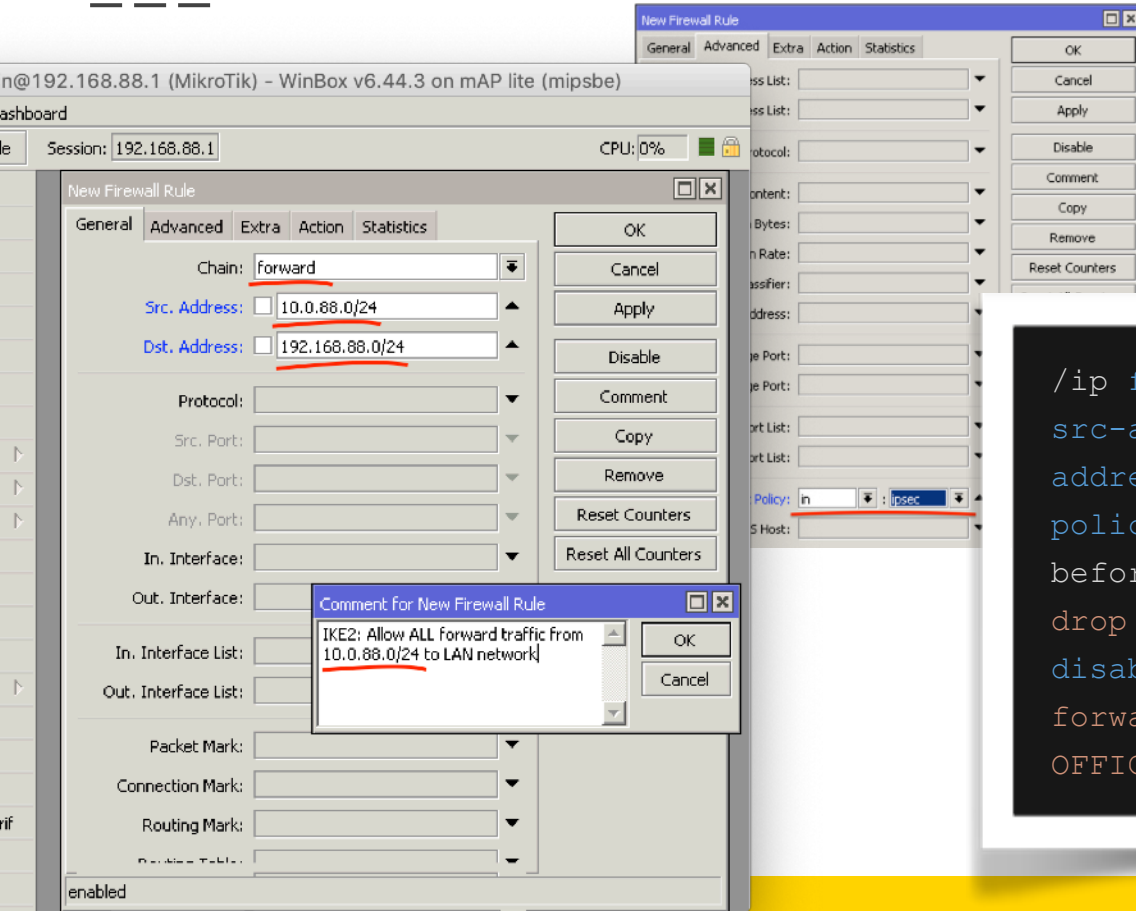
**VPN** = 10.0.88.0/24

**LAN** = 192.168.88.0/24



# Traffic rules from VPN hosts to LAN network

FORWARD chain



FROM VPN to LAN accept

VPN = 10.0.88.0/24

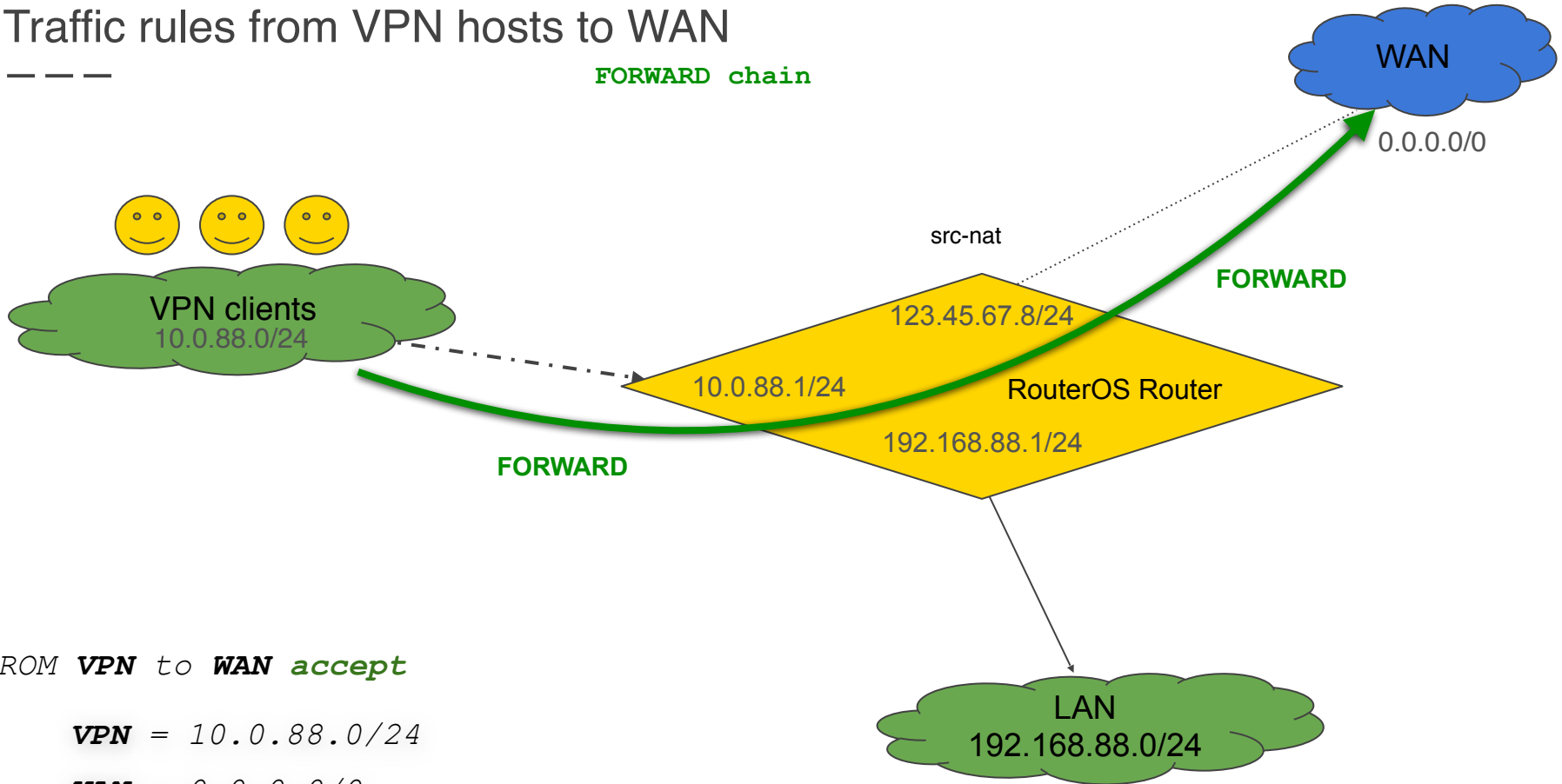
LAN = 192.168.88.0/24

```
/ip firewall filter add chain=forward  
src-address=10.0.88.0/24 dst-  
address=192.168.88.0/24 ipsec-  
policy=in,ipsec action=accept place-  
before=[ find where comment~"defconf:  
drop all from WAN not DSTNATED" ]  
disabled=no comment="IKE2: Allow ALL  
forward traffic from 10.0.88.0/24 to  
OFFICE network"
```

# Traffic rules from VPN hosts to WAN

---

FORWARD chain



FROM **VPN** to **WAN** *accept*

**VPN** = 10.0.88.0/24

**WAN** = 0.0.0.0/0

# Traffic rules from VPN hosts to WAN

FORWARD chain

min@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)  
Dashboard  
Mode: Session: 192.168.88.1 CPU: 14%

**New Firewall Rule**

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address: 10.0.88.0/24

Dst. Address: 0.0.0.0/0

Protocol: [ ]

Src. Port: [ ]

Dst. Port: [ ]

Any. Port: [ ]

In. Interface: [ ]

Out. Interface: [ ]

In. Interface List: [ ]

Out. Interface List: [ ]

Packet Mark: [ ]

Connection Mark: [ ]

Routing Mark: [ ]

Enabled

**Comment for New Firewall Rule**

IKE2: Allow ALL forward traffic from 10.0.88.0/24 to ANY network

Policy: in : ipsec

FROM **VPN** to **WAN** *accept*

**VPN** = 10.0.88.0/24

**WAN** = 0.0.0.0/0

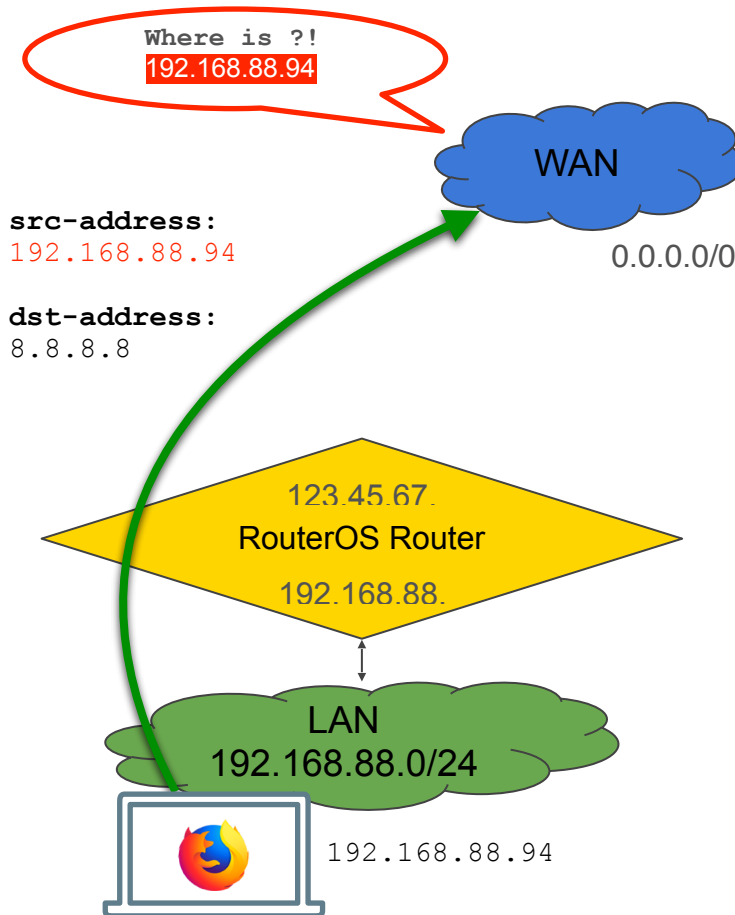
```
/ip firewall filter add chain=forward  
src-address=10.0.88.0/24 dst-  
address=0.0.0.0/0 ipsec-policy=in,ipsec  
action=accept place-before=[ find where  
comment~"defconf: drop all from WAN  
not DSTNATED" ] disabled=no  
comment="IKE2: Allow ALL forward  
traffic from 10.0.88.0/24 to ANY  
network"
```

# Setting up NAT

# Setting up NAT

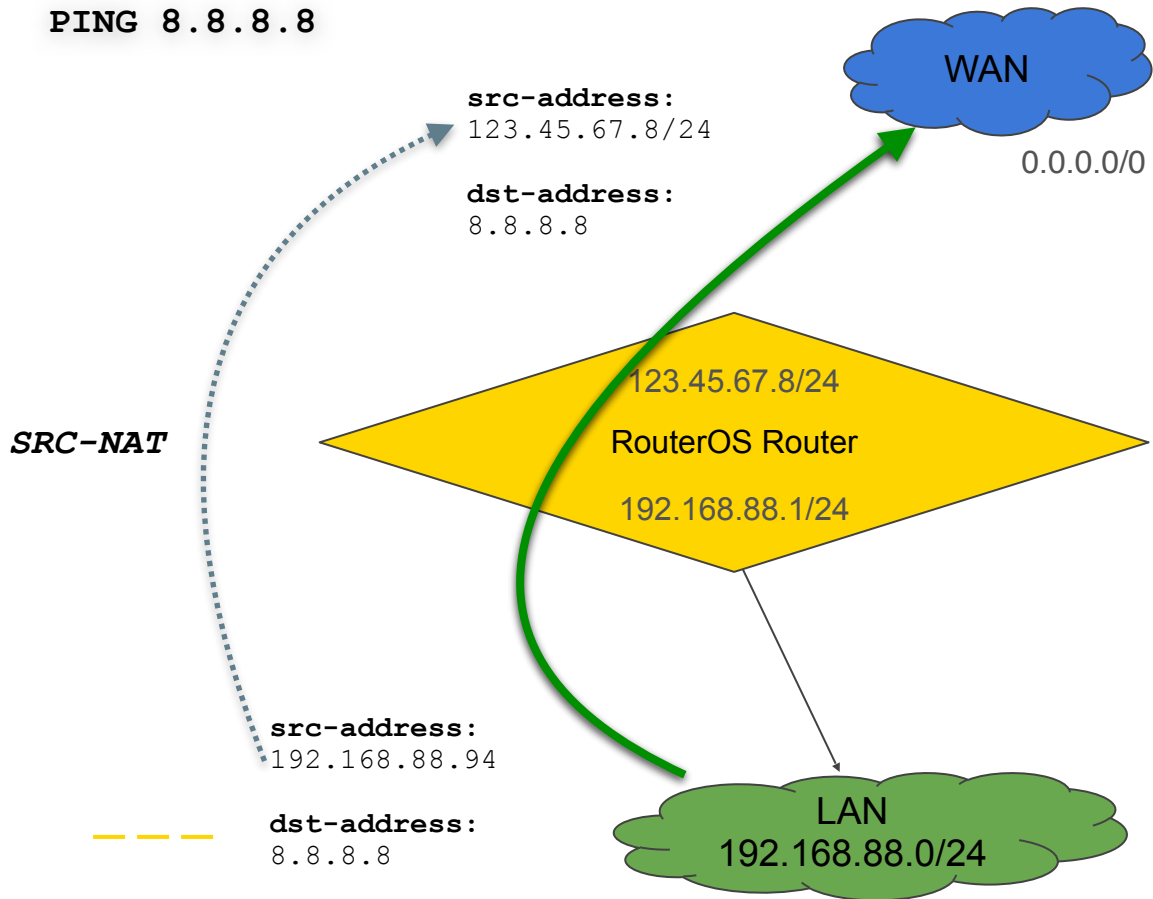
1. Default src-nat overview
2. SRC-NAT VPN traffic to WAN

PING 8.8.8.8



# Setting up NAT

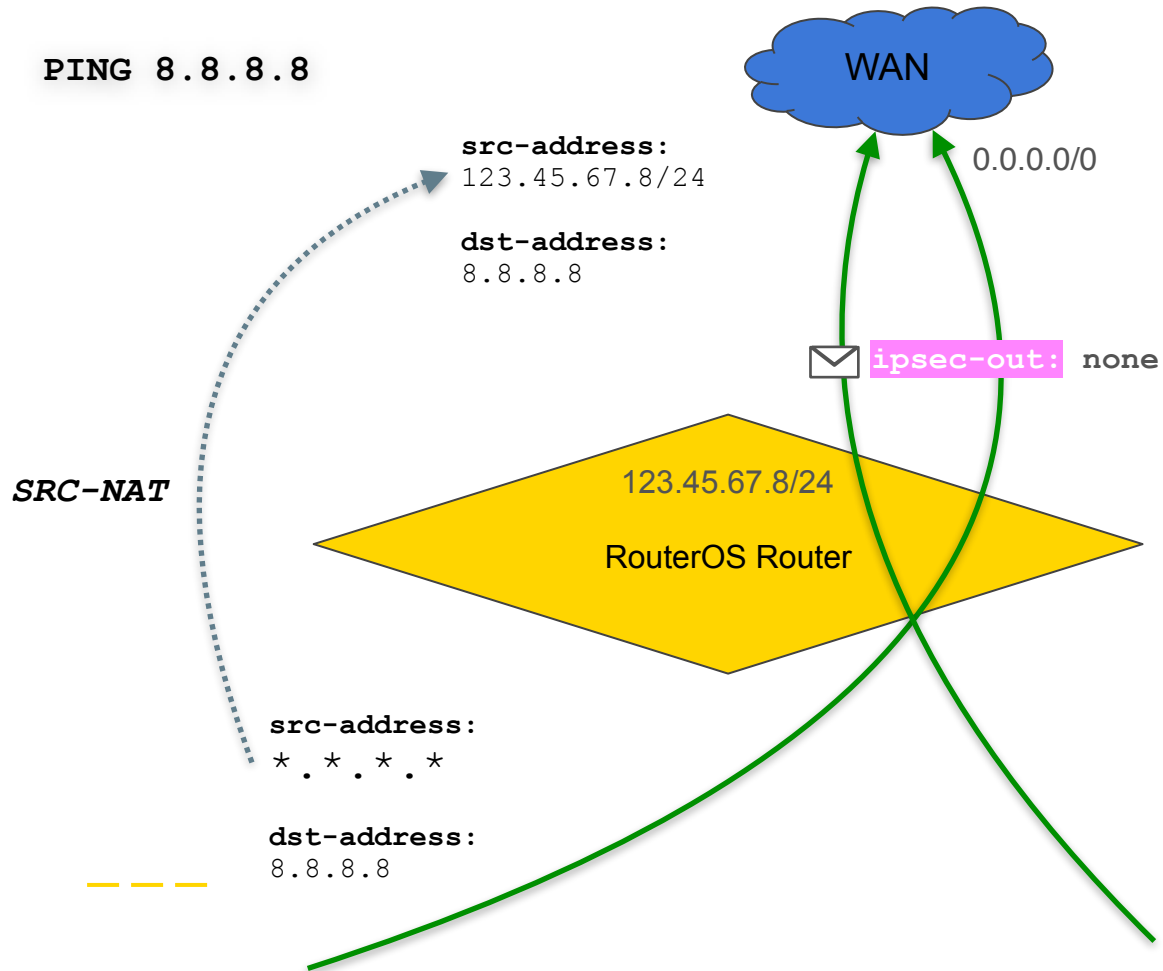
1. Default src-nat overview
2. SRC-NAT VPN traffic to WAN





# Setting up NAT

1. Default src-nat overview
2. SRC-NAT VPN traffic to WAN



# Masquerade non-IPSec WAN traffic (defconf)

— — —

The screenshot displays the Mikrotik WinBox interface for configuring a NAT Rule. The main window shows the 'General' tab with the following settings:

- Chain: srcnat
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)
- Out. Interface: (empty)
- In. Interface List: (empty)
- Out. Interface List:  WAN
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Routing Table: (empty)

The 'Out. Interface List' field is highlighted with a red underline. The 'WAN' option is also highlighted with a red underline. The 'enabled' checkbox at the bottom is checked.

An inset window titled 'NAT Rule <>' shows the 'Advanced' tab with the following settings:

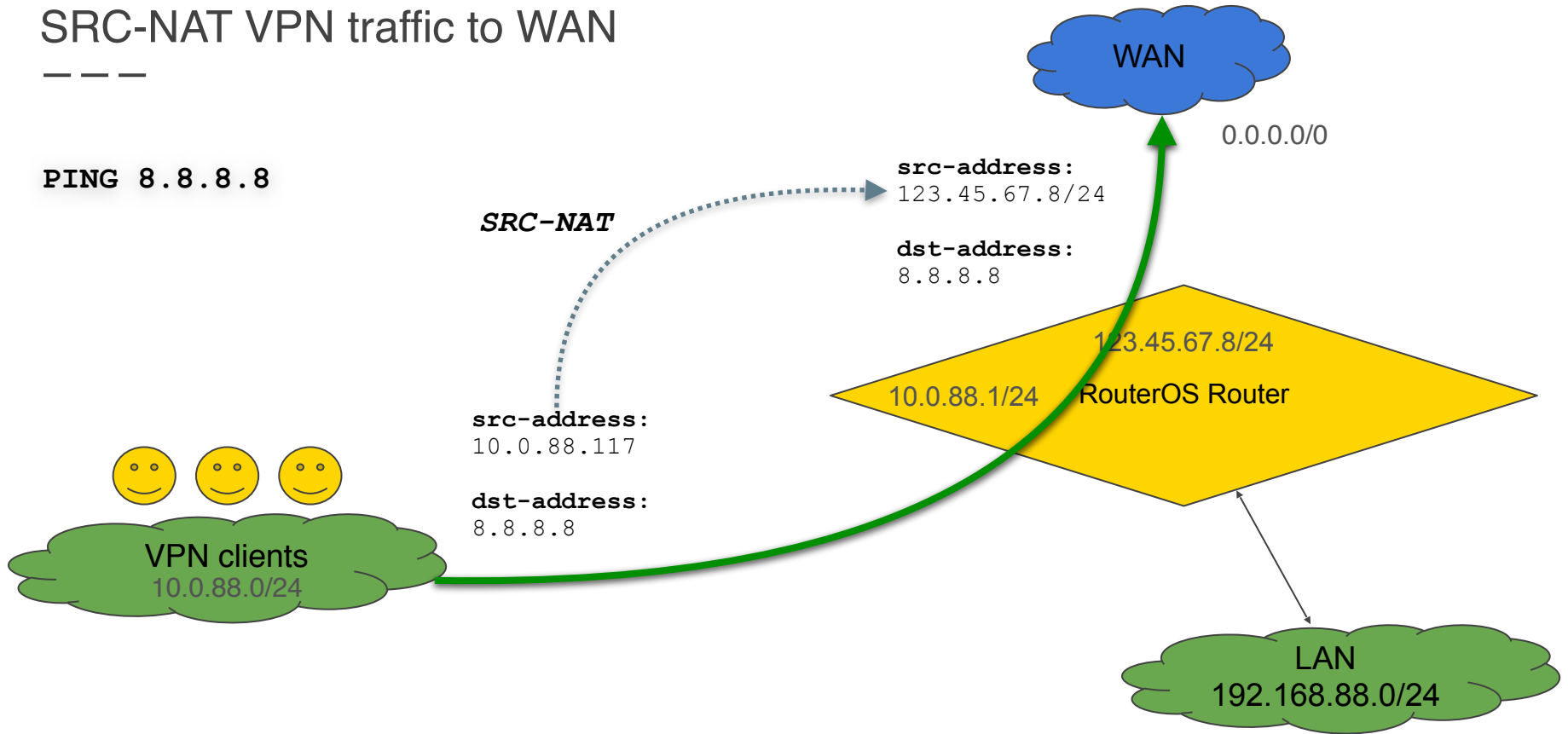
- Src. Address List: (empty)
- Dst. Address List: (empty)
- Layer7 Protocol: (empty)
- Content: (empty)
- Connection Bytes: (empty)
- Connection Rate: (empty)
- Per Connection Classifier: (empty)
- Src. MAC Address: (empty)
- Out. Bridge Port: (empty)
- In. Bridge Port: (empty)
- In. Bridge Port List: (empty)
- Out. Bridge Port List: (empty)
- IPsec Policy: out : none
- TLS Host: (empty)

The 'IPsec Policy' field is highlighted with a red underline. The 'out' and 'none' options are also highlighted with a red underline. The 'enabled' checkbox at the bottom is checked.

Below the inset window, there is a text box containing an envelope icon followed by the text: `ipsec-out: none`.

# SRC-NAT VPN traffic to WAN

PING 8.8.8.8



# Masquerade VPN traffic

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU: 2%

**New NAT Rule**

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address:  10.0.88.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:  WAN

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

**New NAT Rule**

General | Advanced | Extra | Action | Statistics

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

Ipssec Policy: out : none

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

**New NAT Rule**

General | Advanced | Extra | Action | Statistics

Action: masquerade

Log

Log Prefix:

To Ports:

```
/ip firewall nat add place-before=0
chain=srcnat src-address=10.0.88.0/24
out-interface-list=WAN ipsec-
policy=out,none action=masquerade
comment="MSQRD IKE2:10.0.88.0/24 -->
WAN traffic"
```

# SRC-NAT VPN traffic (recommended) 🍌

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU: 0%

### New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address: 10.0.88.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

**Out. Interface: ether1**

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Comment For New NAT Rule

SRC-NAT IKE2:10.0.88.0/24 --> ether1 traffic

OK

Cancel

### New NAT Rule

General | Advanced | Extra | Action | Statistics

**Action: src-nat**

Log

Log Prefix:

**To Addresses: 123.45.67.8**

To Ports:

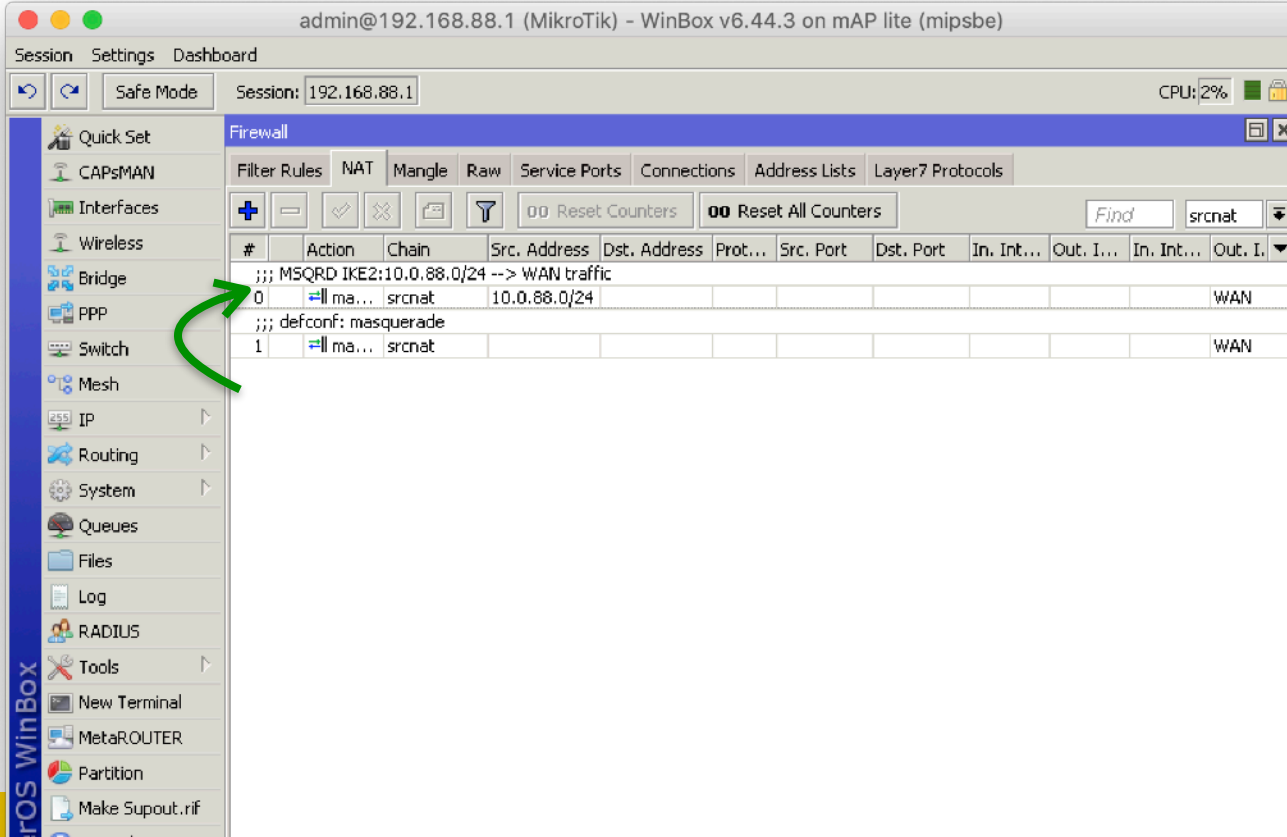
Reset Counters

Reset All Counters

```
/ip firewall nat add place-before=0
chain=srcnat src-address=10.0.88.0/24
out-interface=ether1 ipsec-
policy=out,none action=src-nat to-
addresses=123.45.67.8 comment="SRC-NAT
IKE2:10.0.88.0/24 --> ether1 traffic"
```

# Place SRC-NAT or MSQRD NAT rules on top

---



The screenshot shows the Mikrotik WinBox interface for configuring Firewall NAT rules. The window title is "admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)". The "NAT" tab is selected, and the "Filter Rules" sub-tab is active. The "Find" field contains "srcnat". The table below shows the NAT rules:

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...
;;; MSQRD IKE2:10.0.88.0/24 --> WAN traffic											
0	masquerade	srcnat	10.0.88.0/24								WAN
;;; defconf: masquerade											
1	masquerade	srcnat									WAN

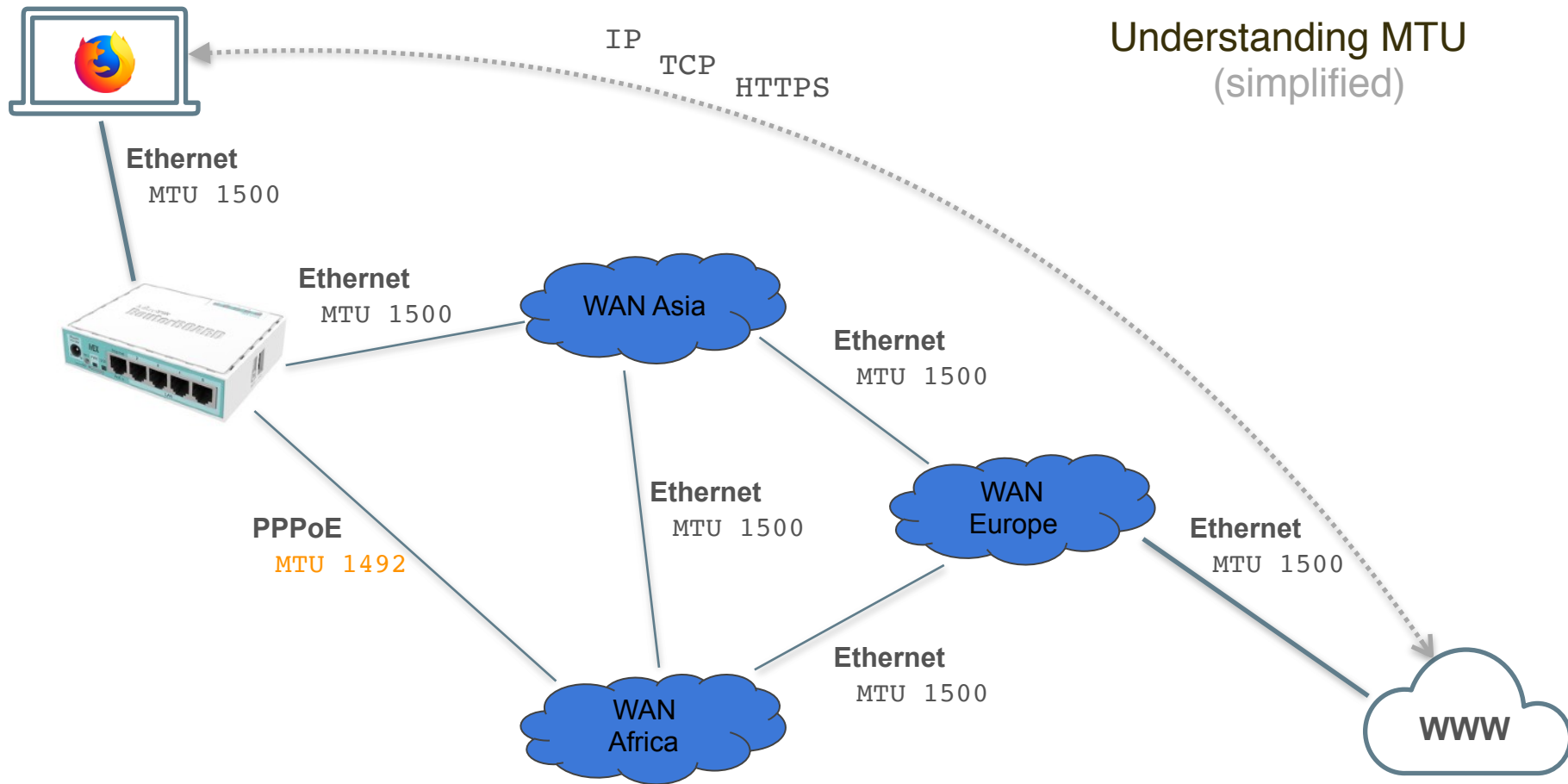
# Setting up TCP MSS

## Agenda for next slides

1. Understanding MTU and IP fragmentation
2. Understanding IPsec MTU
3. Understanding TCP MSS
4. Setting up TCP MSS over IKE2

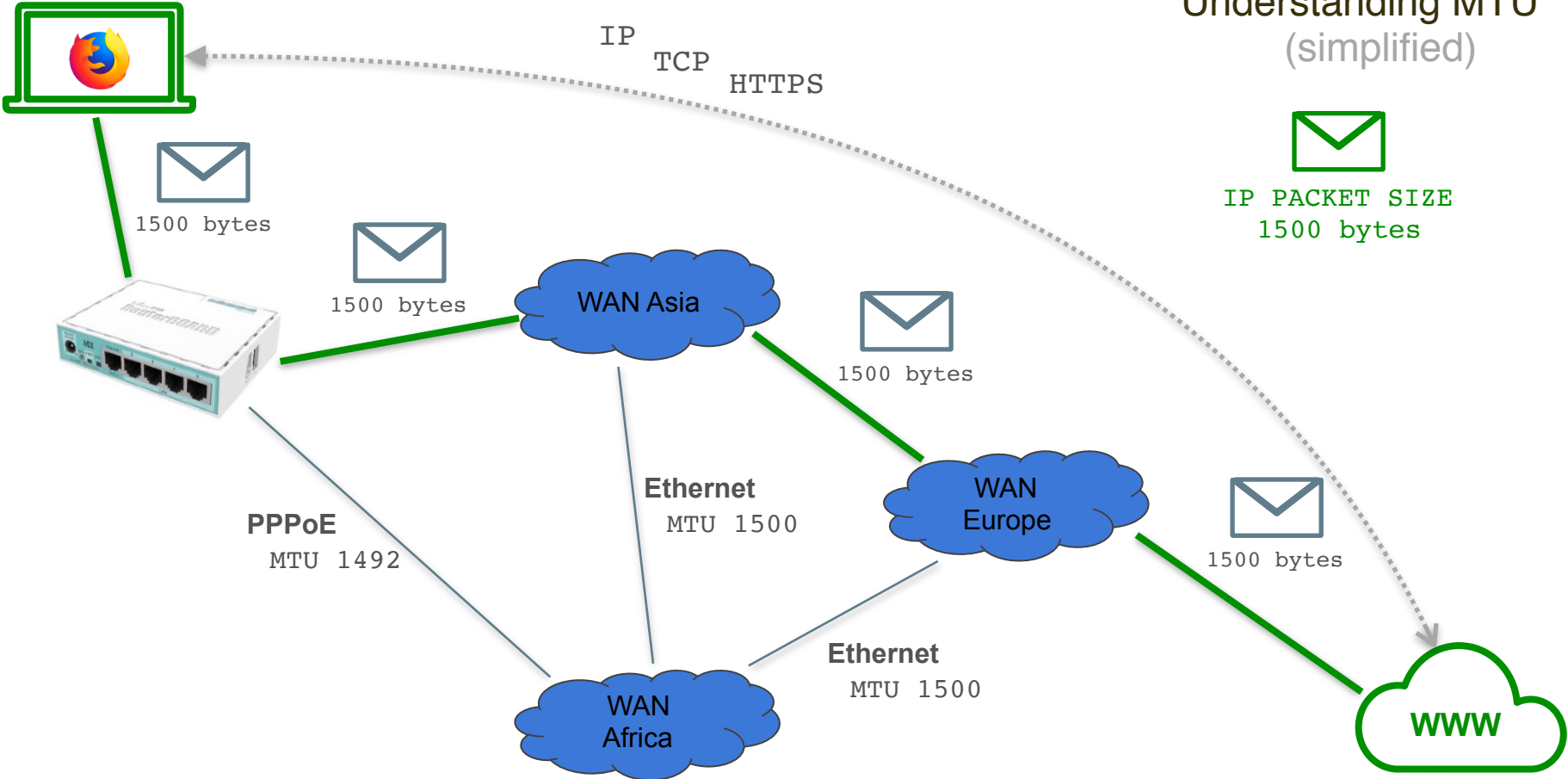


# Understanding MTU (simplified)

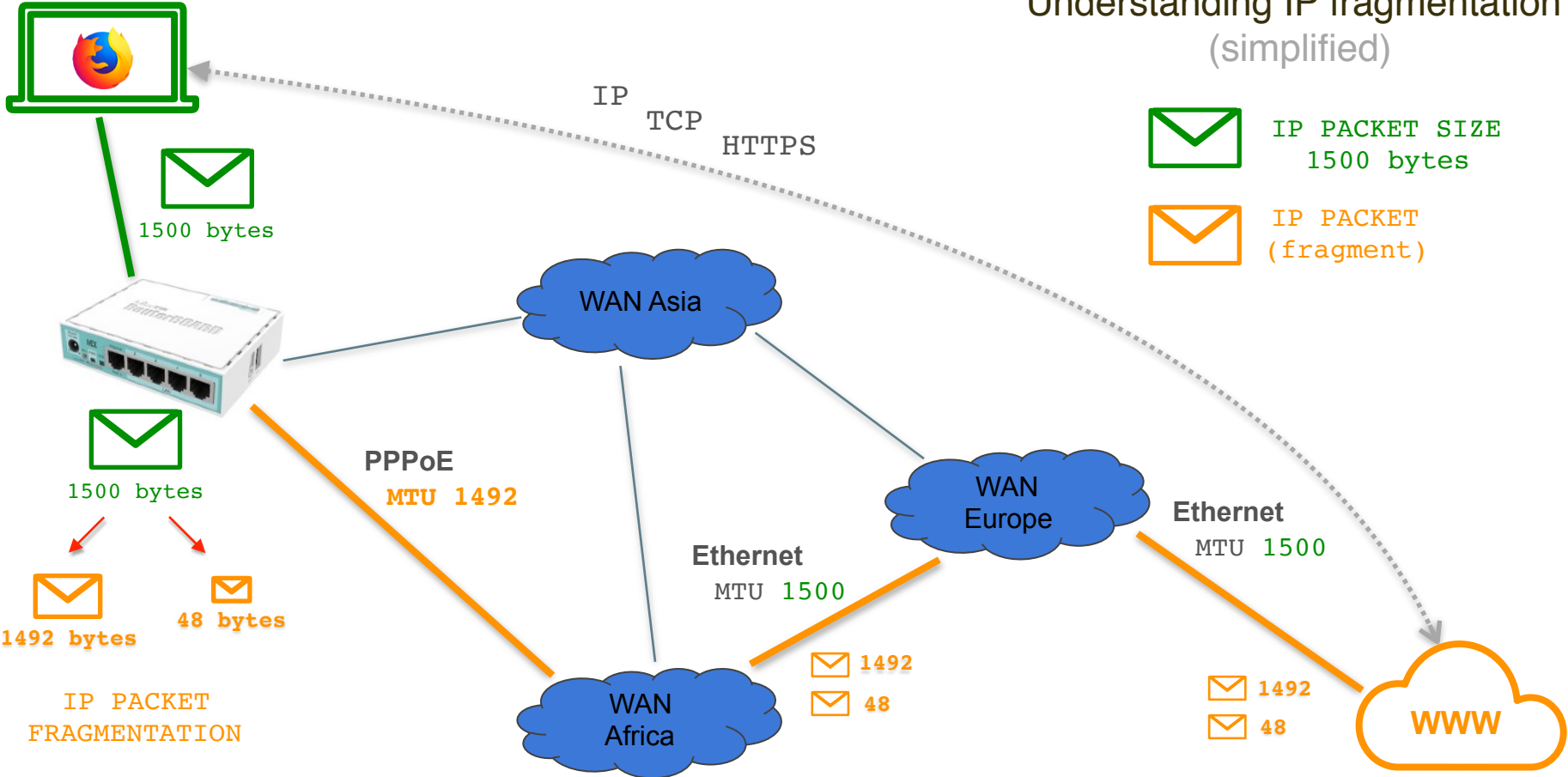




# Understanding MTU (simplified)



# Understanding IP fragmentation (simplified)



# MTU mismatch → IP fragmentation



1500



Ethernet  
MTU 1500



1500



PPPoE  
MTU 1492



1492 bytes



48 bytes



Ethernet  
MTU 1500



1492 bytes



48 bytes



IPSec tunnel  
MTU 1400



1400 bytes



48 bytes

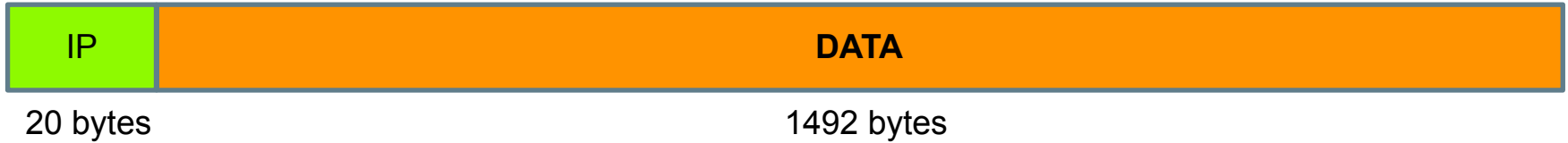


132 bytes

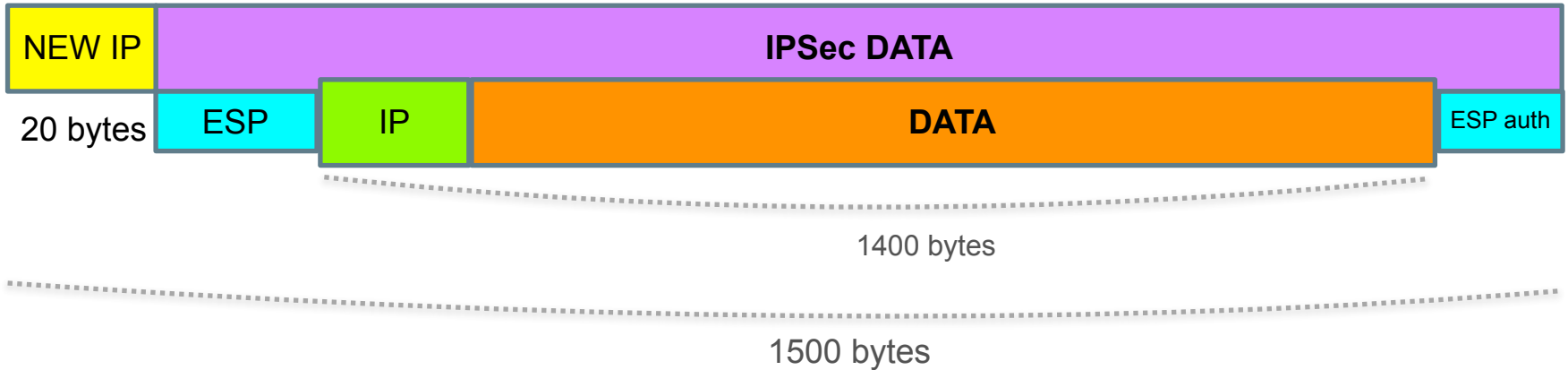


# Understanding IPSec MTU (simplified)

## IP packet

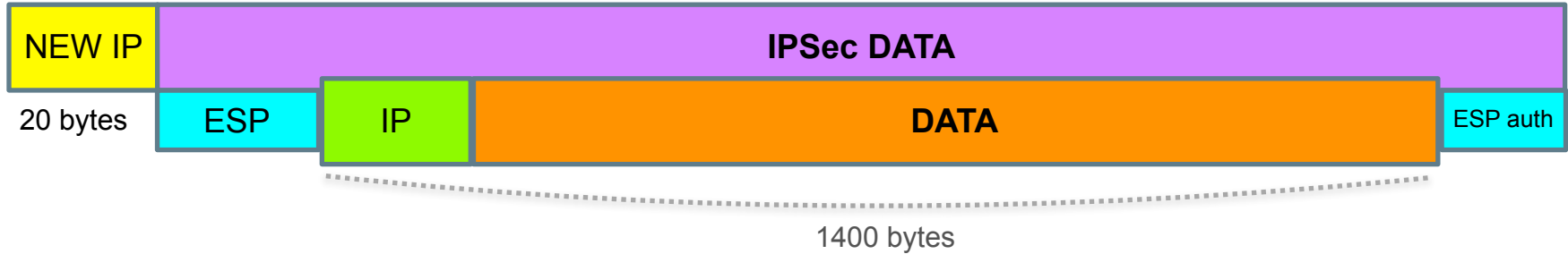


## IPSec ESP packet (tunnel mode)

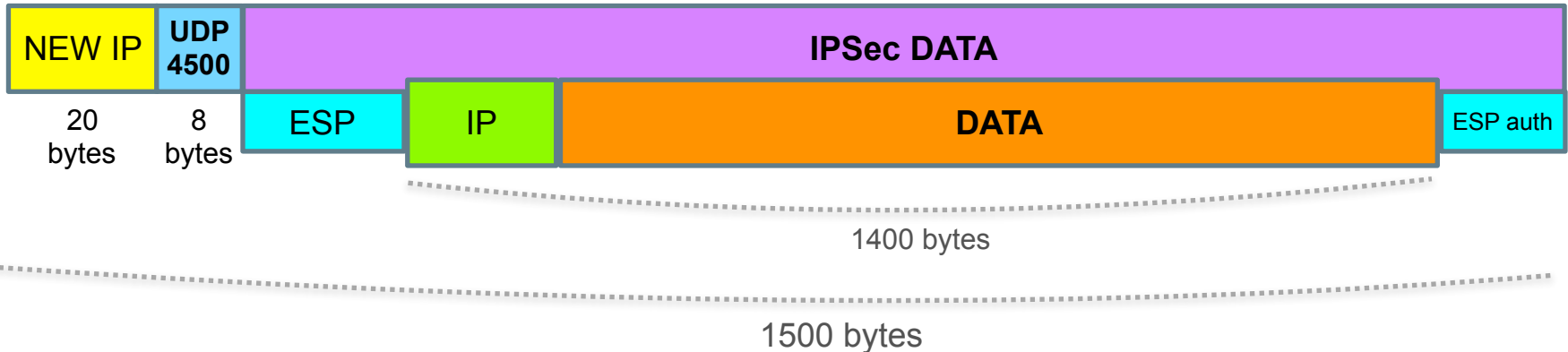


# Understanding IPSec MTU (simplified)

## IPSec ESP packet (*tunnel mode*)

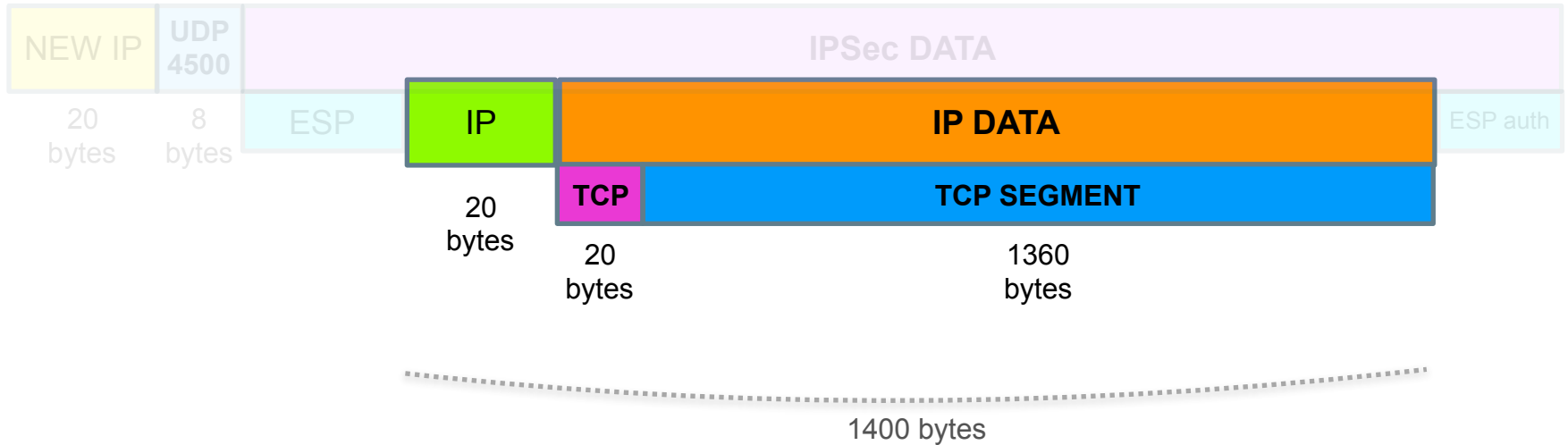


## IPSec ESP packet with NAT-T (*tunnel mode*)



# Understanding IPsec MTU (simplified)

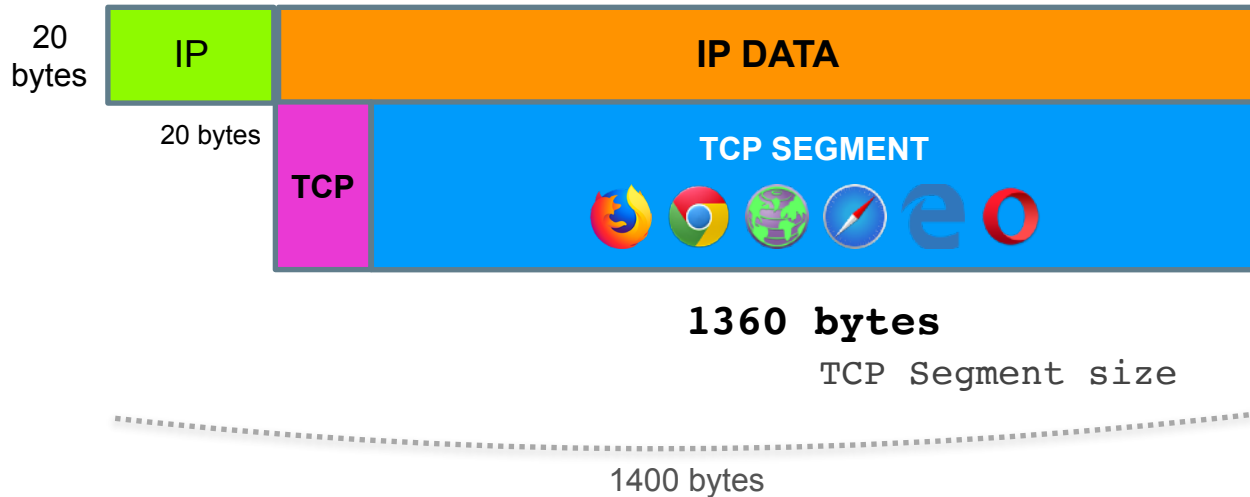
## IPsec ESP packet with NAT-T (tunnel mode)



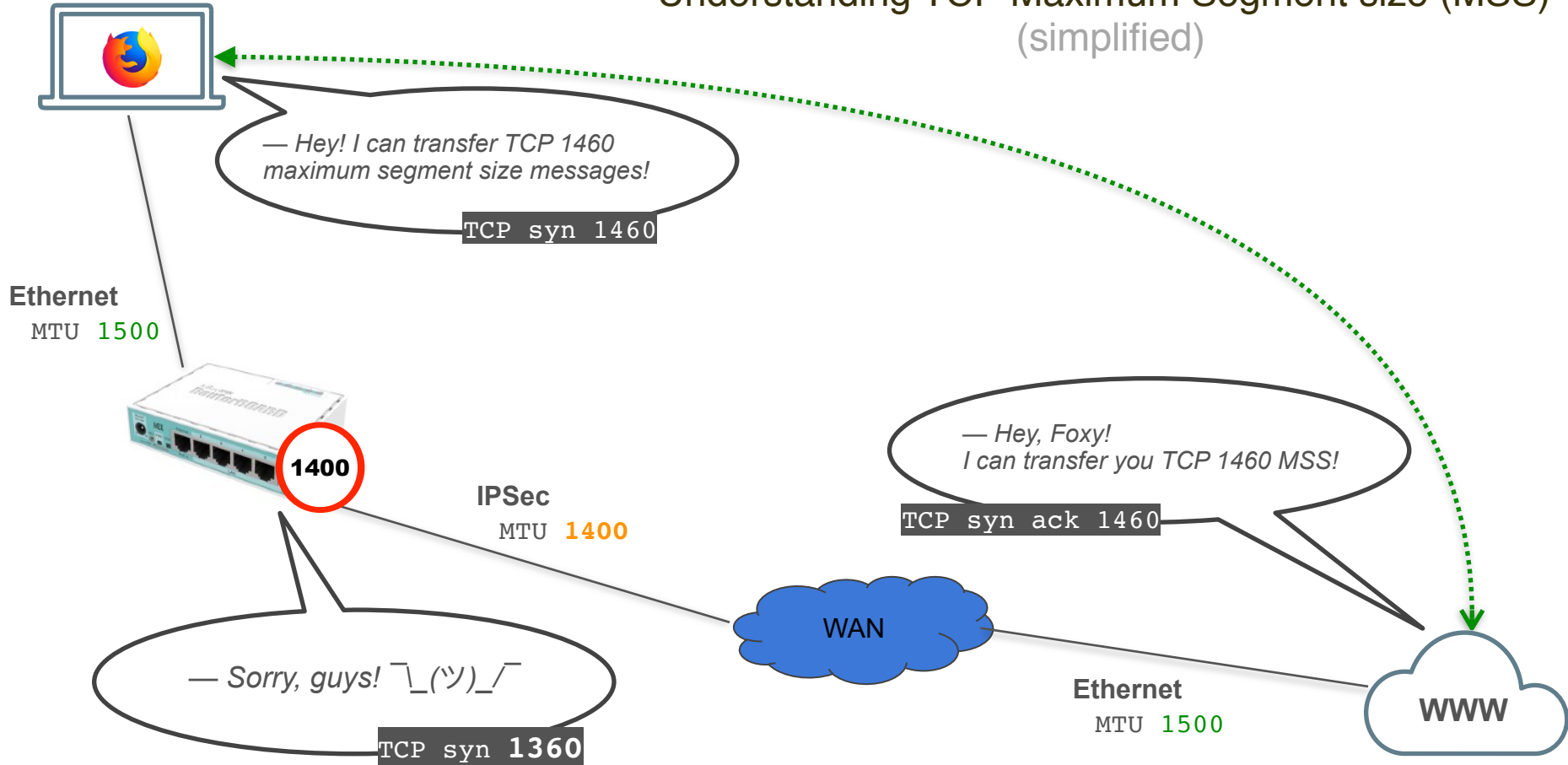
# Understanding TCP MSS (simplified)

---

TCP Segment size = MTU - 40 bytes

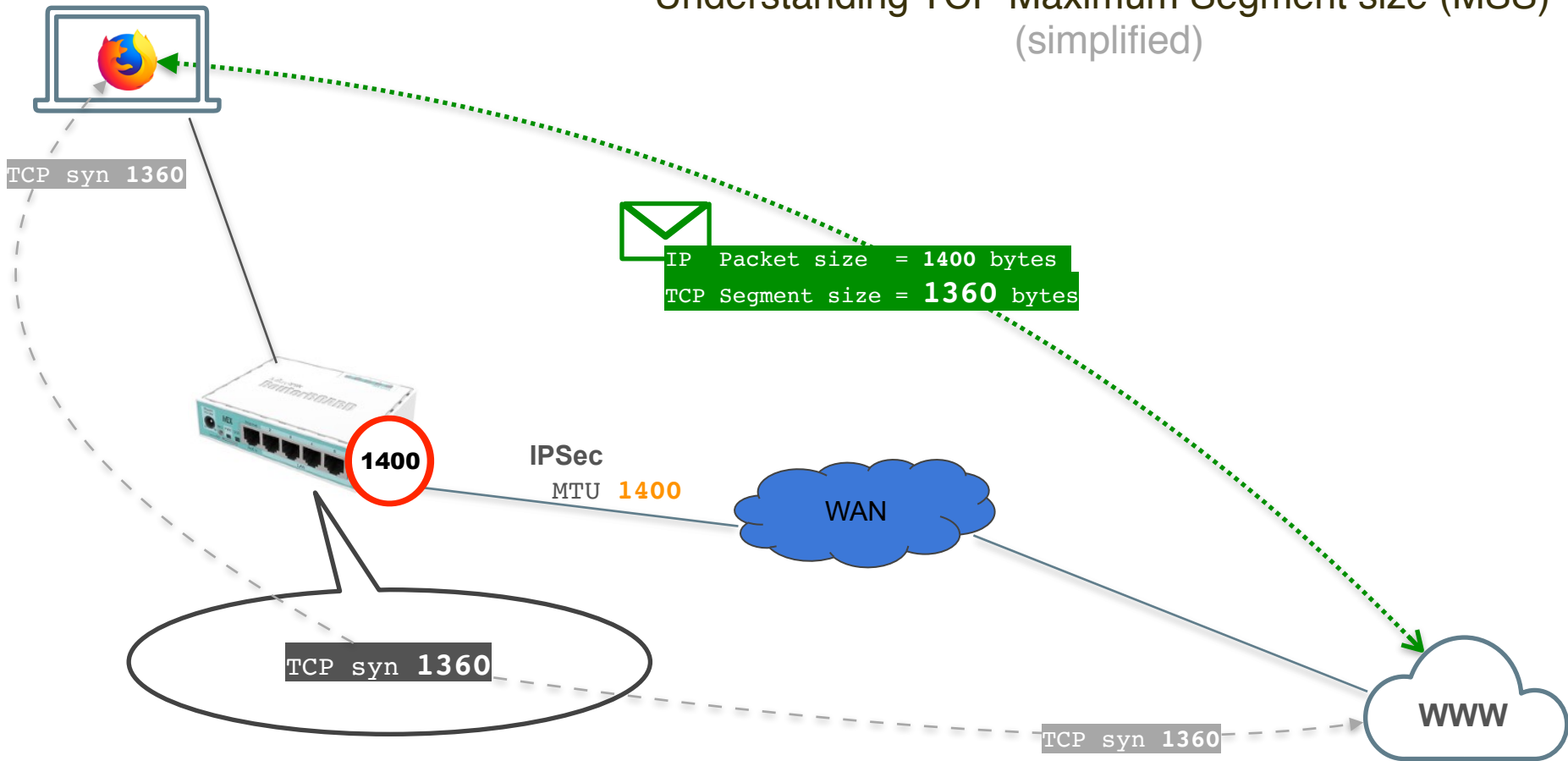


# Understanding TCP Maximum Segment size (MSS) (simplified)

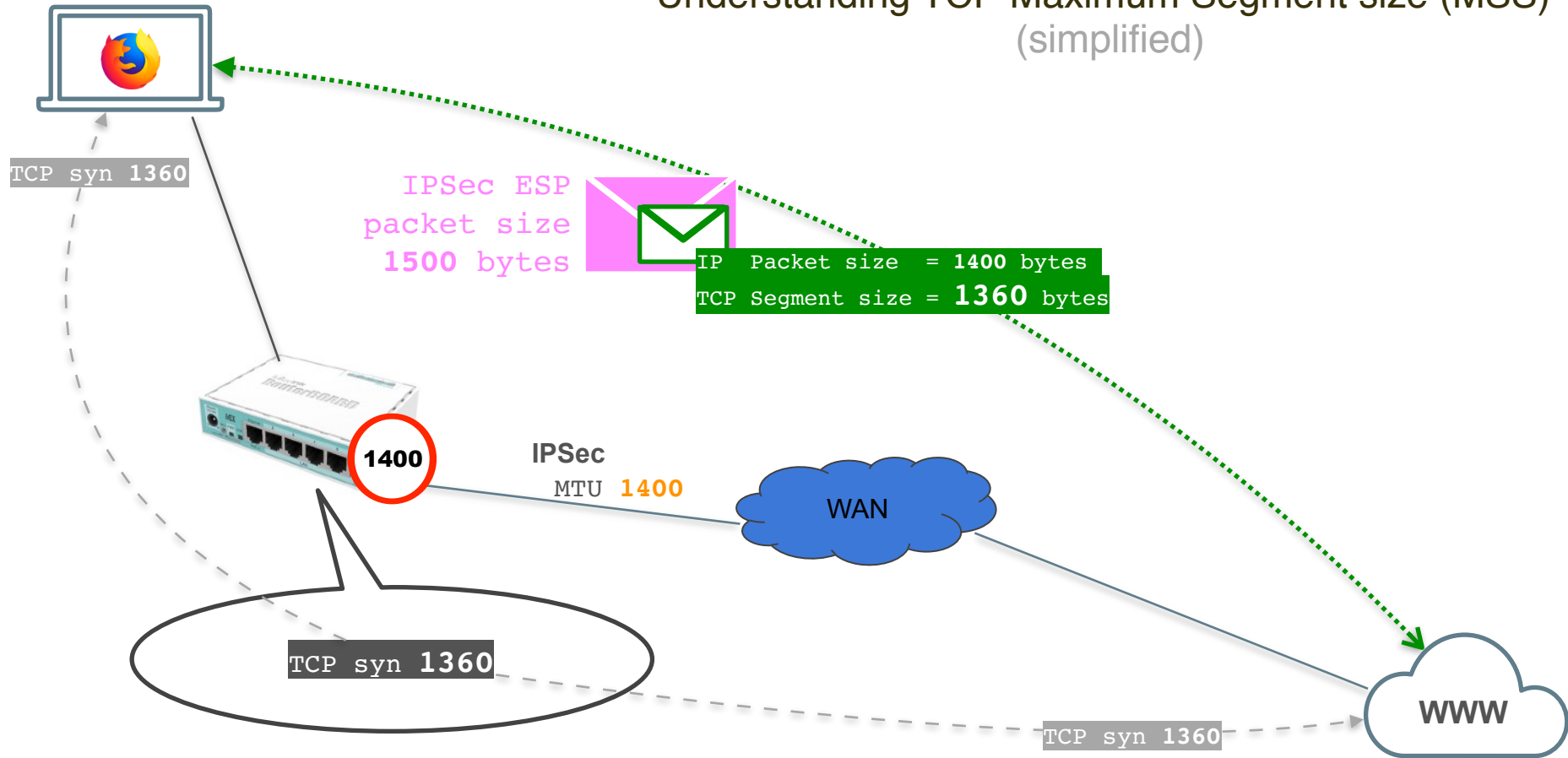




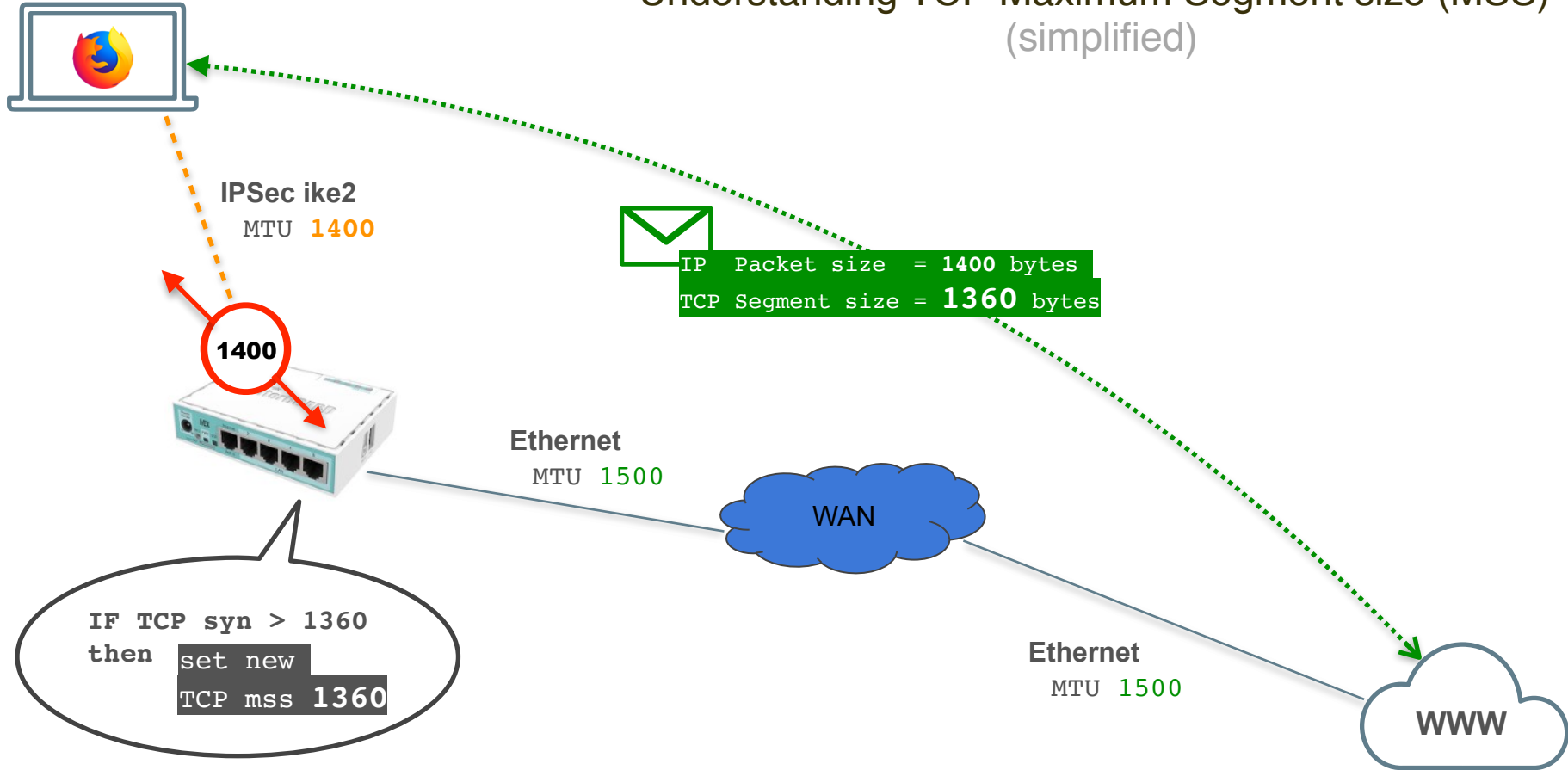
# Understanding TCP Maximum Segment size (MSS) (simplified)



# Understanding TCP Maximum Segment size (MSS) (simplified)



# Understanding TCP Maximum Segment size (MSS) (simplified)



# Adjust TCP MSS from IPsec IKE2 addresses

The image shows a sequence of three screenshots from Mikrotik WinBox v6.44.3 on mAP lite (mipsbe) illustrating the configuration of a new mangle rule to adjust TCP MSS for IKE2 addresses.

**Left Screenshot:** The 'New Mangle Rule' dialog box is open. The 'Chain' is set to 'forward', 'Src. Address' is '10.0.88.0/24', and 'Protocol' is 'tcp'. The 'Action' dropdown is set to 'change MSS'. The 'Log' checkbox is unchecked, and 'Log Prefix' is empty. The 'New TCP MSS' dropdown is set to '1360' and is circled in red. The 'Passthrough' checkbox is checked. A 'Comment for New Mangle Rule' dialog box is also open, containing the text: 'IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY'.

**Middle Screenshot:** The 'New Mangle Rule' dialog box is open. The 'IPsec Policy' dropdown is set to 'in' and 'ipsec'. The 'TCP MSS' dropdown is set to '0-1360' and is circled in red. The 'TCP Flags' dropdown is set to 'syn'.

**Right Screenshot:** The 'New Mangle Rule' dialog box is open. The 'Action' dropdown is set to 'change MSS'. The 'Log' checkbox is unchecked, and 'Log Prefix' is empty. The 'New TCP MSS' dropdown is set to '1360' and is circled in red. The 'Passthrough' checkbox is checked.

```
/ip firewall mangle add action=change-mss chain=forward new-mss=1360 src-address=10.0.88.0/24 protocol=tcp tcp-flags=syn tcp-mss=!0-1360 ipsec-policy=in,ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY"
```

# Adjust TCP MSS to IPsec IKE2 addresses

The screenshot displays the Mikrotik WinBox interface for configuring a New Mangle Rule. The 'General' tab is active, showing the following settings:

- Chain: forward
- Src. Address: (empty)
- Dst. Address: 10.0.88.0/24
- Protocol: 6 (tcp)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)
- Out. Interface: (empty)
- In. Interface List: (empty)
- Out. Interface List: (empty)
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Routing Table: (empty)
- Connection Type: (empty)
- Connection State: (empty)
- Connection NAT State: (empty)

The 'Advanced' tab is also visible, showing:

- Src. Address List: (empty)
- Dst. Address List: (empty)
- Layer7 Protocol: (empty)
- Content: (empty)
- Connection Bytes: (empty)
- Connection Rate: (empty)
- Per Connection Classifier: (empty)
- Src. MAC Address: (empty)
- Out. Bridge Port: (empty)
- In. Bridge Port: (empty)
- In. Bridge Port List: (empty)
- Out. Bridge Port List: (empty)
- IPsec Policy: out : ipsec
- TLS Host: (empty)
- Ingress Priority: (empty)
- Priority: (empty)
- DSCP (TOS): (empty)
- TCP MSS: 0-1360
- Packet Size: (empty)
- Random: (empty)
- TCP Flags: syn
- ICMP Options: (empty)

The 'Action' tab is selected, showing:

- Action: change MSS
- Log: (unchecked)
- Log Prefix: (empty)
- New TCP MSS: 1360
- Passthrough: (checked)

A comment dialog box is open, containing the text: "IKE2: Clamp TCP MSS from ANY to 10.0.88.0/24".

```
/ip firewall mangle add action=change-mss chain=forward new-mss=1360 dst-address=10.0.88.0/24 protocol=tcp tcp-flags=syn tcp-mss=!0-1360 ipsec-policy=out,ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from ANY to 10.0.88.0/24"
```

# Demo lab

# Demo lab

Free live demo is  
available

1. Request certificate via form
2. Receive certificates
3. Connect to VPN server
4. Access via Winbox



# Demo lab

1. **Request certificate via form**
2. Receive certificates
3. Connect to VPN server
4. Access via Winbox

Request your certificate via form

<https://forms.gle/nZTDK2wex5nneqo6A>





# Demo lab

1. Request certificate via form
2. **Receive certificates**
3. Connect to VPN server
4. Access via Winbox

Wait for your certificate

Manual processing for this LAB, sorry :)



# Demo lab

1. Request certificate via form
2. Receive certificates
3. **Connect to VPN server**
4. Access via Winbox

IKE2 VPN Server address

`<check your email>`



# Demo lab

1. Request certificate via form
2. Receive certificates
3. Connect to VPN server
4. **Access via Winbox**

## Access LAB router via Winbox

**Address**

10.0.88.1

**Login** lab

**Password** lab



# Configure clients

# Windows 10

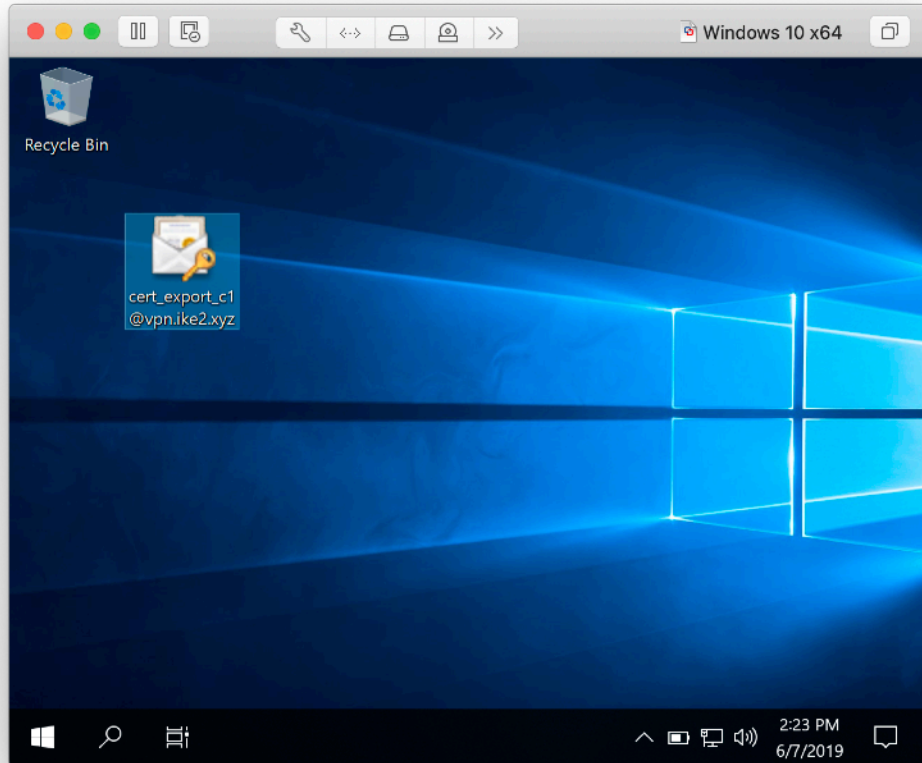
## Agenda for next slides

1. Import SSL certificate
2. Setup IKEv2 connection
3. Testing IKEv2 VPN routing



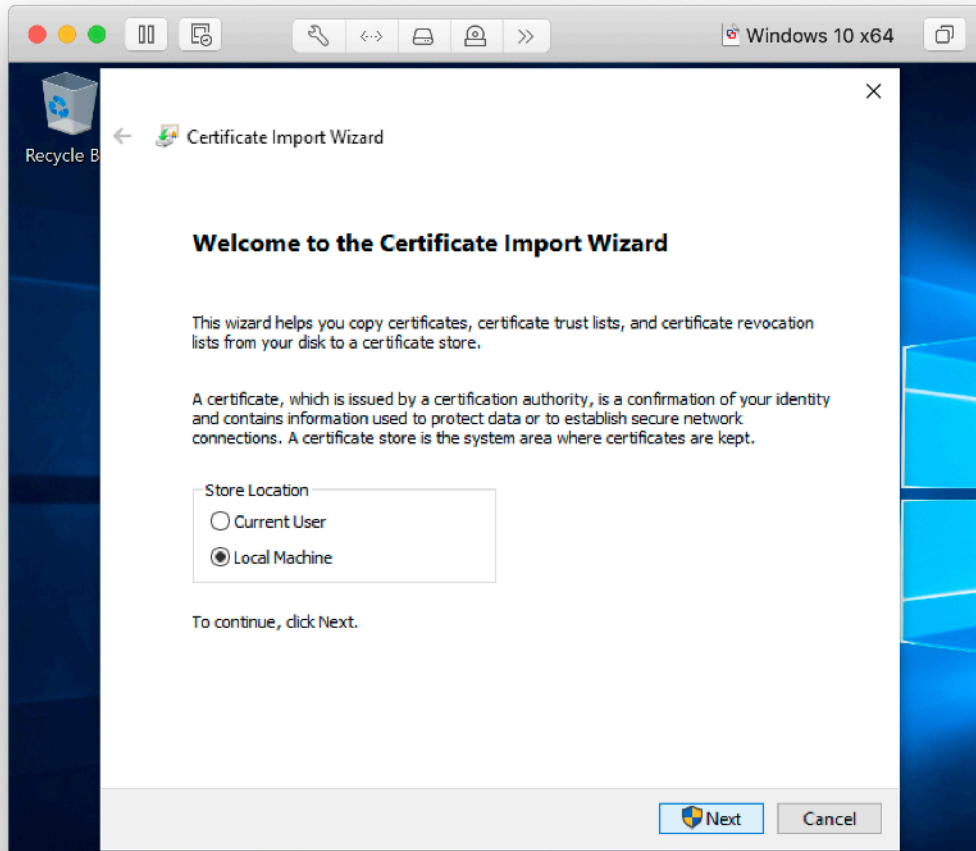
# Windows 10: Import SSL certificates

---



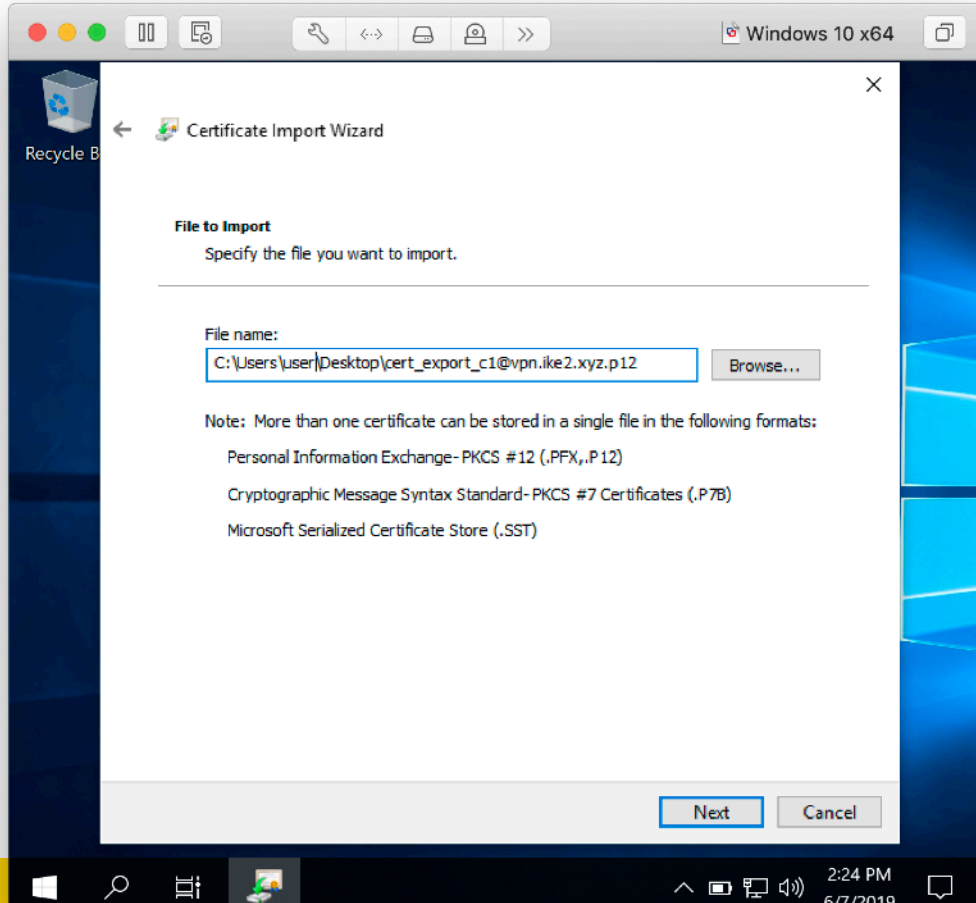
Download .p12 certificate

# Windows 10: Import SSL certificates



Select **Local Machine** store location  
—> **Next**

# Windows 10: Import SSL certificates

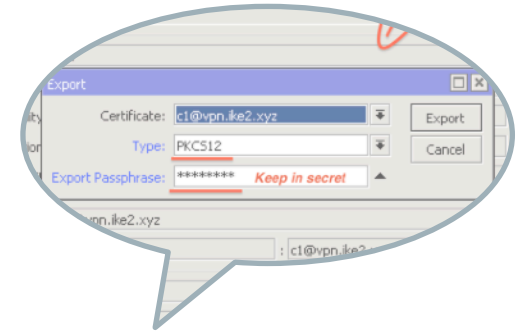
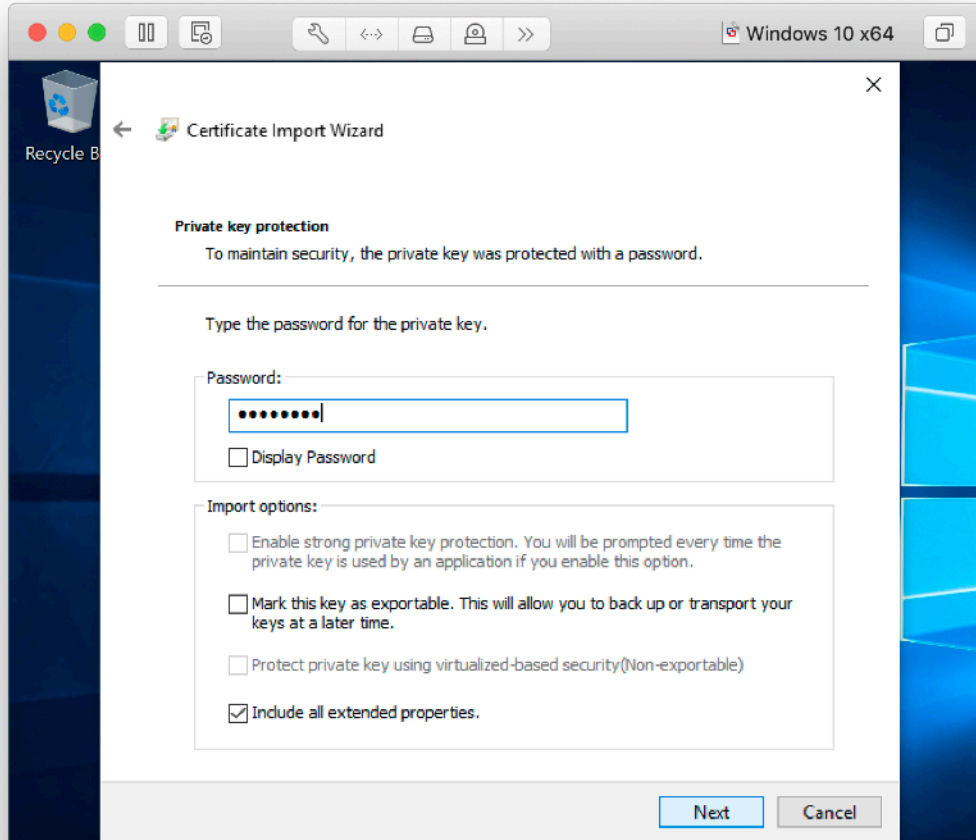


File name already selected

—> **Next**

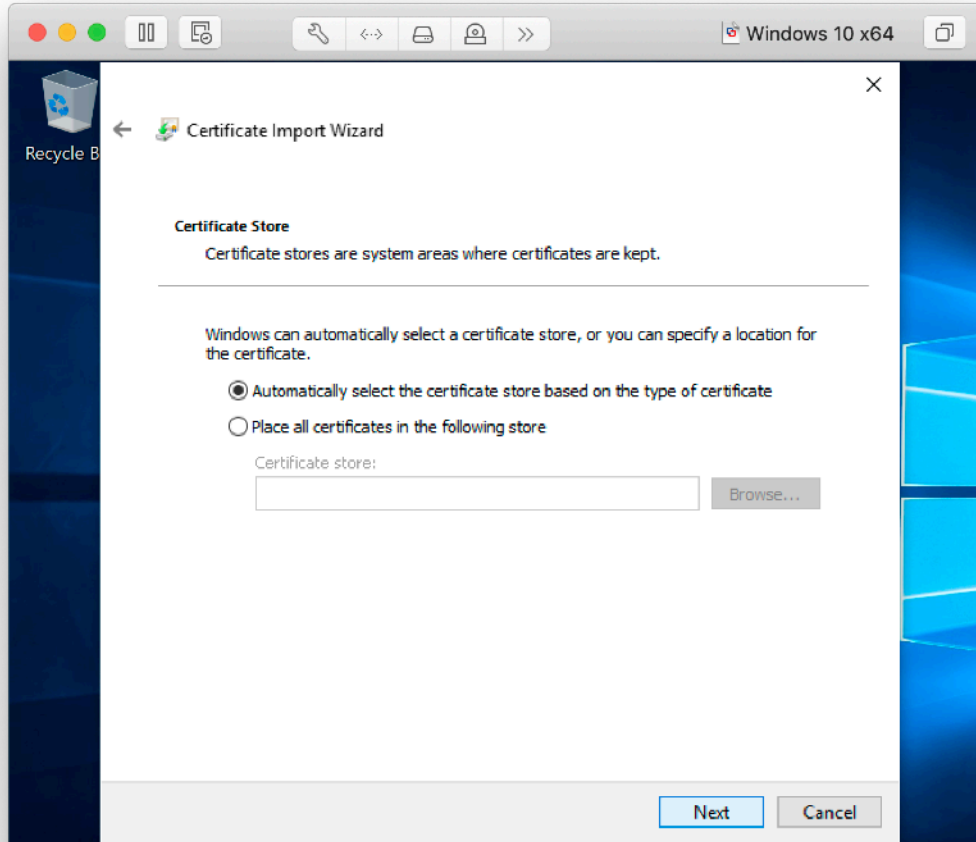


# Windows 10: Import SSL certificates



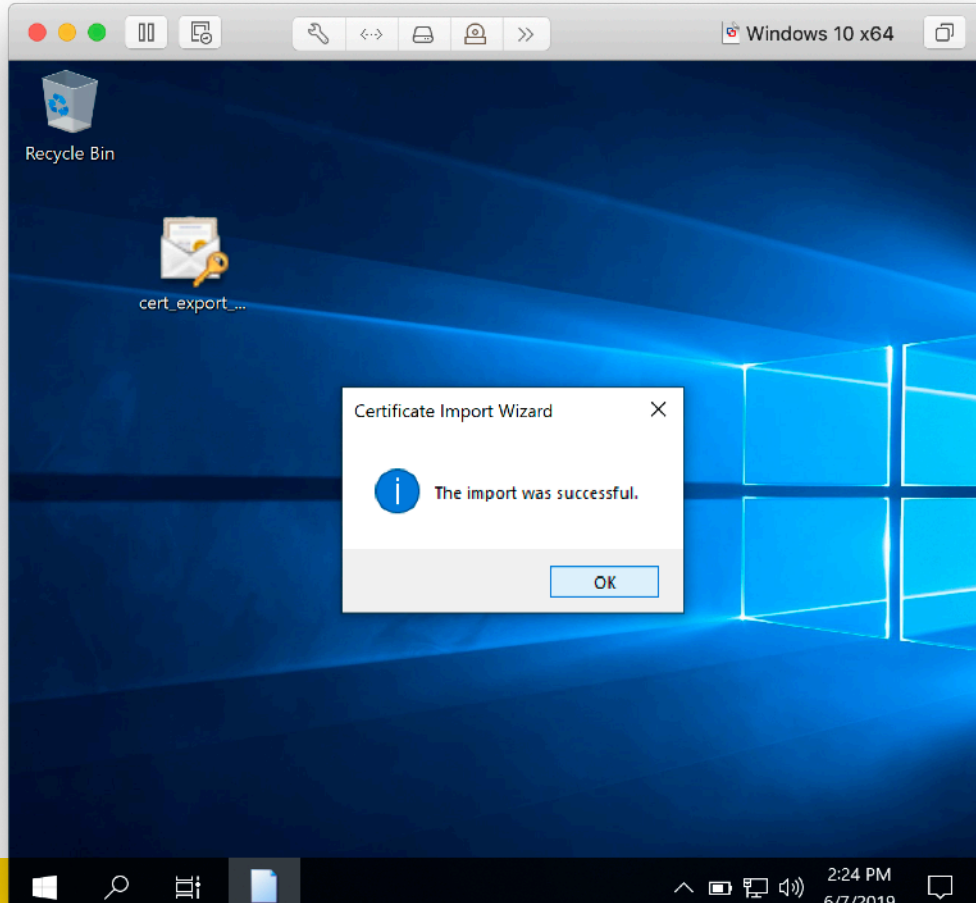
Type your  
SSL certificate password  
—> **Next**

# Windows 10: Import SSL certificates



Automatic  
—> Next

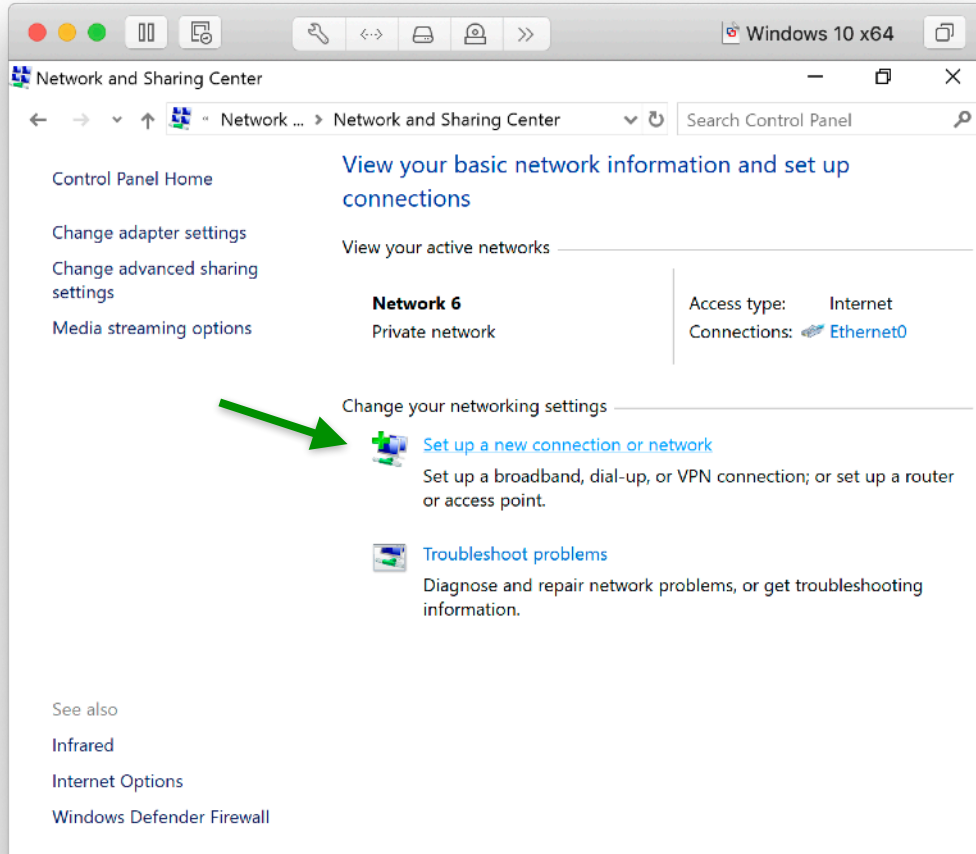
# Windows 10: Import SSL certificates



SSL Certificate  
imported successfully

—> **OK**

# Windows 10: Setup IKEv2 VPN connection



- > Control panel
- > Network and Internet
- > Network and Sharing Center

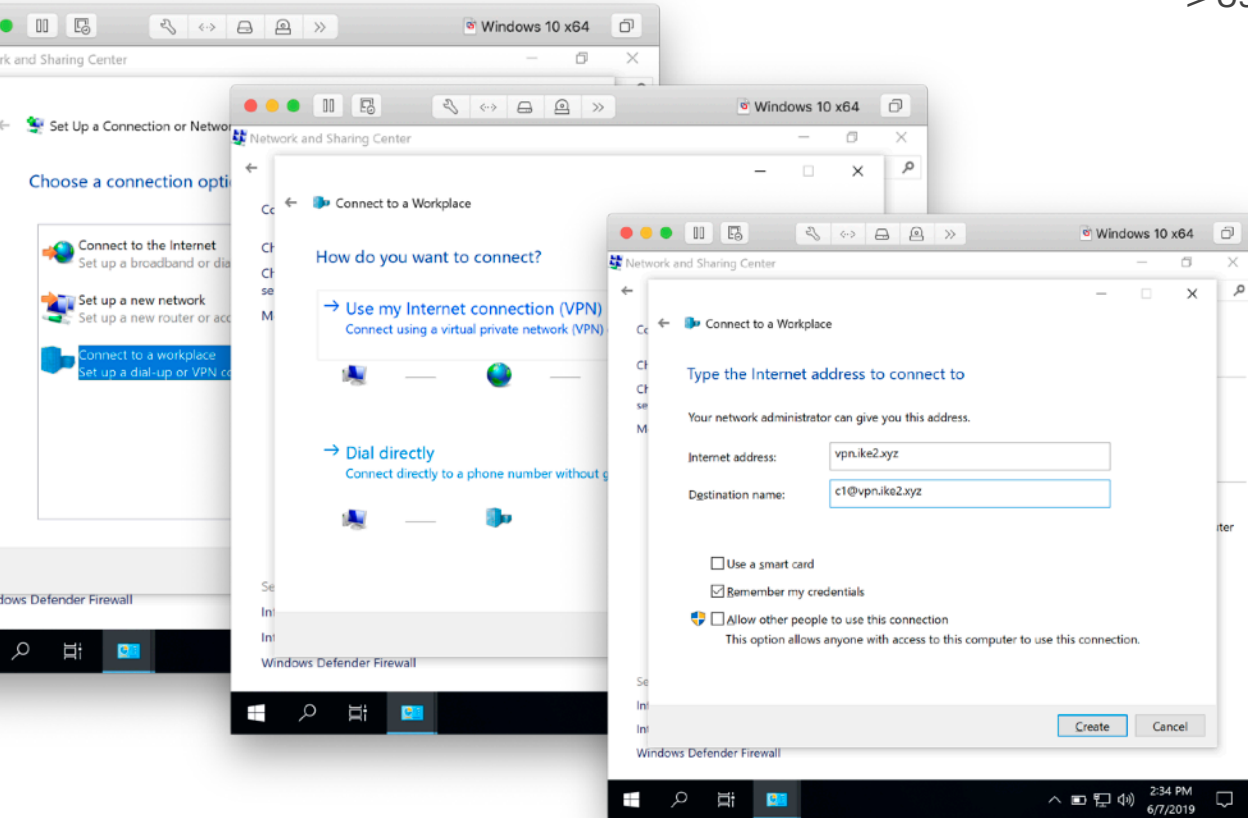
**Set up a new connection or network**

# Windows 10: Setup IKEv2 VPN connection

—> Connect to a workspace

—> Use my Internet connection (VPN)

—> **Next**



Internet address:

**vpn.ike2.xyz**

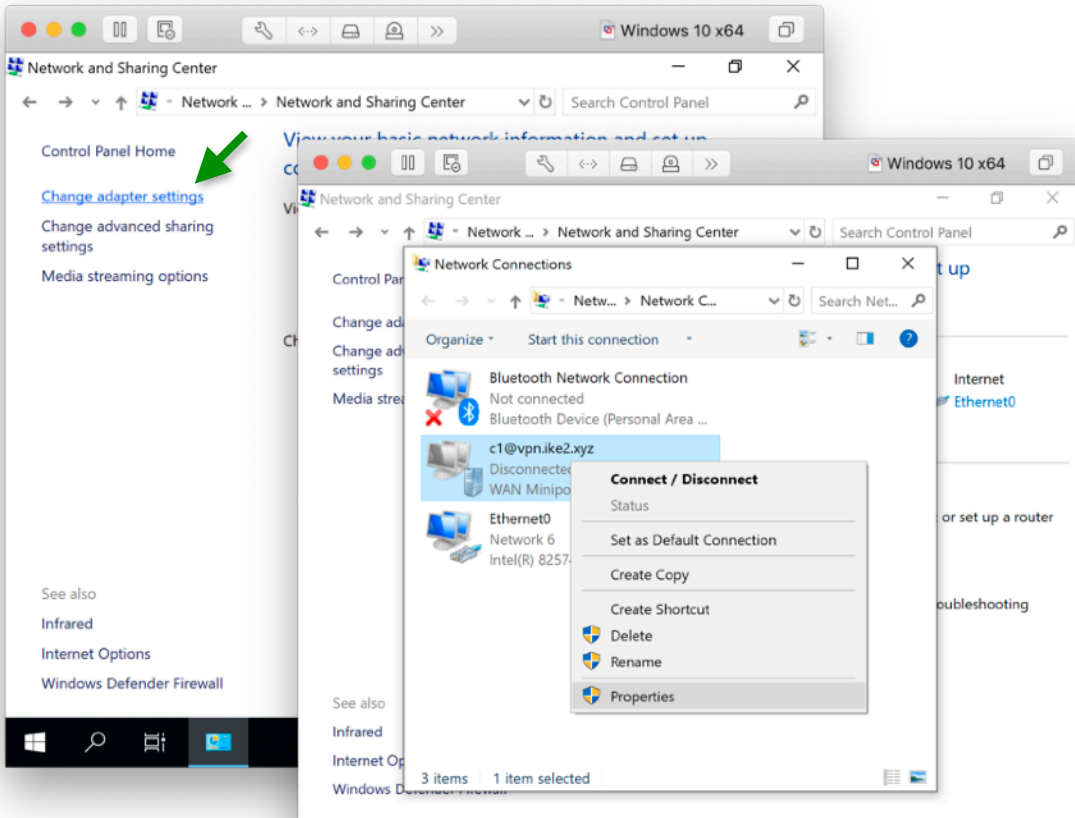
Destination name:

**c1@vpn.ike2.xyz**

—> **Create**

# Windows 10: Setup IKEv2 VPN connection

— — —



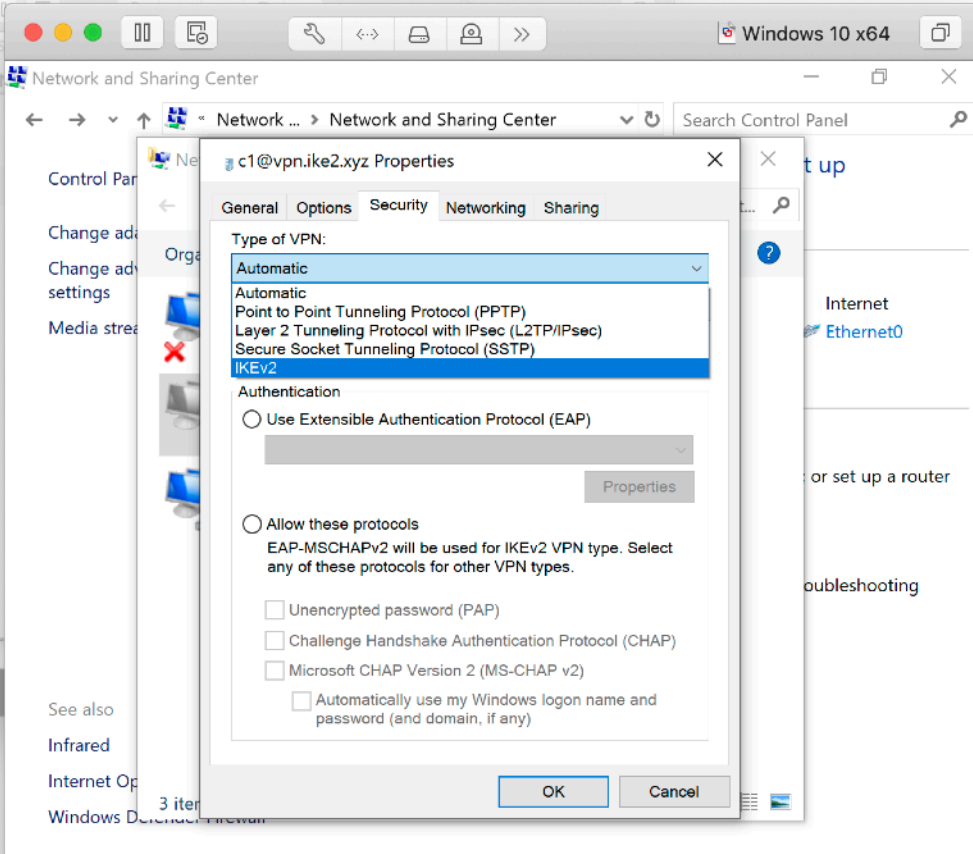
—> Change adapter settings

`c1@vpn.ike2.xyz`

—> **Properties**



# Windows 10: Setup IKEv2 VPN connection



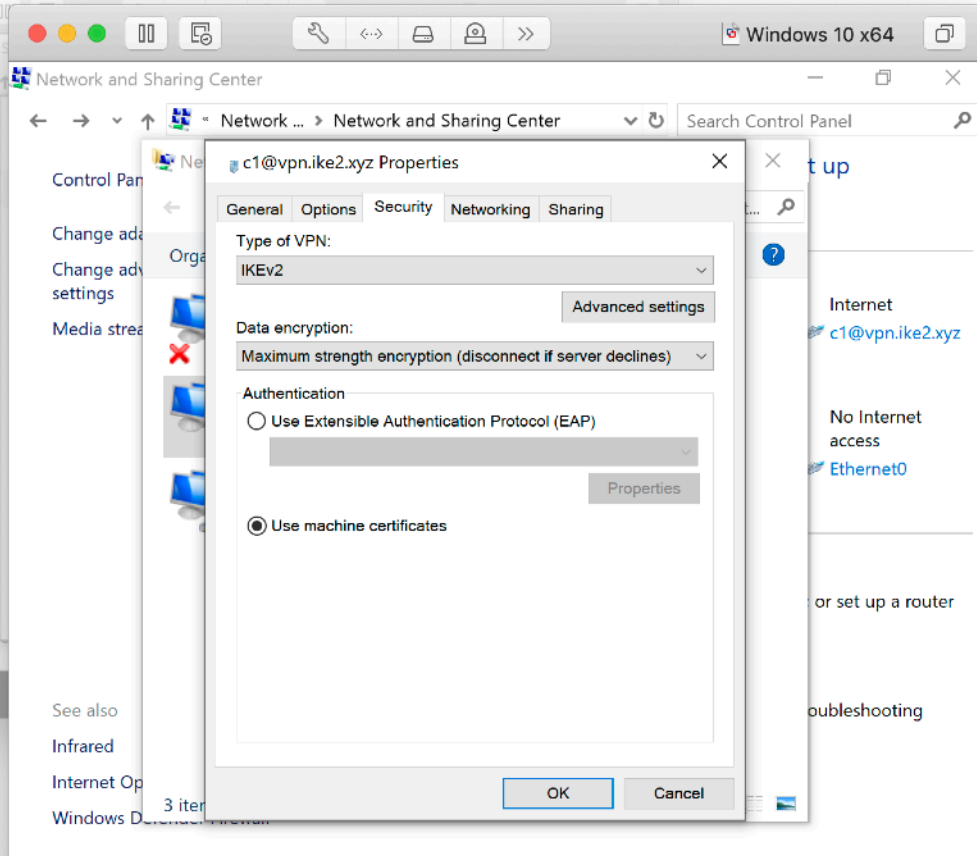
Properties -> Security tab

Type of VPN:

**IKEv2**



# Windows 10: Setup IKEv2 VPN connection



Properties -> Security tab

Data encryption:

**Maximum strength  
encryption**

Authentication:

**Use machine  
certificates**

—> OK



# Windows 10: Testing IKEv2 VPN connection

The screenshot displays a Windows 10 desktop with several windows open. The background is the standard Windows 10 blue wallpaper. In the foreground, there are three windows:

- c1@vpn.ike2.xyz Status**: A window showing the status of the VPN connection. It has two tabs: "General" and "Details". Under "General", it lists:
  - Connection: Internet
  - IPv4 Connectivity: (checked)
  - IPv6 Connectivity: (checked)
  - Media State: (checked)
  - Duration: (empty)There is a "Details..." button. Under "Activity", there is a graph showing data sent. The "Bytes" sent is 16,011, and "Compression" is 0%. There are "Properties", "Disconnect", and "Diagnose" buttons at the bottom.
- Network Connection Details**: A window showing the details for the "Internet" connection. It lists the following properties and values:

Property	Value
Connection-specific DNS Suffix	
Description	c1@vpn.ike2.xyz
Physical Address	
DHCP Enabled	No
IPv4 Address	10.0.88.2
IPv4 Subnet Mask	255.255.255.255
IPv4 Default Gateway	
IPv4 DNS Server	10.0.88.1
IPv4 WINS Server	
NetBIOS over Tcpip Enabled	Yes
- Network 6 Connected**: A notification card in the bottom right corner of the desktop. It shows the VPN icon and the text "c1@vpn.ike2.xyz Connected". A green arrow points from this notification to the "c1@vpn.ike2.xyz Status" window.

The taskbar at the bottom shows the system tray with icons for network, volume, and date/time (2:47 PM, 6/7/2019). The taskbar also shows "Airplane mode" is turned off.

# Windows 10: Testing IKEv2 VPN routes

```
Windows 10 x64
Command Prompt
C:\Users>route -4 print

=====
Interface List
 9...00 0c 29 e6 e6 ce .....Intel(R) 82574L Gigabit Network Connection
25.....c1@vpn.ike2.xyz
 6...00 50 56 fc fe e4 .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
 0.0.0.0                    0.0.0.0          192.168.88.1     192.168.88.252   4250
 0.0.0.0                    0.0.0.0          On-link         10.0.88.2        26
 10.0.88.2                  255.255.255.255 On-link         10.0.88.2        281
123.45.67.8                 255.255.255.255 192.168.88.1     192.168.88.252   4251
127.0.0.0                   255.0.0.0        On-link         127.0.0.1        4556
127.0.0.1                   255.255.255.255 On-link         127.0.0.1        4556
127.255.255.255            255.255.255.255 On-link         127.0.0.1        4556
192.168.88.0               255.255.255.0   On-link         192.168.88.252   4506
192.168.88.252             255.255.255.255 On-link         192.168.88.252   4506
192.168.88.255             255.255.255.255 On-link         192.168.88.252   4506
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        4556
224.0.0.0                  240.0.0.0        On-link         192.168.88.252   4506
224.0.0.0                  240.0.0.0        On-link         10.0.88.2        26
255.255.255.255            255.255.255.255 On-link         127.0.0.1        4556
255.255.255.255            255.255.255.255 On-link         192.168.88.252   4506
255.255.255.255            255.255.255.255 On-link         10.0.88.2        281
=====
```

```
route -4 print
```

Destination  
0.0.0.0/0 (default)

Gateway:  
On-link

Interface:  
10.0.88.2

Metric (distance):  
26

# Windows 10: Testing IKEv2 VPN routes

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Dashboard

Session: 192.168.88.1 CPU: 1%

IPsec

Mode Configs

Name	Resp...	Address Pool	Address	Address Pr...	Split Include	System ...	Sr
modeconf vpn.ike2...	yes	pool vpn.ike2.xyz		32	192.168.99.0/24, 17...	yes	
request-only	no						

IPsec Mode Config <modeconf vpn.ike2.xyz>

Name: modeconf vpn.ike2.xyz

Responder

Address Pool: pool vpn.ike2.xyz

Address:

Address Prefix Length: 32

Split Include:

- 192.168.99.0/24
- 172.16.0.0/22
- 10.20.0.0/21

System DNS

Command Prompt

IPv4 Route Table

```
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                   0.0.0.0         192.168.88.1    192.168.88.252  4250
0.0.0.0                   0.0.0.0         On-link         10.0.88.2        26
10.0.88.2                 255.255.255.255 On-link         10.0.88.2        281
10.20.0.0                 255.255.248.0   On-link         10.0.88.2        26
10.20.0.0/22             255.255.255.255 On-link         10.0.88.2        281
123.45.67.8              255.255.255.255 192.168.88.1    192.168.88.252  4251
127.0.0.0                 255.0.0.0       On-link         127.0.0.1        4556
127.0.0.1                 255.255.255.255 On-link         127.0.0.1        4556
127.255.255.255          255.255.255.255 On-link         127.0.0.1        4556
172.16.0.0                255.255.252.0   On-link         10.0.88.2        26
172.16.0.0/22           255.255.255.255 On-link         10.0.88.2        281
192.168.88.0              255.255.255.0   On-link         192.168.88.252  4506
192.168.88.252           255.255.255.255 On-link         192.168.88.252  4506
192.168.88.255           255.255.255.255 On-link         192.168.88.252  4506
192.168.99.0             255.255.255.0   On-link         10.0.88.2        26
192.168.99.0/22         255.255.255.255 On-link         10.0.88.2        281
224.0.0.0                 240.0.0.0       On-link         127.0.0.1        4556
224.0.0.0                 240.0.0.0       On-link         192.168.88.252  4506
224.0.0.0                 240.0.0.0       On-link         10.0.88.2        26
255.255.255.255          255.255.255.255 On-link         127.0.0.1        4556
255.255.255.255          255.255.255.255 On-link         192.168.88.252  4506
255.255.255.255          255.255.255.255 On-link         10.0.88.2        281
=====
Persistent Routes:
None
```

# Windows 10: Testing IKEv2 VPN routes

— 0.0.0.0/0 ???

Address:  Copy

Address Prefix Length:  Remove

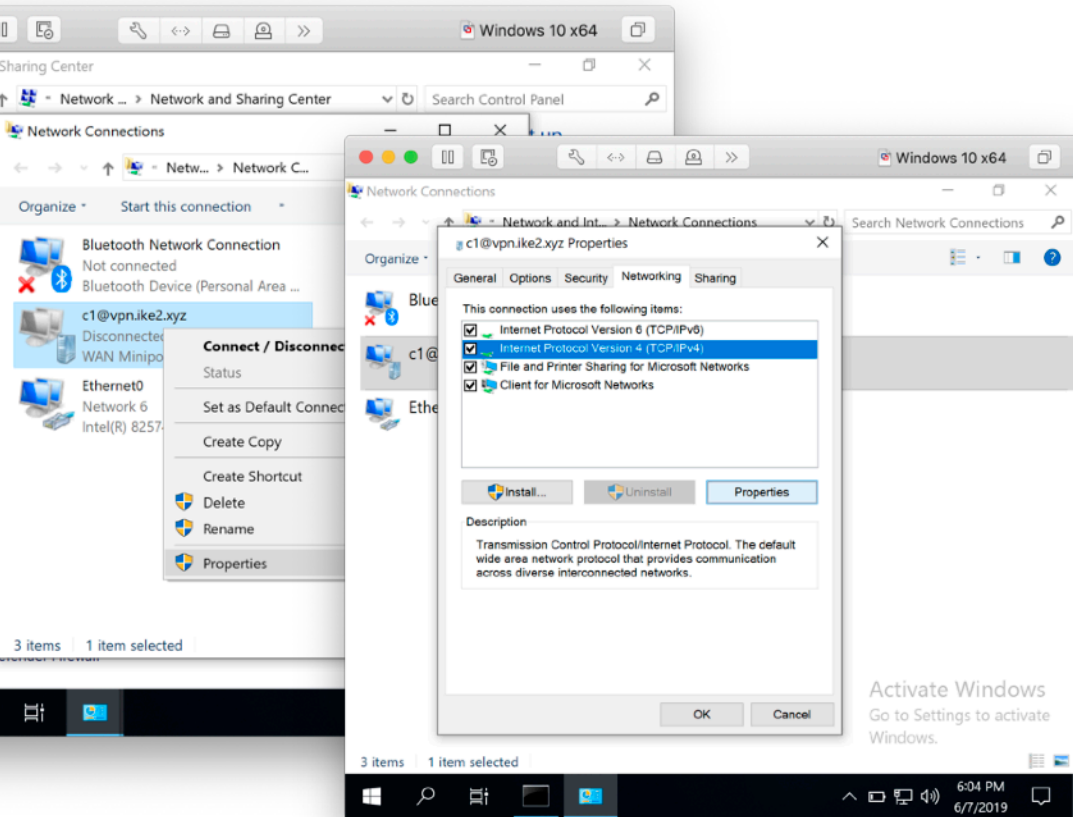
Split Include:

System DNS

```
Windows 10 x64
Command Prompt

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.88.1    192.168.88.252   4250
0.0.0.0                    0.0.0.0          On-link         10.0.88.2        26
10.0.88.2                  255.255.255.255 On-link         10.0.88.2        281
10.20.0.0                  255.255.248.0   On-link         10.0.88.2        26
10.20.7.255                255.255.255.255 On-link         10.0.88.2        281
123.45.67.8                255.255.255.255 192.168.88.1    192.168.88.252   4251
127.0.0.0                  255.0.0.0       On-link         127.0.0.1        4556
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        4556
127.255.255.255           255.255.255.255 On-link         127.0.0.1        4556
172.16.0.0                 255.255.252.0   On-link         10.0.88.2        26
172.16.3.255              255.255.255.255 On-link         10.0.88.2        281
192.168.88.0               255.255.255.0   On-link         192.168.88.252   4506
192.168.88.252             255.255.255.255 On-link         192.168.88.252   4506
192.168.88.255             255.255.255.255 On-link         192.168.88.252   4506
192.168.99.0               255.255.255.0   On-link         10.0.88.2        26
192.168.99.255            255.255.255.255 On-link         10.0.88.2        281
224.0.0.0                  240.0.0.0       On-link         127.0.0.1        4556
224.0.0.0                  240.0.0.0       On-link         192.168.88.252   4506
224.0.0.0                  240.0.0.0       On-link         10.0.88.2        26
255.255.255.255           255.255.255.255 On-link         127.0.0.1        4556
255.255.255.255           255.255.255.255 On-link         192.168.88.252   4506
255.255.255.255           255.255.255.255 On-link         10.0.88.2        281
=====
Persistent Routes:
None
```

# Windows 10: Disable IKEv2 VPN default gateway

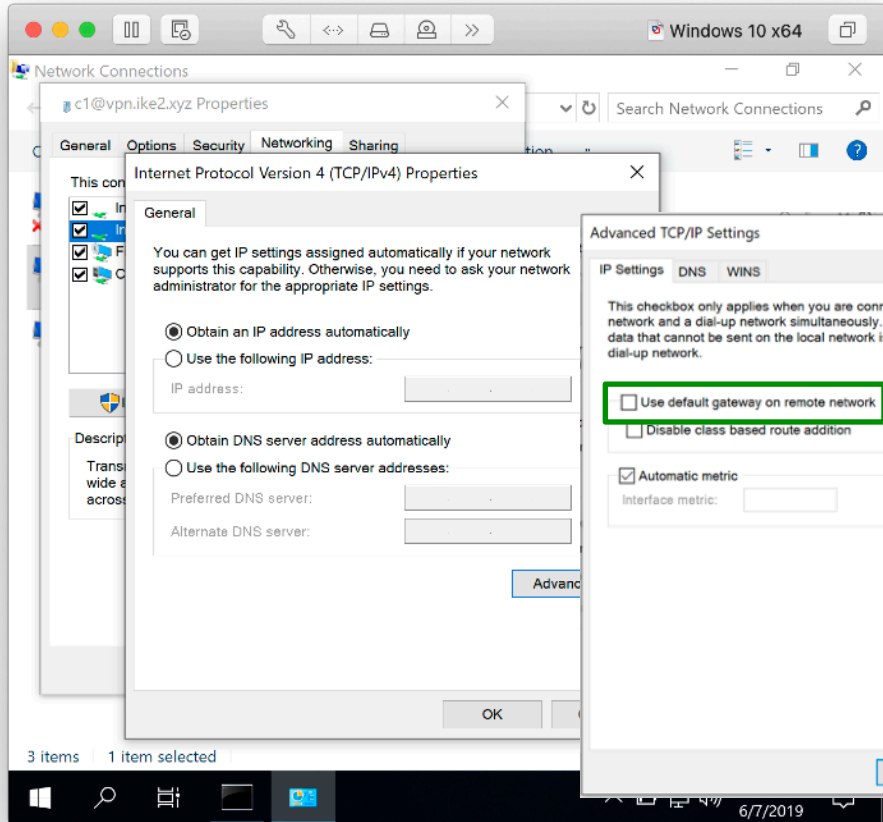


Properties -> Networking tab

✓ TCP/IPv4

→ Properties

# Windows 10: Disable IKEv2 VPN default gateway



Properties -> Networking tab

TCP/IPv4 Properties

- ✓ Obtain an IP address automatically
- ✓ Obtain DNS address automatically

—> **Advanced**

Advanced TCP/IP Settings

- Use default gateway on remote network

# Apple Mac OS

≥ 10.11 El Capitan

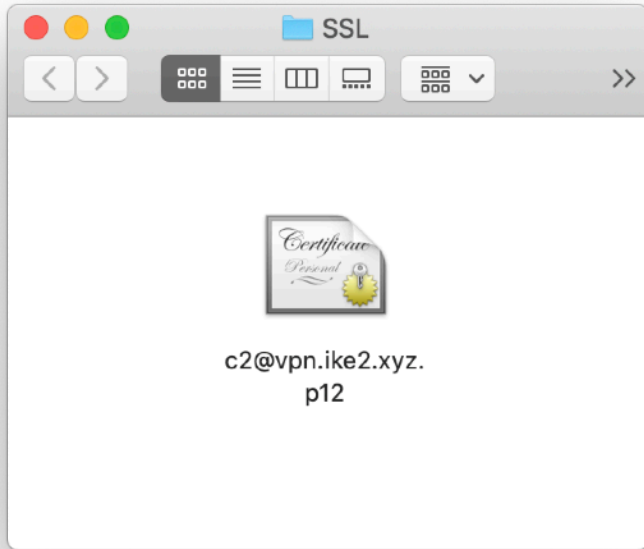
## Agenda for next slides

1. Import SSL certificate
2. Setup IKEv2 VPN connection
3. Check IKEv2 VPN routes



# MacOS: Import SSL certificates

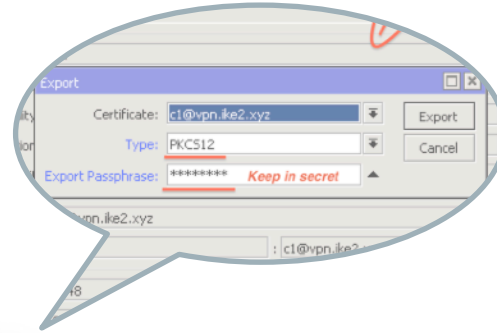
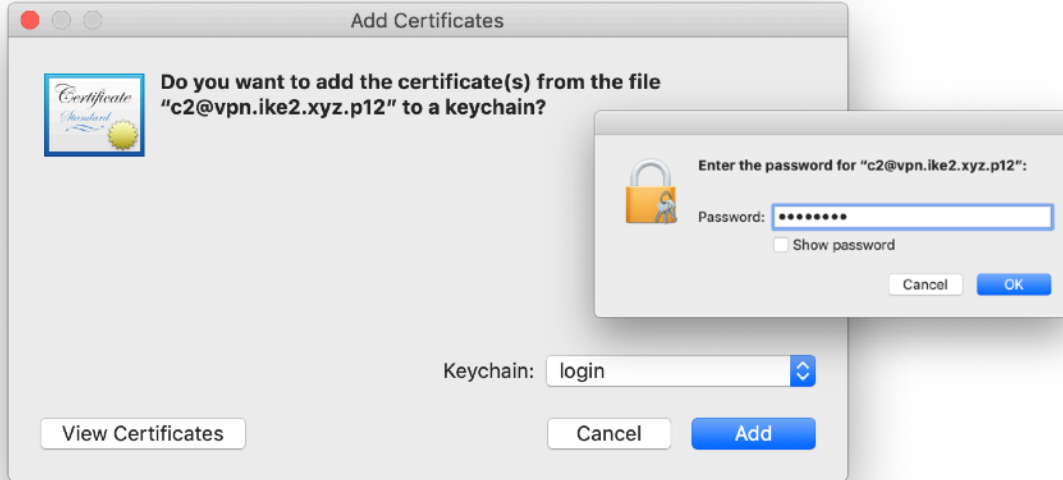
— — —



Download .p12 certificate



# MacOS: Import SSL certificates



Keychain:  
login (default)

→ Add

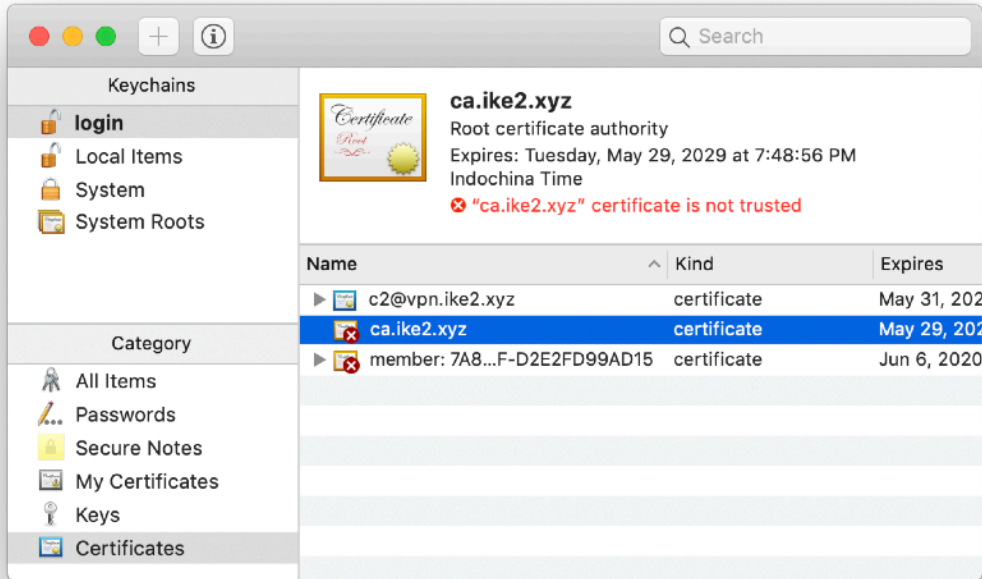
Type your  
SSL certificate password

→ OK

# MacOS: Manage SSL certificates



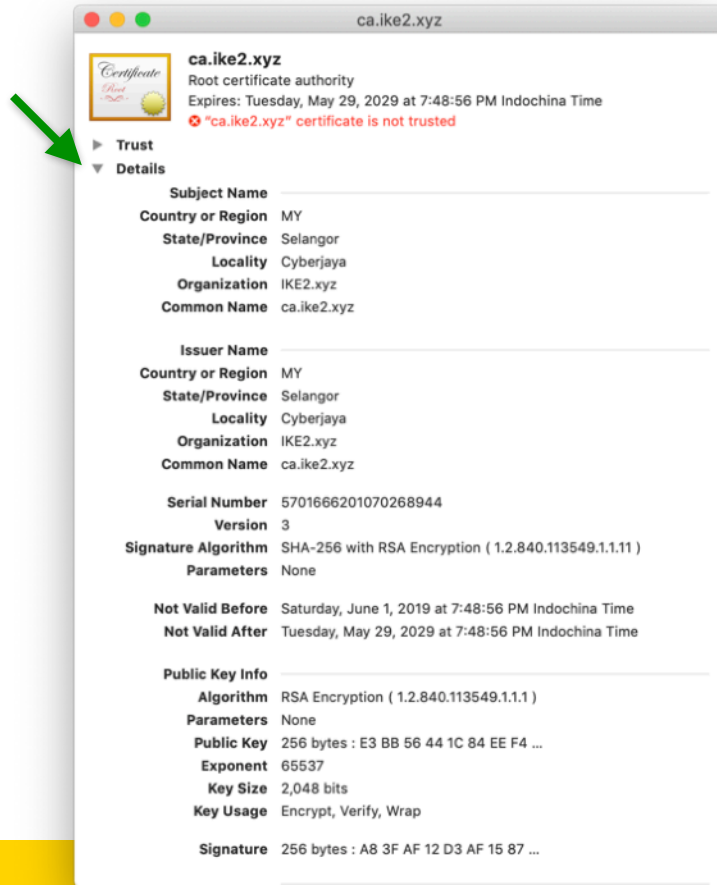
## Keychain access



1. Launch keychain access
2. Find **ca.ike2.xyz** root certificate authority

# MacOS: Manage SSL certificates

Important



## Keychain access

Verify CA certificate details



# MacOS: Manage SSL certificates

Important



## Keychain access

ca.ike2.xyz

**Public Key Info**

**Algorithm** RSA Encryption ( 1.2.840.113549.1.1.1 )

**Parameters** None

**Public Key** 256 bytes : E3 BB 56 44 1C 84 EE F4 ...

**Exponent** 65537

**Key Size** 2,048 bits

**Key Usage** Encrypt, Verify, Wrap

**Signature** 256 bytes : A8 3F AF 12 D3 AF 15 87 ...

---

**Extension** Key Usage ( 2.5.29.15 )

**Critical** YES

**Usage** Digital Signature, Key Encipherment, Data Encipherment, Key Cert Sign, CRL Sign

---

**Extension** Basic Constraints ( 2.5.29.19 )

**Critical** YES

**Usage** Digital Signature, Key Encipherment, Data Encipherment, Key Cert Sign, CRL Sign

---

**Extension** Subject Key Identifier ( 2.5.29.14 )

**Critical** NO

**Key ID** 25 FD 0B D3 3A 6C F8 96 04 A9 FA 19 24 A9 E3 85 58 C3 9B CF

---

**Extension** Subject Alternative Name ( 2.5.29.17 )

**Critical** NO

**DNS Name** ca.ike2.xyz

---

**Extension** Netscape Certificate Comment ( 2.16.840.1.113730.1.13 )

**Critical** NO

**Data** Generated by RouterOS

---

**Fingerprints**

**SHA-256** B5 7C AF 68 13 B3 52 A0 AB AB AA 4E 42 F8 C5 69 44 87 57  
EE DA F8 30 B9 3E 4B 05 C6 D7 33 D9 4B

**SHA-1** 6B A4 71 8B 3F 22 4E 3D C7 83 05 69 BF D8 94 C3 38 56  
87 D8

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Dashboard

Mode: Session: 192.168.88.1 CPU:0%

Certificate <ca.ike2.xyz>

General	Key Usage	Status
CA CRL Host:		
SCEP URL:		
CA:		
Serial Number:		
Fingerprint:	b57:af6813b352a0ababaate42f8c569448757eedaf830b93e4b05c6d733d94b	
Req. Fingerprint:		
CA Fingerprint:		
Invalid Before:	Jun/01/2019 20:48:56	
Invalid After:	May/29/2029 20:48:56	
Expires After:	3641d 03:49:00	
Revoked:		

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

private key authority expired smart card key trusted

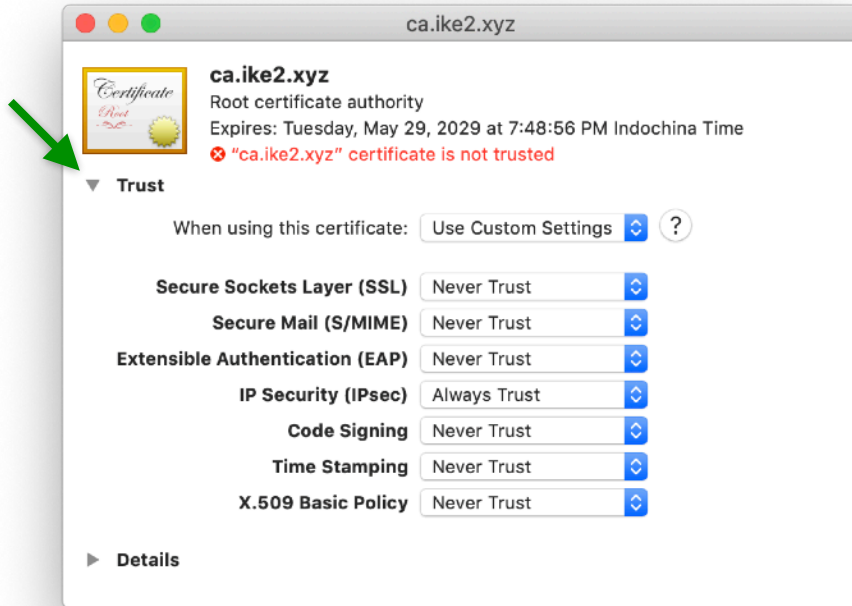
Compare CA certificate fingerprints

# MacOS: Manage SSL certificates

Important



Keychain access

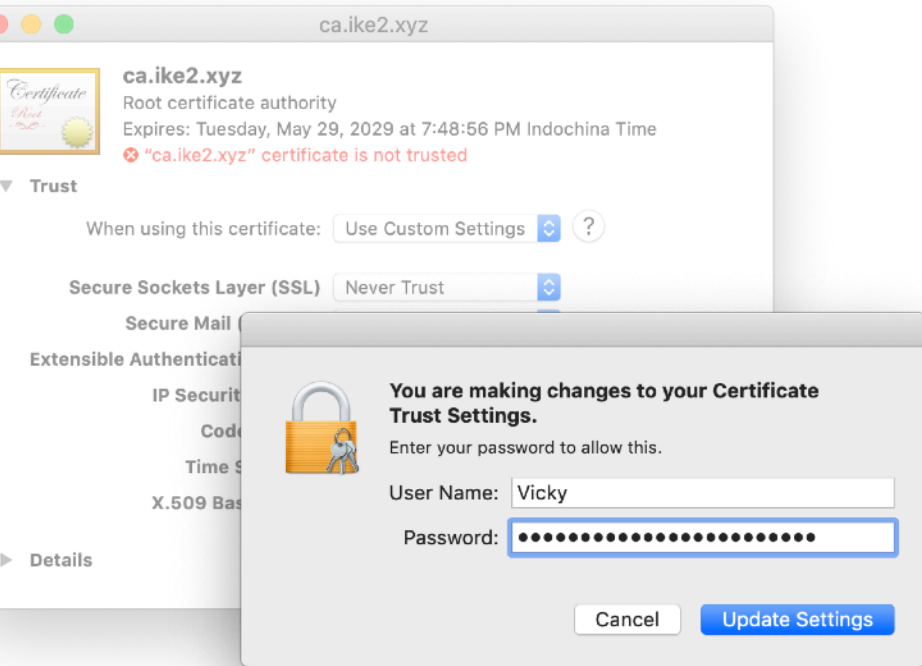


✓ IP Security (IPSec)

✗ Everything else

# MacOS: Manage SSL certificates

Important



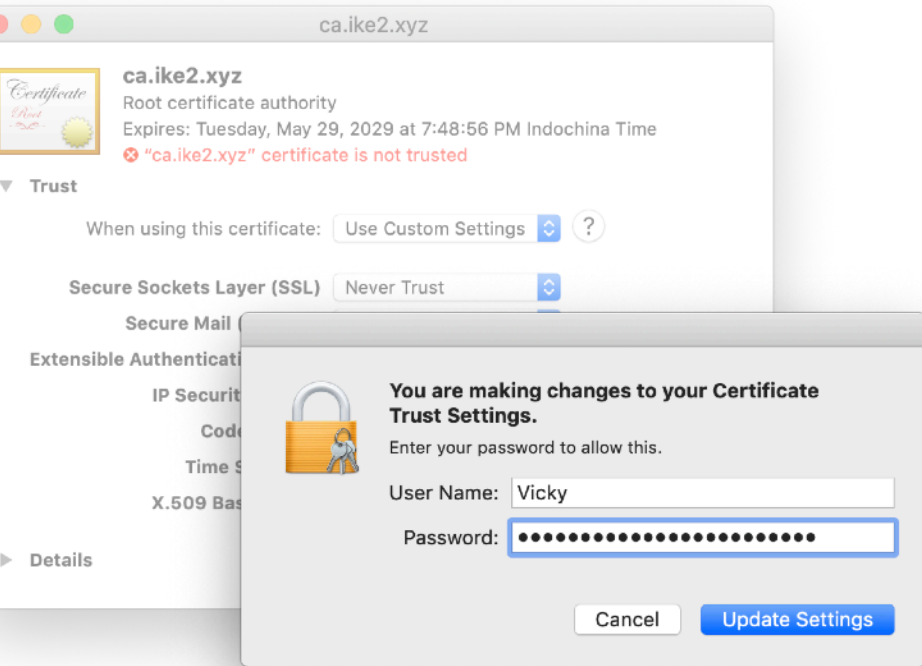
Keychain access

Type your  
MacOS password

—> Update settings

# MacOS: Manage SSL certificates

Important



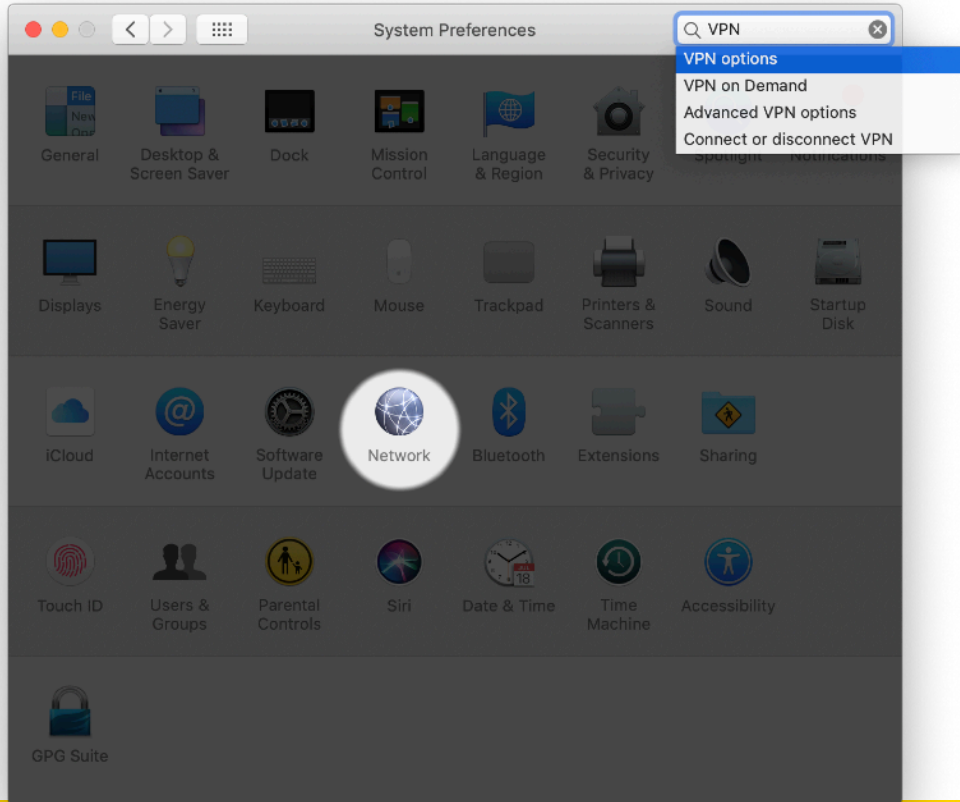
Keychain access

Type your  
MacOS password

—> Update settings

# MacOS: Setup IKEv2 VPN connection

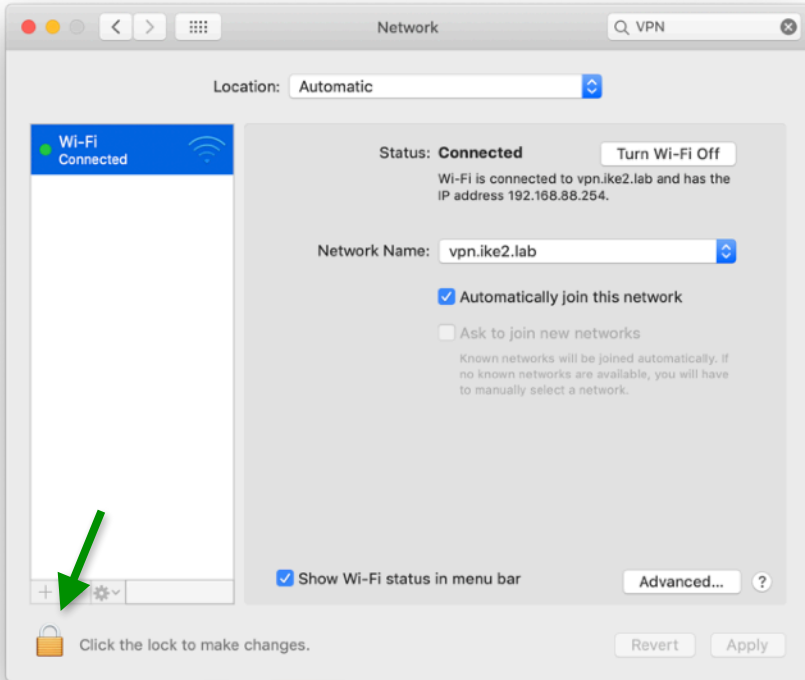
— — —



System preferences ->  
Network



# MacOS: Setup IKEv2 VPN connection

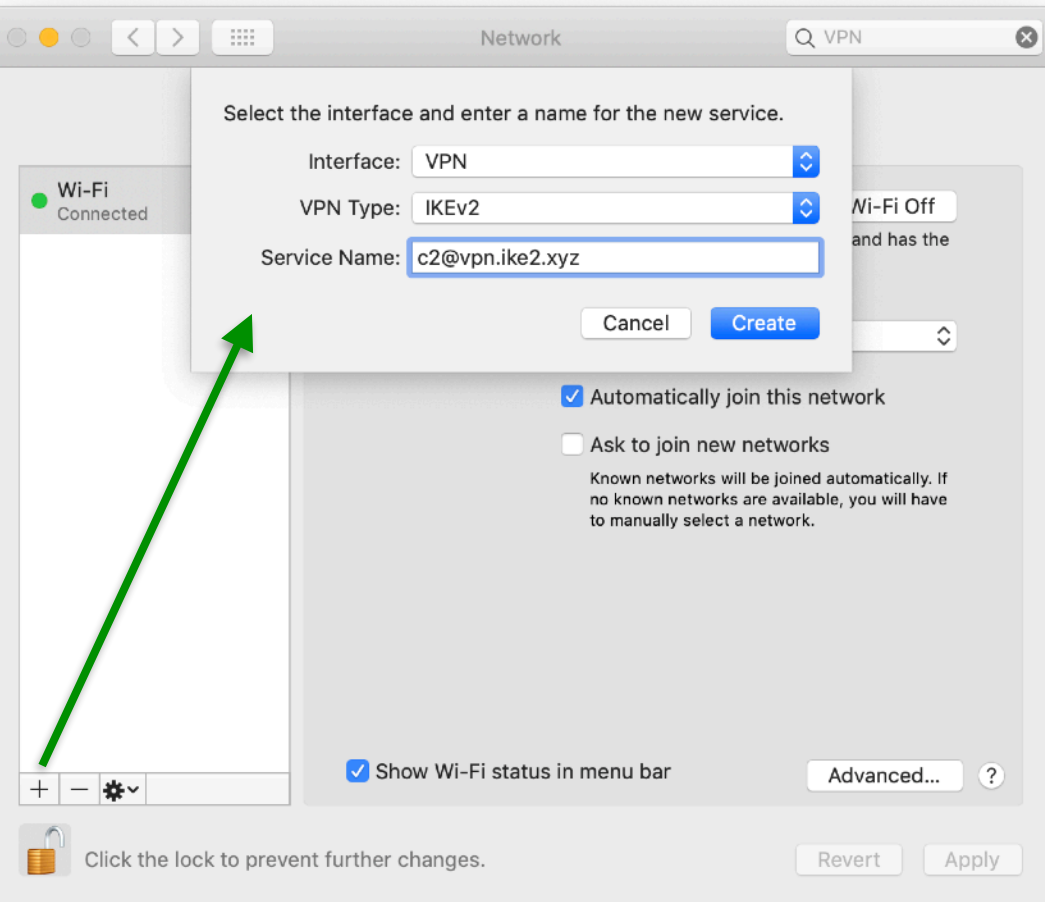


Unlock to make changes

User Name:

Password:

# MacOS: Setup IKEv2 VPN connection



Create new connection

Interface:

**VPN**

VPN Type:

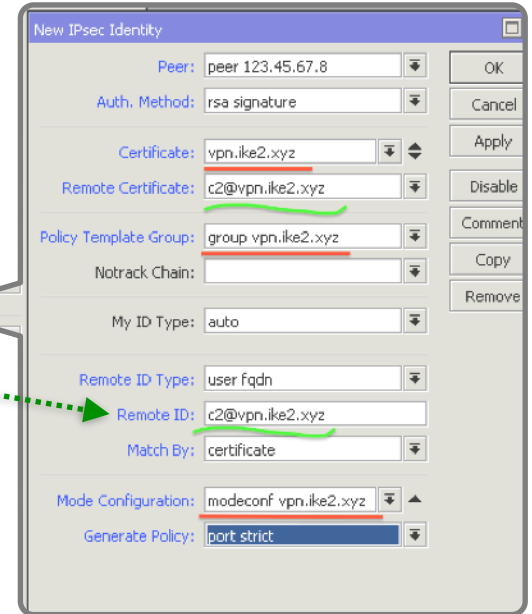
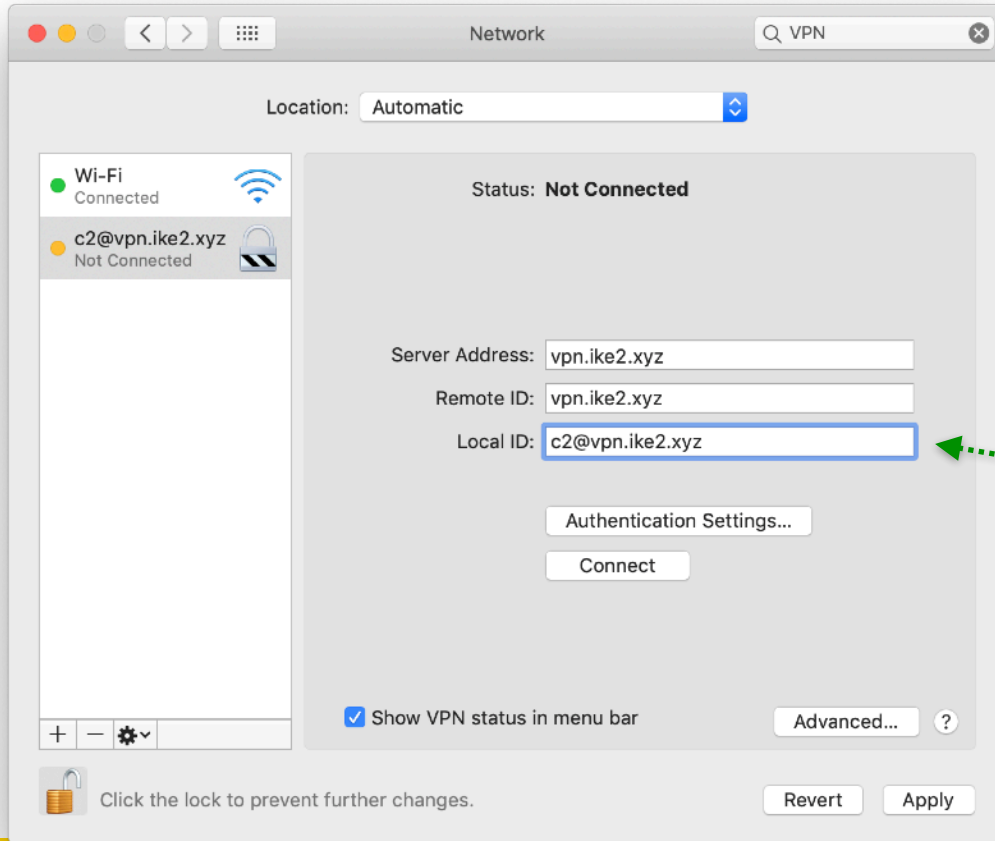
**IKEv2**

Service name:

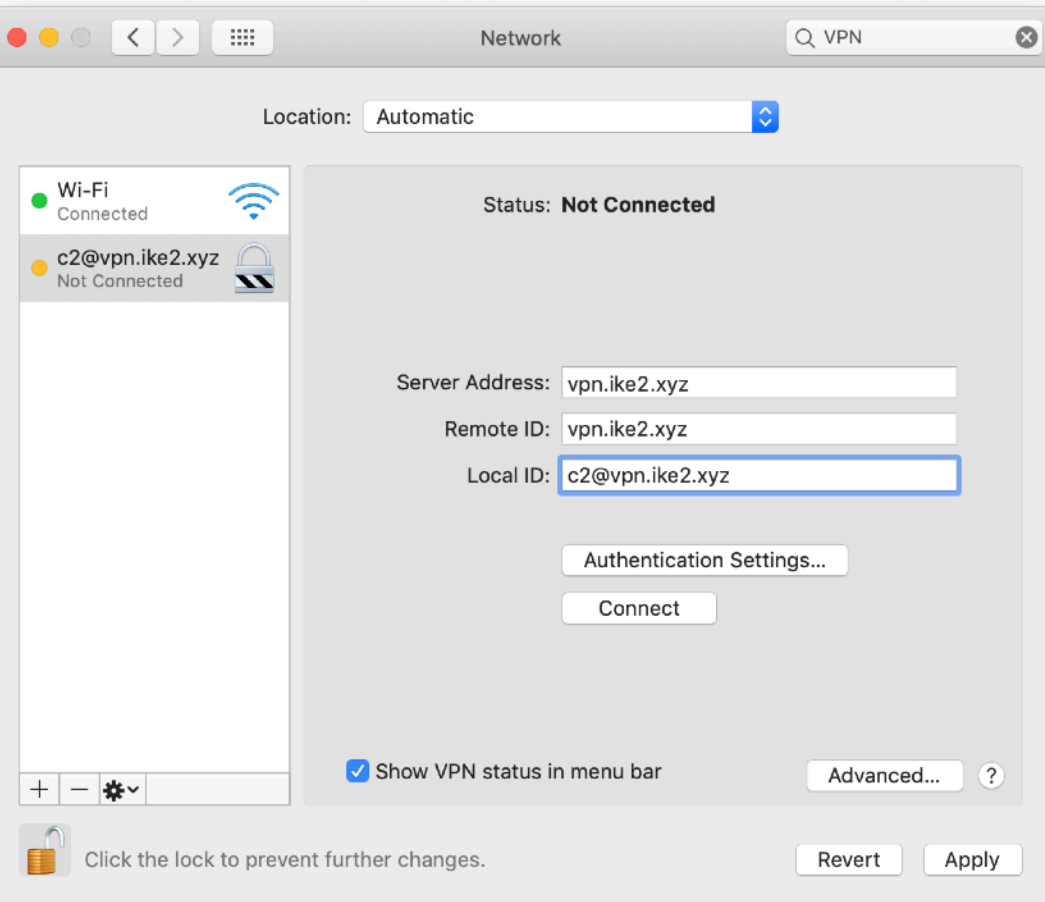
**c2@vpn.ike2.xyz**

→ **Create**

# MacOS: Setup IKEv2 VPN connection



# MacOS: Setup IKEv2 VPN connection



Create new connection

Server Address:

**vpn.ike2.xyz**

Remote ID:

**vpn.ike2.xyz**

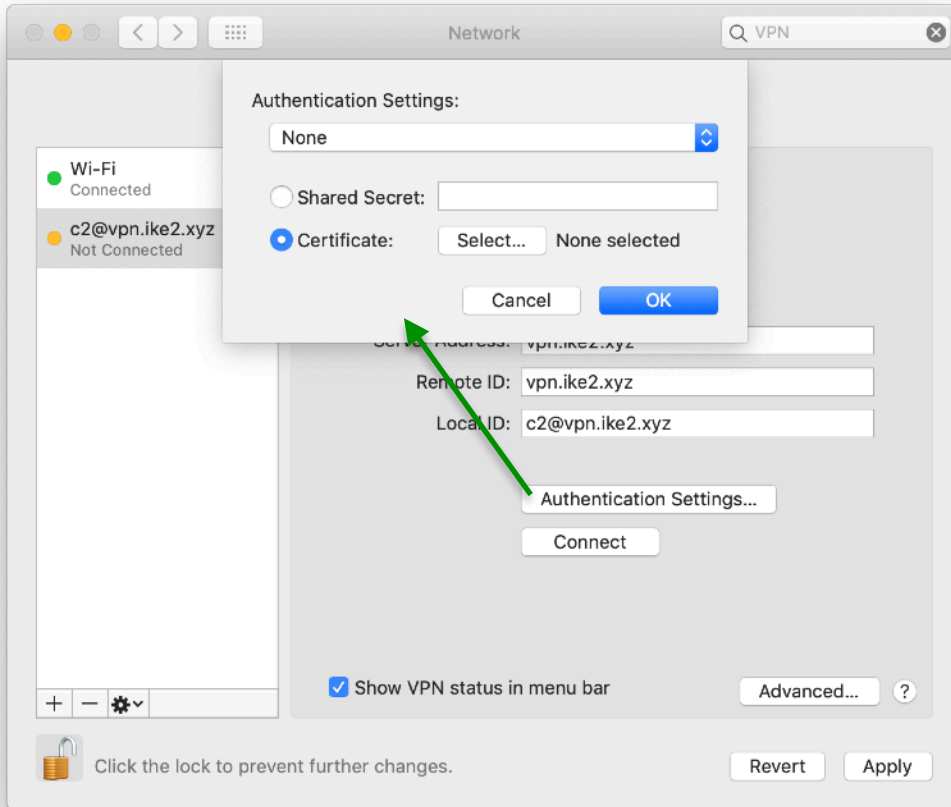
Local ID:

**c2@vpn.ike2.xyz**

✓ Show VPN status in menu bar

→ **Apply**

# MacOS: Setup IKEv2 VPN connection



## Authentication Settings

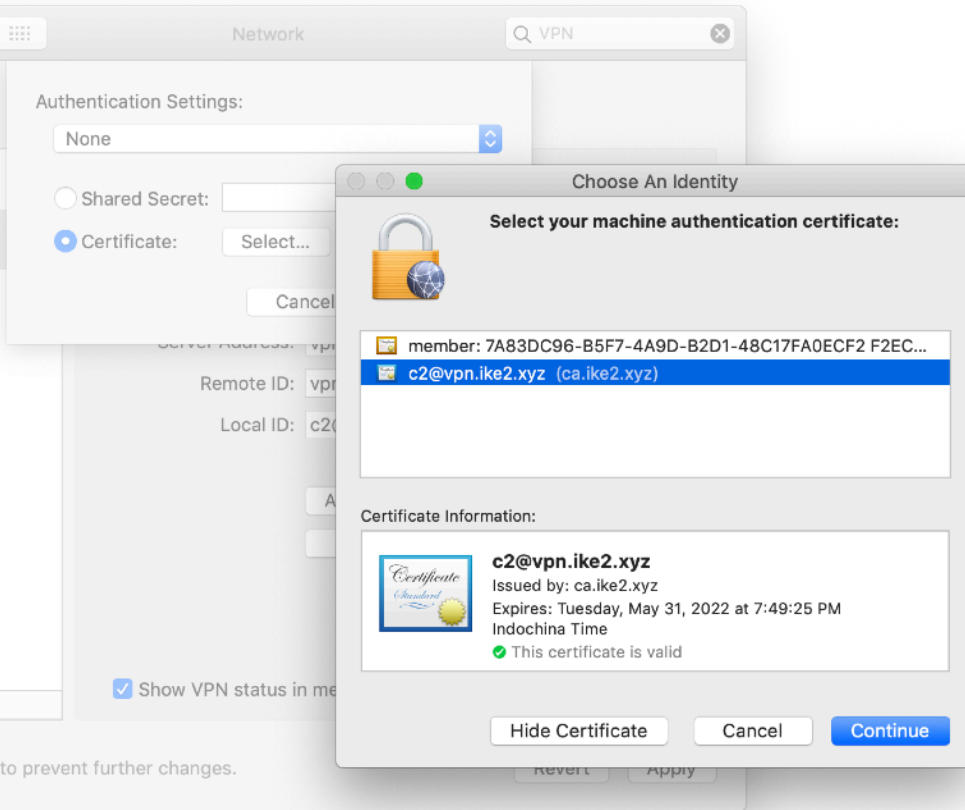
Authentication Settings:

**None**

Certificate:

→ **Select**

# MacOS: Setup IKEv2 VPN connection

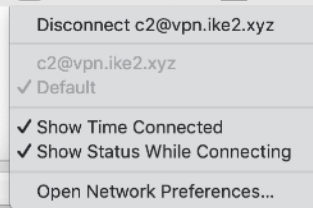
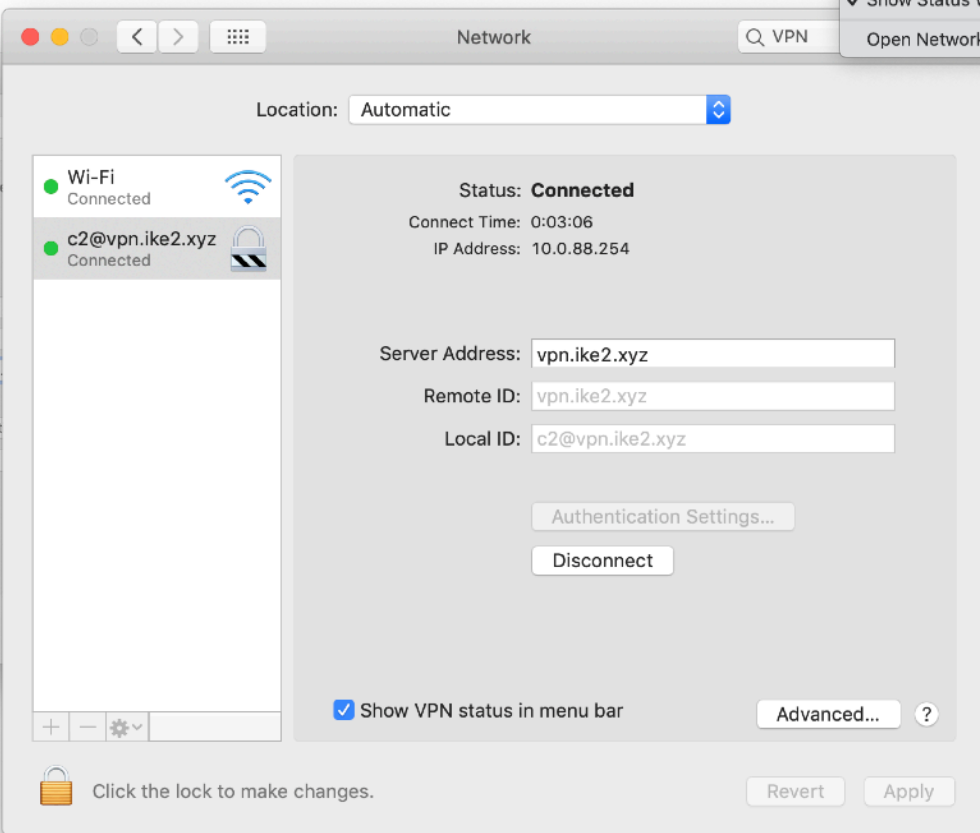
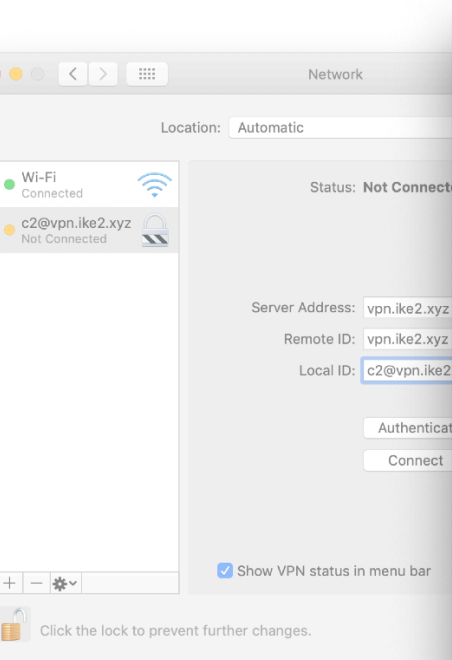



## Authentication Settings


Select machine auth certificate:  
**c2@vpn.ike2.xyz**

→ **Continue**

# MacOS: Connecting IKEv2 VPN



 Don't forget to lock settings

 Click the lock to make changes.

# MacOS: Check IKEv2 VPN routes

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz

- ✓ Default
- ✓ Show Time Connected
- ✓ Show Status While Connecting

Open Network Preferences...

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU: 1%

IPsec

Name	Resp...	Address Pool	Address	Address Pr...	Split Include	System ...
modeconf vpn.ike...	yes	pool vpn.ike2.xyz		32	192.168.99.0/24, 17...	yes
request-only	no					

IPsec Mode Config <modeconf vpn.ike2.xyz>

Name: modeconf vpn.ike2.xyz

Responder

Address Pool: pool vpn.ike2.xyz

Address:

Address Prefix Length: 32

Split Include: 192.168.99.0/24, 172.16.0.0/22, 10.20.0.0/21

System DNS

```

➔ ~ netstat -nr |grep ipsec
default          link#23          UCSI             0             0 ipsec0
10.0.88.254      10.0.88.254     UH              3             0 ipsec0
10.20/21         10.0.88.254     UGSc           0             0 ipsec0
172.16/22        10.0.88.254     UGSc           0             0 ipsec0
192.168.99       10.0.88.254     UGSc           0             0 ipsec0
224.0.0/4        link#23          UmCSI          0             0 ipsec0
255.255.255.255/32 link#23          UCSI           0             0 ipsec0
➔ ~
    
```



# MacOS: Check IKEv2 VPN routes

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz  
 Default

Show Time Connected  
 Show Status While Connecting

Open Network Preferences...

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Dashboard

Session: 192.168.88.1 CPU: 3%

IPsec

Peers Identities Profiles Remote Peers Mode Configs Installed SAs Keys ...

Name	Resp...	Address Pool	Address	Address Pr...	Split Include
modeconf vpn.ike...	yes	pool vpn.ike2.xyz		32	0.0.0.0/0
request-only	no				

IPsec Mode Config <modeconf vpn.ike2.xyz>

Name: modeconf vpn.ike2.xyz

Responder

Address Pool: pool vpn.ike2.xyz

Address:

Address Prefix Length: 32

Split Include: 0.0.0.0/0

System DNS

Static DNS: 10.0.88.1

```
~ netstat -nr |grep ipsec
default      link#23      UCS          1614         0 ipsec0
1.           9            link#23      UHW3I       0            1 ipsec0
1.          159          link#23      UHW3I       0            1 ipsec0
1.          .112        link#23      UHW3I       0            1 ipsec0
1.          .222        link#23      UHW3I       0            1 ipsec0
1.          .131        link#23      UHW3I       0            1 ipsec0
1.          .22         link#23      UHW3I       0            1 ipsec0
1.          31          link#23      UHW3I       0            1 ipsec0
1.          143         link#23      UHW3I       0            1 ipsec0
2.          156         link#23      UHW3I       0            1 ipsec0
2.          64          link#23      UHW3I       0            1 ipsec0
2.          27          link#23      UHW3I       0            1 ipsec0
2.          01          link#23      UHW3I       0            1 ipsec0
2.          204         link#23      UHW3I       0            1 ipsec0
2.          23          link#23      UHW3I       0            1 ipsec0
2.          5           link#23      UHW3I       0            1 ipsec0
2.          53          link#23      UHW3I       0            1 ipsec0
2.          21          link#23      UHW3I       0            1 ipsec0
2.          33          link#23      UHW3I       0            1 ipsec0
2.          .111        link#23      UHW3I       0            5 ipsec0
2.          .62         link#23      UHW3I       0            1 ipsec0
2.          100         link#23      UHW3I       0            1 ipsec0
2.          95          link#23      UHW3I       0            1 ipsec0
```

# Apple iOS

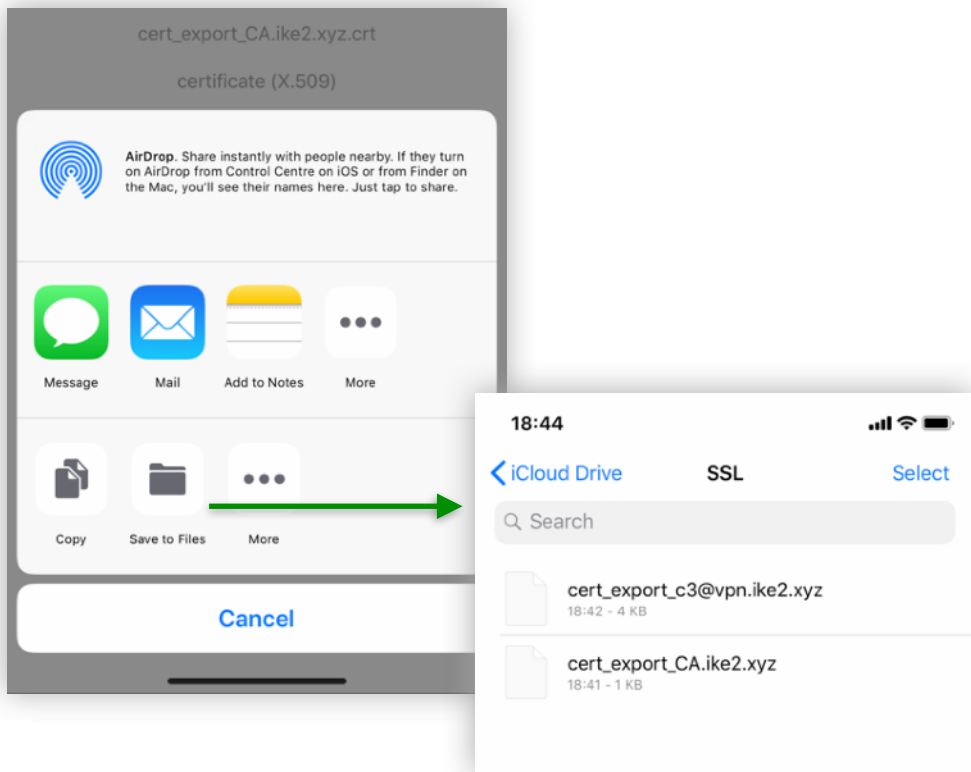
≥ version 9

Agenda for next slides

1. Import SSL certificates
2. Setup IKEv2 VPN connection



# iOS: Import SSL certificates

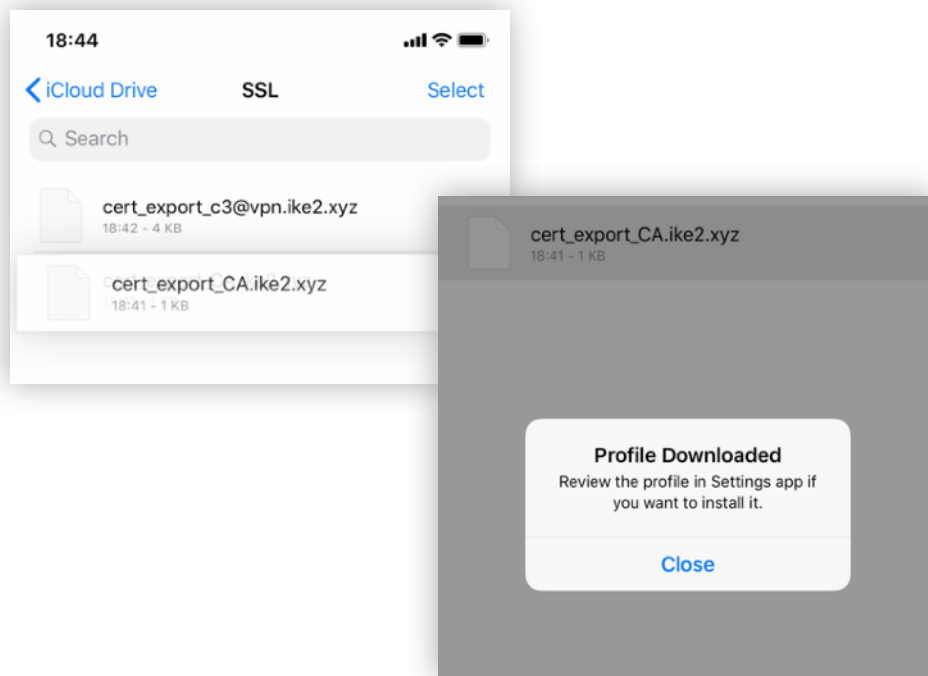


Download **CA** certificate .crt

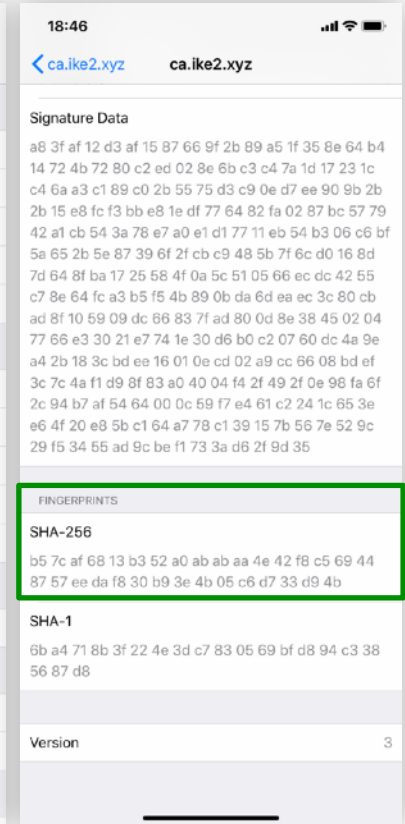
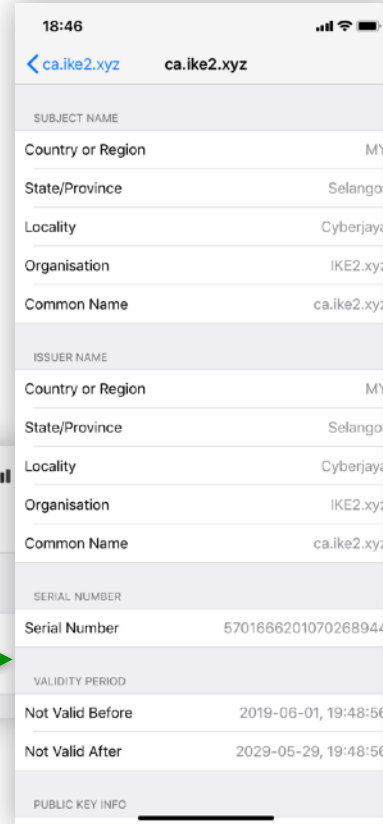
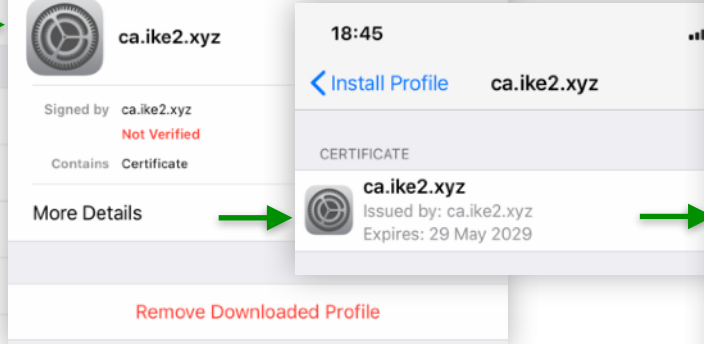
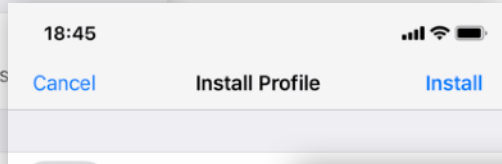
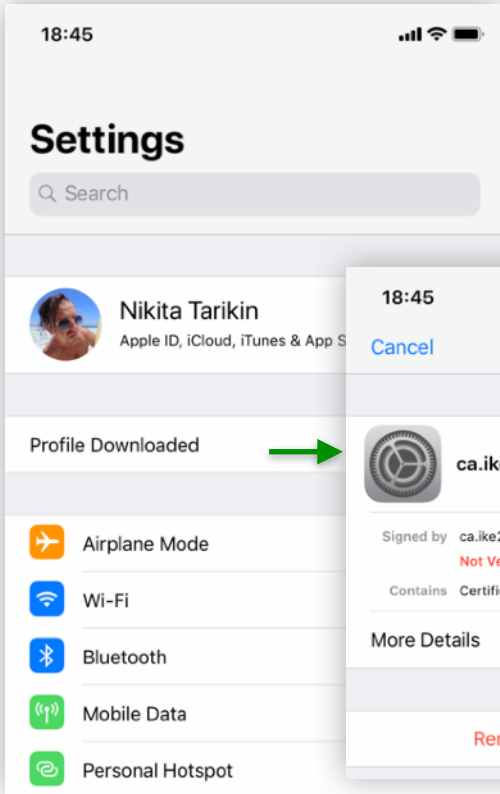
Download **client** certificate .p12

# iOS: Import CA SSL certificate

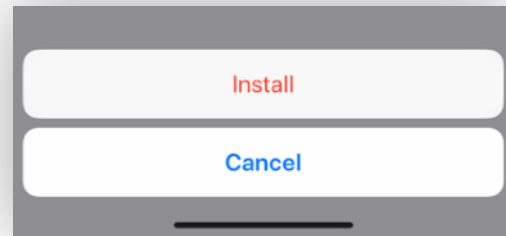
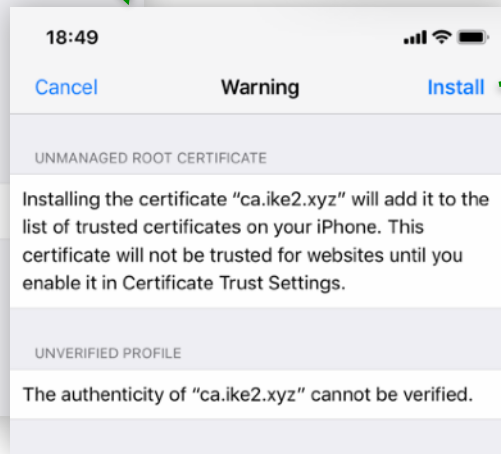
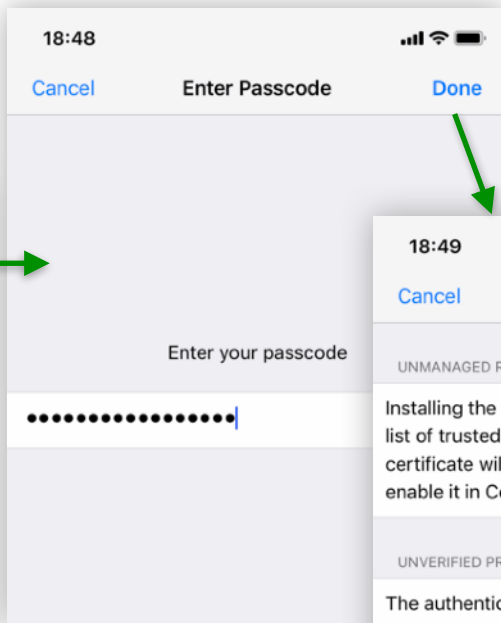
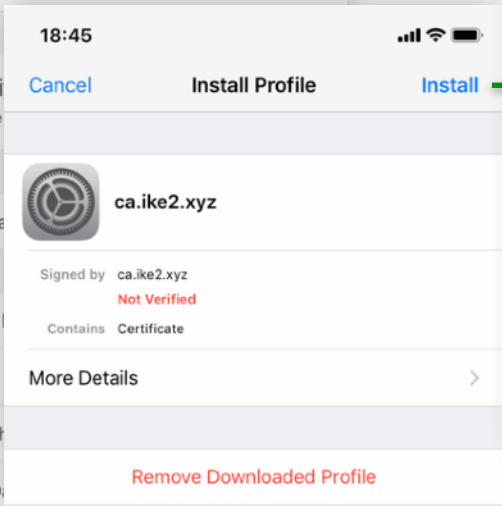
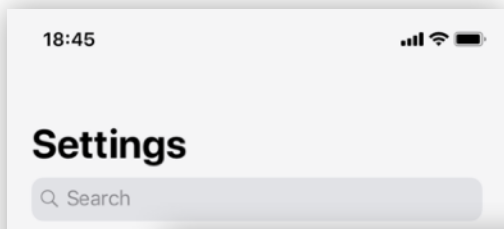
— — —



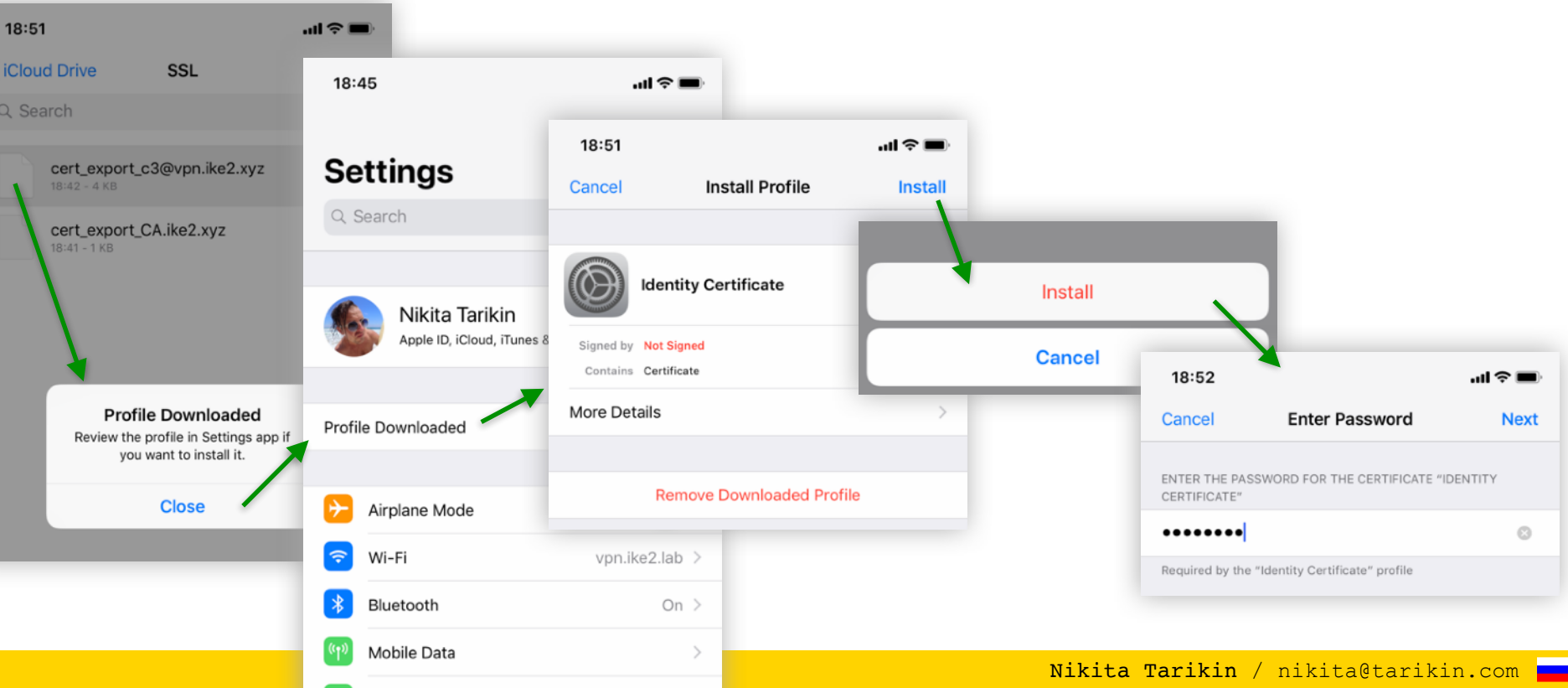
# iOS: Import CA SSL certificate



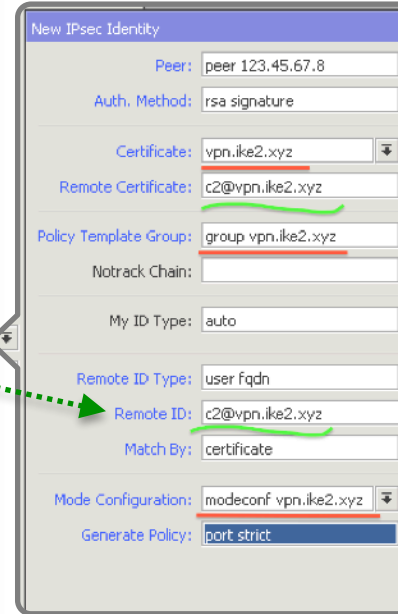
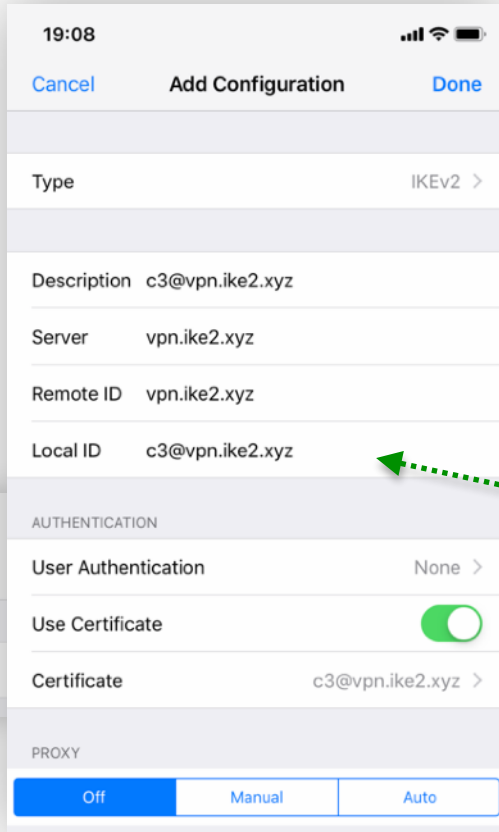
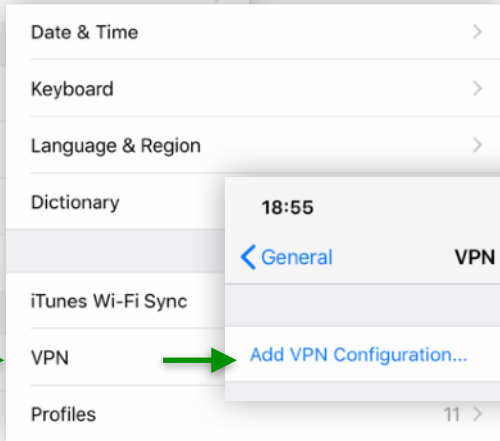
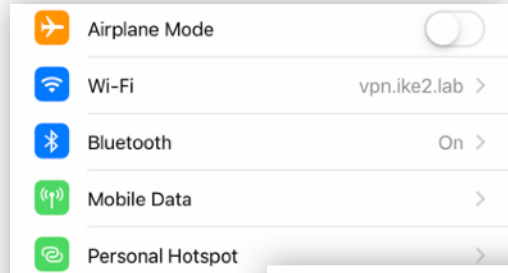
# iOS: Import CA SSL certificate



# iOS: Import client SSL certificate

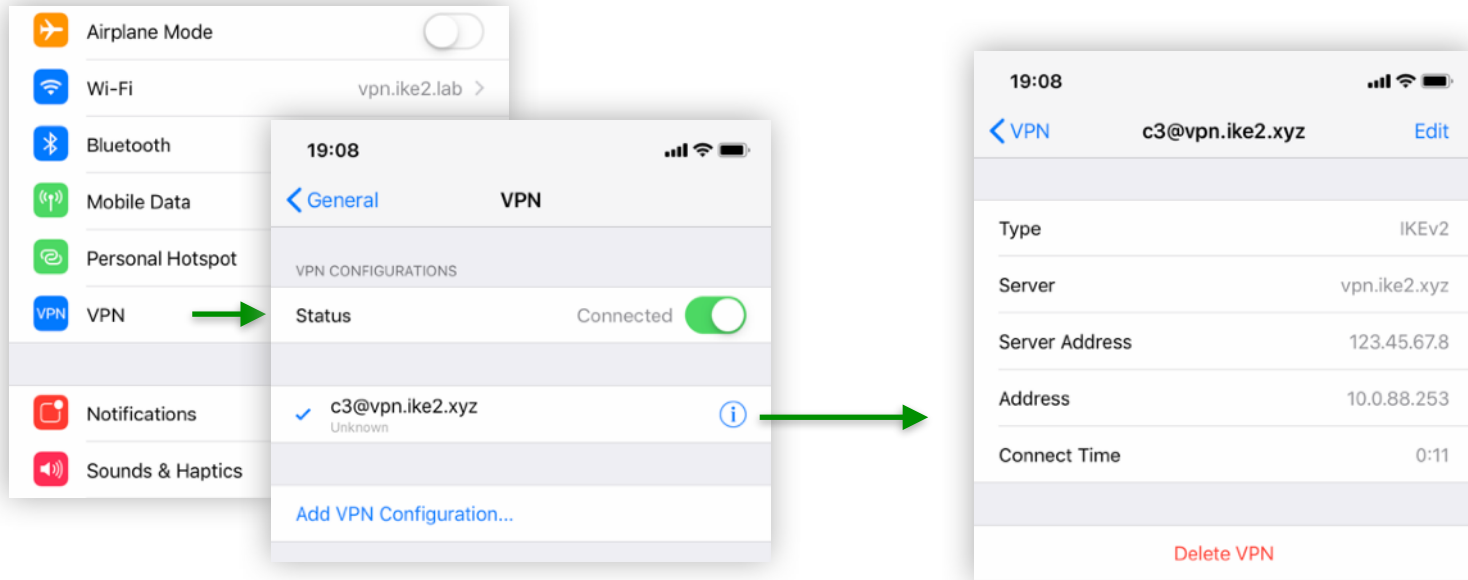


# iOS: Setup IKEv2 VPN connection





# iOS: Connect IKEv2 VPN



# Android

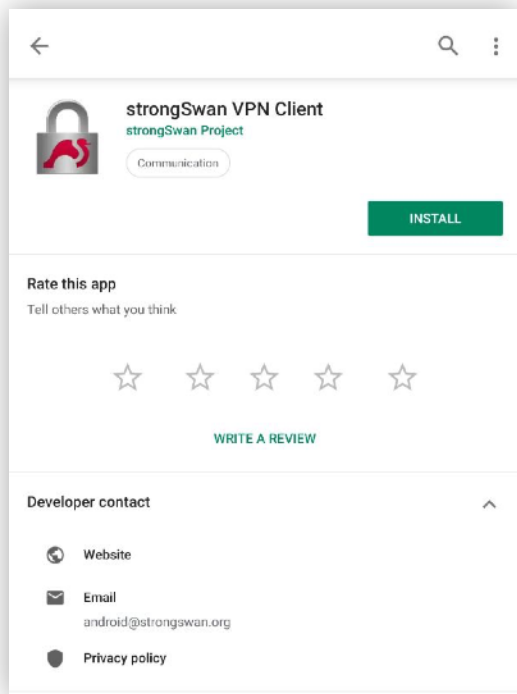
## Agenda for next slides

1. Install 3rd party app StrongSwan
2. Import SSL certificates
3. Setup IKEv2 VPN connection



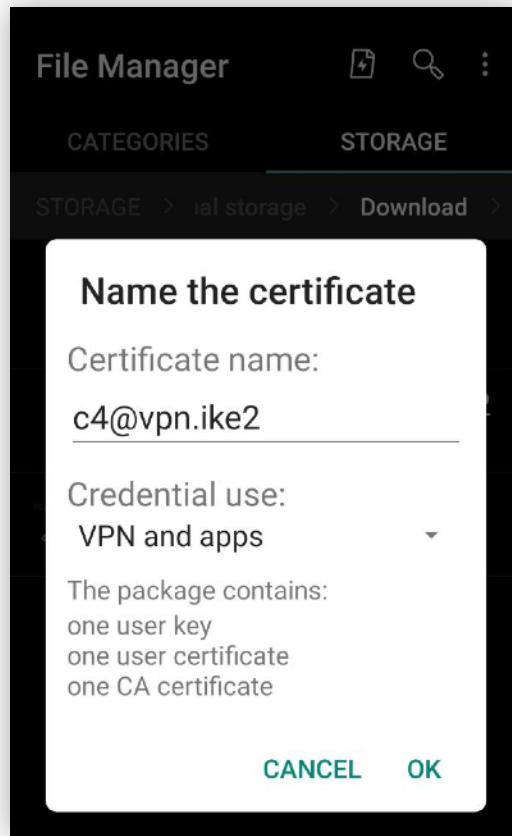
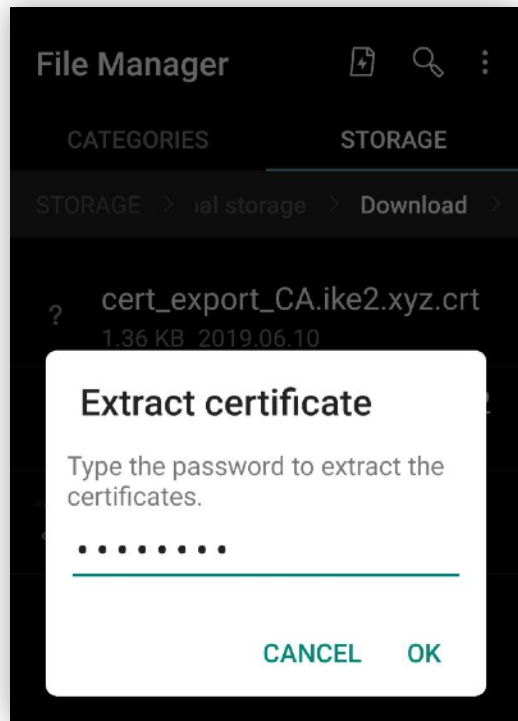
# Android: Install StrongSwan

— — —



Find **StrongSwan** app on the Google Play

# Android: Import SSL certificates



Download and install

**user certificate .p12**

# Android: Setup IKEv2 VPN connection

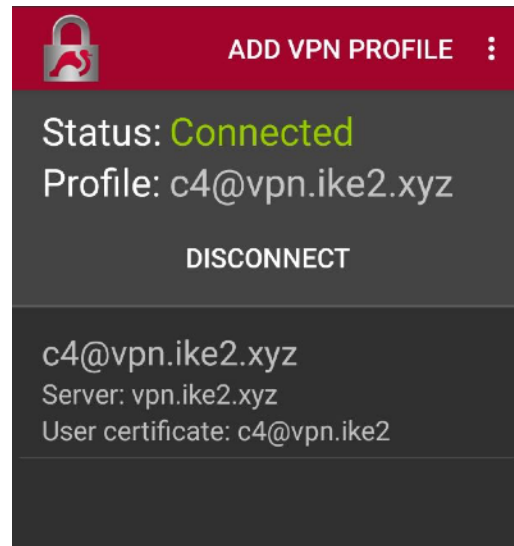
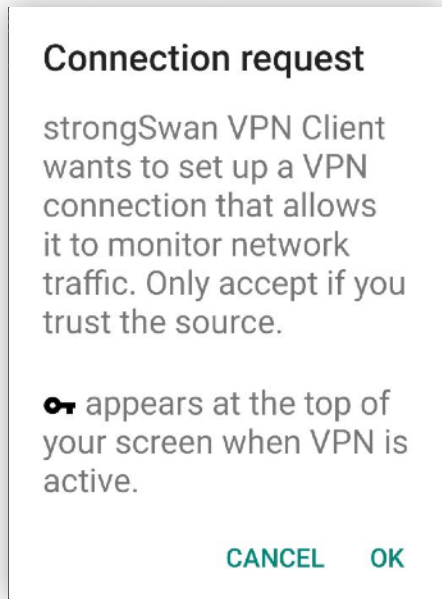
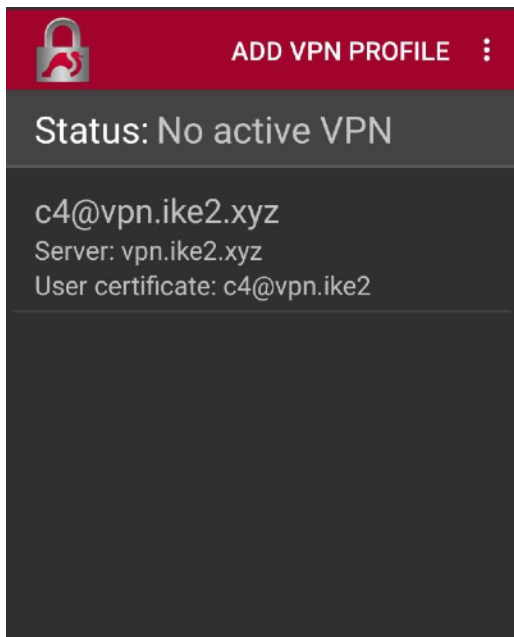
**ADD VPN PROFILE** :  
Status: No active VPN  
No VPN profiles.

**Add VPN pro...** SAVE CANCEL  
Server  
vpn.ike2.xyz  
VPN Type  
IKEv2 Certificate  
User certificate  
c4@vpn.ike2  
CN=c4@vpn.ike2.xyz  
User identity  
Default (CN=c4@vpn.ike2.xy..  
CA certificate  
 Select automatically  
Profile name (optional)  
c4@vpn.ike2.xyz  
Defaults to "vpn.ike2.xyz"  
 Show advanced settings

**Choose certificate**  
The app strongSwan VPN Client has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.  
 c4@vpn.ike2  
CN=c4@vpn.ike2.xyz  
+ Install certificate  
DENY SELECT

# Android: Connect IKEv2 VPN

---



The end \\_(ツ)\_/

YouTube video for this presentation is available

<https://mum.mikrotik.com/2019/MY/agenda/EN>



Please  
contact me

**E-mail me:**

nikita@tarikin.com

**Add me to your Facebook:**

Nikita Tarikin

**Follow me on Instagram:**

@tarikin

**Start private conversation:**

 **Telegram** [t.me/tarikin](https://t.me/tarikin)

 **Messenger** Nikita Tarikin



Please  
contact me

**Nikita Tarikin**

`nikita@tarikin.com`



# Demo lab

Request your certificate via form

<https://forms.gle/nZTDK2wex5nneqo6A>

