MikroTik IPSec ike2 VPN server

Easy and clear step-by-step guide

Nikita Tarikin / nikita@tarikin.com

Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia

Nikita Tarikin / nikita@tarikin.com

Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia

Since 2016

MTCNA 90%

MTCRE 93%

MTCWE 84%

MTCTCE 76%

MTCUME 90%

Nikita Tarikin / nikita@tarikin.com

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%

Nikita Tarikin / nikita@tarikin.com

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

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?

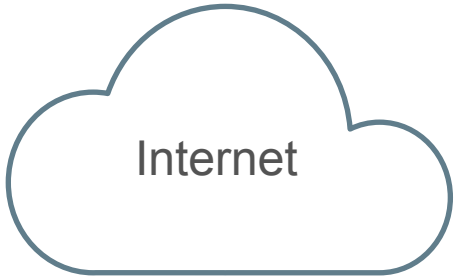
1. Blazing fast throughput performance
2. Instant connection establishment
3. Military grade security standards
4. Supported by most modern OS’s
5. Can push routes to clients
6. Bypasses any NAT
7. Mobile friendly

Network diagram

Networking for dummies 😀

My laptop

Magic

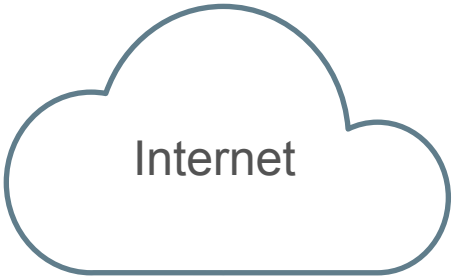


Internet

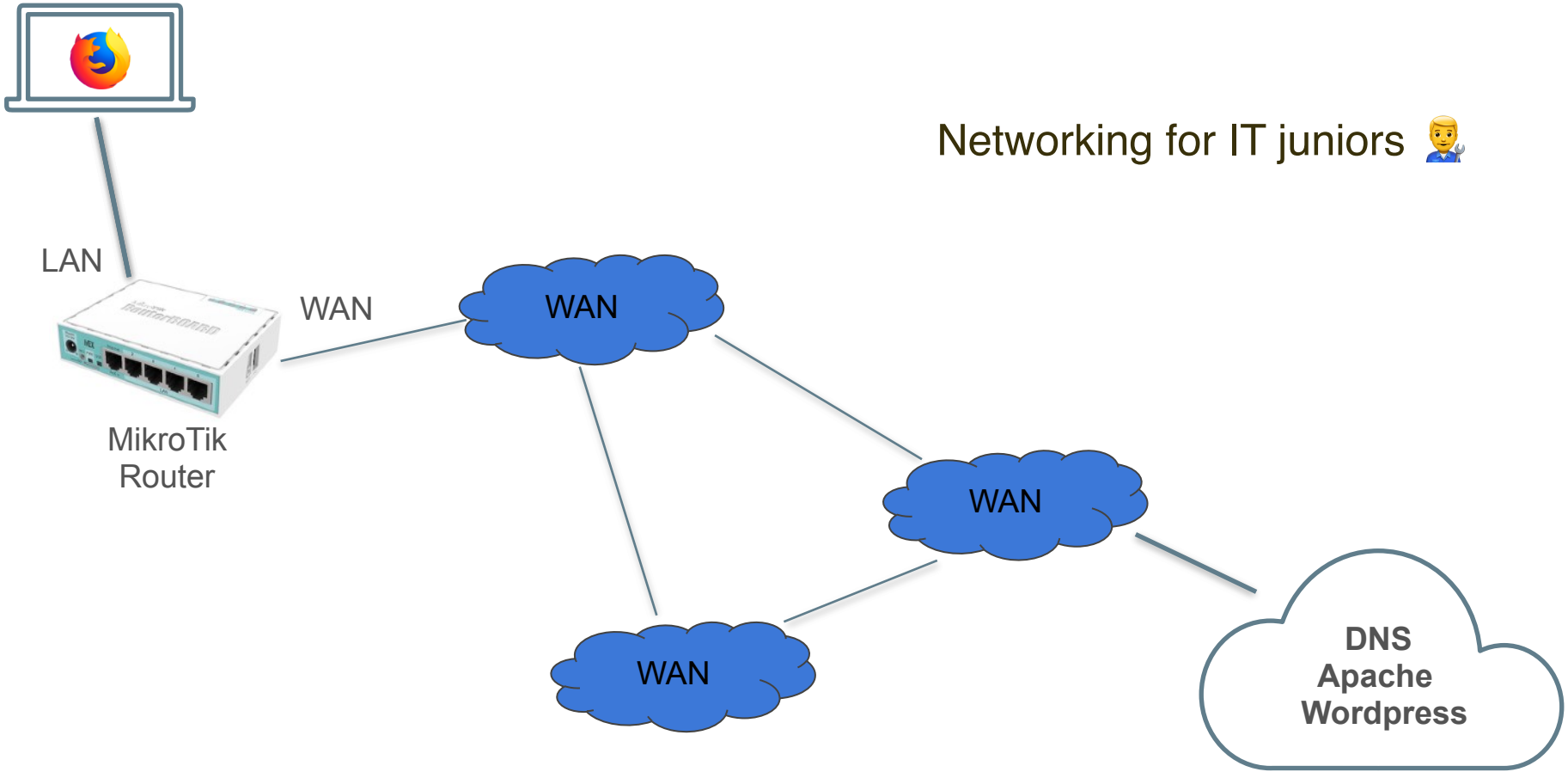
Networking for advanced users 😎

My laptop

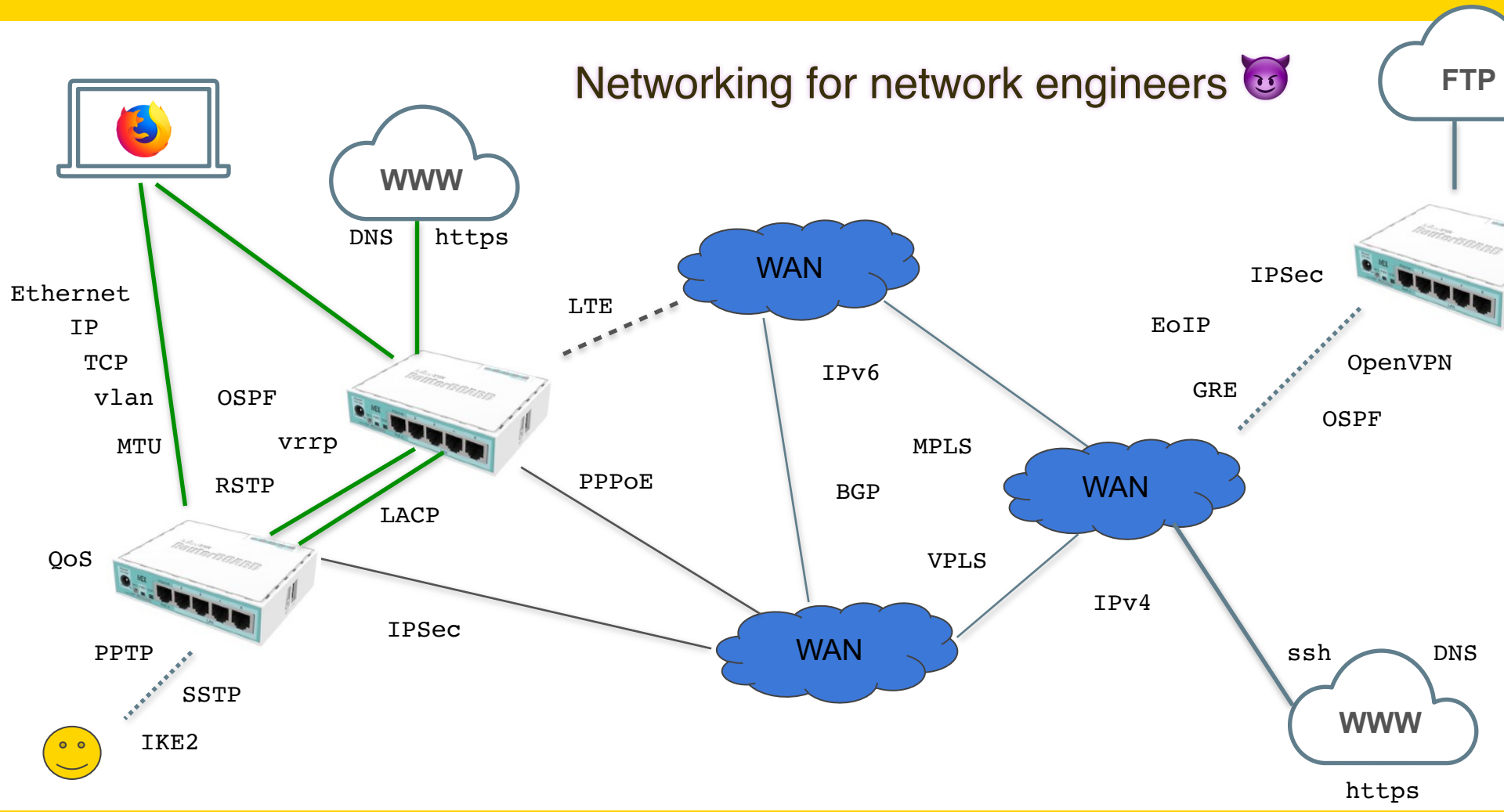
My router

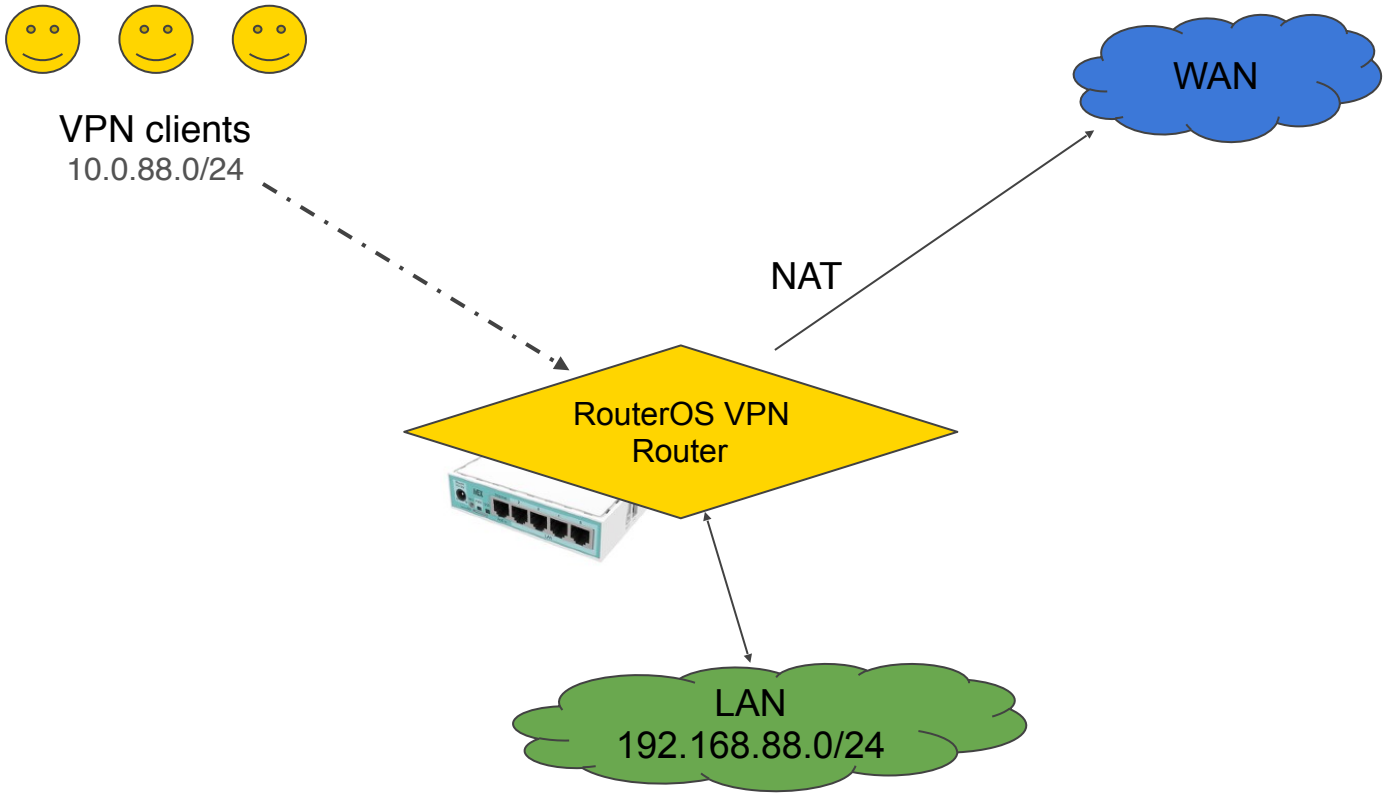


Networking for IT juniors 👨‍🔧

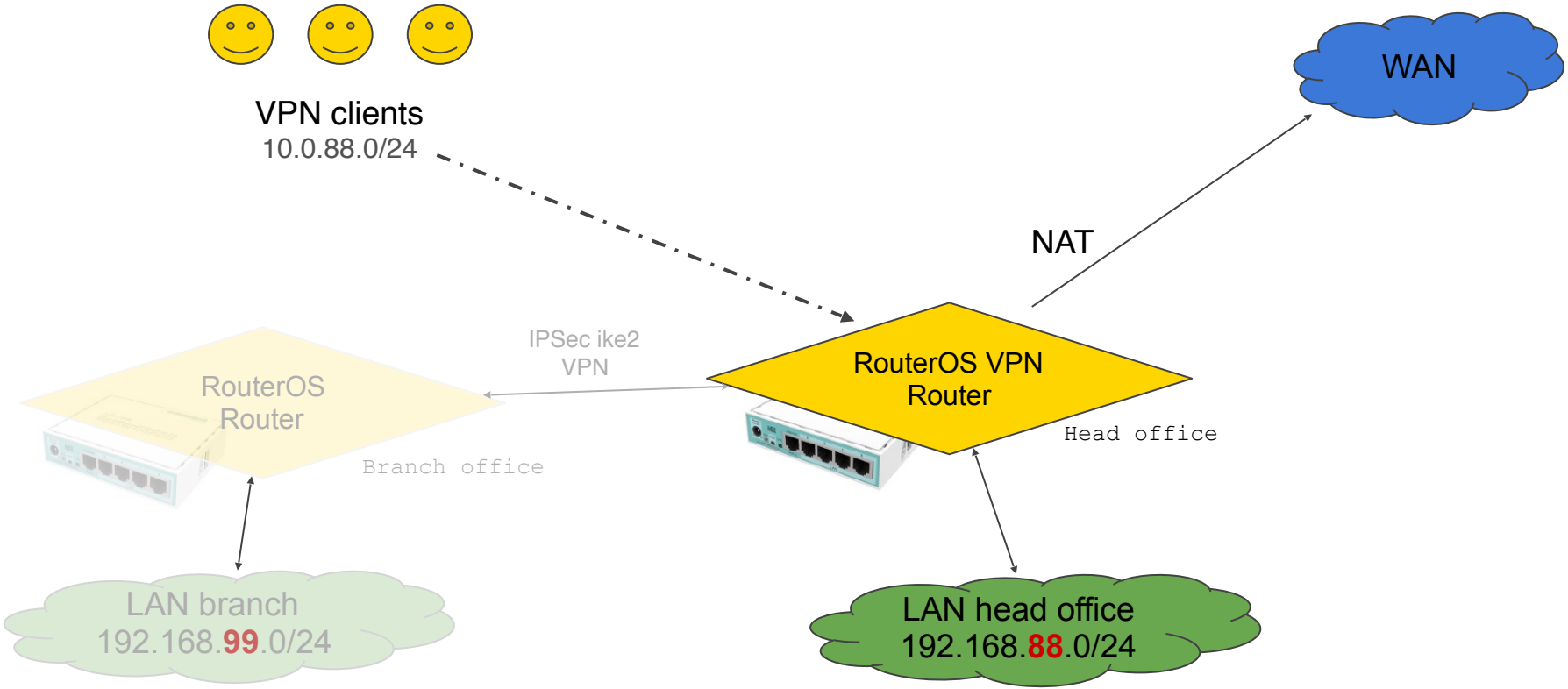


Networking for network engineers





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

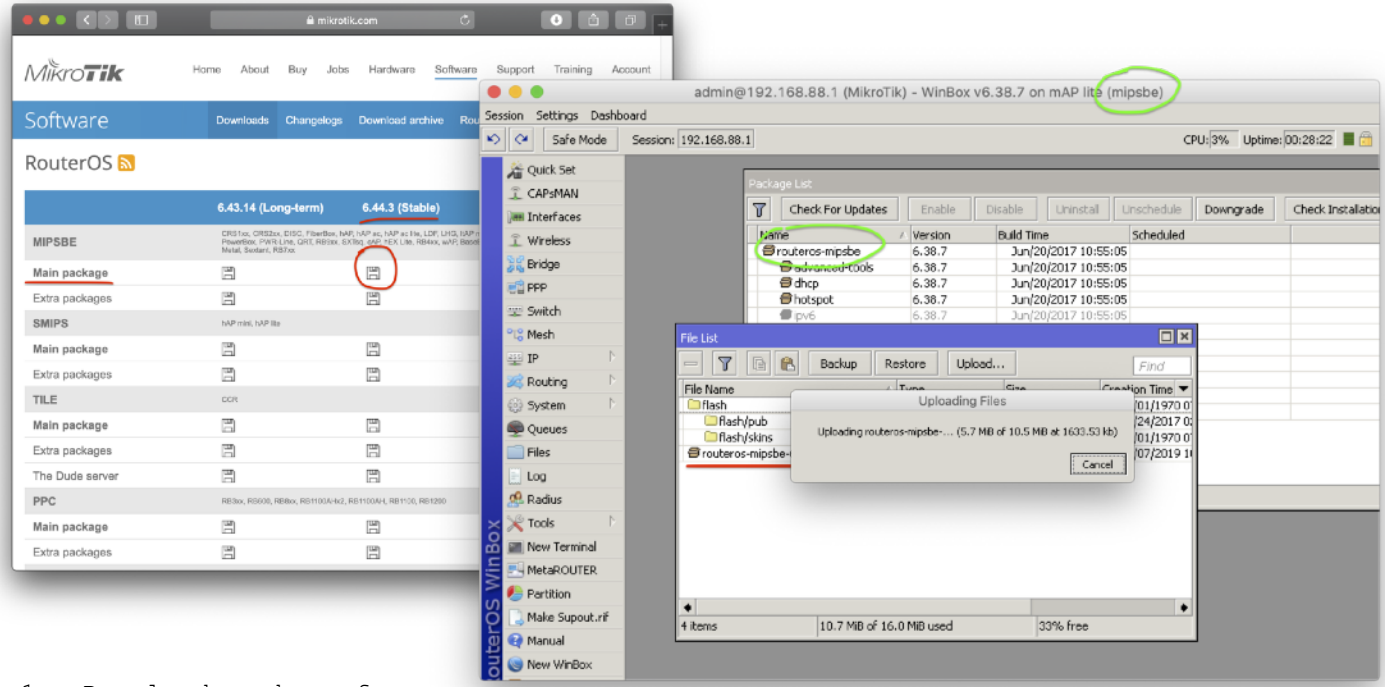
Nikita Tarikin / nikita@tarikin.com

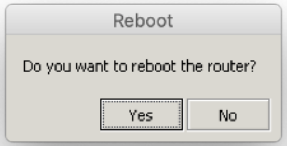
Before you start

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

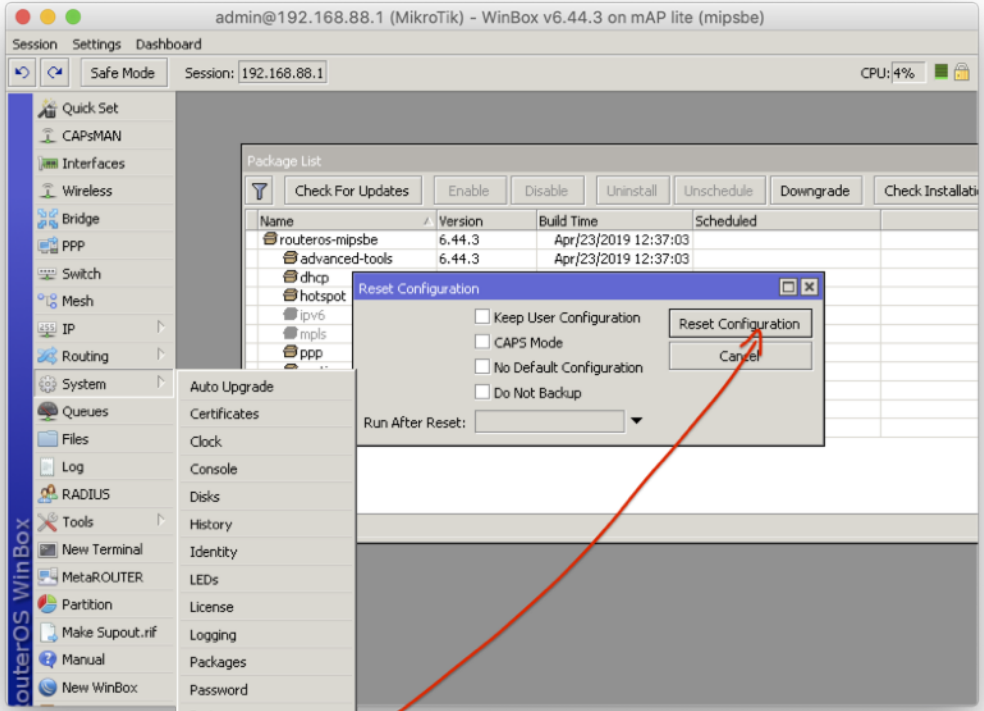
Upgrade RouterOS to 6.44+



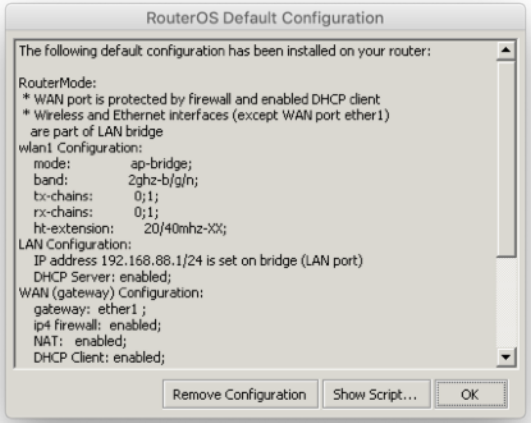


1. Download package from www.mikrotik.com/download
2. Upload package to / of your RouterBoard
3. System -> Reboot

Reset RouterBoard to default v6.44+ configuration



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



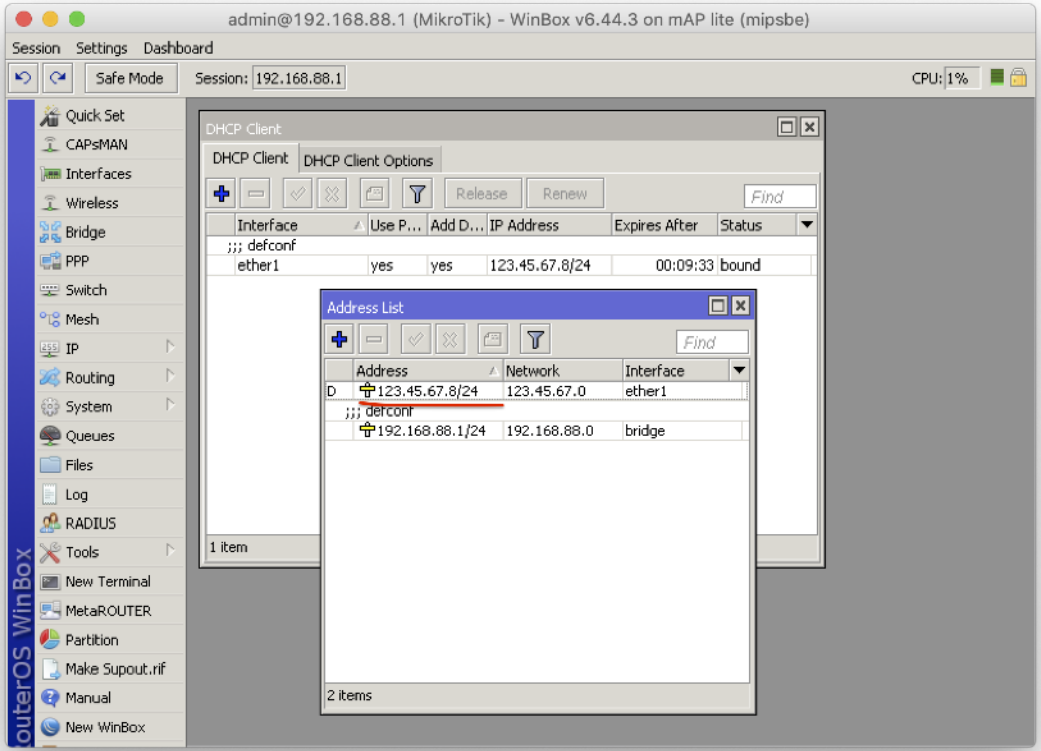
`System -> Reset configuration`

General system settings

Agenda for next slides:

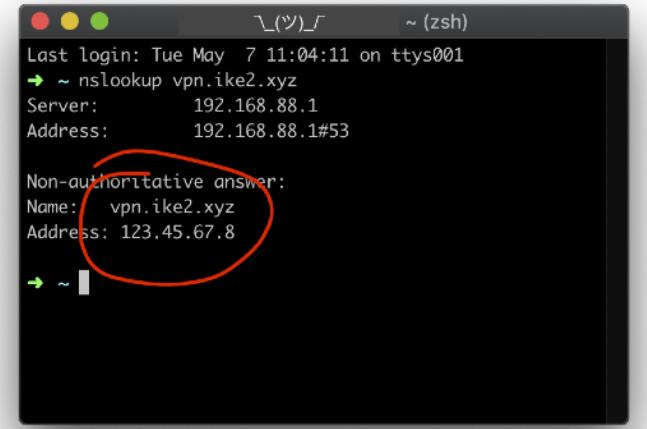
1. WAN IP/DNS addresses
2. Timezone
3. NTP
4. Loopback bridge
5. IP pool

WAN IP and DNS addresses for IKE2 VPN server



123.45.67.8 is on WAN interface

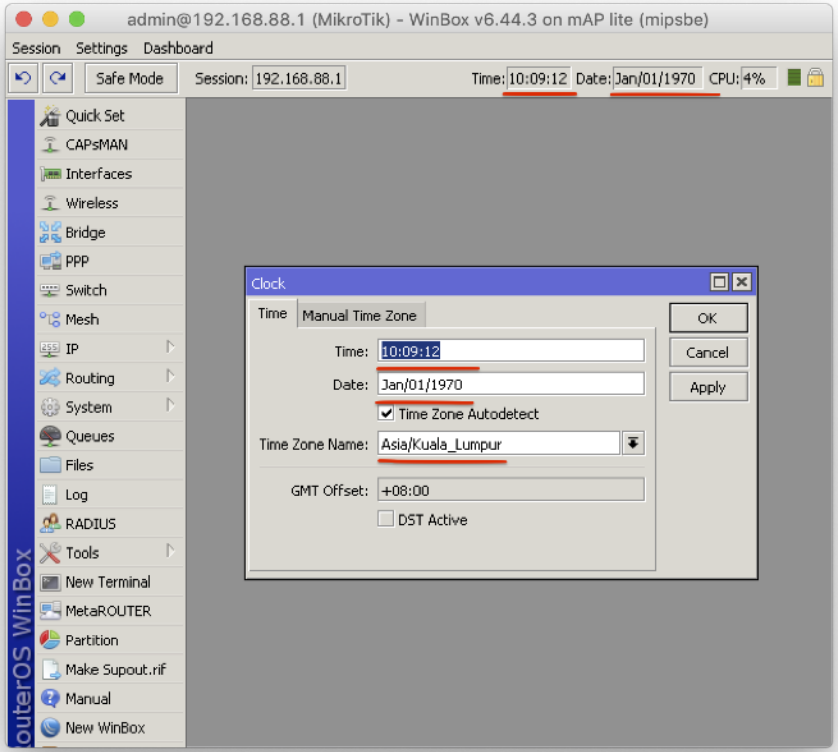
Check DNS records:
Name: **vpn.ike2.xyz**
Address: **123.45.67.8**



* Set DNS records with your domain name registrar control panel

Setup correct timezone

Important

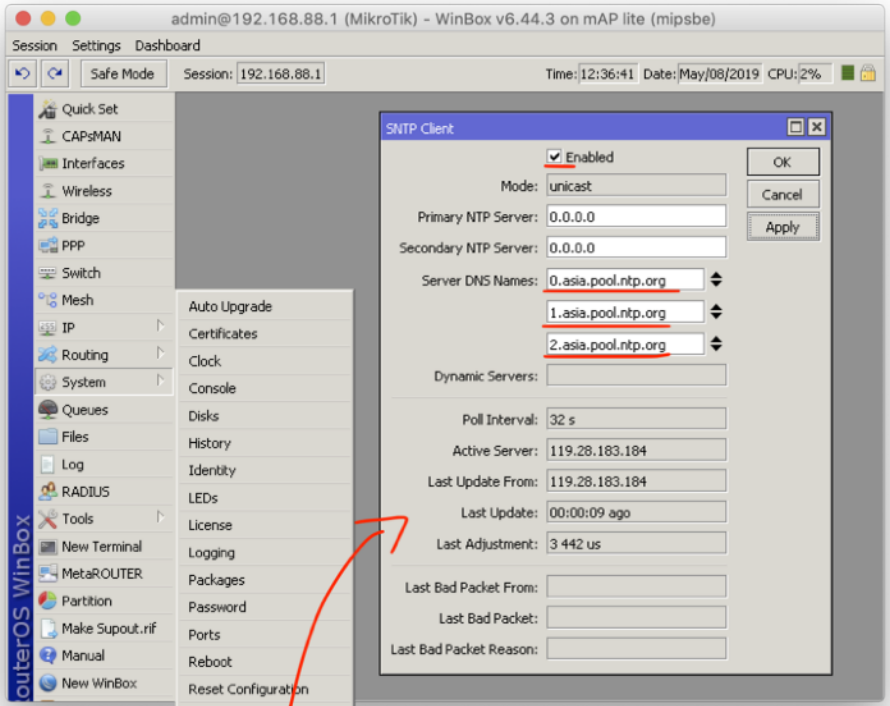


System -> Clock

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

Setup auto date/time

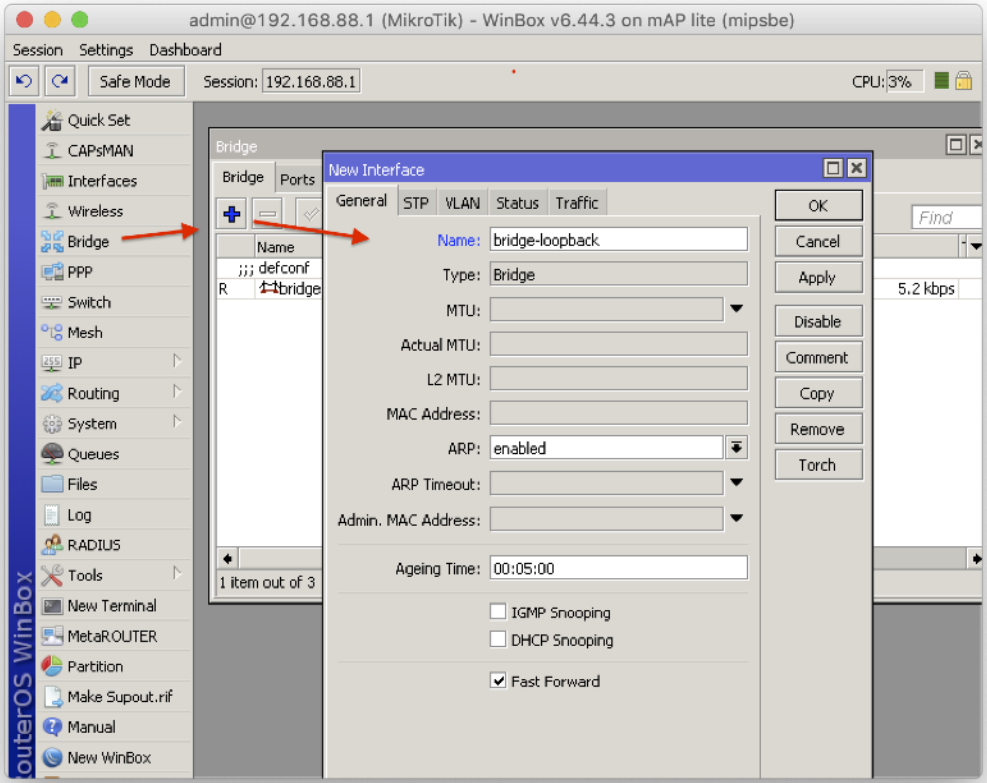
Important



Activate NTP client

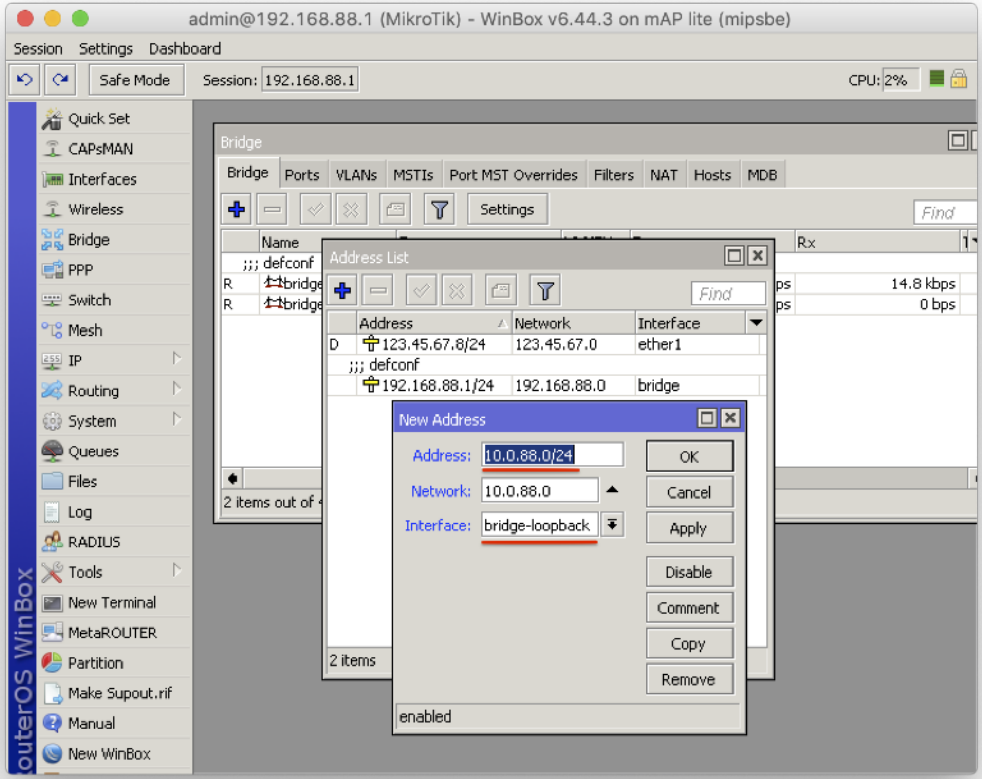
```
/system ntp client set enabled=yes
server-dns-names=0.asia.pool.ntp.org,
1.asia.pool.ntp.org,2.asia.pool.ntp.org
```

Add new loopback bridge



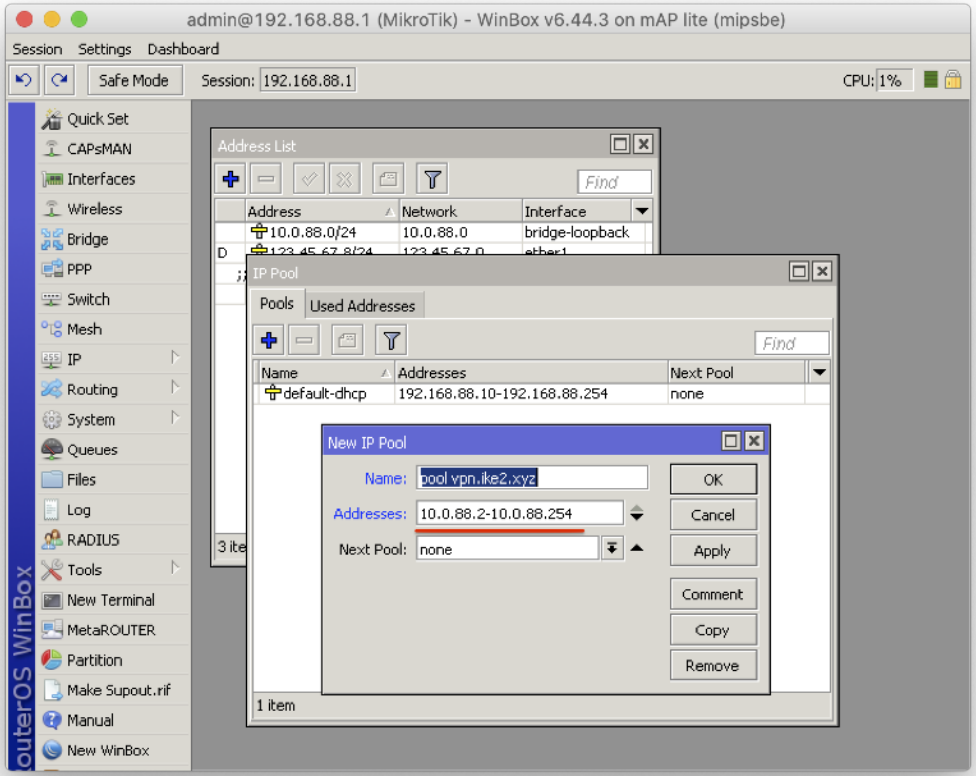

```
/interface bridge add
name=bridge-loopback
```

Set loopback bridge IP address




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

Add new IP Pool for ike2 VPN clients



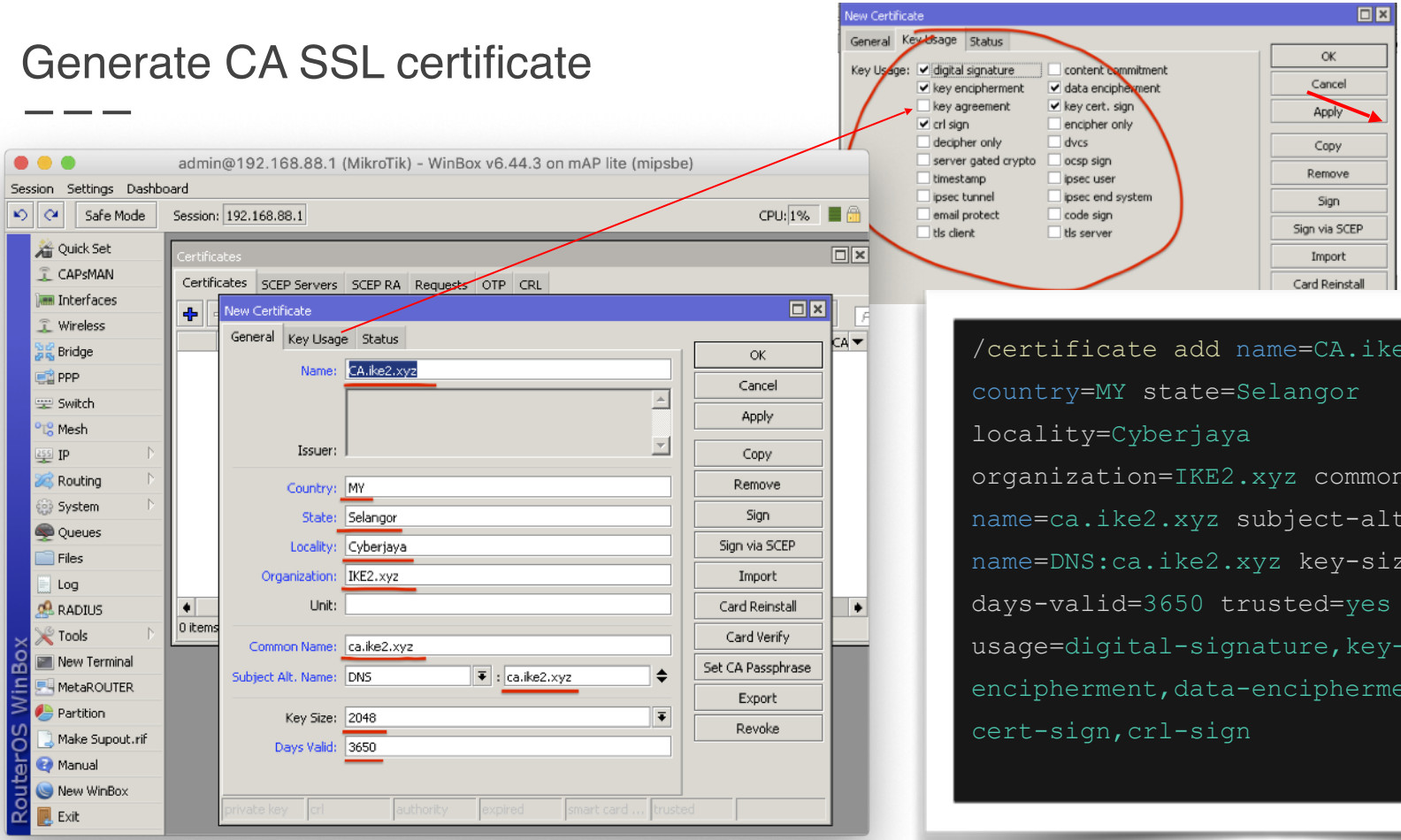

```
/ip pool add name="pool
vpn.ike2.xyz"
ranges=10.0.88.2-10.0.88.254
```

Generate SSL certificates

Agenda for next slides

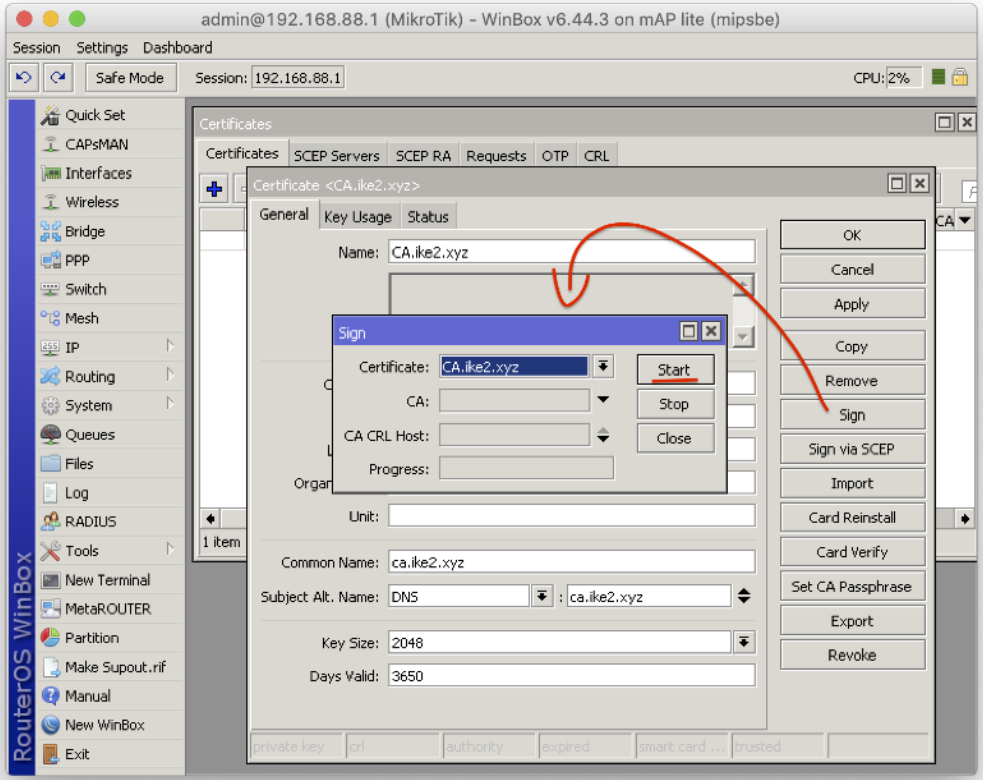
1. Generate CA
2. Generate server SSL
3. Generate client SSL
4. Export client SSL

Generate CA SSL certificate



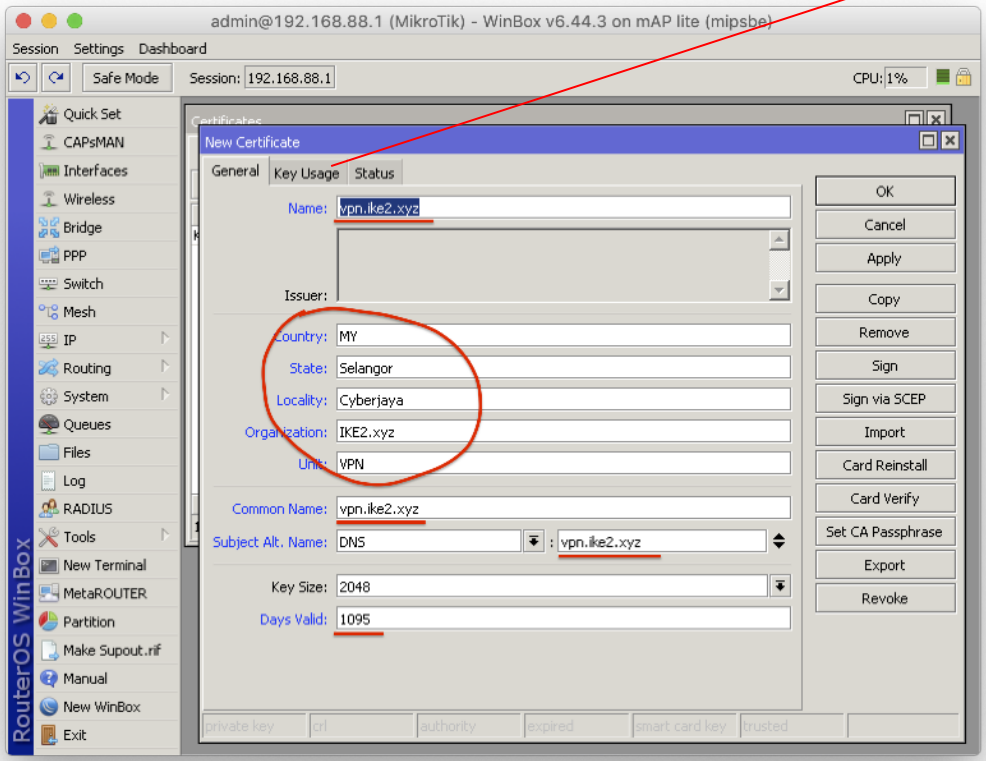

```
/certificate add name=CA.ike2.xyz
country=MY state=Selangor
locality=Cyberjaya
organization=IKE2.xyz common-
name=ca.ike2.xyz subject-alt-
name=DNS:ca.ike2.xyz key-size=2048
days-valid=3650 trusted=yes key-
usage=digital-signature,key-
encipherment,data-encipherment,key-
cert-sign,crl-sign
```

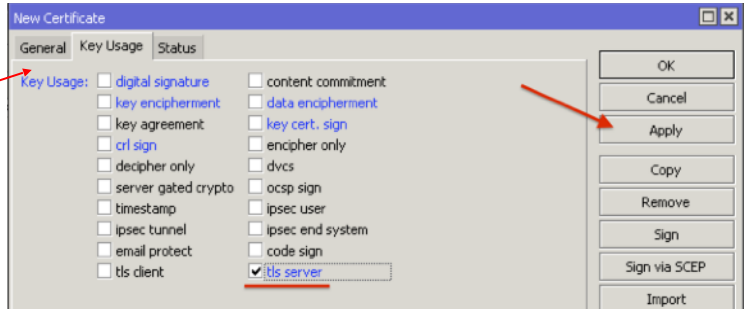
Self-sign CA SSL certificate *(Certificate Authority)*




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

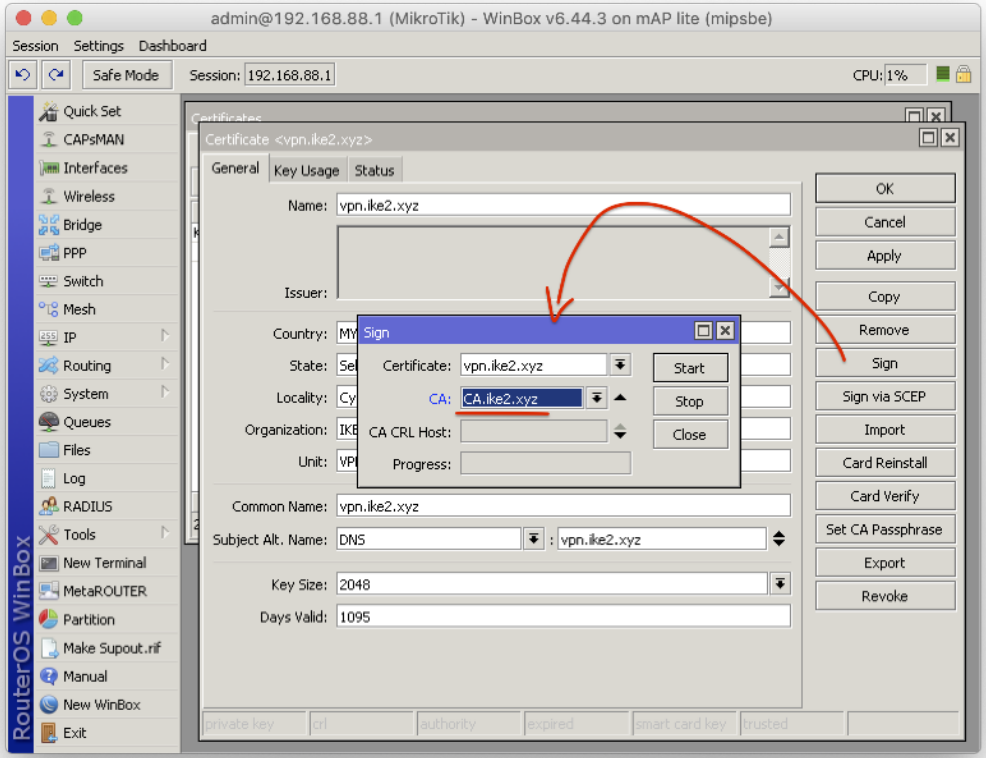
Generate server SSL certificate





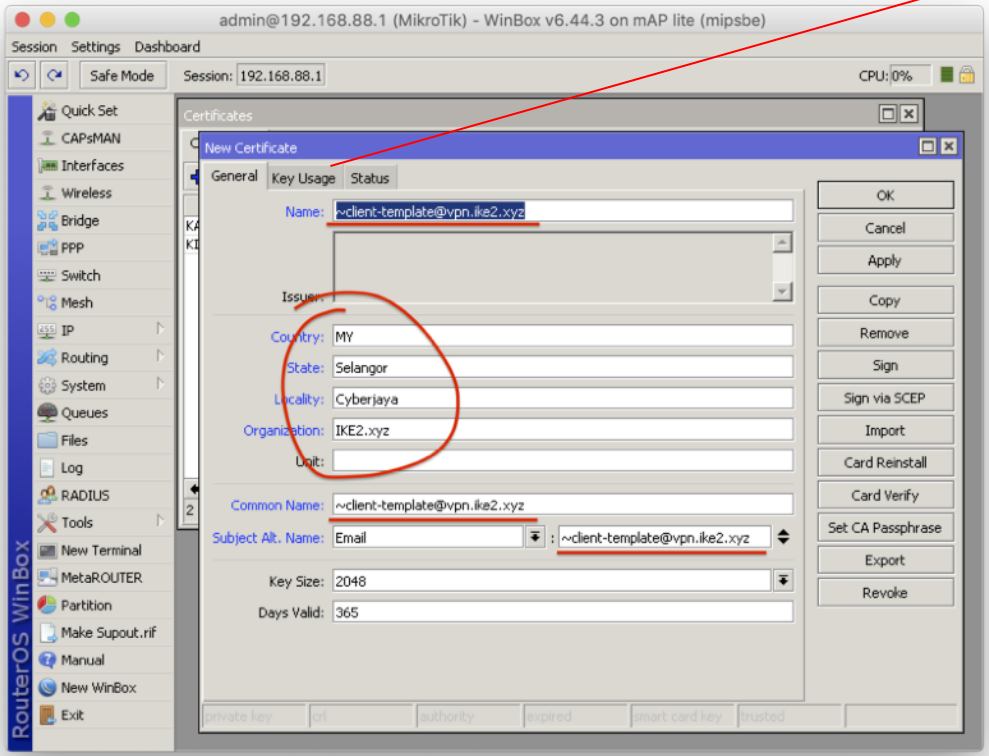

```
/certificate add name=vpn.ike2.xyz
country=MY state=Selangor
locality=Cyberjaya
organization=IKE2.xyz unit=VPN
common-name=vpn.ike2.xyz subject-
alt-name=DNS:vpn.ike2.xyz key-
size=2048 days-valid=1095
trusted=yes key-usage=tls-server
```

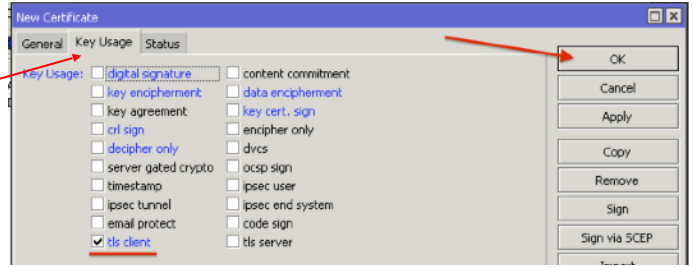
Sign server SSL certificate with CA.ike2.xyz authority




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

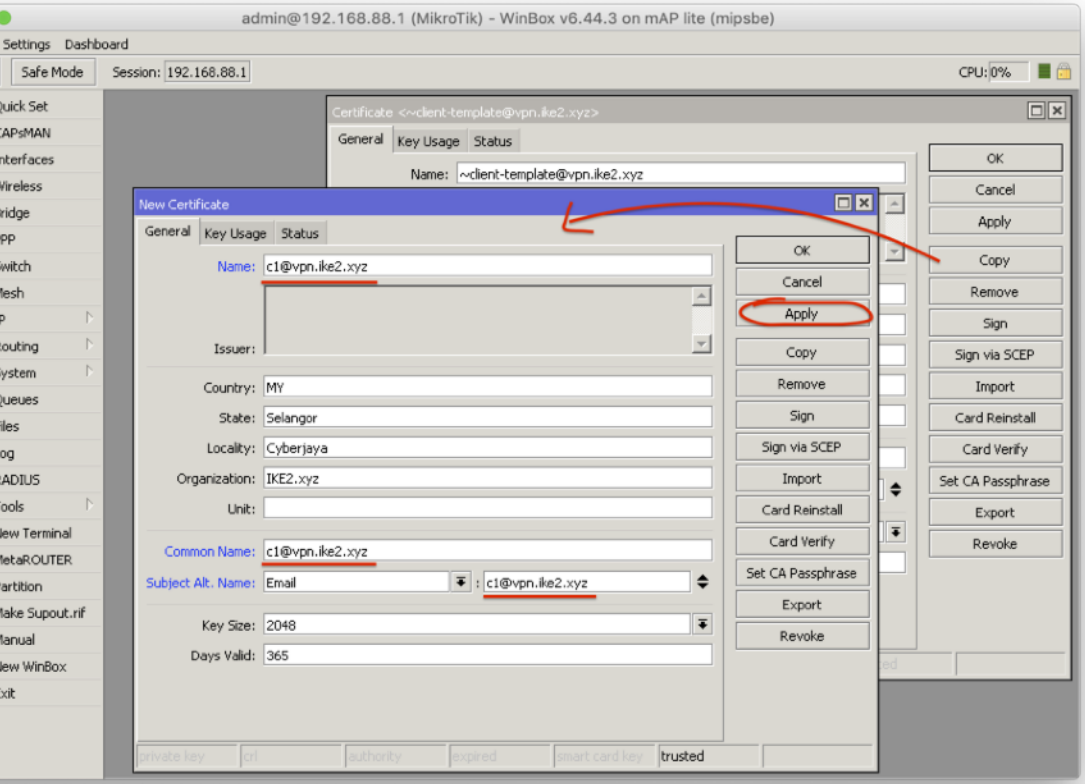
Client certificate template





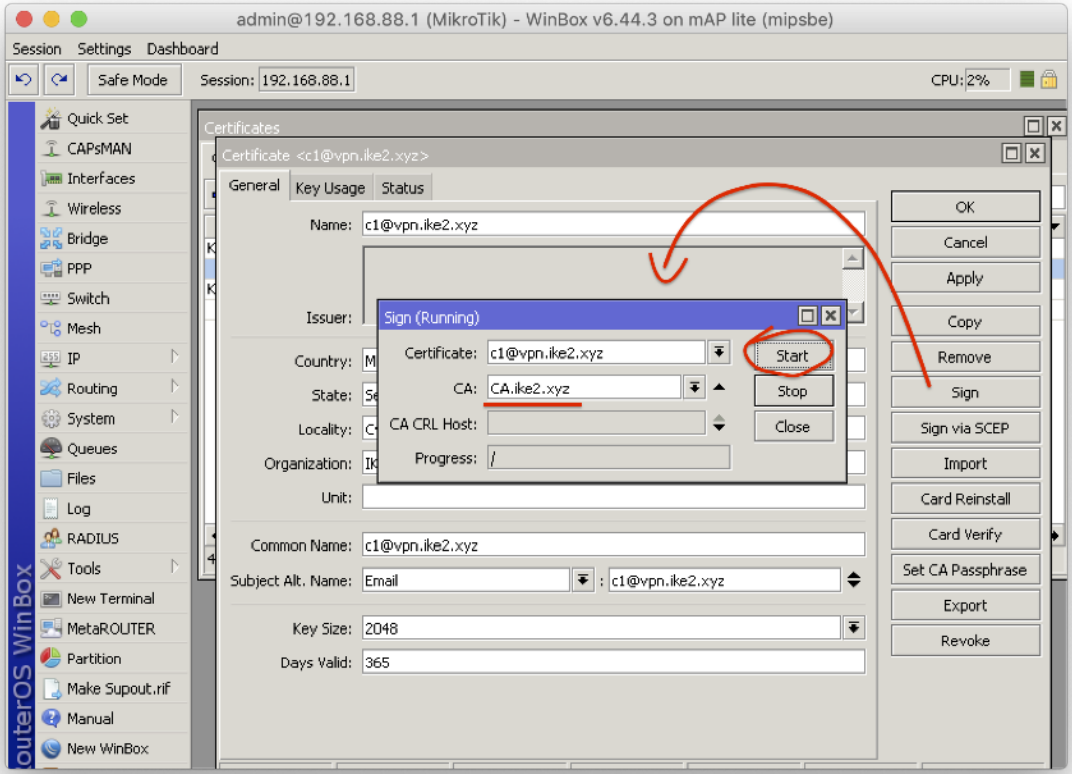

```
/certificate add name=~client-
template@vpn.ike2.xyz country=MY
state=Selangor locality=Cyberjaya
organization=IKE2.xyz common-
name=~client-template@vpn.ike2.xyz
subject-alt-name=email:~client-
template@vpn.ike2.xyz key-size=2048
days-valid=365 trusted=yes key-
usage=tls-client
```

Generate client SSL certificate from template



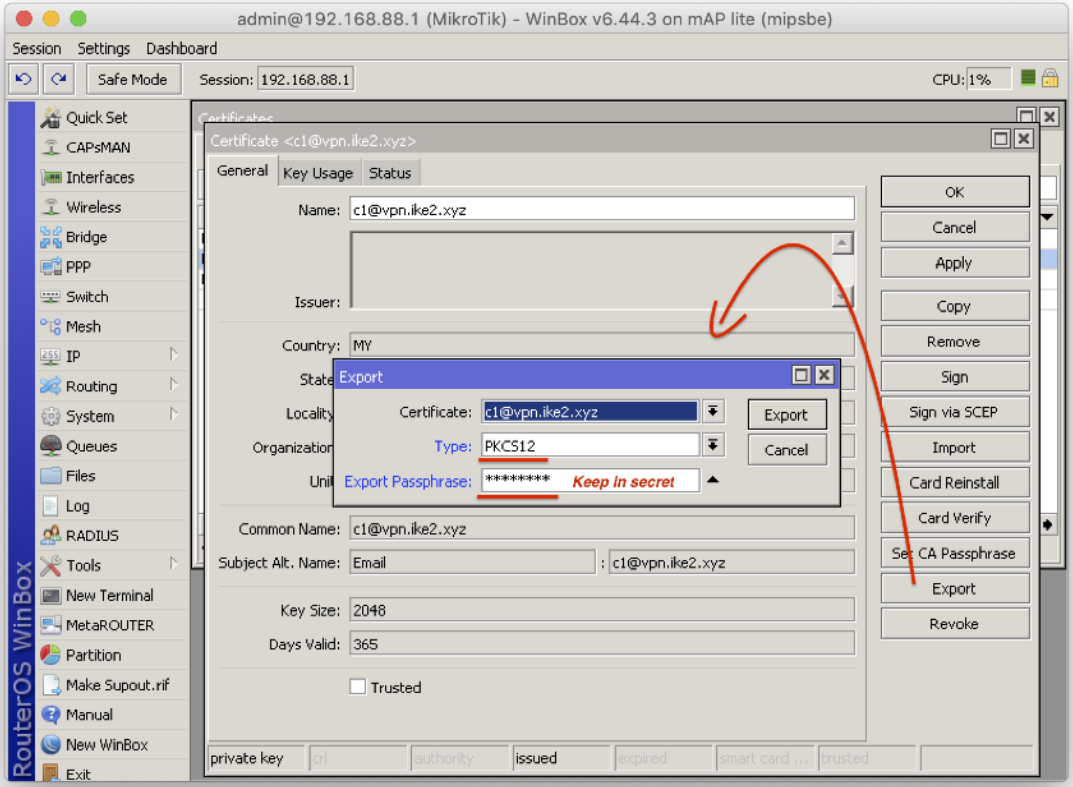

```
/certificate add copy-from=~client-template@vpn.ike2.xyz name=c1@vpn.ike2.xyz common-name=c1@vpn.ike2.xyz subject-alt-name=email:c1@vpn.ike2.xyz
```

Sign client SSL certificate with CA.ike2.xyz authority



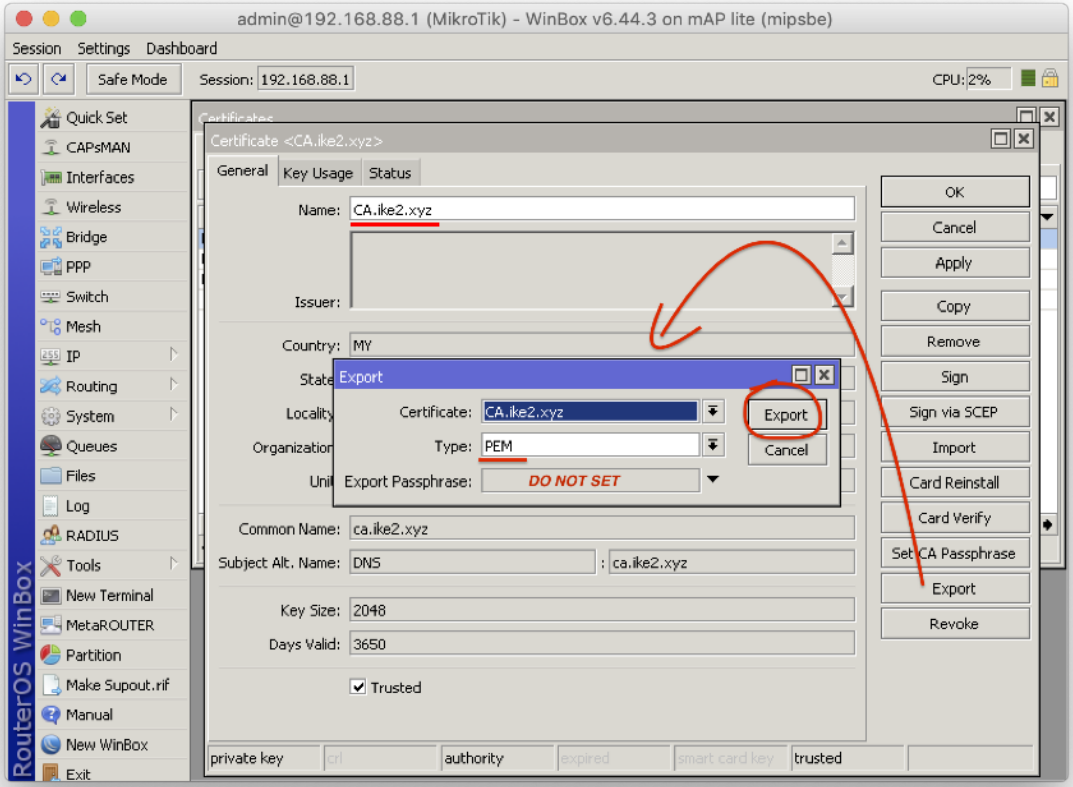

```
/certificate sign
c1@vpn.ike2.xyz ca=CA.ike2.xyz
```

Export client SSL certificate + private key to .p12 file



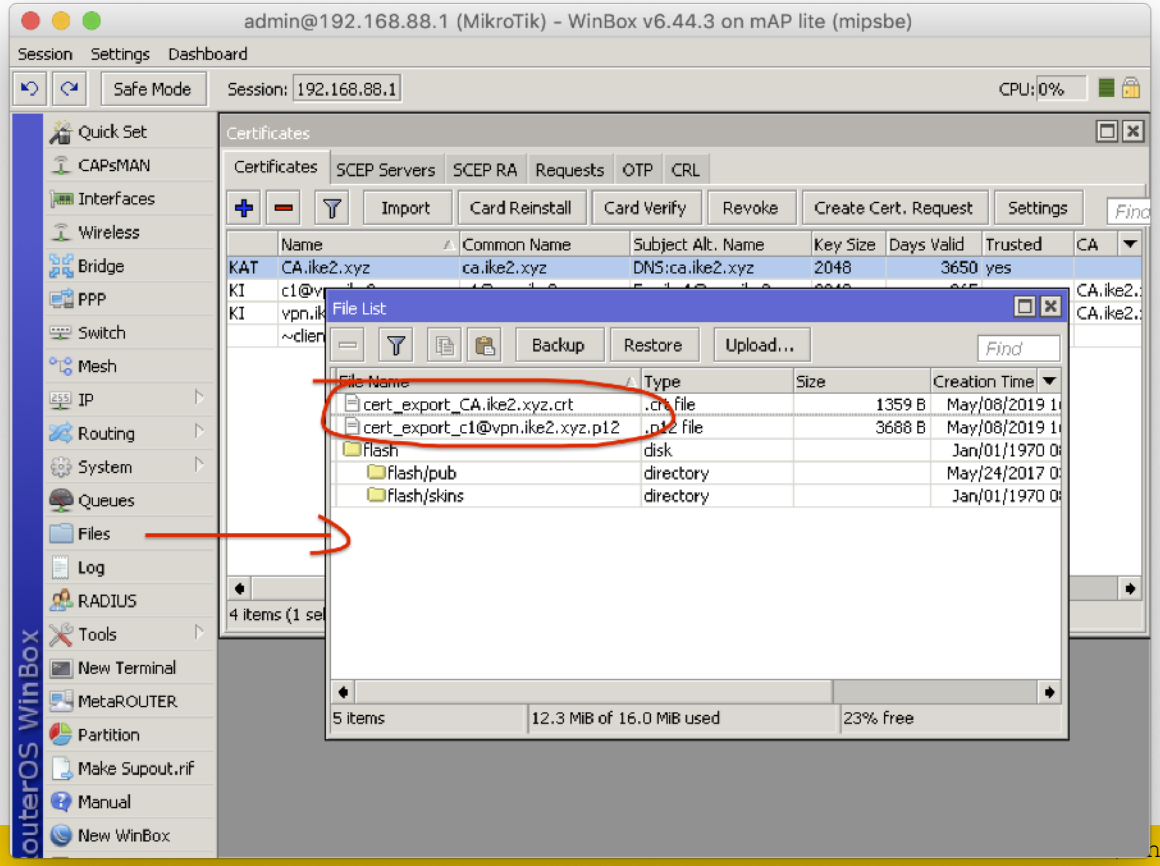

```
/certificate export-certificate
c1@vpn.ike2.xyz type=pkcs12
export-passphrase=keepinsecret
```

Export CA SSL certificate .crt file




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

Download exported SSL certificates



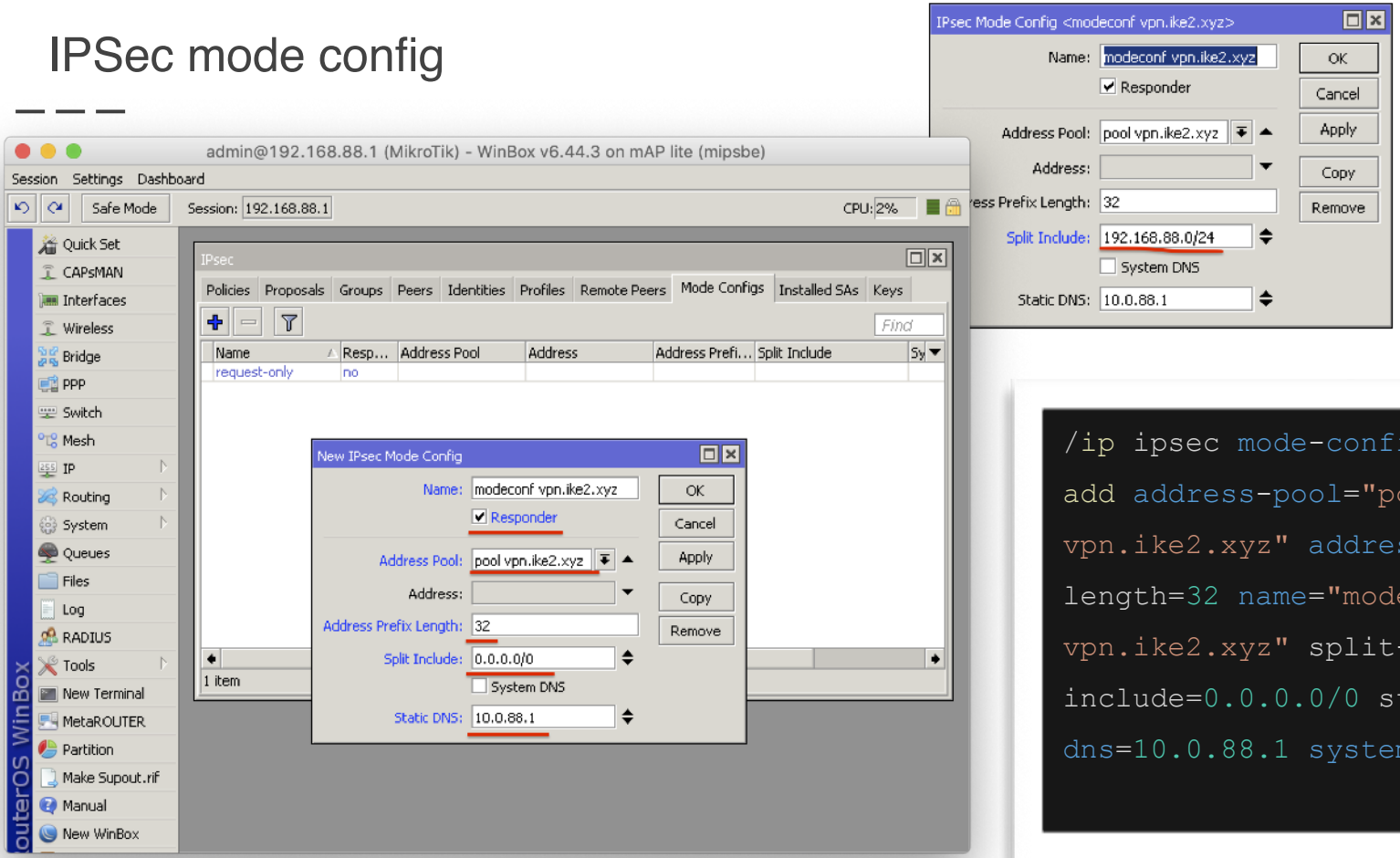
Setting up IPSec

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

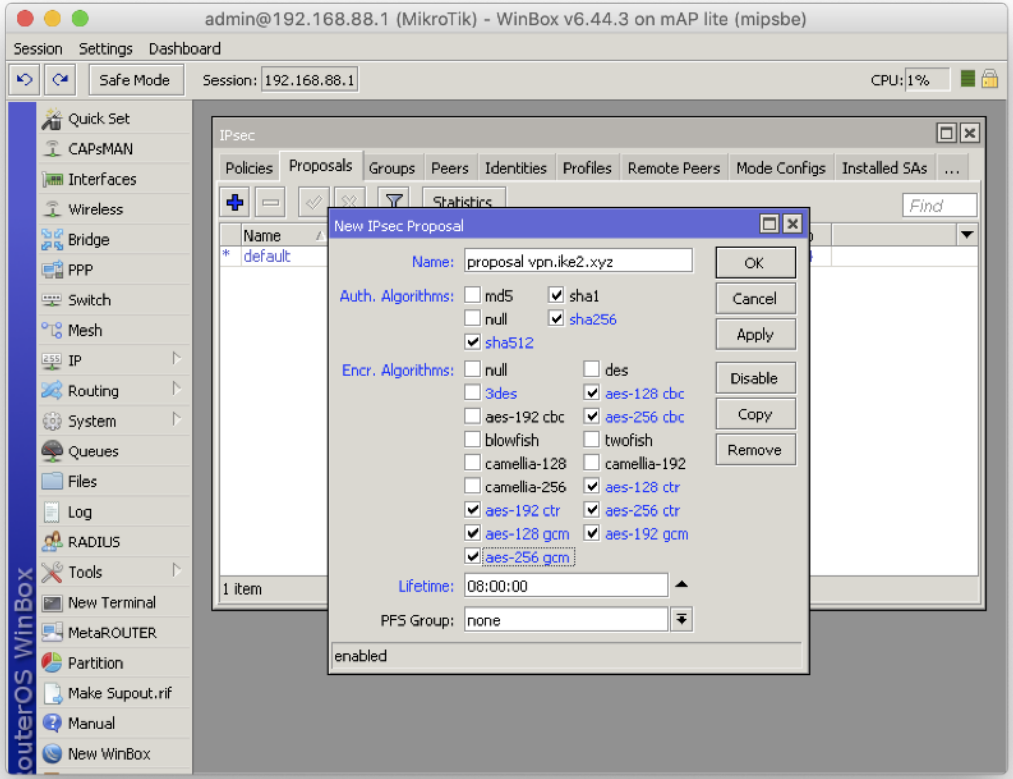
Nikita Tarikin / nikita@tarikin.com

IPSec mode config



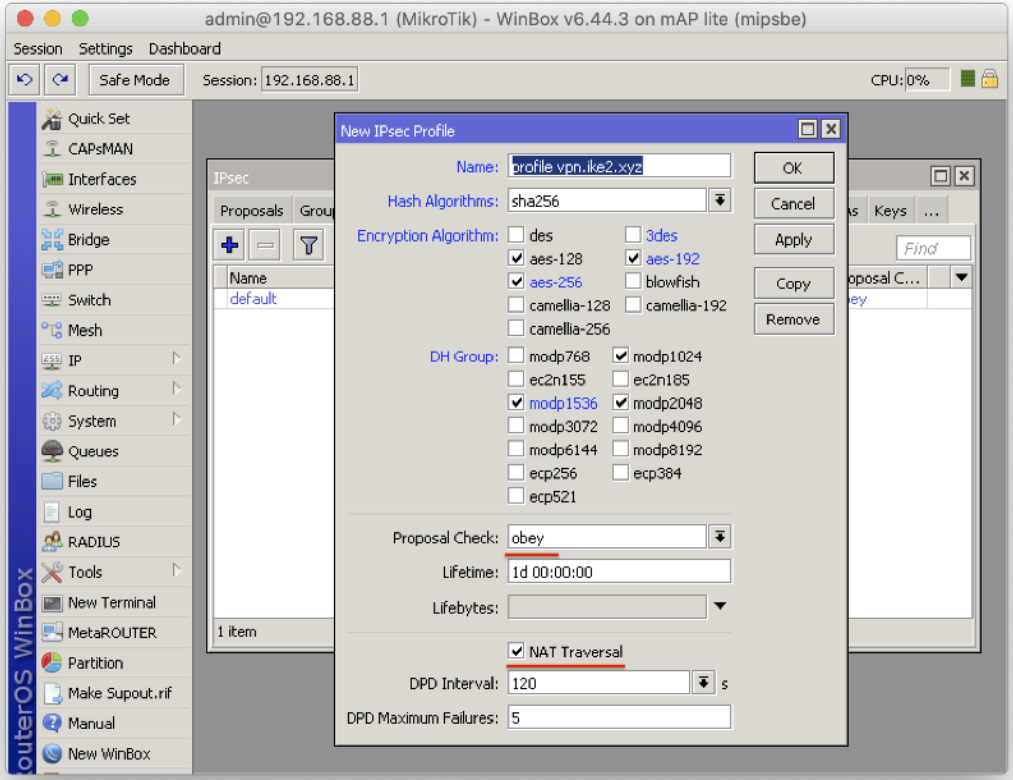

```
/ip ipsec mode-config
add address-pool="pool
vpn.ike2.xyz" address-prefix-
length=32 name="modeconf
vpn.ike2.xyz" split-
include=0.0.0.0/0 static-
dns=10.0.88.1 system-dns=no
```

IPSec proposal *(phase 2)*



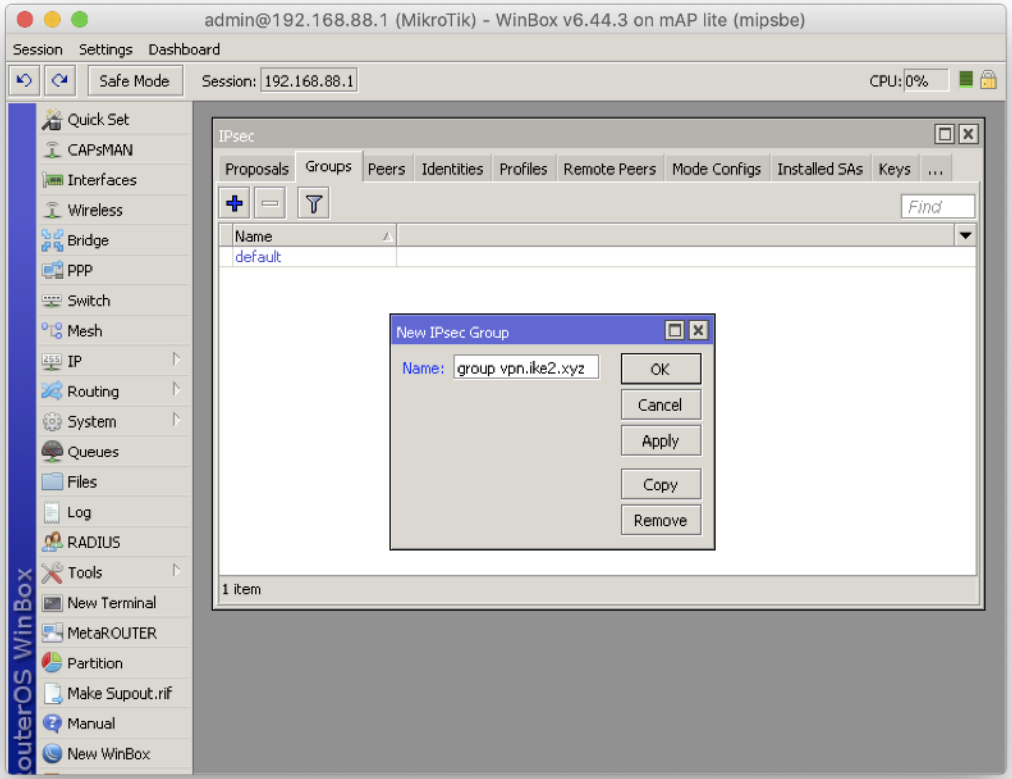

```
/ip ipsec proposaladd auth-
algorithms=sha512,sha256,sha1
enc-algorithms=aes-256-
cbc,aes-256-ctr,aes-256-
gcm,aes-192-ctr,aes-192-
gcm,aes-128-cbc,aes-128-
ctr,aes-128-gcm lifetime=8h
name="proposal vpn.ike2.xyz"
pfs-group=none
```

IPSec peer profile



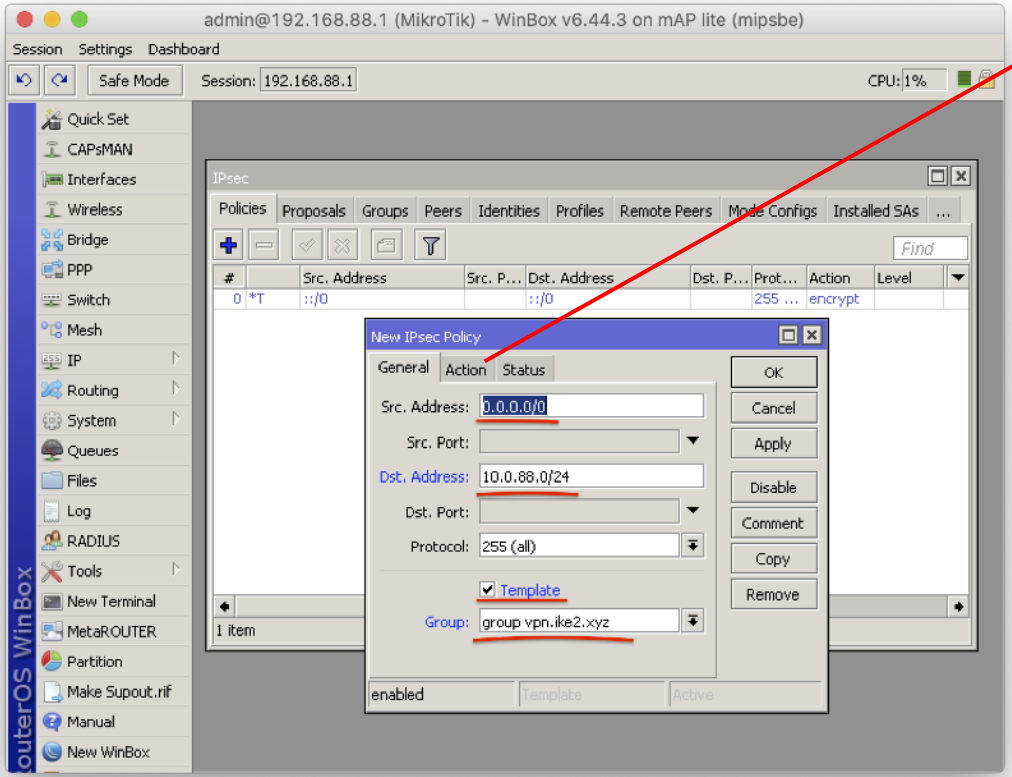

```
/ip ipsec profile add dh-
group=modp2048,modp1536,modp102
4 enc-
algorithm=aes-256,aes-192,aes-1
28 hash-algorithm=sha256
name="profile vpn.ike2.xyz"
nat-traversal=yes proposal-
check=obey
```

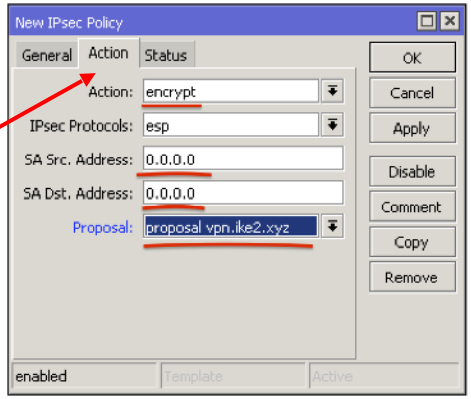
IPSec policy group




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

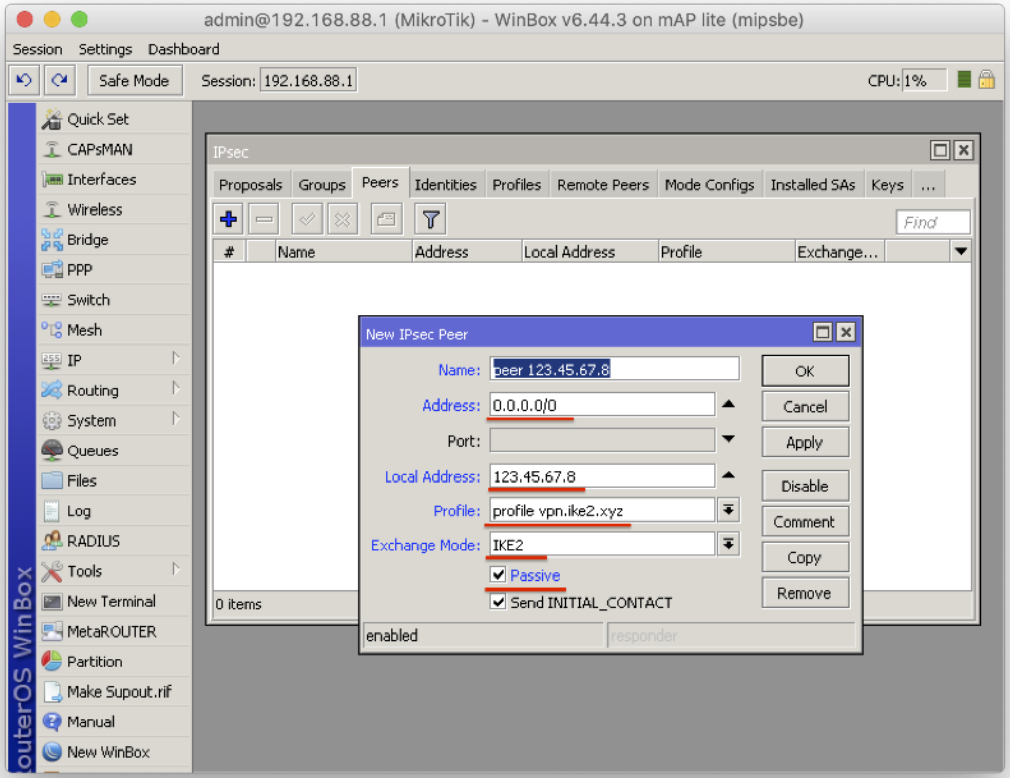
IPSec policy template





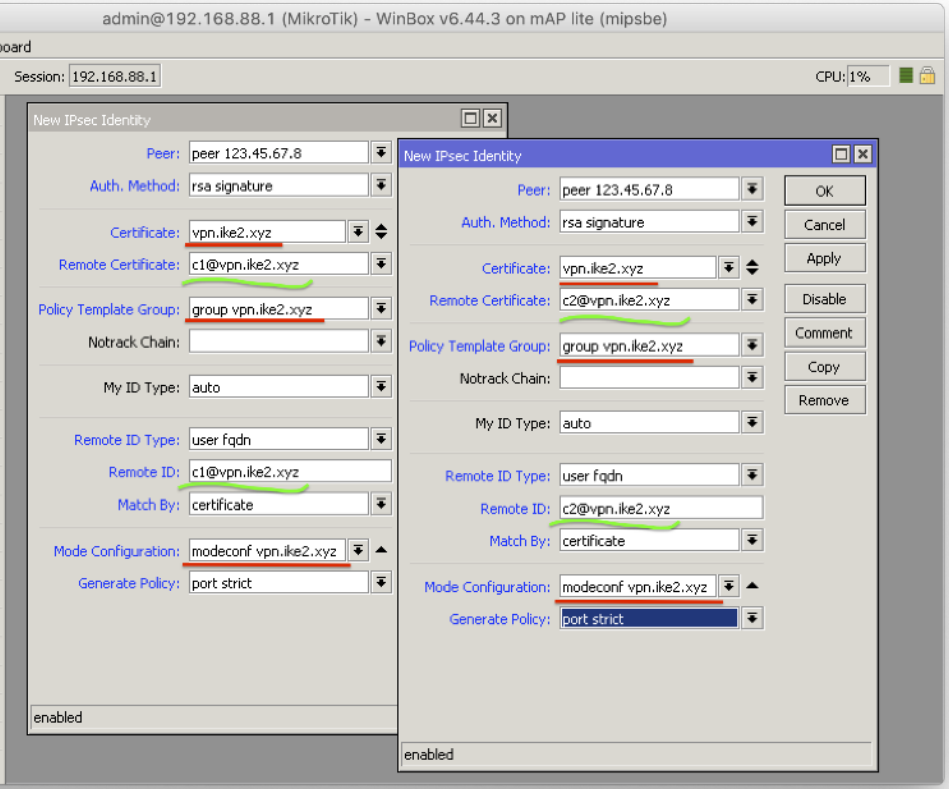

```
/ip ipsec policy add dst-
address=10.0.88.0/24 group="group
vpn.ike2.xyz" proposal="proposal
vpn.ike2.xyz" src-address=0.0.0.0/0
template=yes sa-src-address=0.0.0.0
sa-dst-address=0.0.0.0 ipsec-
protocols=esp level=require
protocol=all action=encrypt
```

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"
```

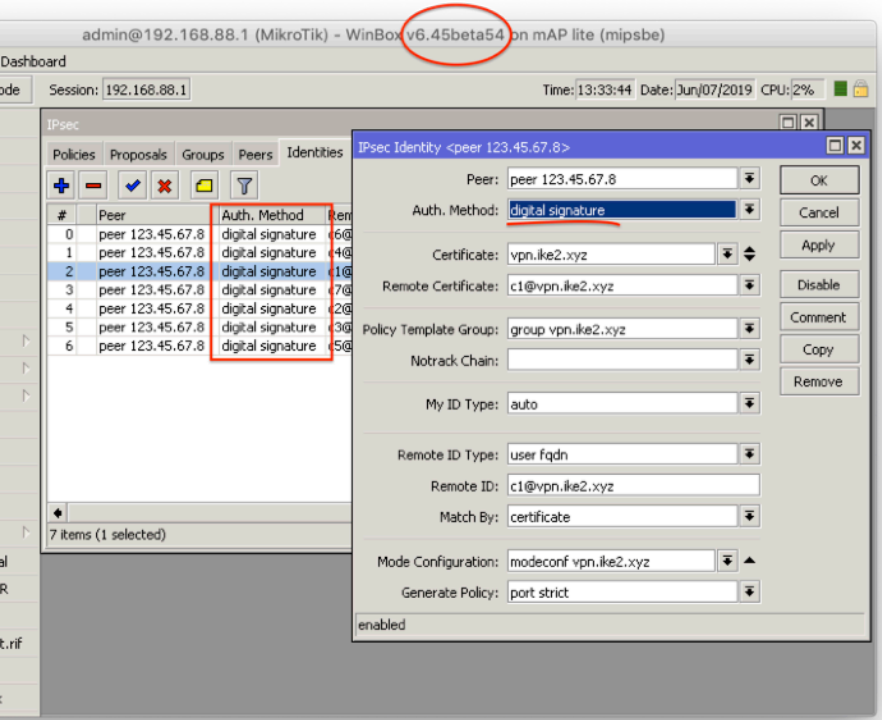
IPSec identities *(RouterOS 6.44)*




```
/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+)*



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

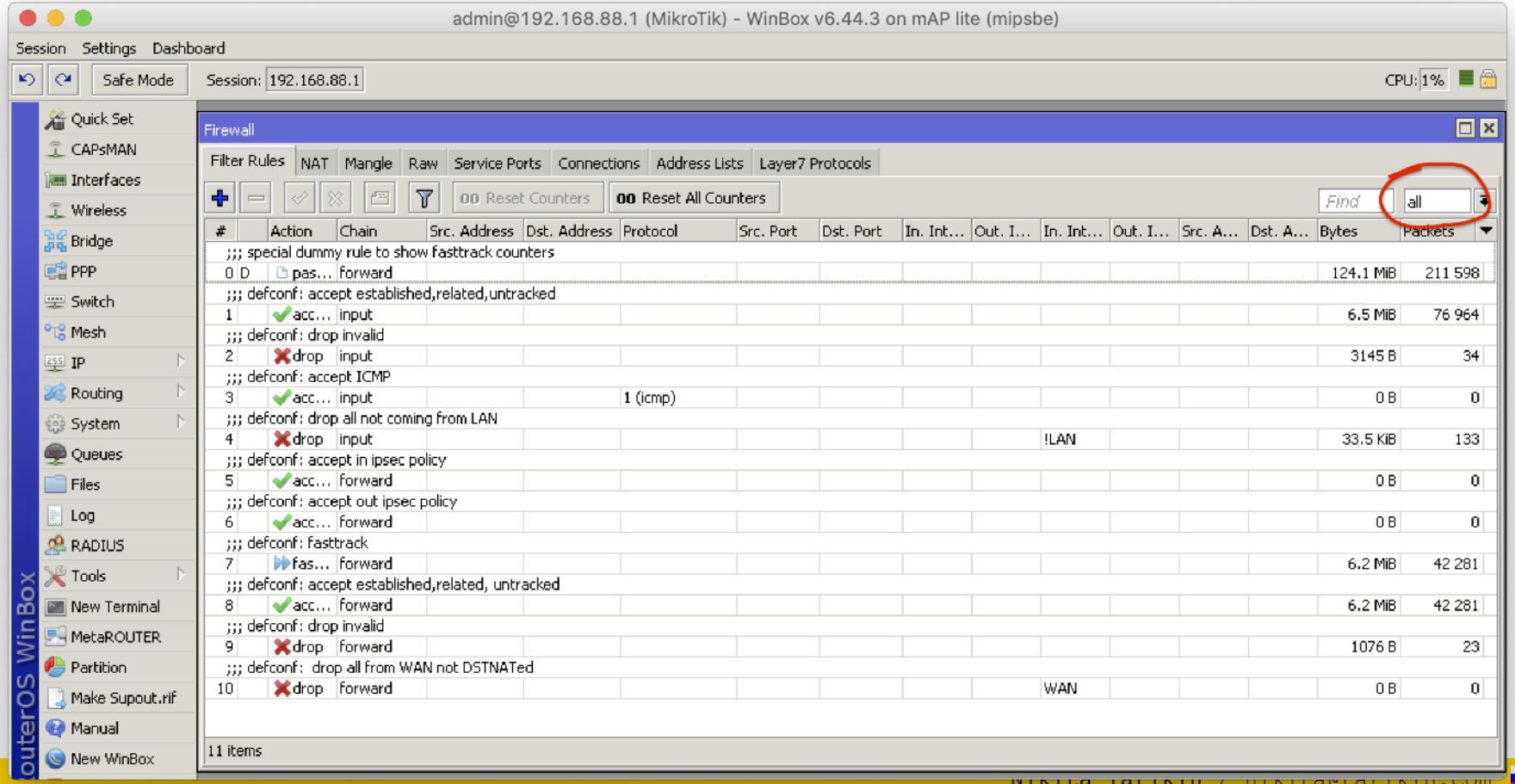
1. Default firewall overview
2. IPSec traffic rules
3. VPN traffic rules

Setting up Firewall

Understanding the default firewall filter

Nikita Tarikin / nikita@tarikin.com

RouterOS 6.41+ default configuration firewall overview



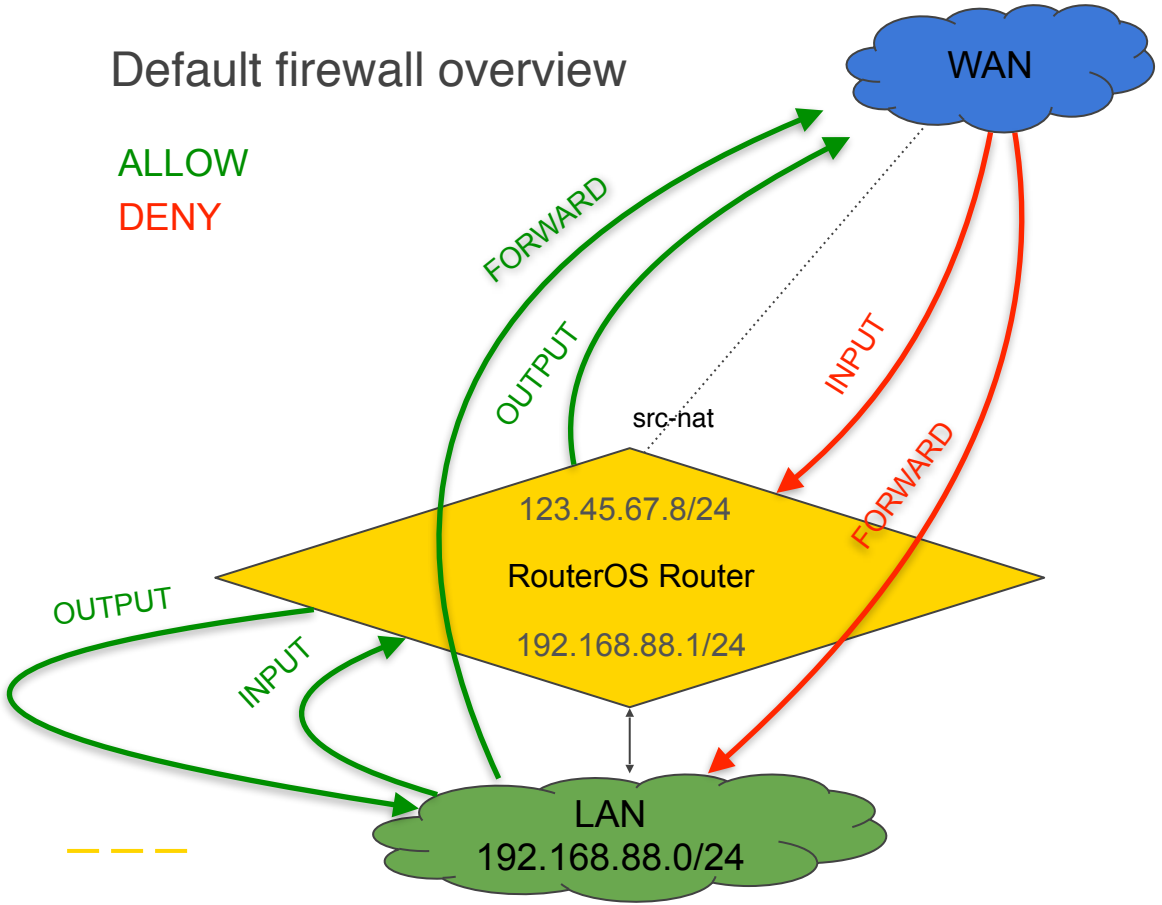
```
#Input Chain Rules
/ip firewall filter
add action=accept chain=input connection-state=established,related,untracked comment="DEFAULT:
Accept established, related, and untracked traffic."
add action=drop chain=input connection-state=invalid comment="DEFAULT: Drop invalid traffic."
add action=accept 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

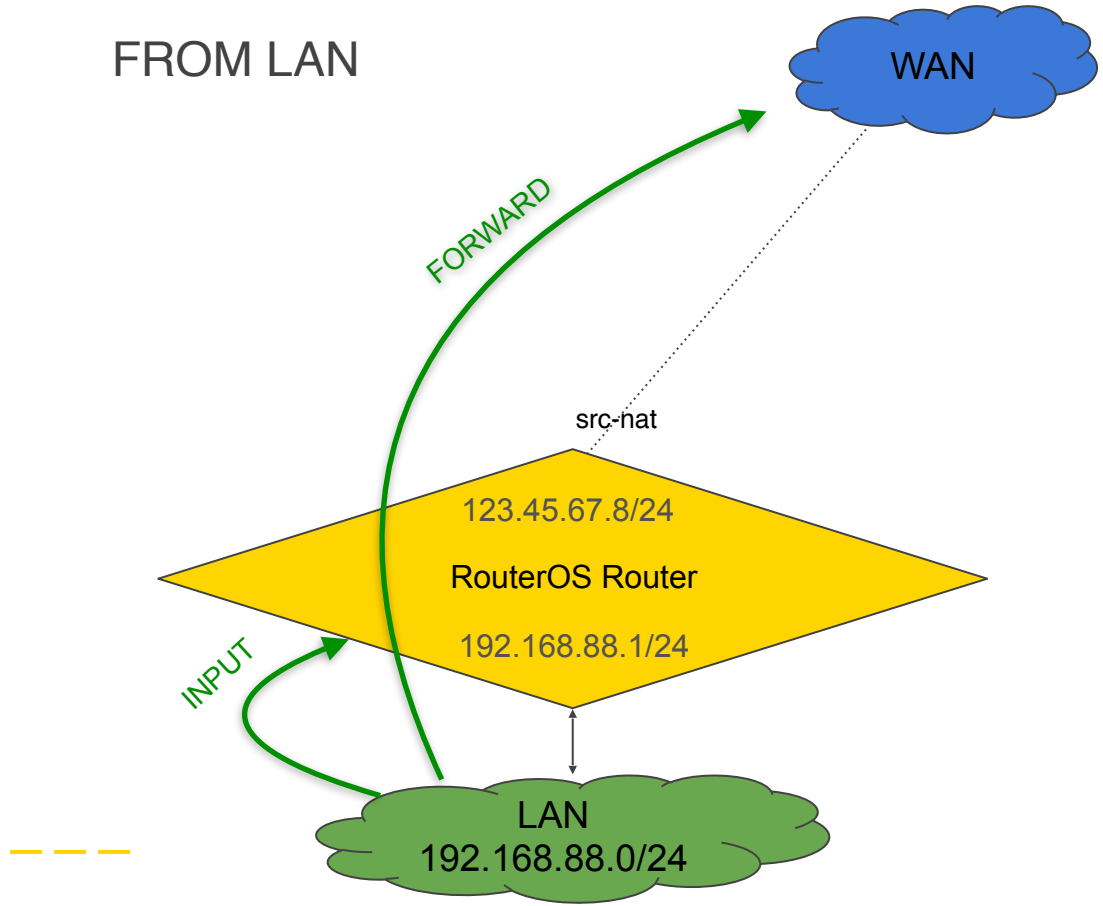
1. **Default firewall overview**
2. IPSec traffic rules
3. VPN traffic rules
4. Testing



Nikita Tarikin / nikita@tarikin.com

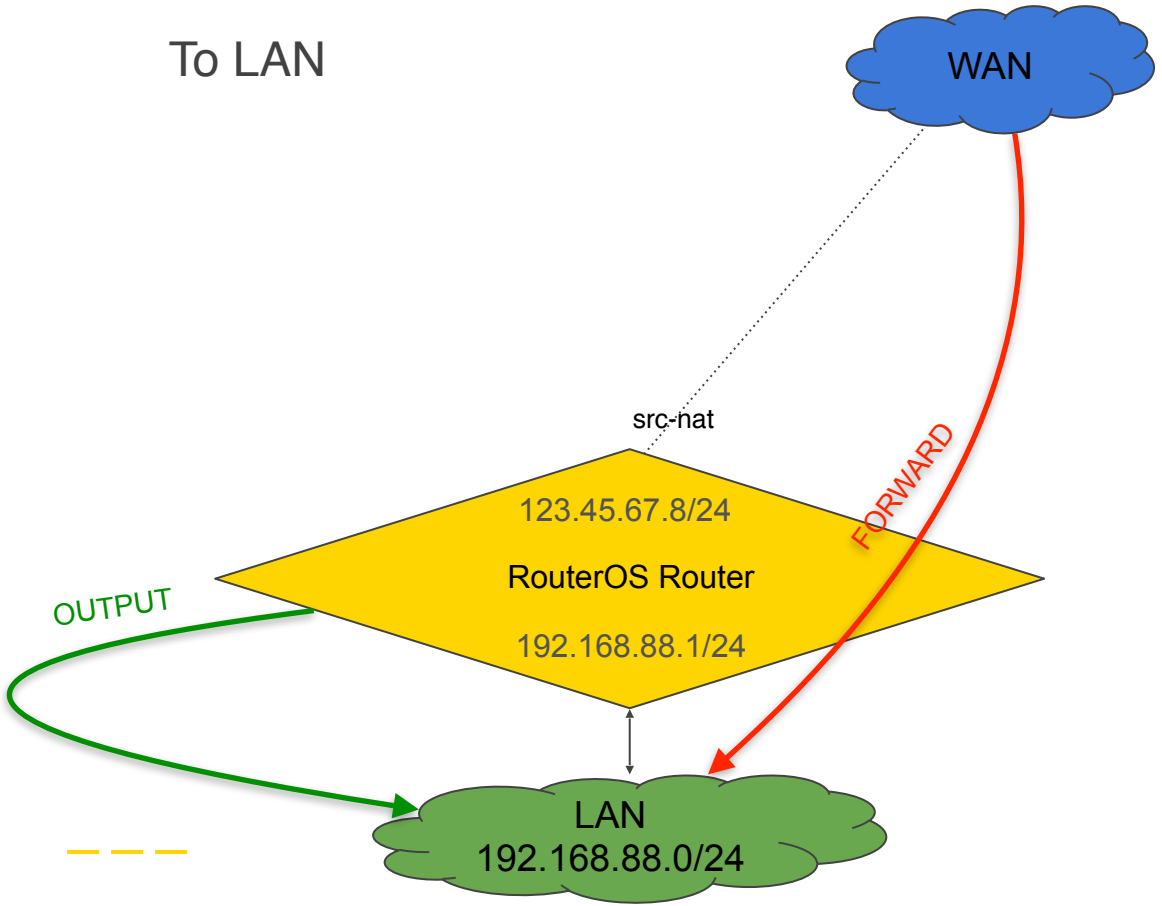
Default Firewall overview

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



Default Firewall overview

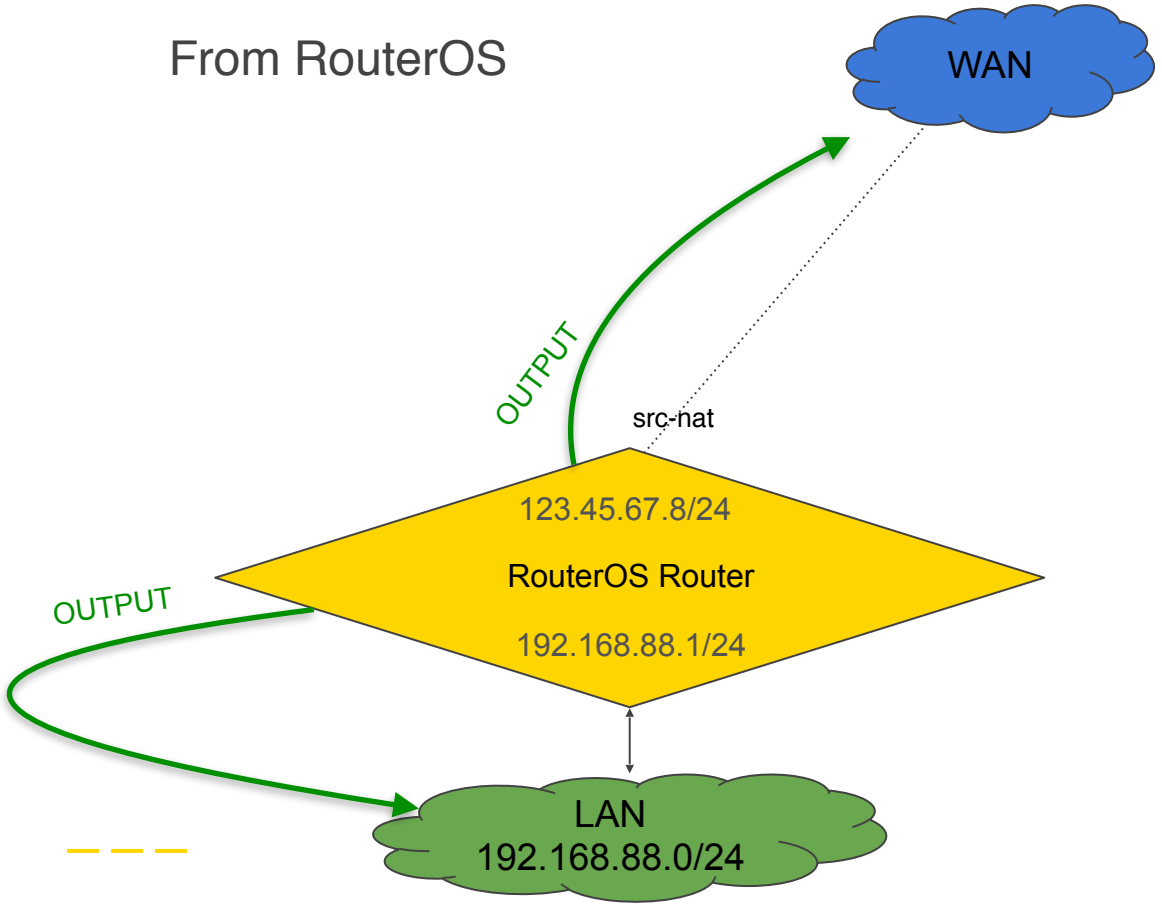
a. From LAN
b. To LAN
c. From RouterOS
d. To RouterOS
e. From WAN
f. To WAN



Nikita Tarikin / nikita@tarikin.com

Default Firewall overview

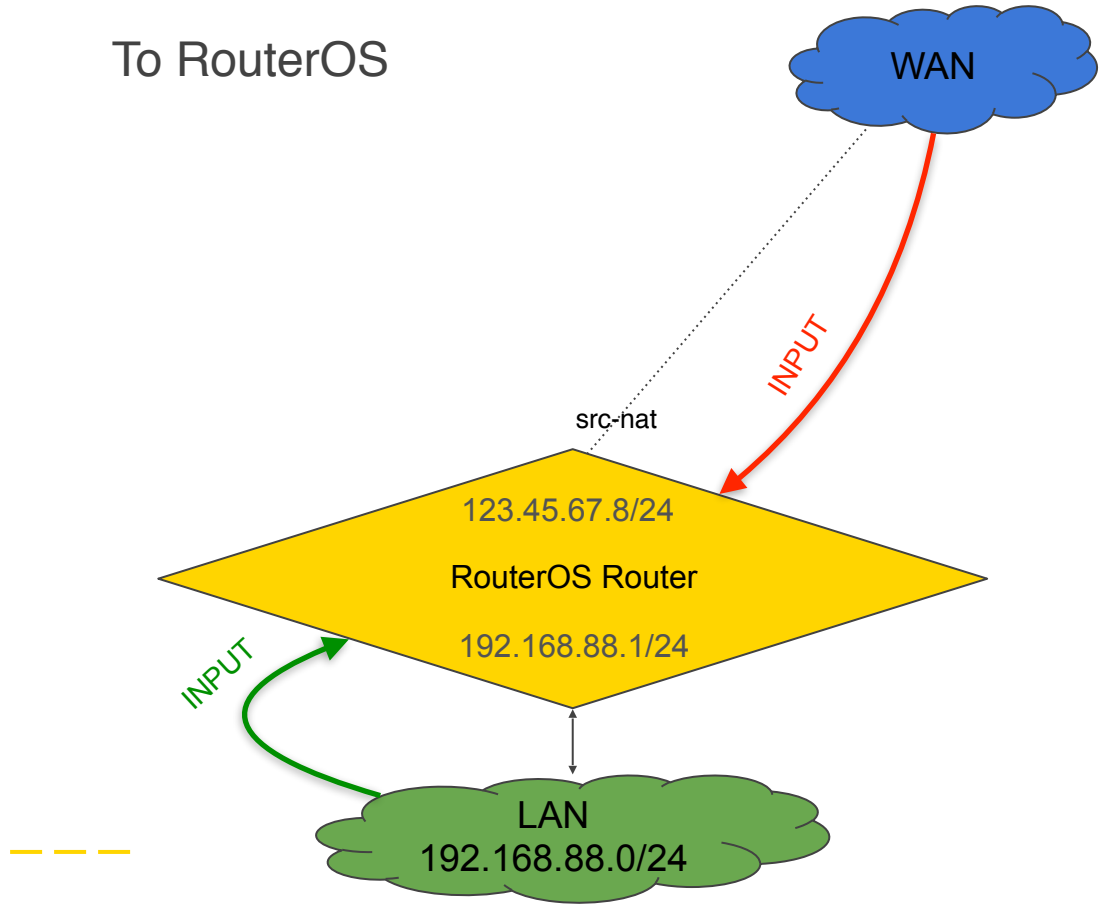
a. From LAN
b. To LAN
c. From RouterOS
d. To RouterOS
e. From WAN
f. To WAN



Nikita Tarikin / nikita@tarikin.com

Default Firewall overview

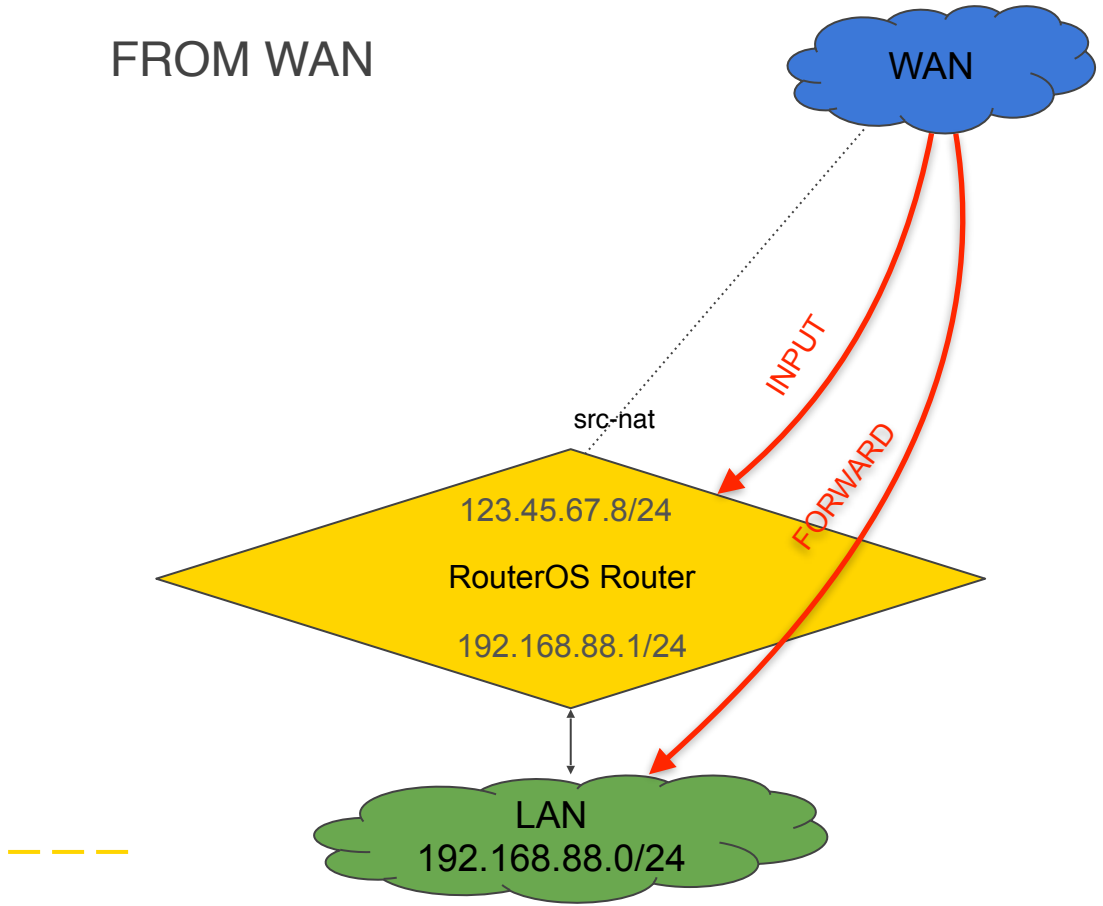
a. From LAN
b. To LAN
c. From RouterOS
d. To RouterOS
e. From WAN
f. To WAN



Nikita Tarikin / nikita@tarikin.com

Default Firewall overview

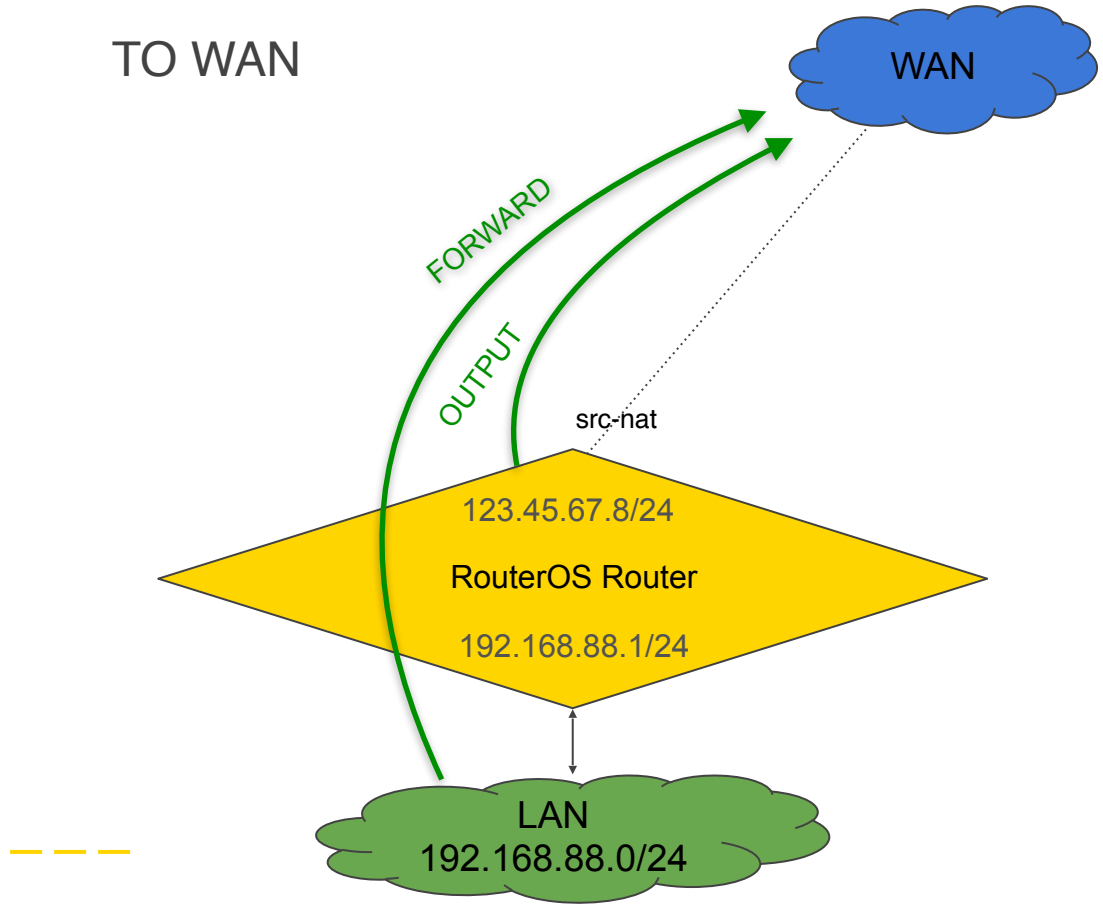
a. From LAN
b. To LAN
c. From RouterOS
d. To RouterOS
e. From WAN
f. To WAN



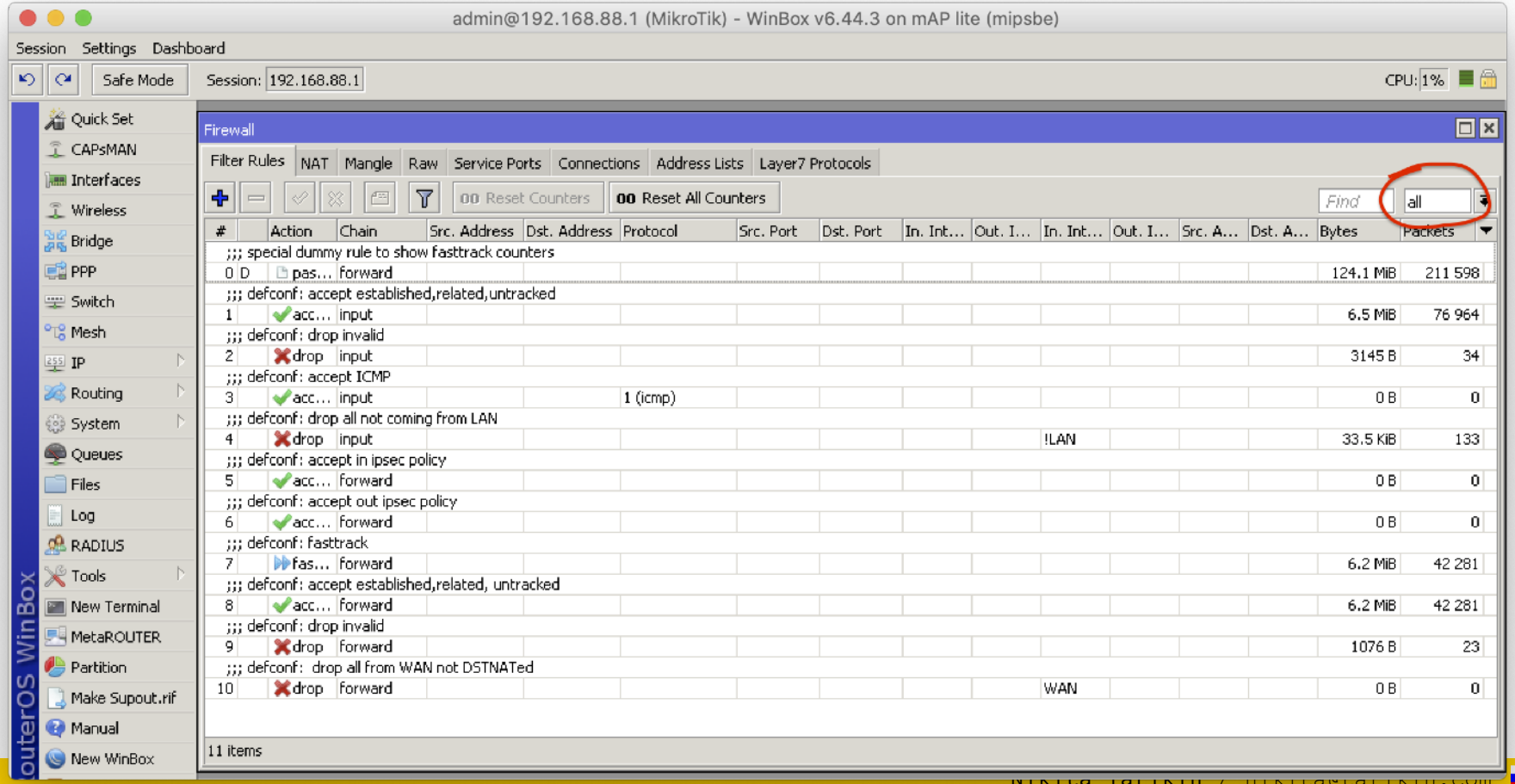
Nikita Tarikin / nikita@tarikin.com

Default Firewall overview

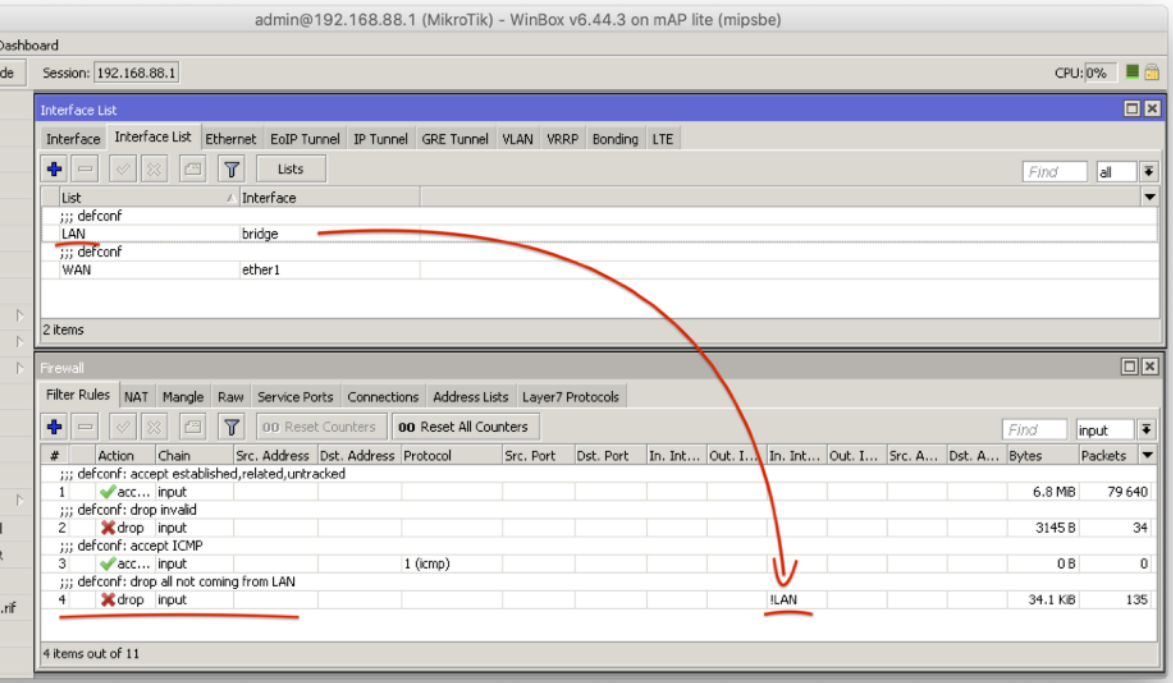
a. From LAN
b. To LAN
c. From RouterOS
d. To RouterOS
e. From WAN
f. To WAN



RouterOS 6.41+ default configuration firewall overview



Default configuration firewall: INPUT chain



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

Short summary

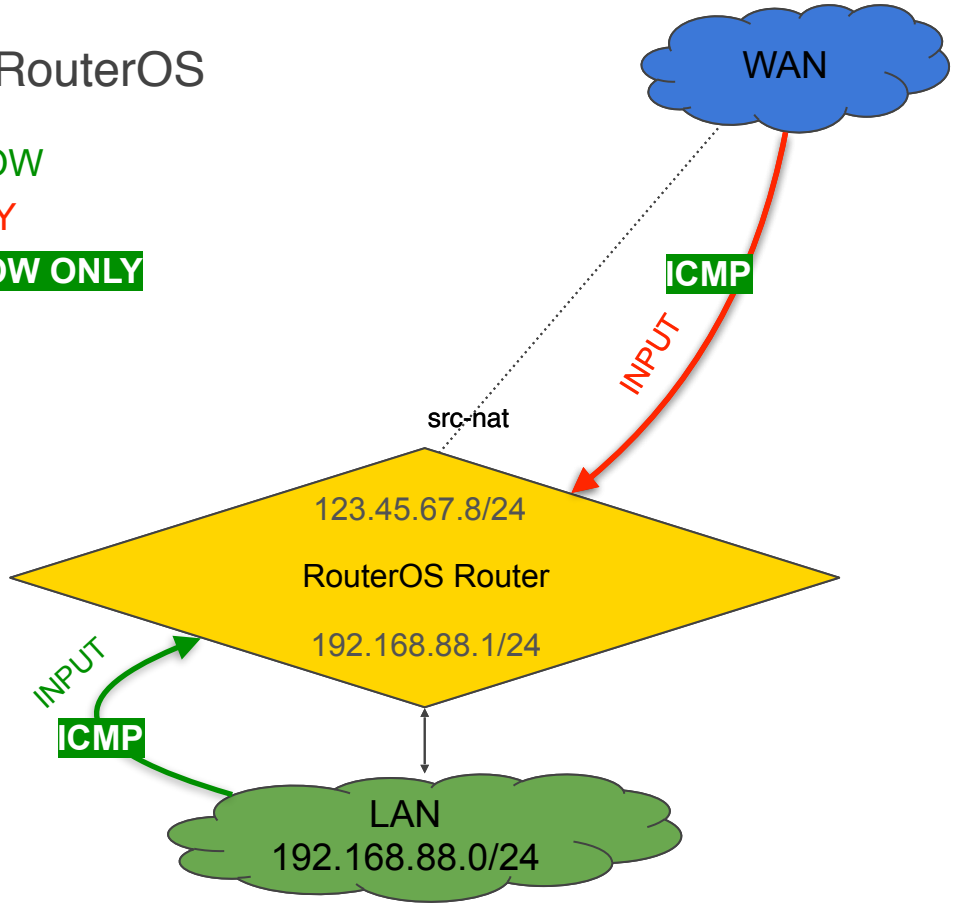
1. **Accept ALL** input packets for **established** connections
2. **Accept ALL** input **ICMP** packets
3. **DROP ALL** input packets (except LAN)
4. Allow everything else

Default Firewall overview

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

TO RouterOS

ALLOW
DENY
ALLOW ONLY



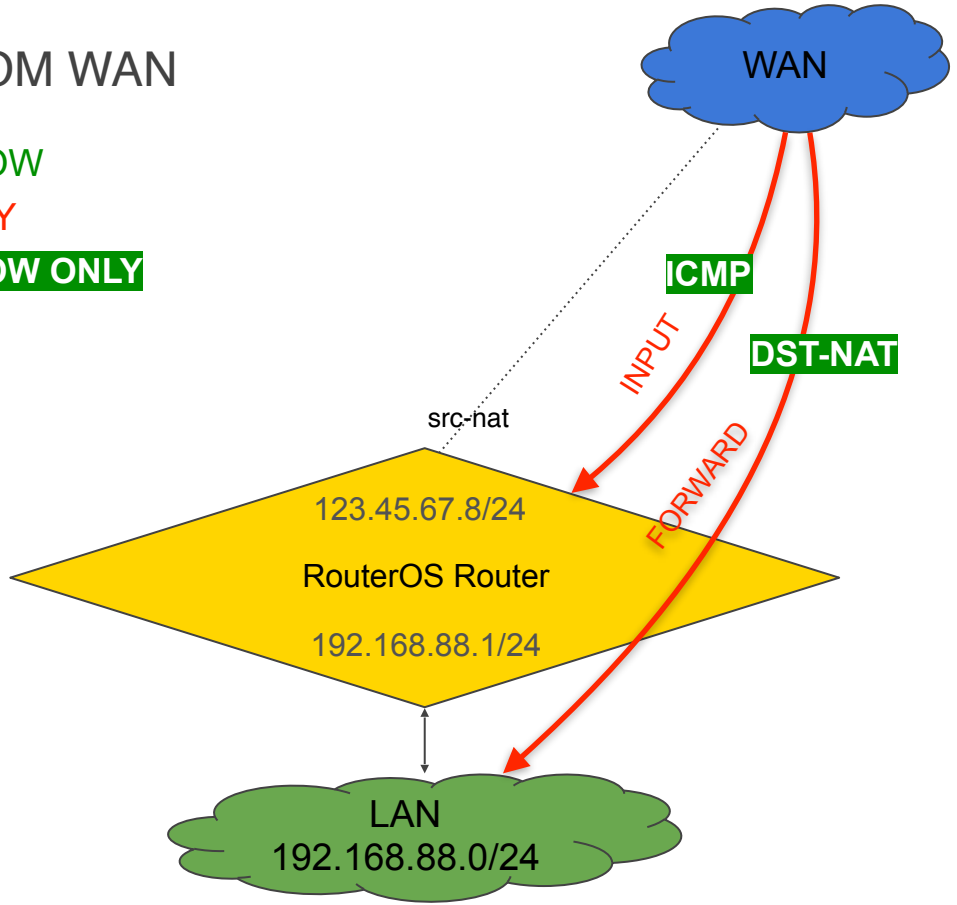
Nikita Tarikin / nikita@tarikin.com

Default Firewall overview

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

FROM WAN

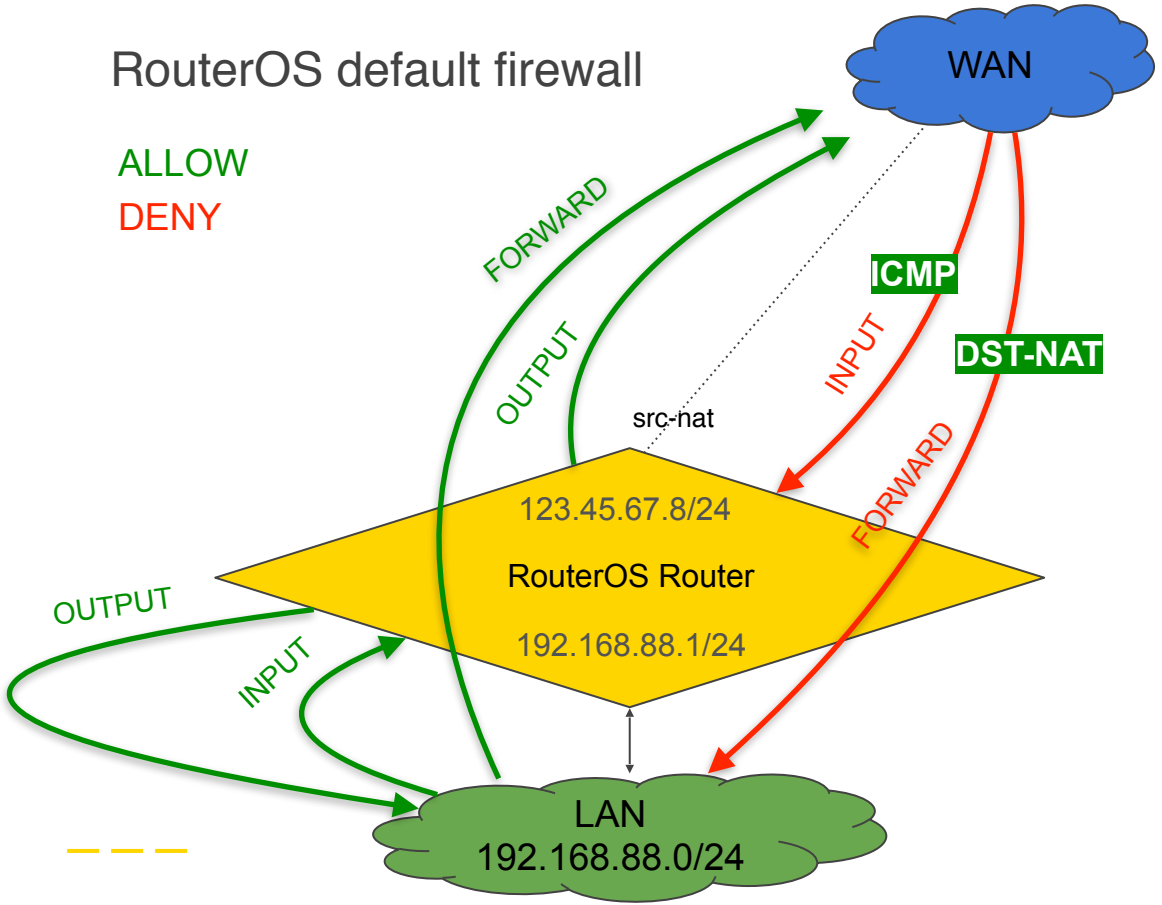
ALLOW
DENY
ALLOW ONLY



Nikita Tarikin / nikita@tarikin.com

Setting up Firewall

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

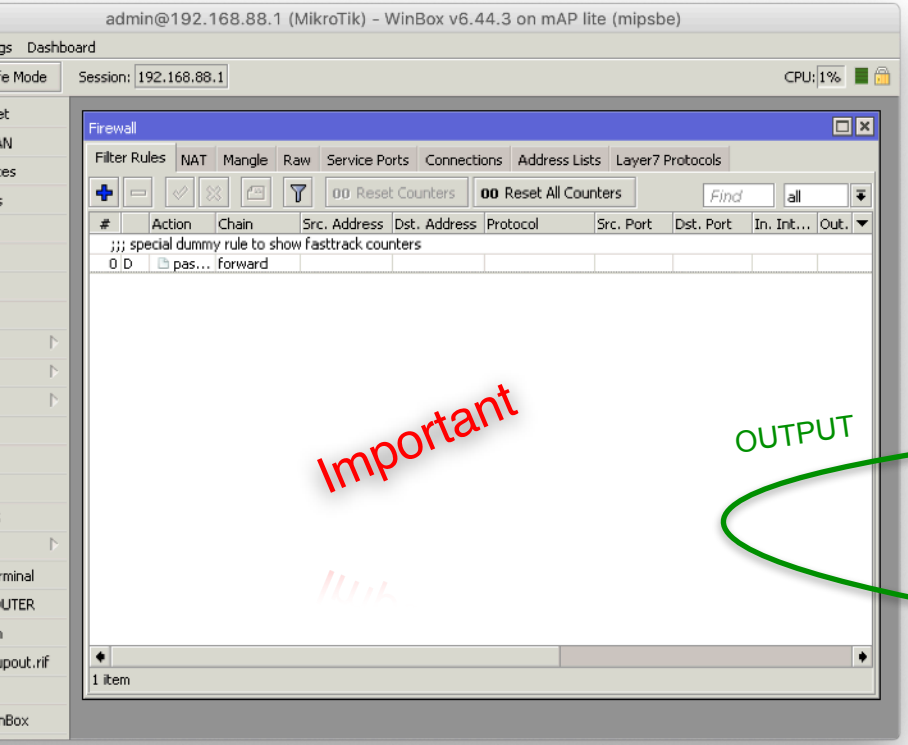


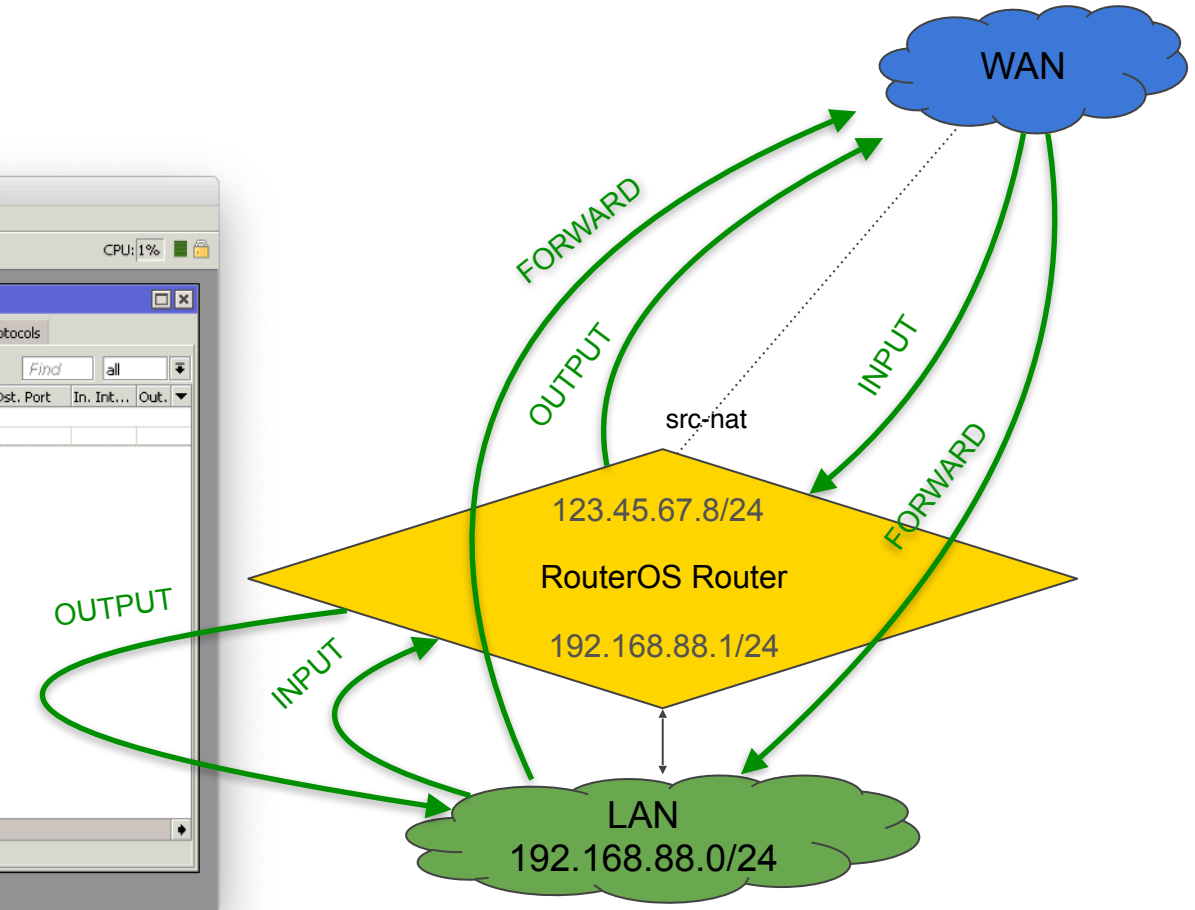
Nikita Tarikin / nikita@tarikin.com

Empty FIREWALL

ALLOW

DENY



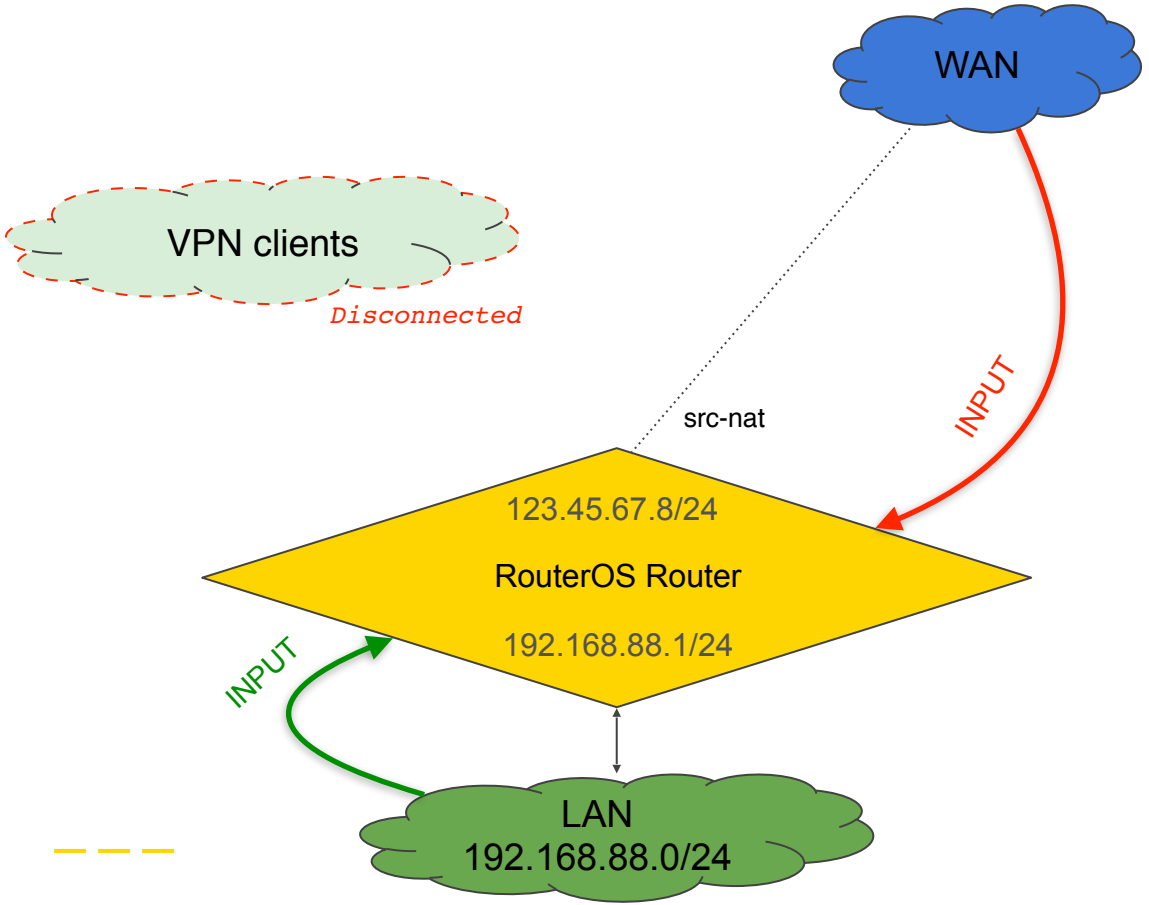


Setting up Firewall

IPSec traffic rules

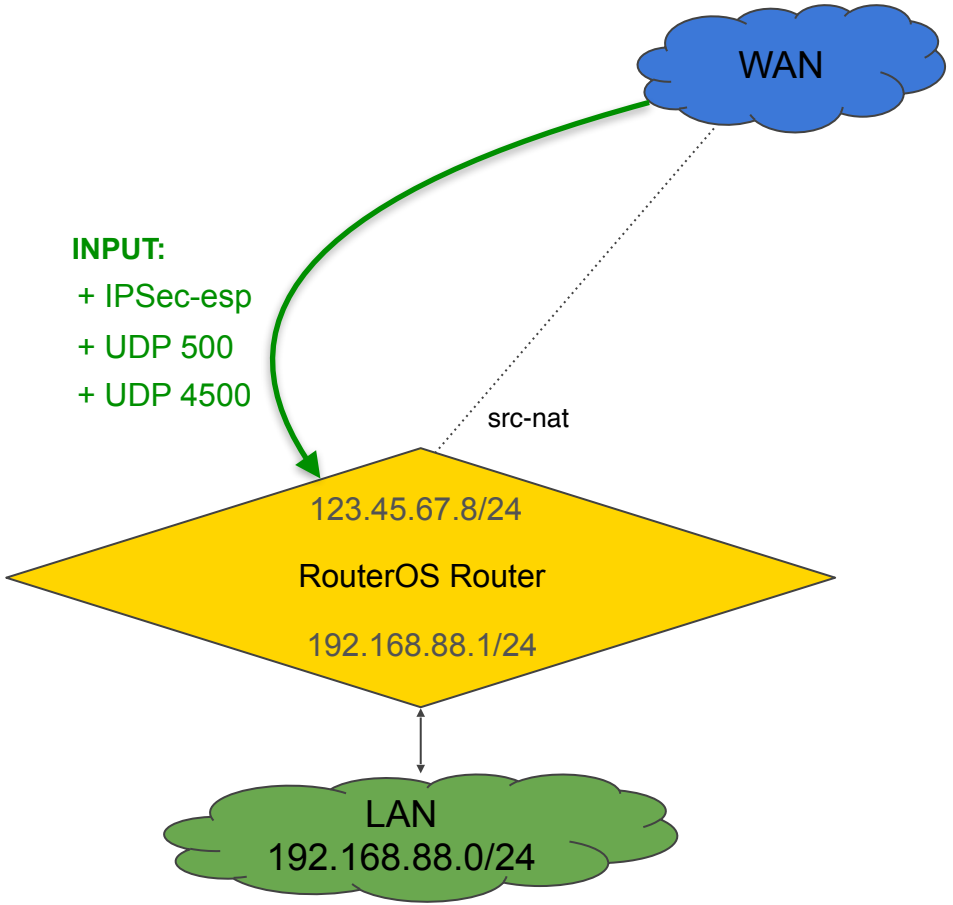
Nikita Tarikin / nikita@tarikin.com

IPSec traffic rules



Nikita Tarikin / nikita@tarikin.com

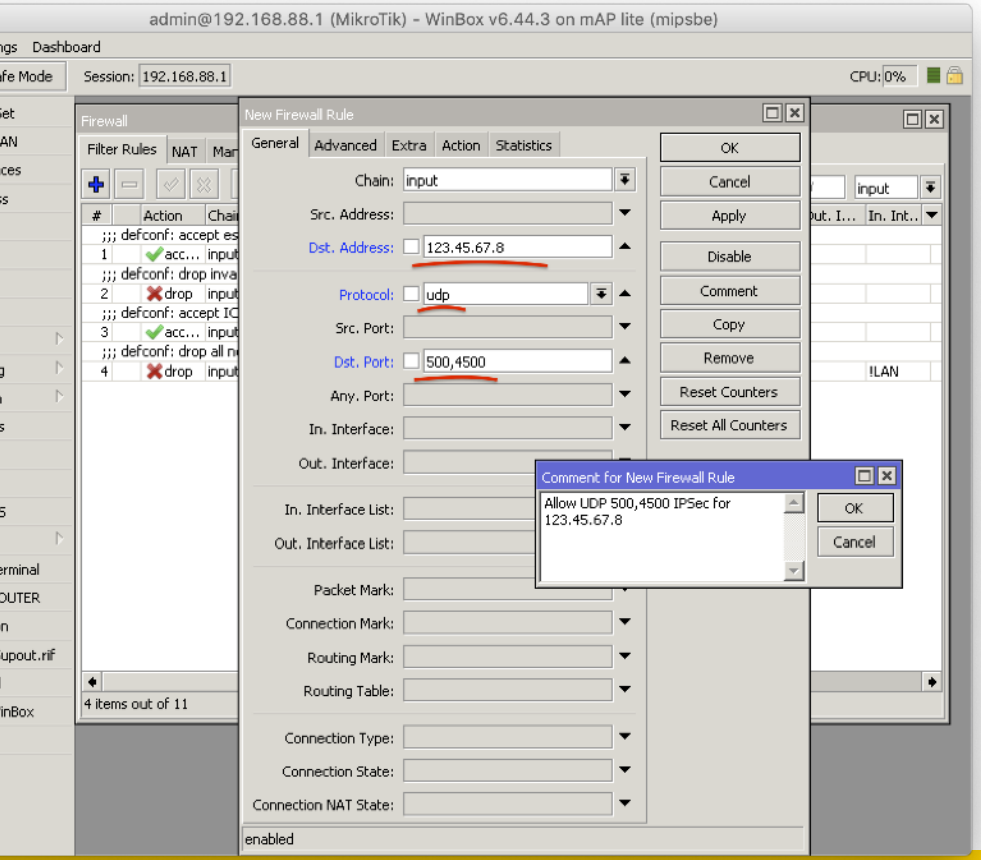
IPSec traffic rules



Firewall filter rules for IPSec ike2 packets (defconf)

INPUT chain

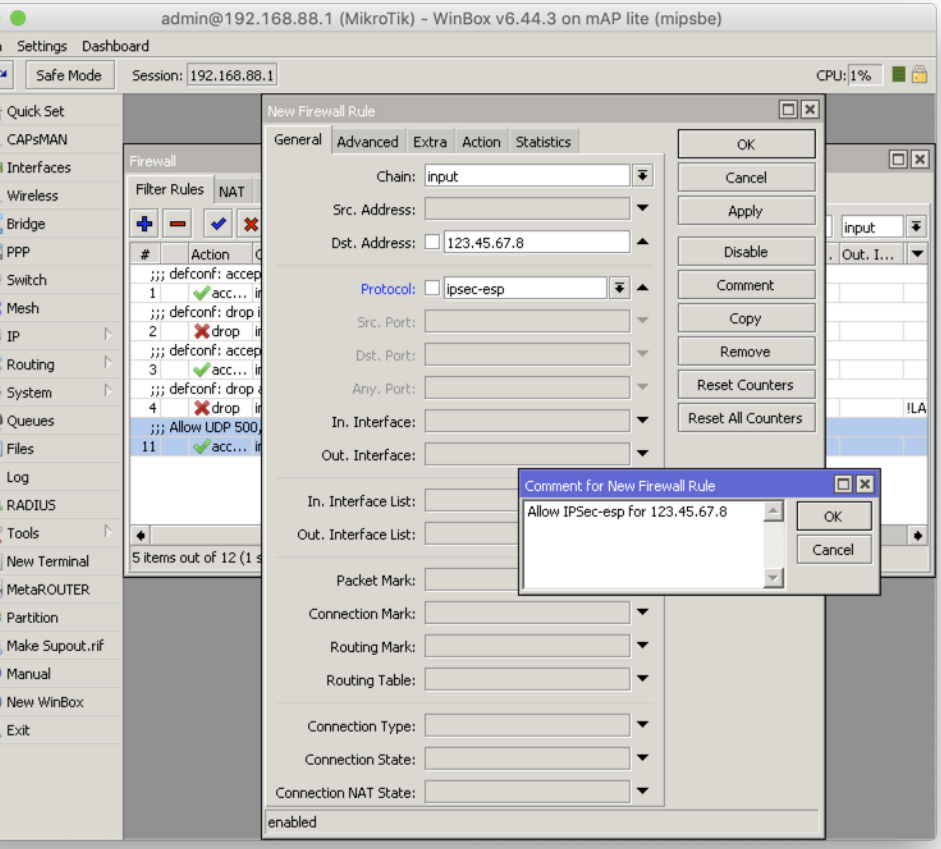
+ UDP 500
+ UDP 4500




```
/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



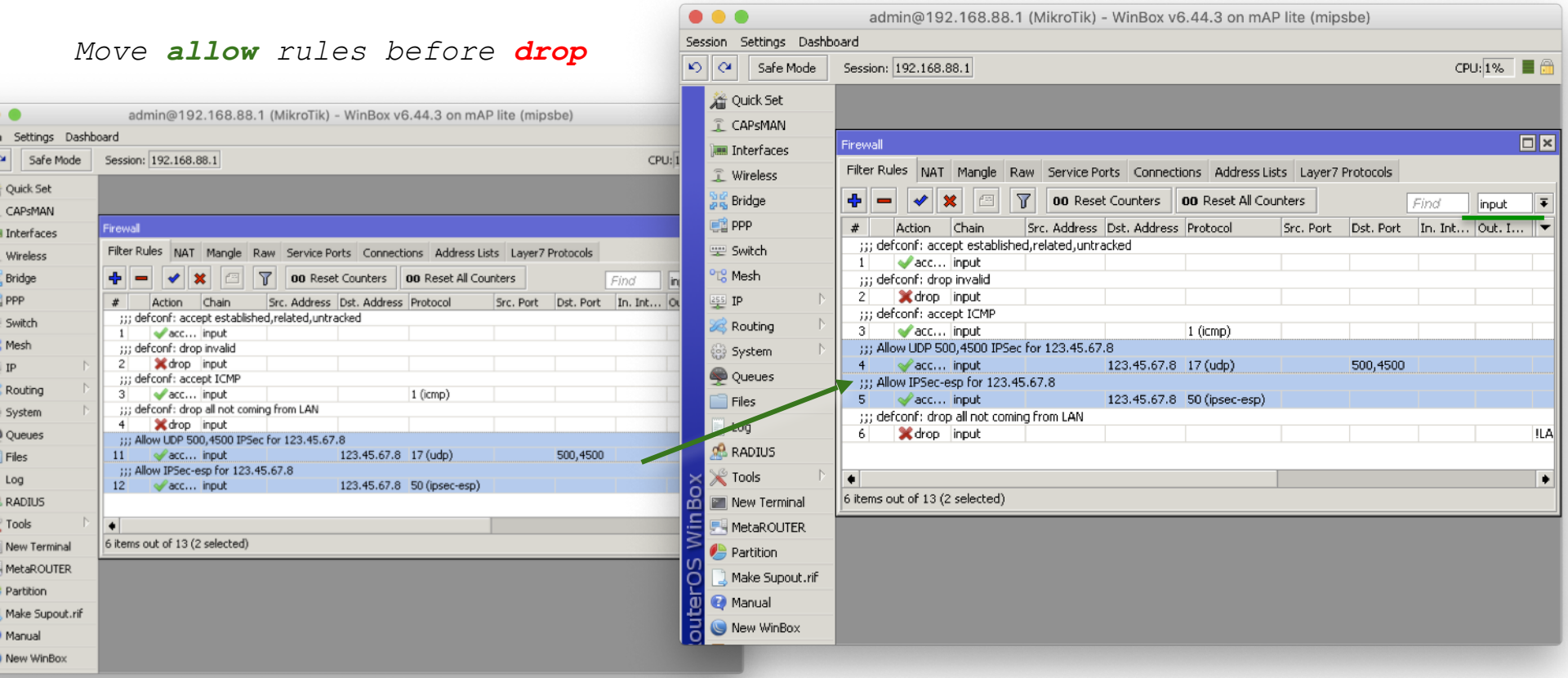
+ IPSec-esp

```
/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"
```

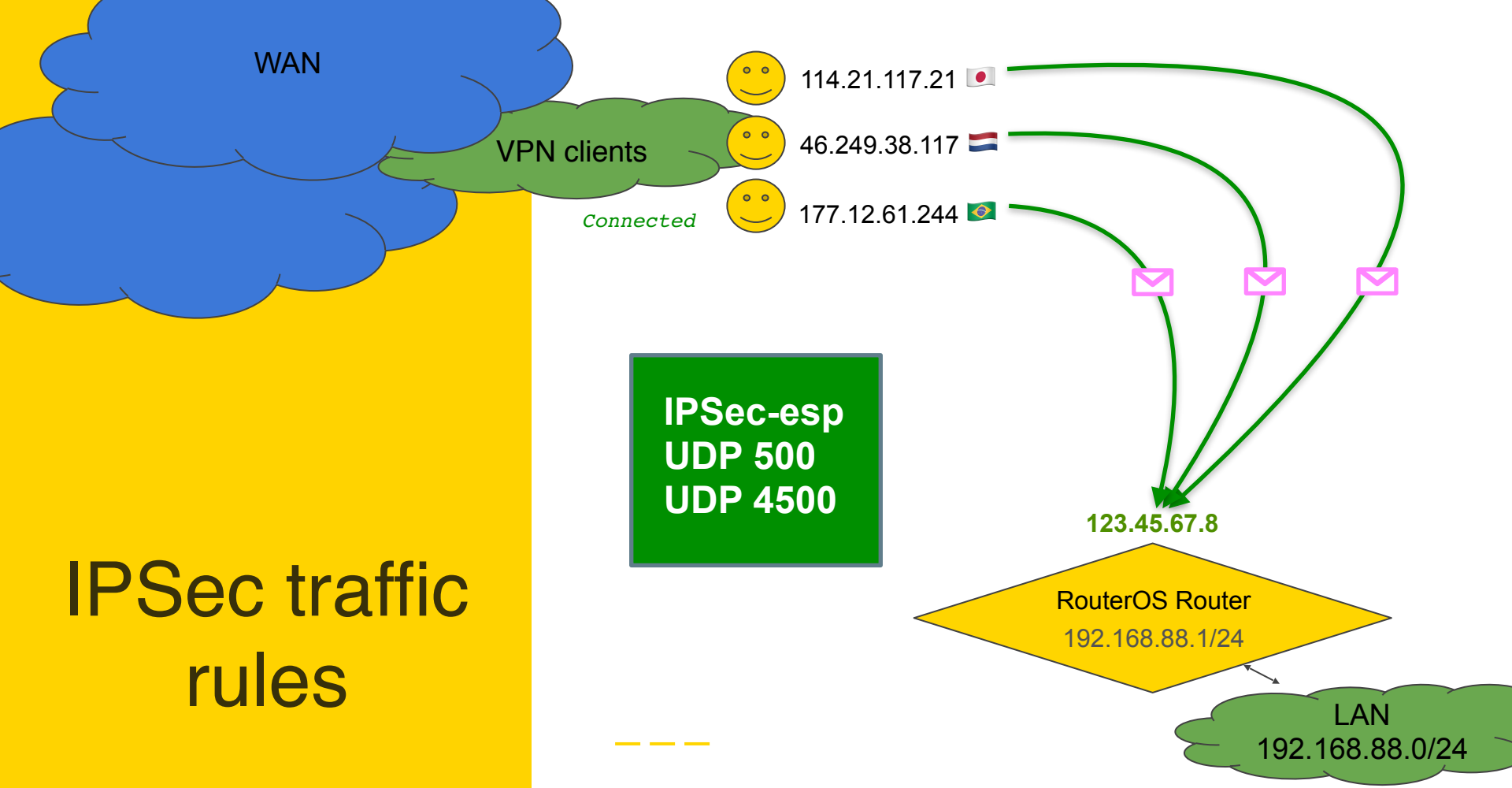
Firewall filter rules for IPSec ike2 packets (defconf)

INPUT chain

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



IPSec traffic rules



Nikita Tarikin / nikita@tarikin.com

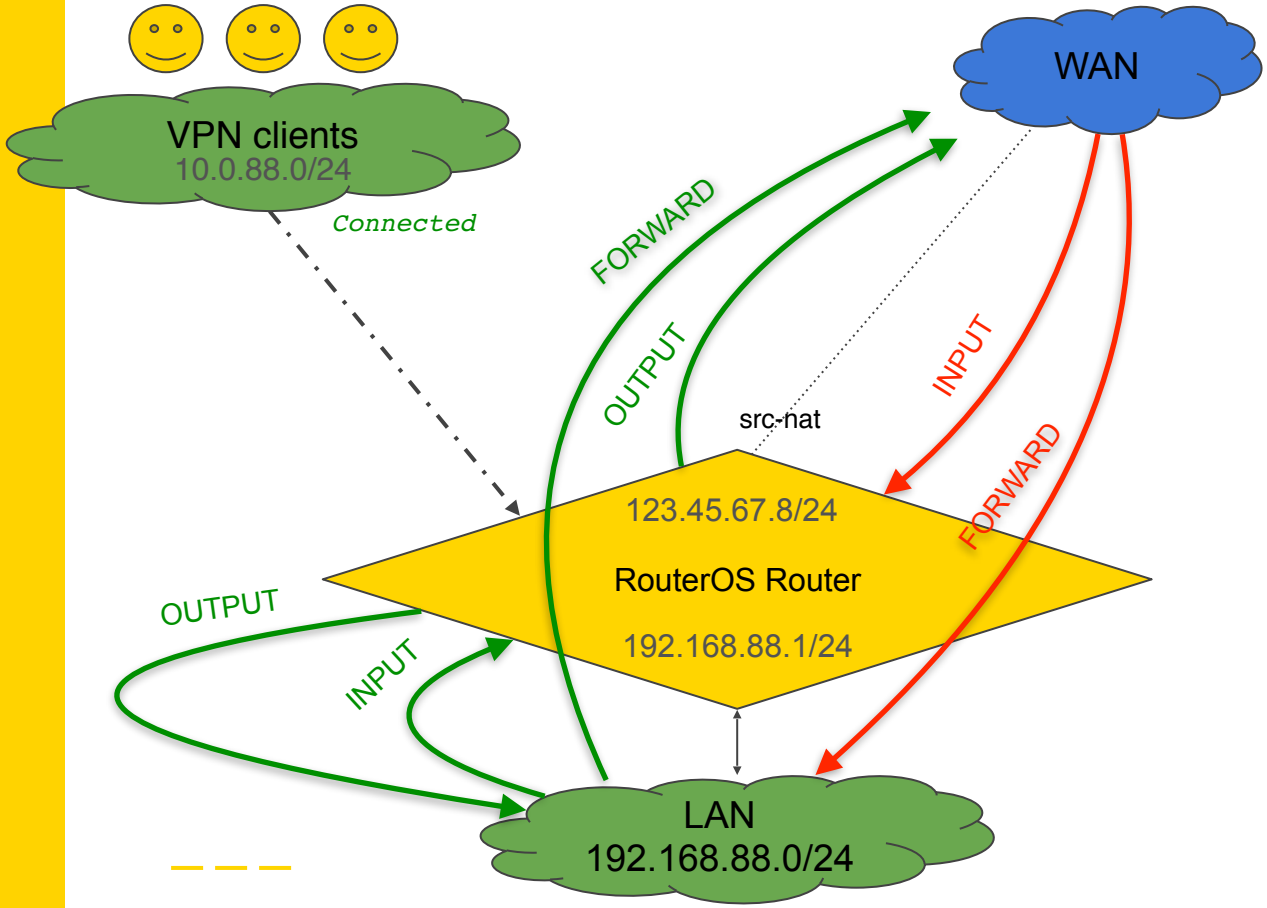
Setting up Firewall

VPN traffic rules

Nikita Tarikin / nikita@tarikin.com

Setting up Firewall

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



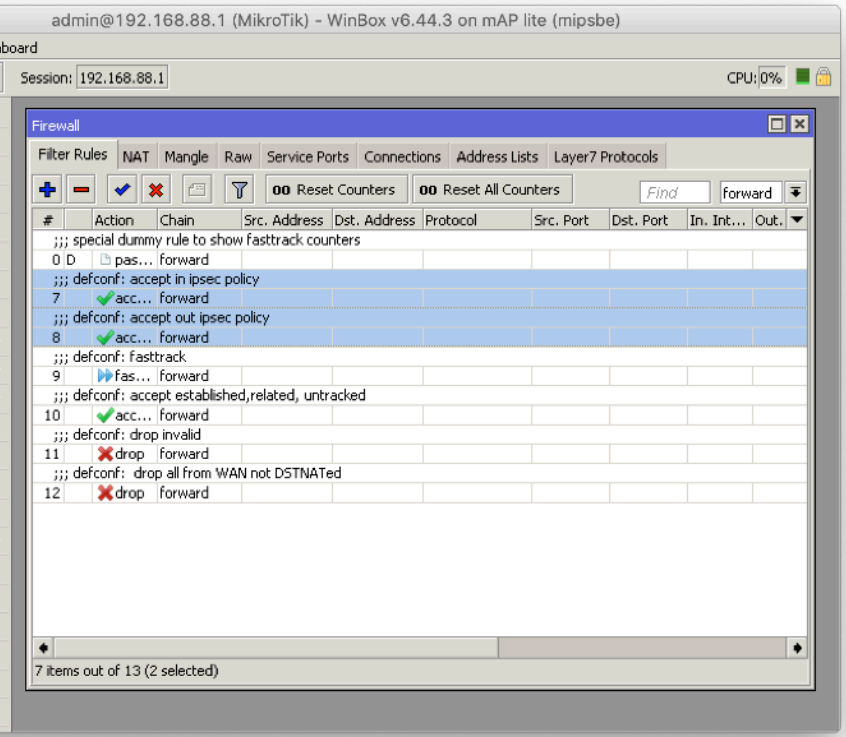
Nikita Tarikin / nikita@tarikin.com

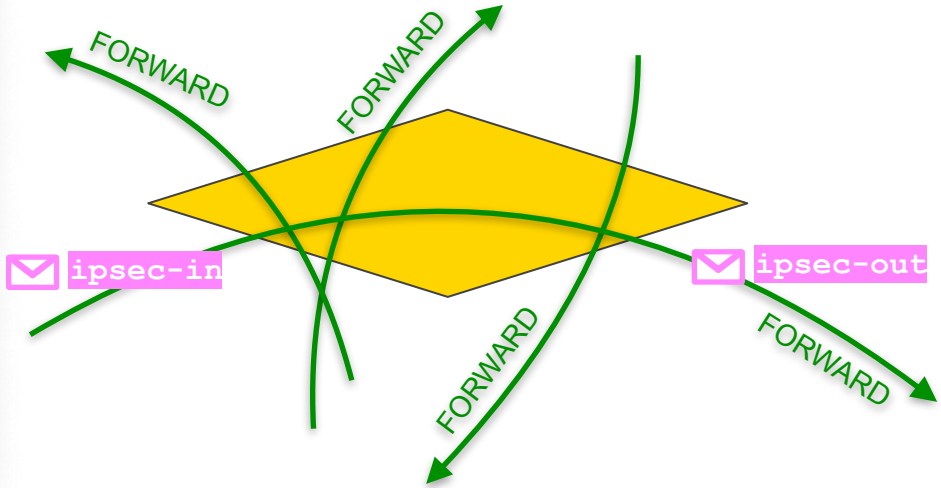
Default ipsec rules (defconf)

FORWARD chain

FROM ***ANY*** *to* ***ANY*** **ipsec-in** ***accept***

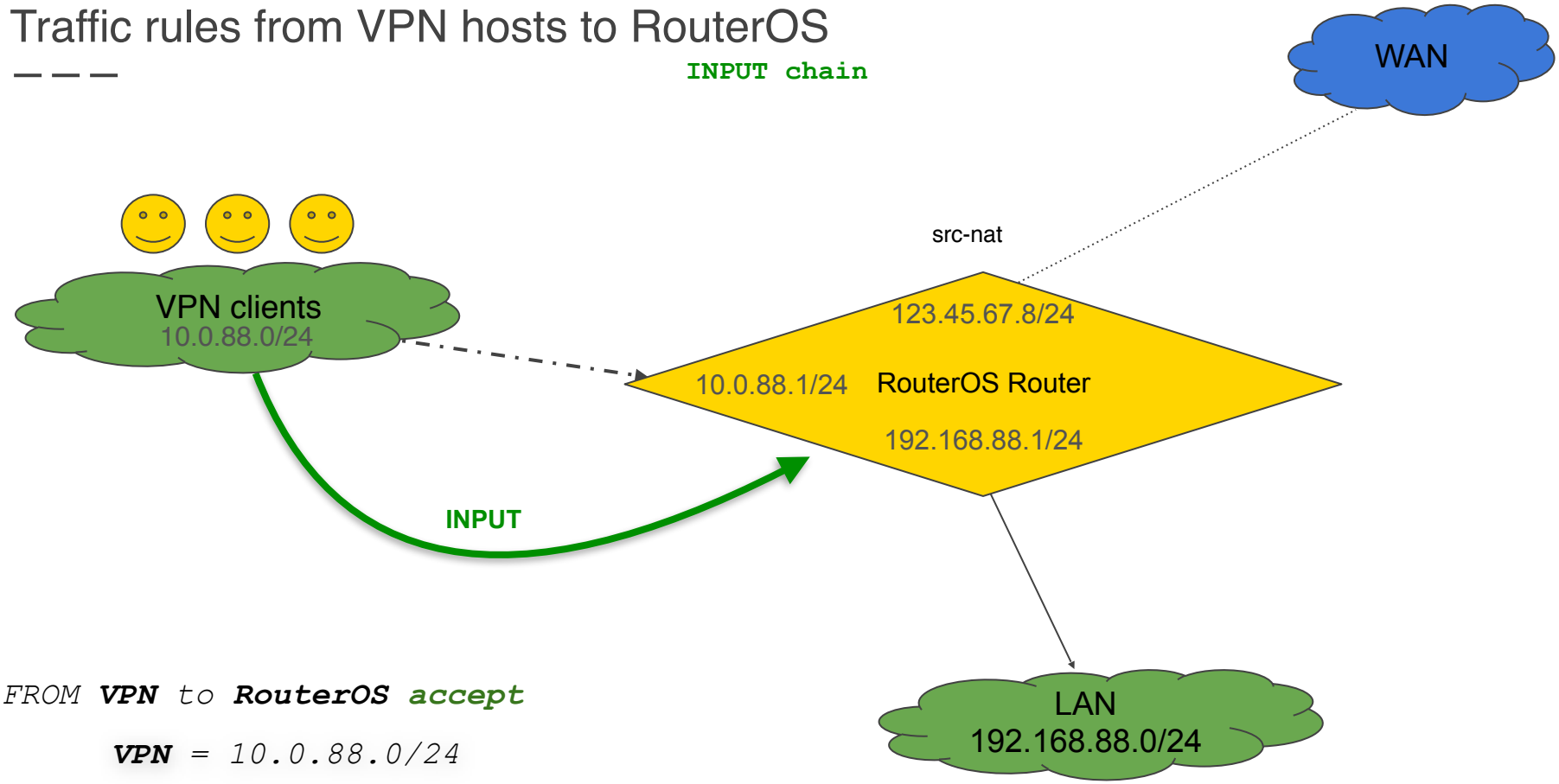
FROM ***ANY*** *to* ***ANY*** **ipsec-out** ***accept***





Traffic rules from VPN hosts to RouterOS

INPUT chain



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

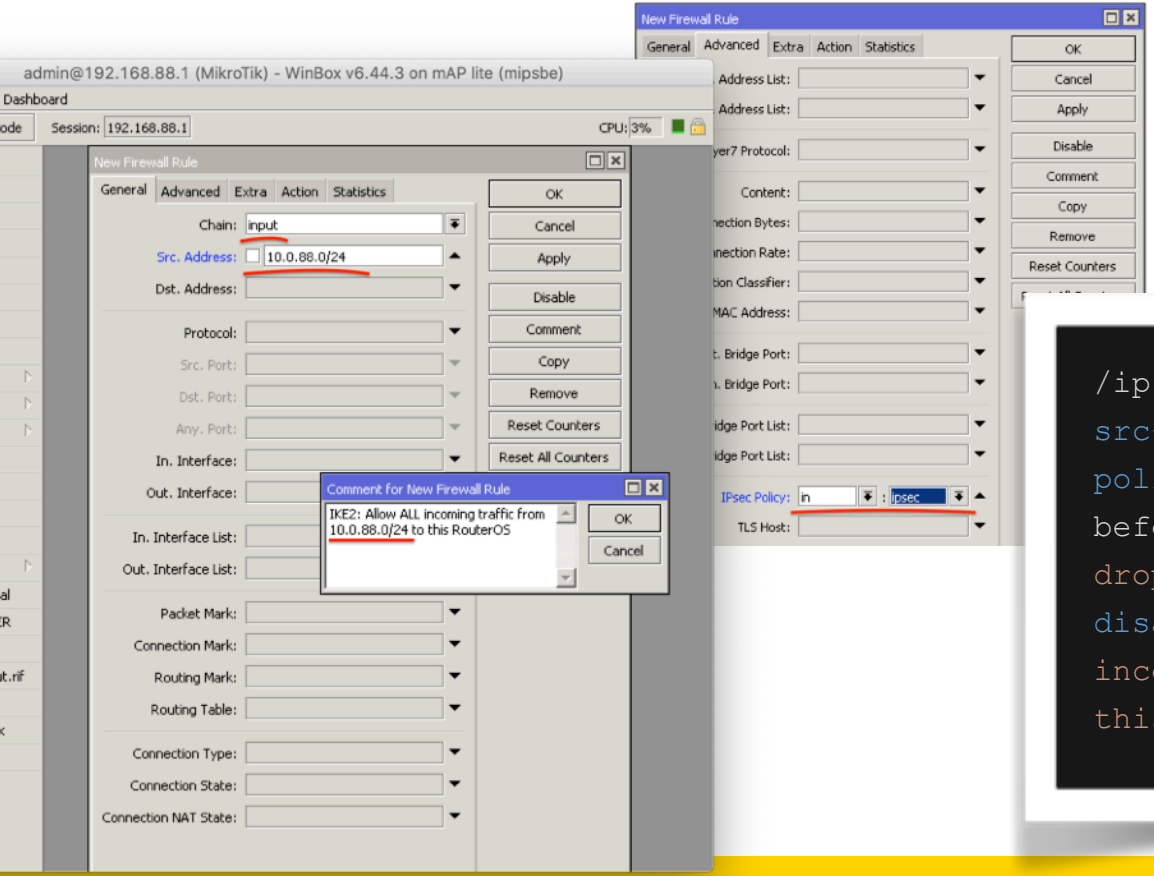
***VPN** = 10.0.88.0/24*

Traffic rules from VPN hosts to RouterOS

INPUT chain

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

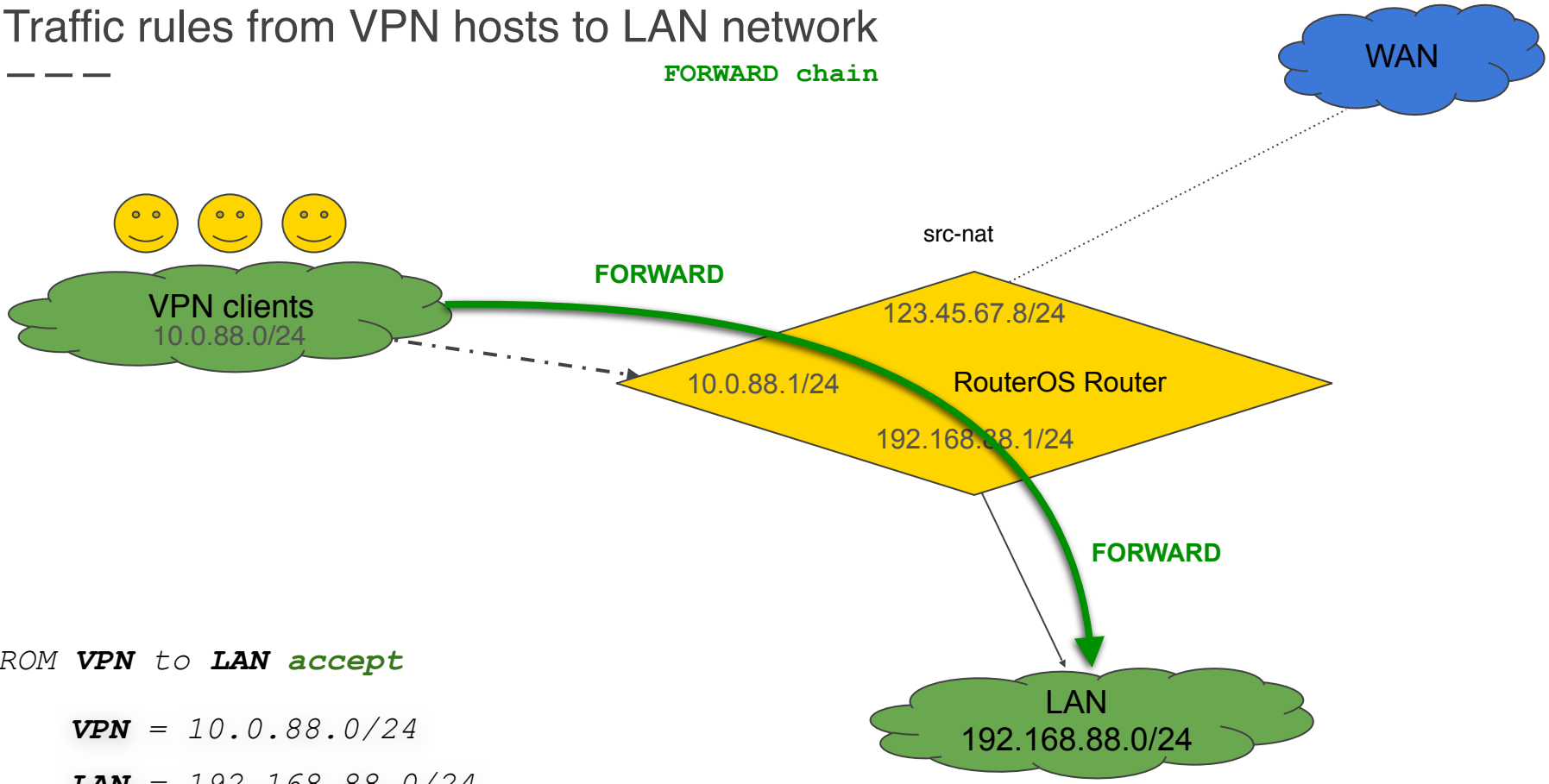
VPN *= 10.0.88.0/24*




```
/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*

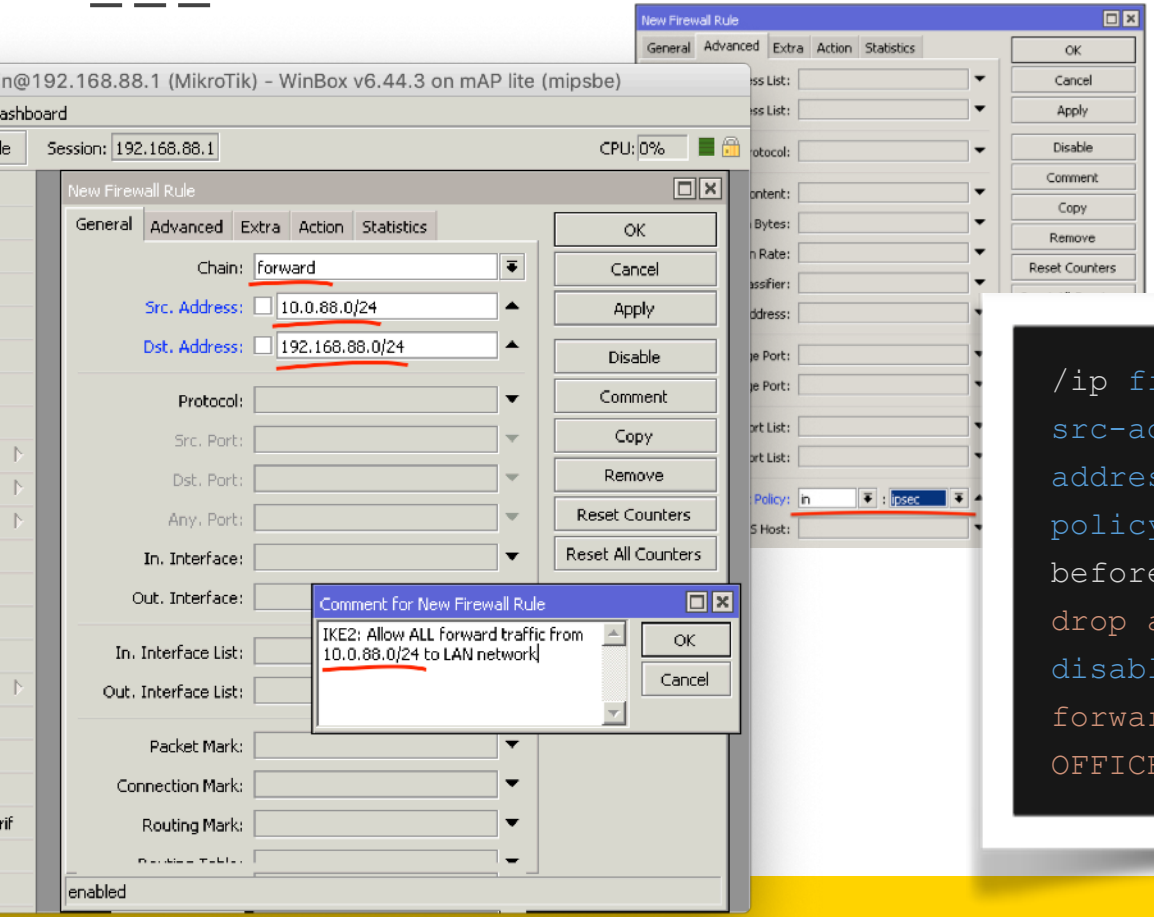
Traffic rules from VPN hosts to LAN network

FORWARD chain

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

***VPN** = 10.0.88.0/24*

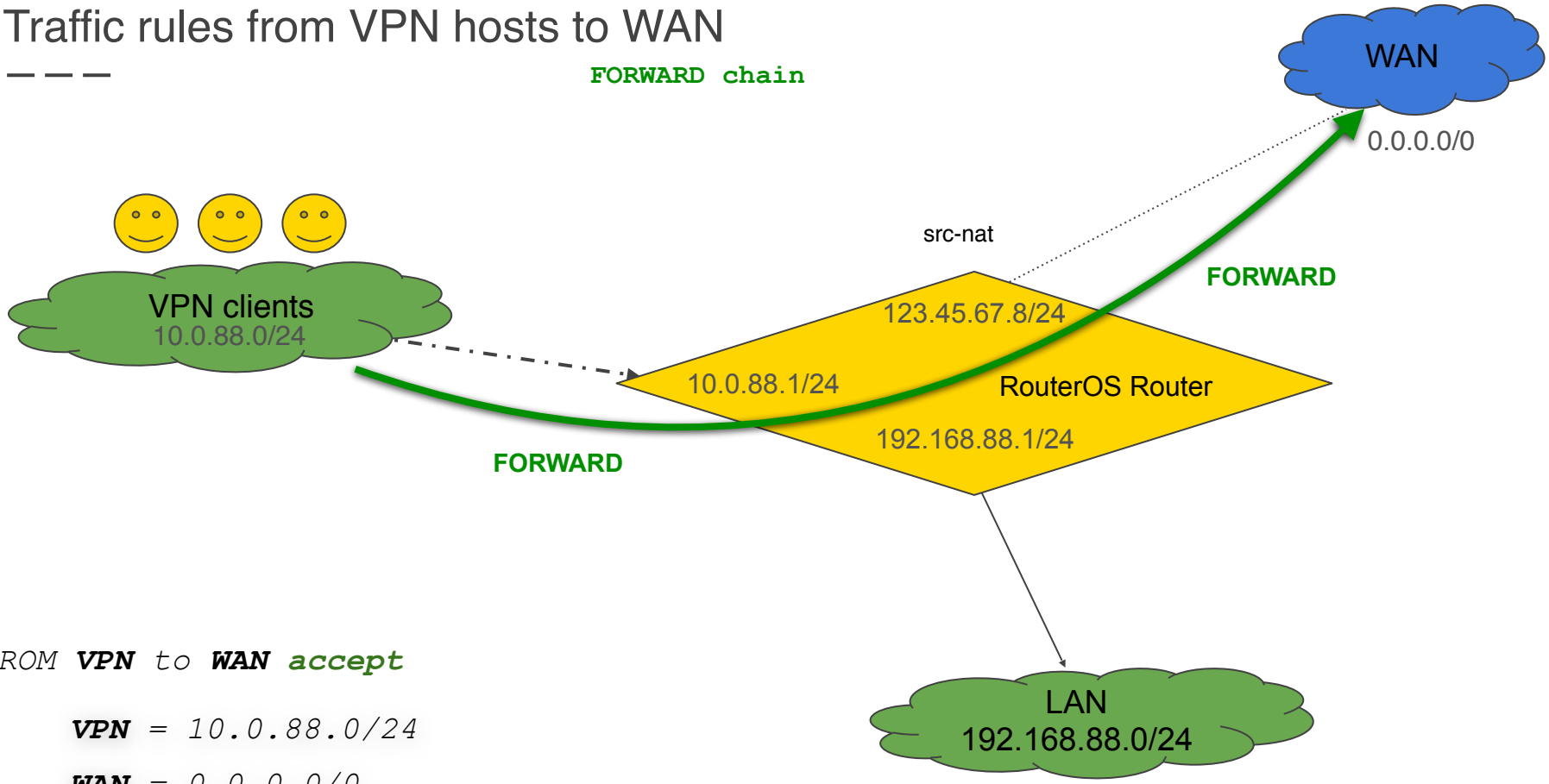
***LAN** = 192.168.88.0/24*




```
/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*

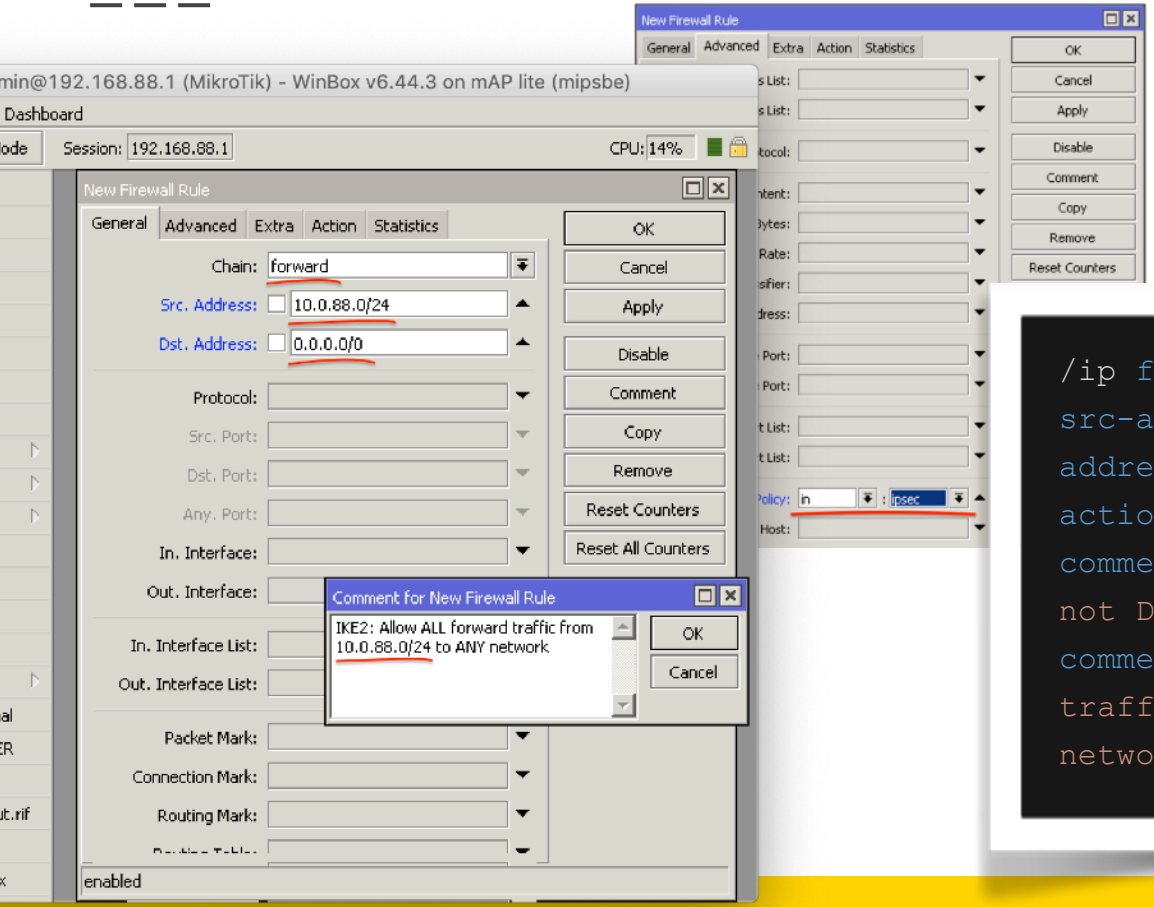
Traffic rules from VPN hosts to WAN

FORWARD chain

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

***VPN** = 10.0.88.0/24*

***WAN** = 0.0.0.0/0*

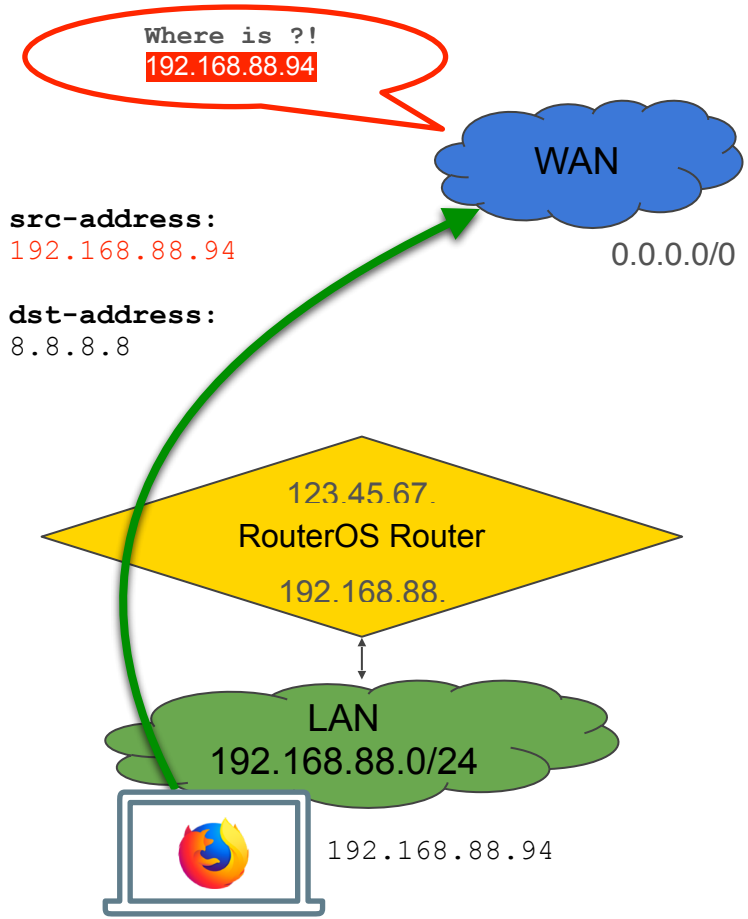



```
/ip firewall filter add chain=forward
src-address=10.0.88.0/24 dst-
address=0.0.0.0/0 ipsec-policy=in,ipsec
action=accept place-before=[ find where
comment~"defconf:  drop all from WAN
not DSTNATed" ] disabled=no
comment="IKE2: Allow ALL forward
traffic from 10.0.88.0/24 to ANY
network"
```

Setting up NAT

Setting up NAT

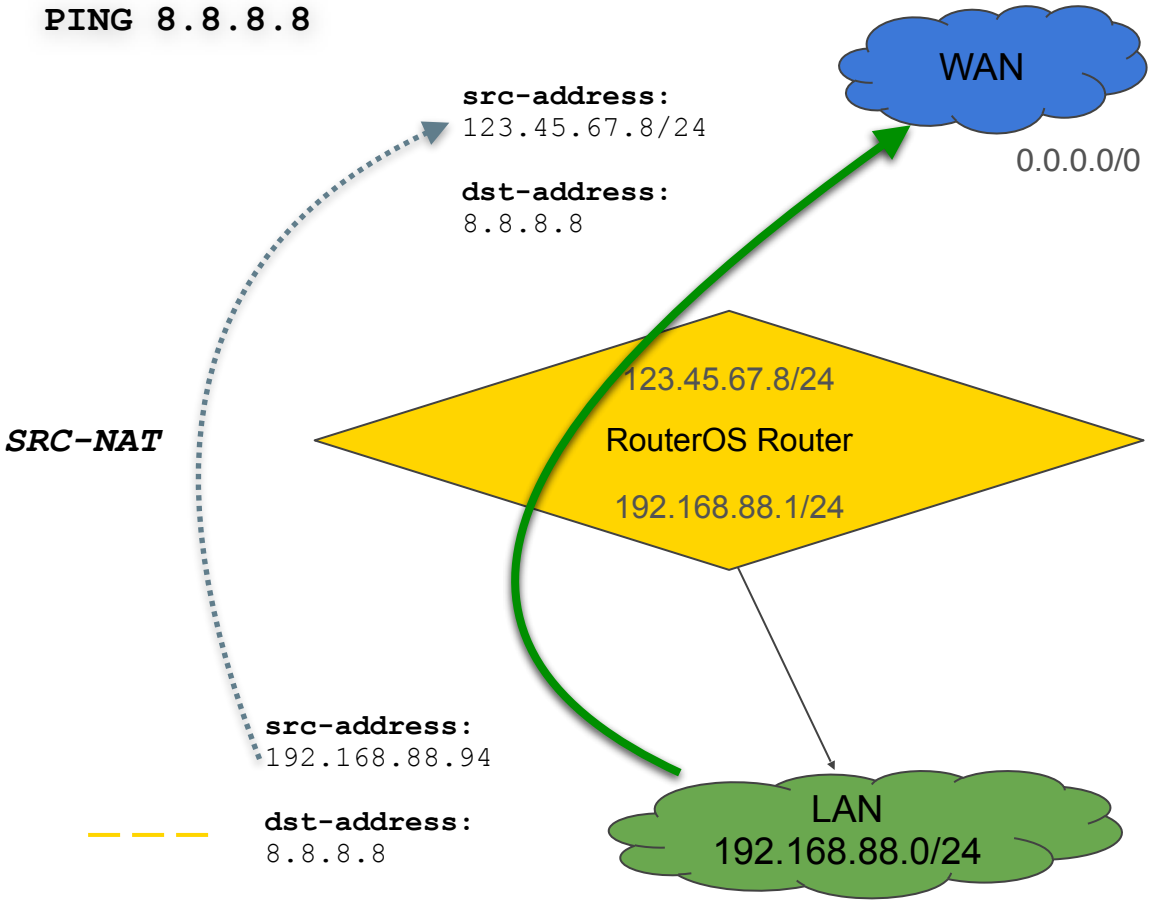
1. **Default src-nat overview**
2. SRC-NAT VPN traffic to WAN



Nikita Tarikin / nikita@tarikin.com

Setting up NAT

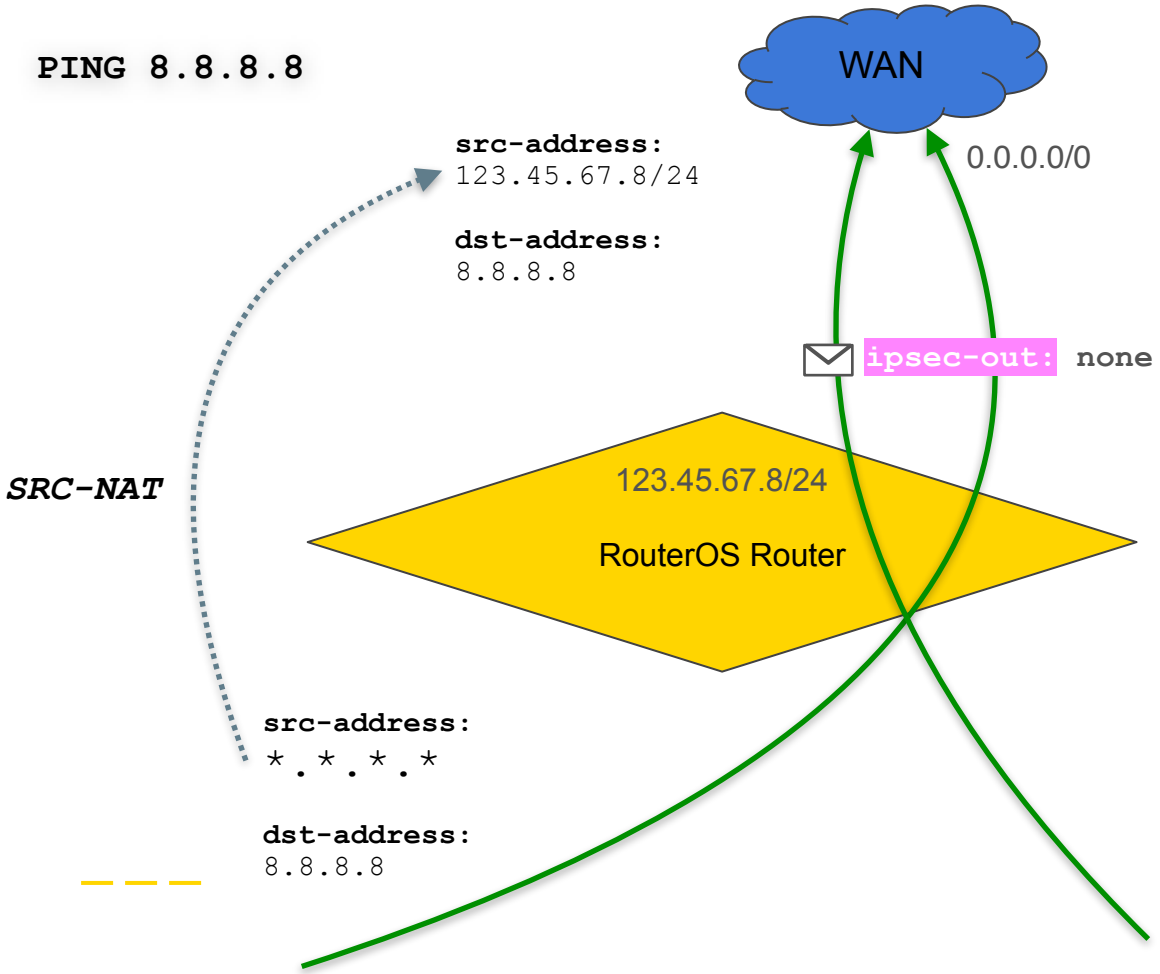
1. **Default src-nat overview**
2. SRC-NAT VPN traffic to WAN



Nikita Tarikin / nikita@tarikin.com

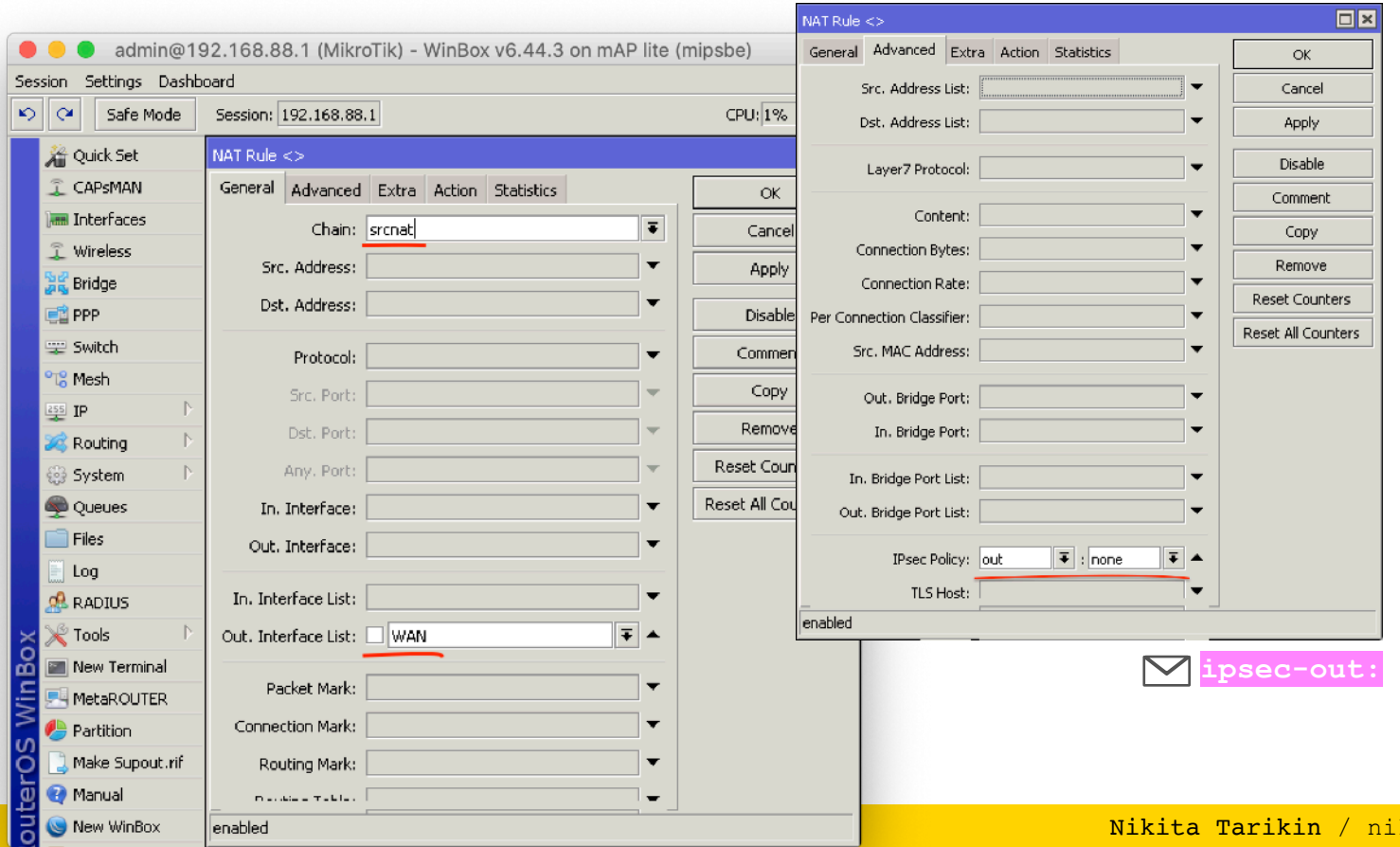
Setting up NAT

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



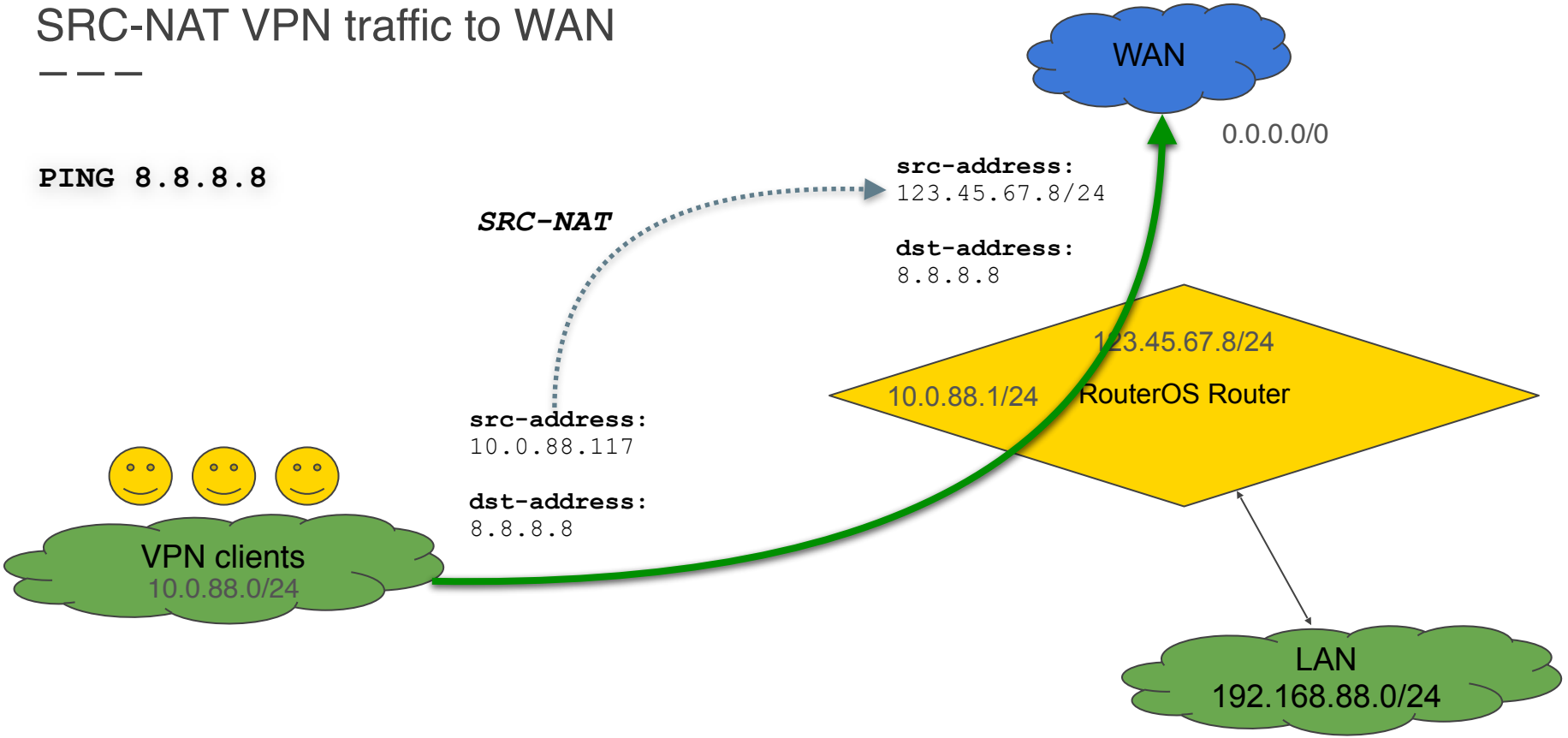
Nikita Tarikin / nikita@tarikin.com

Masquerade non-IPSec WAN traffic (defconf)

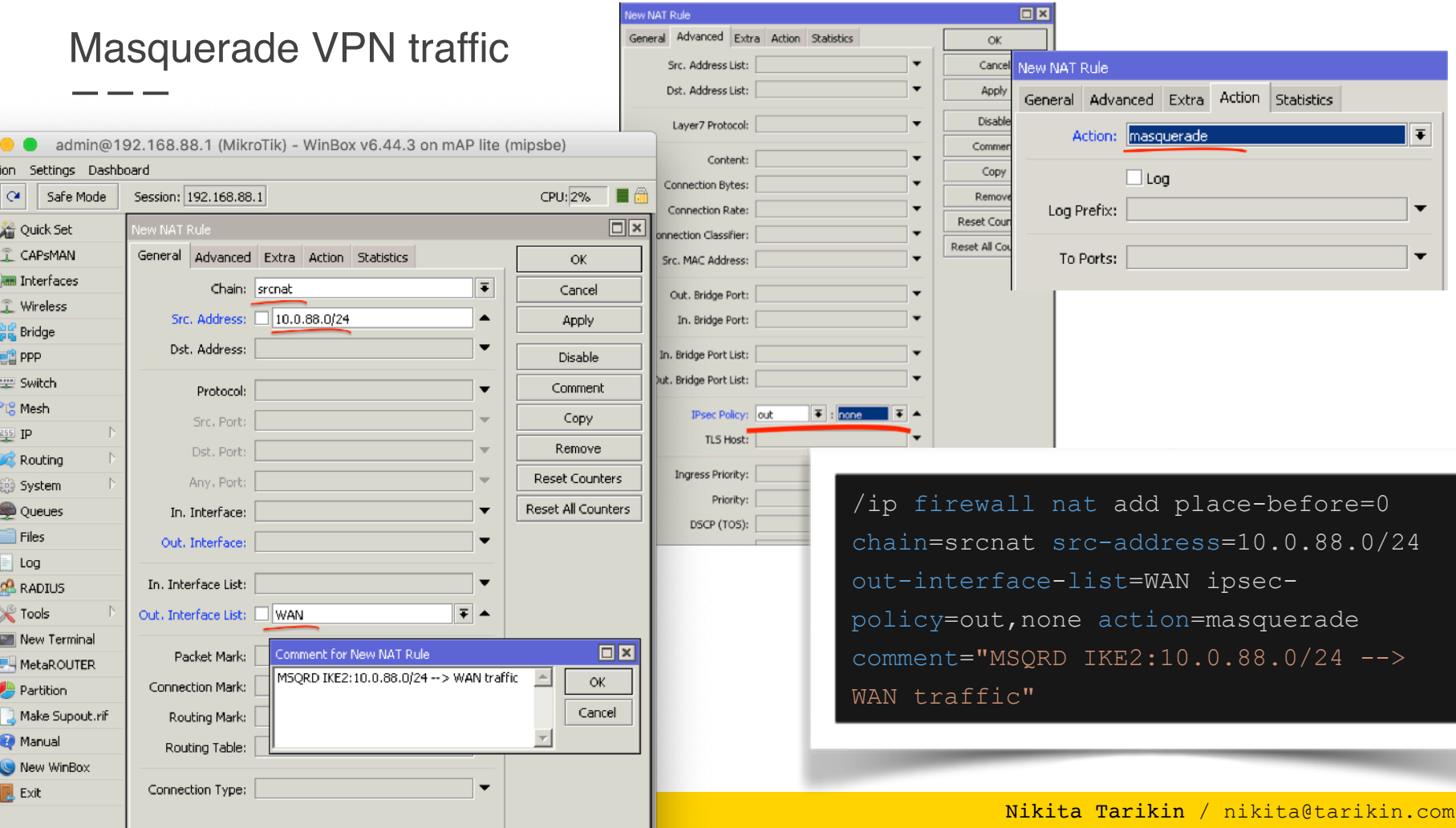


ipsec-out: none

SRC-NAT VPN traffic to WAN

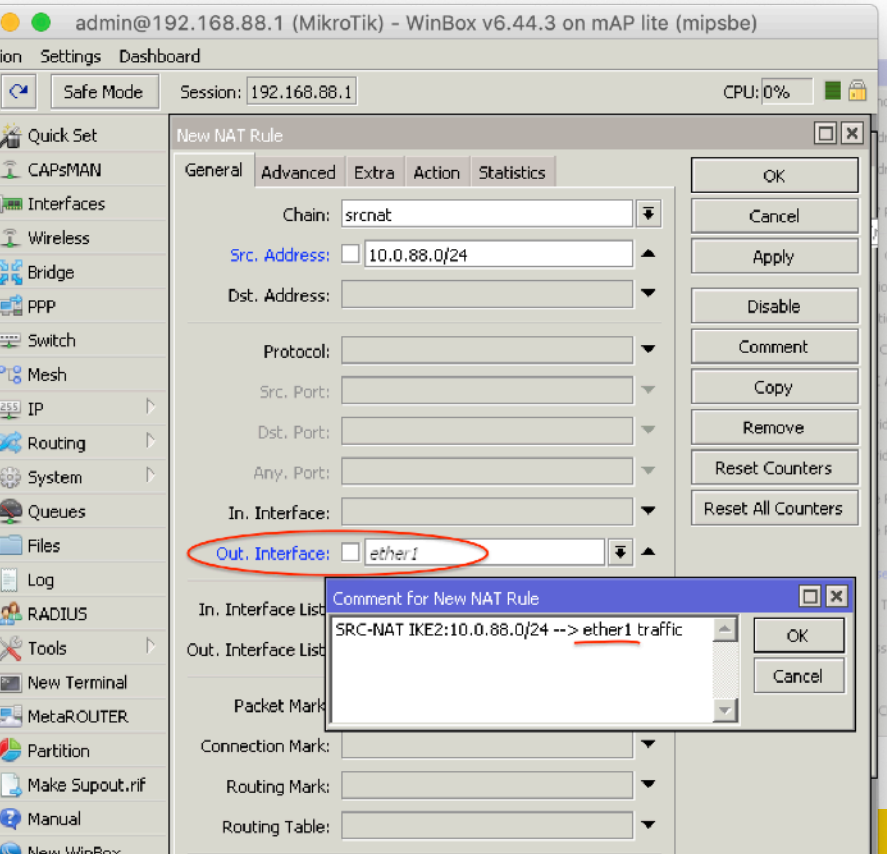


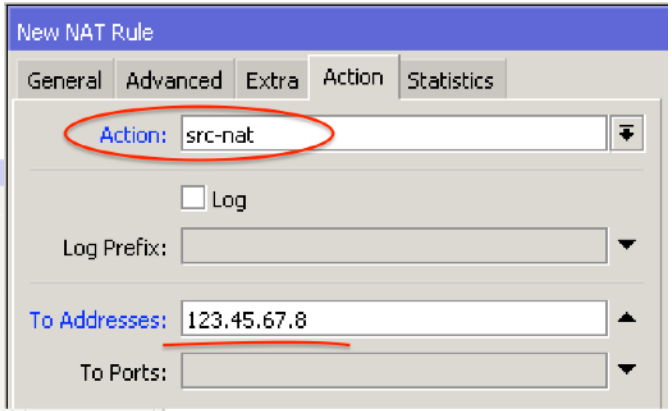
Masquerade VPN traffic




```
/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"
```

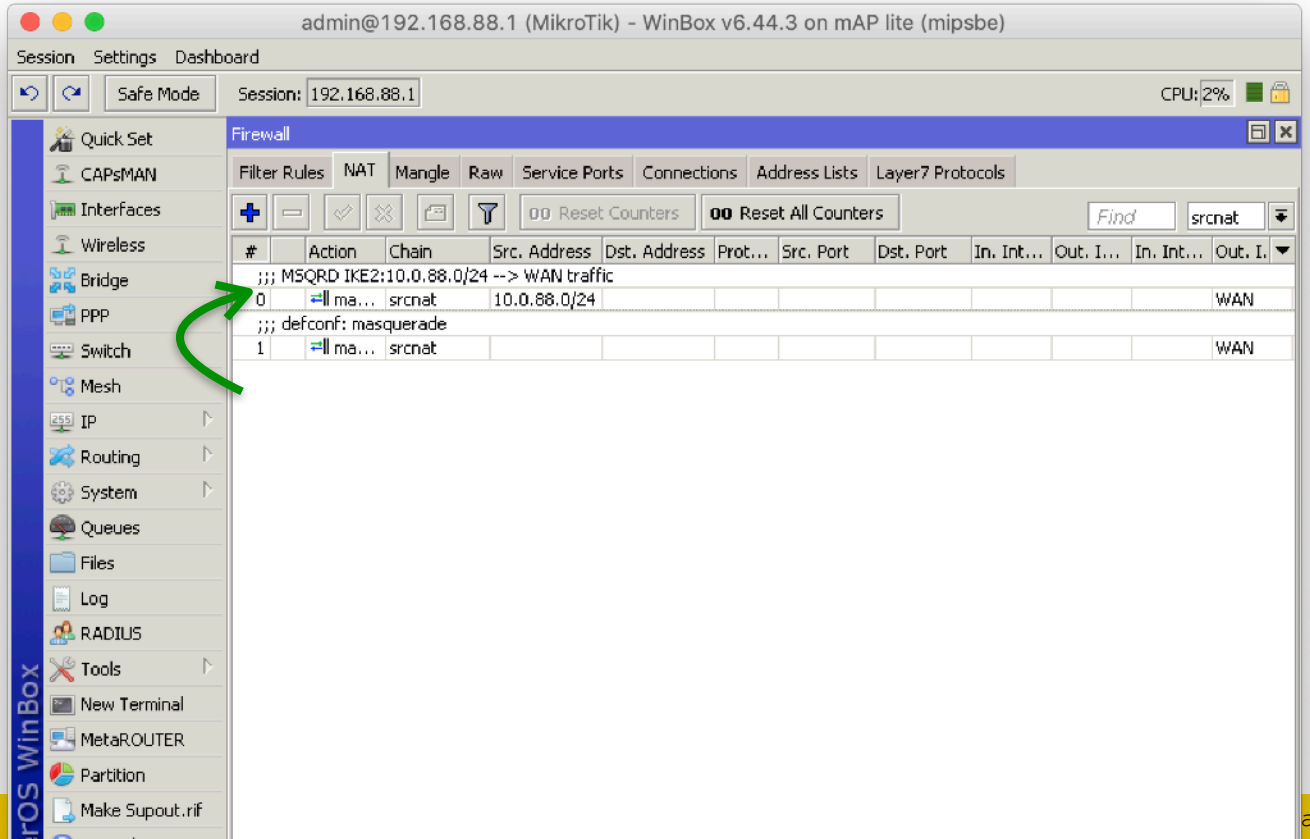
SRC-NAT VPN traffic (recommended) 👍






```
/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



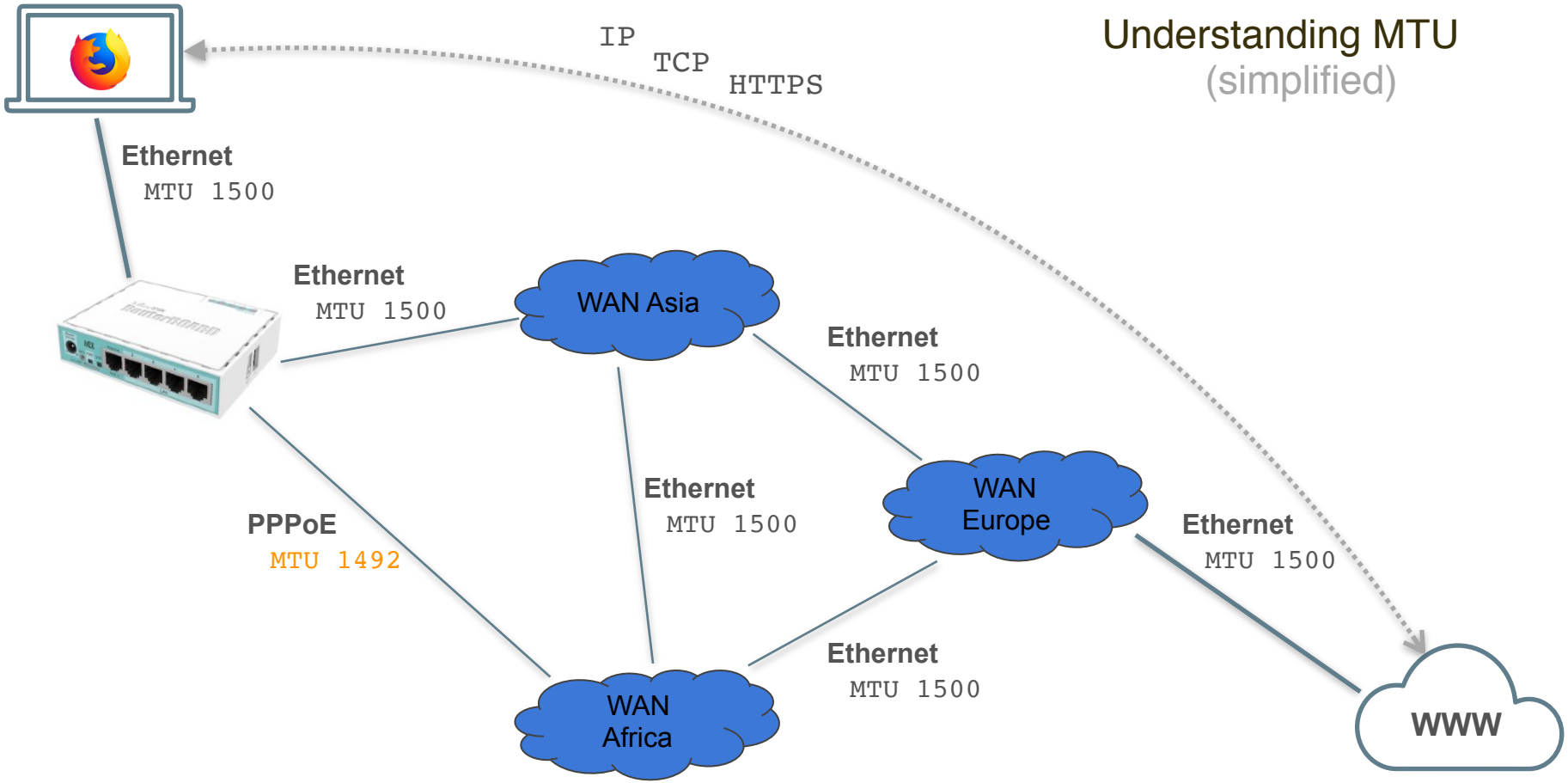
Setting up TCP MSS

Agenda for next slides

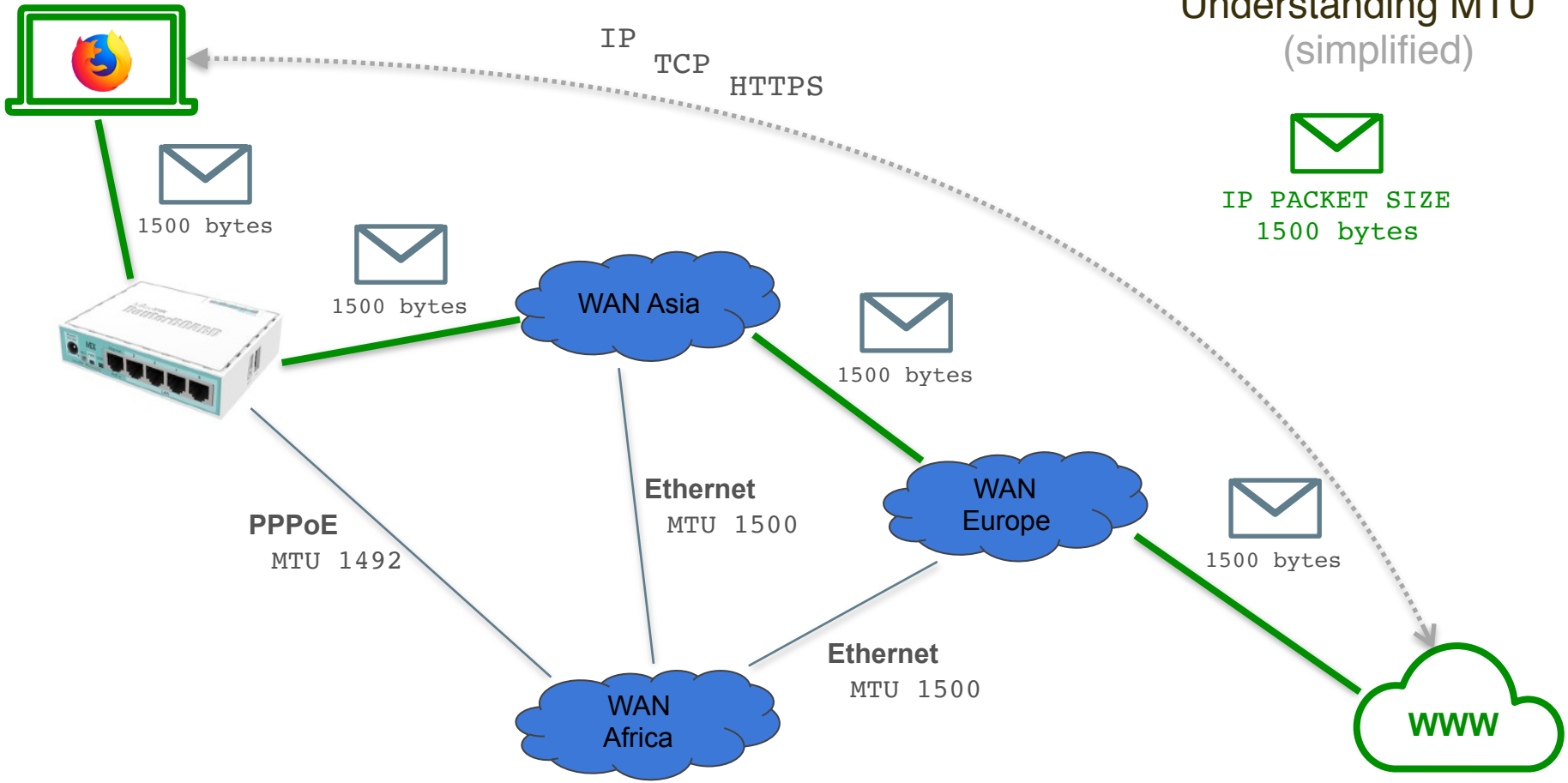
1. Understanding MTU and IP fragmentation
2. Understanding IPSec MTU
3. Understanding TCP MSS
4. Setting up TCP MSS over IKE2

Nikita Tarikin / nikita@tarikin.com

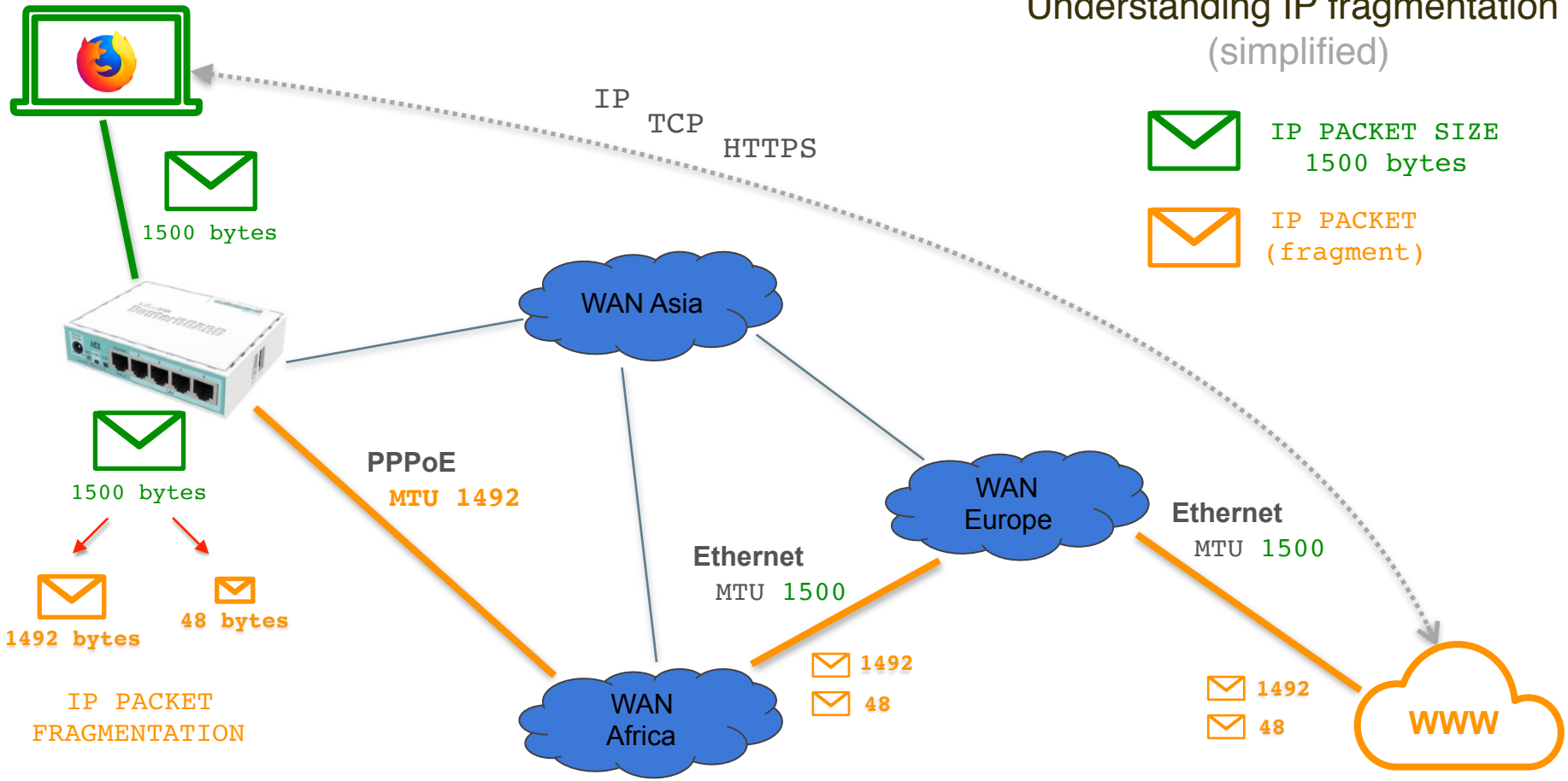
Understanding MTU
(simplified)



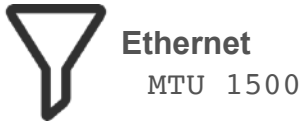
Understanding MTU
(simplified)



Understanding IP fragmentation
(simplified)

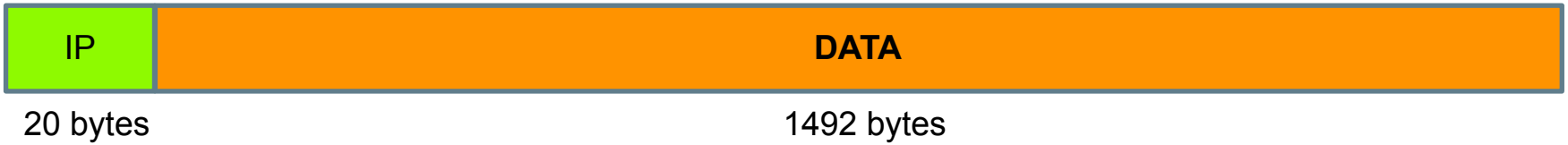


MTU missmatch —> IP fragmentation

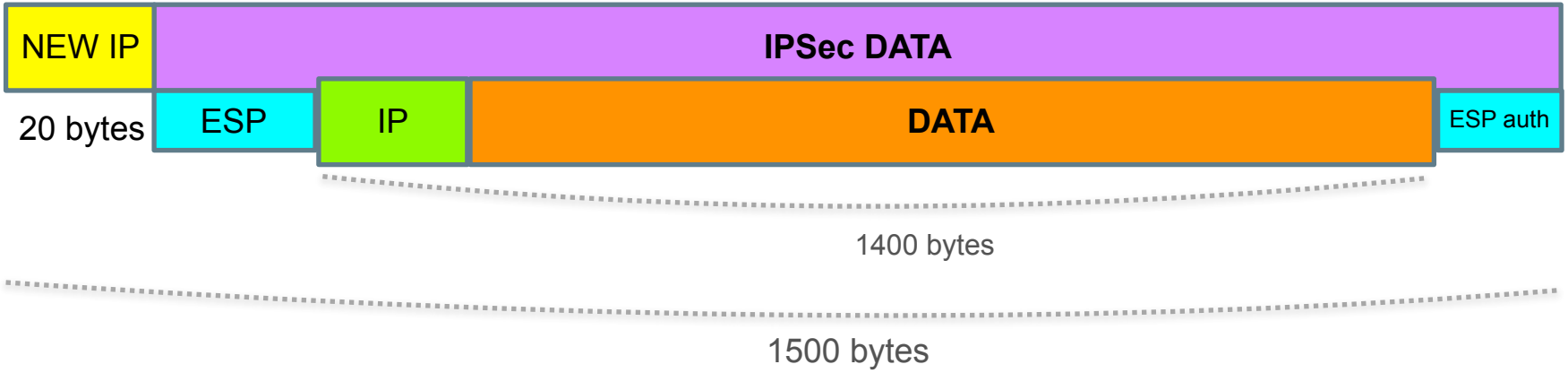


Understanding IPSec MTU (simplified)

IP packet

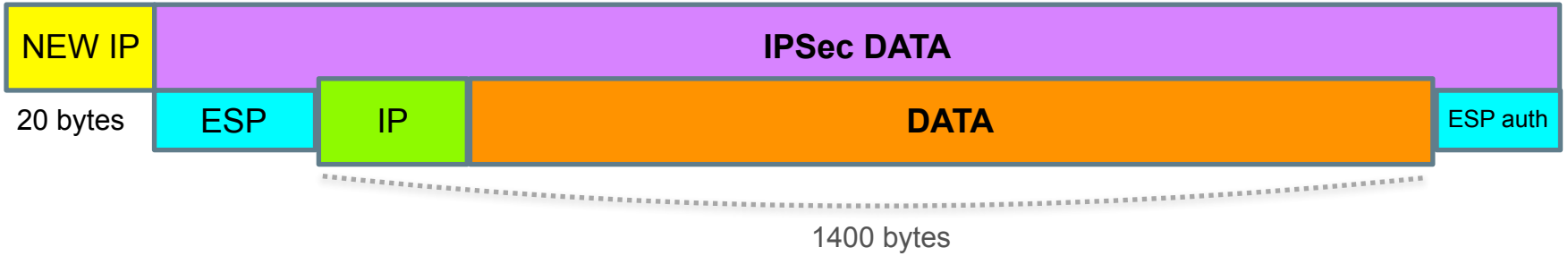


IPSec ESP packet *(tunnel mode)*

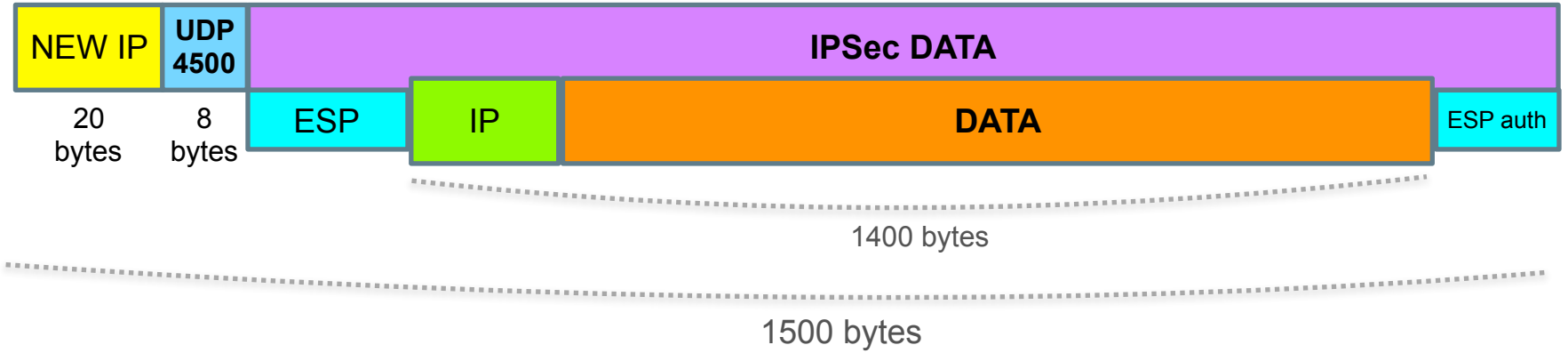


Understanding IPSec MTU (simplified)

IPSec ESP packet *(tunnel mode)*

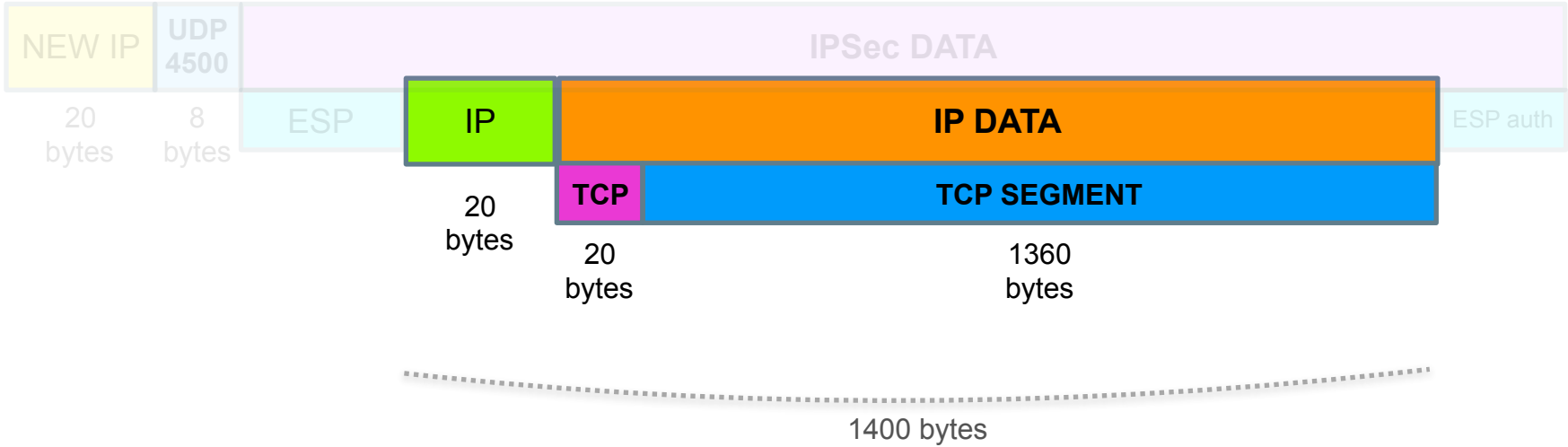


IPSec ESP packet with NAT-T *(tunnel mode)*



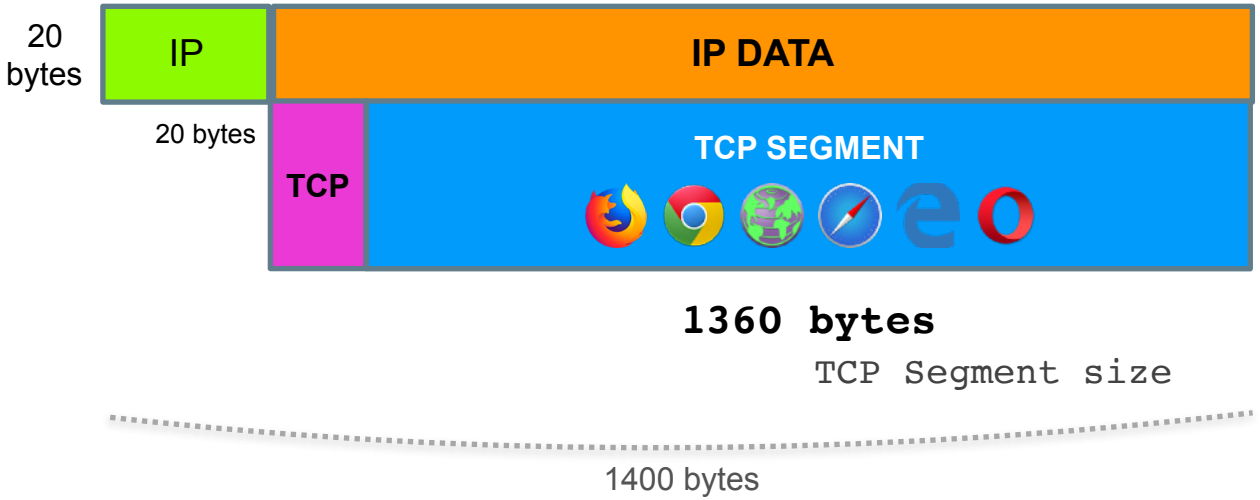
Understanding IPSec MTU (simplified)

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

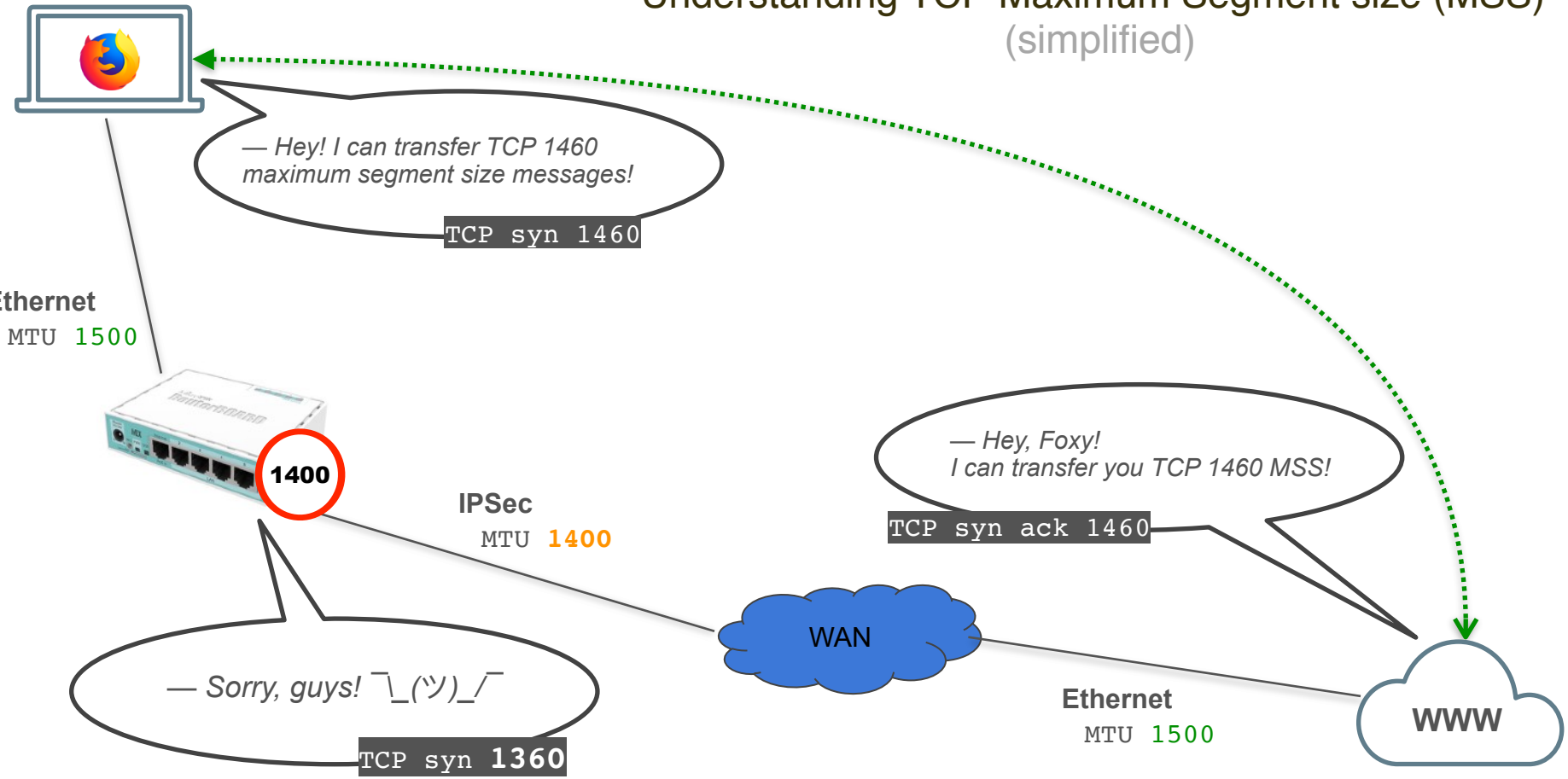


Understanding TCP MSS (simplified)

TCP Segment size = MTU - 40 bytes

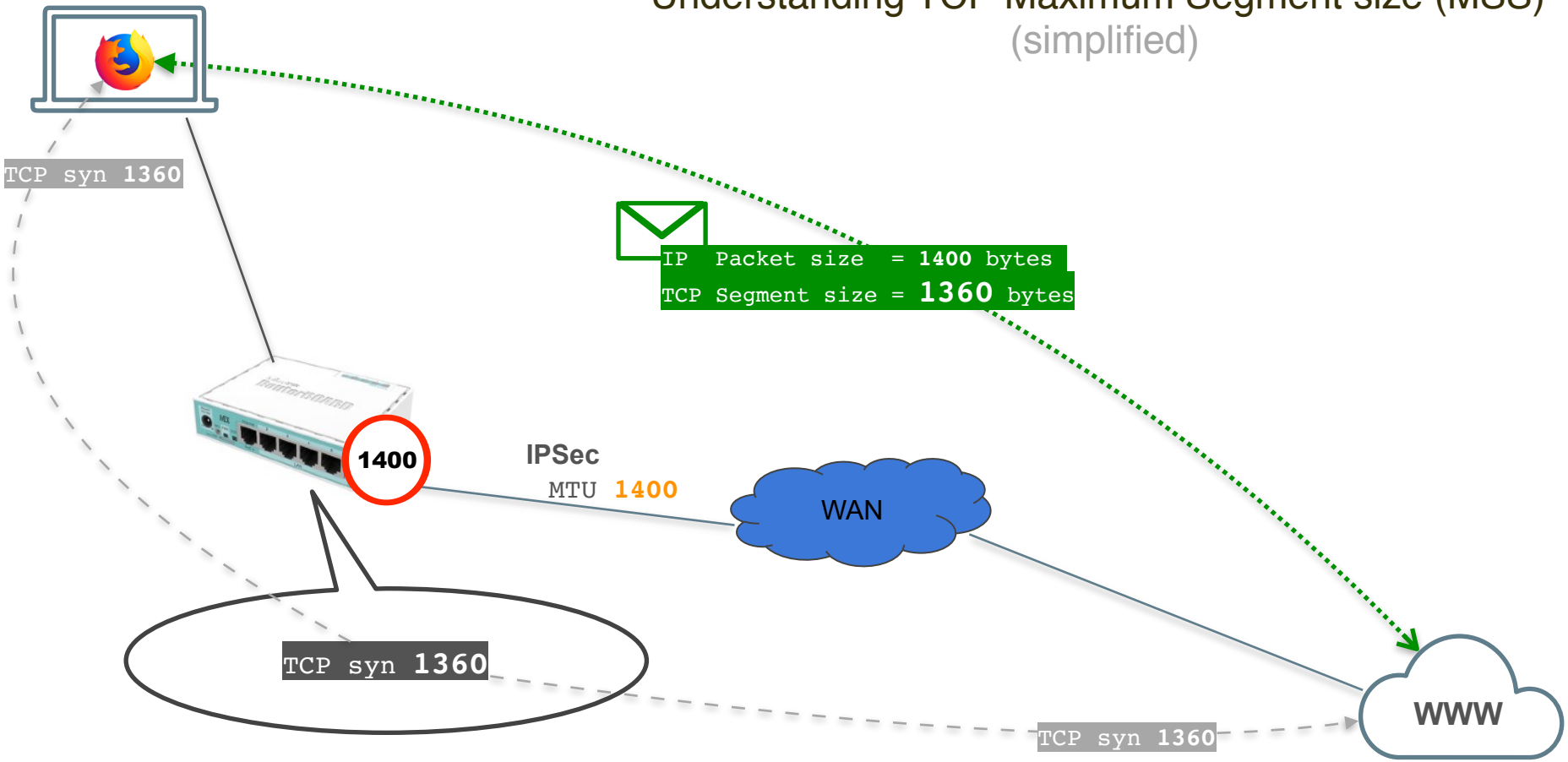


Understanding TCP Maximum Segment size (MSS)
(simplified)



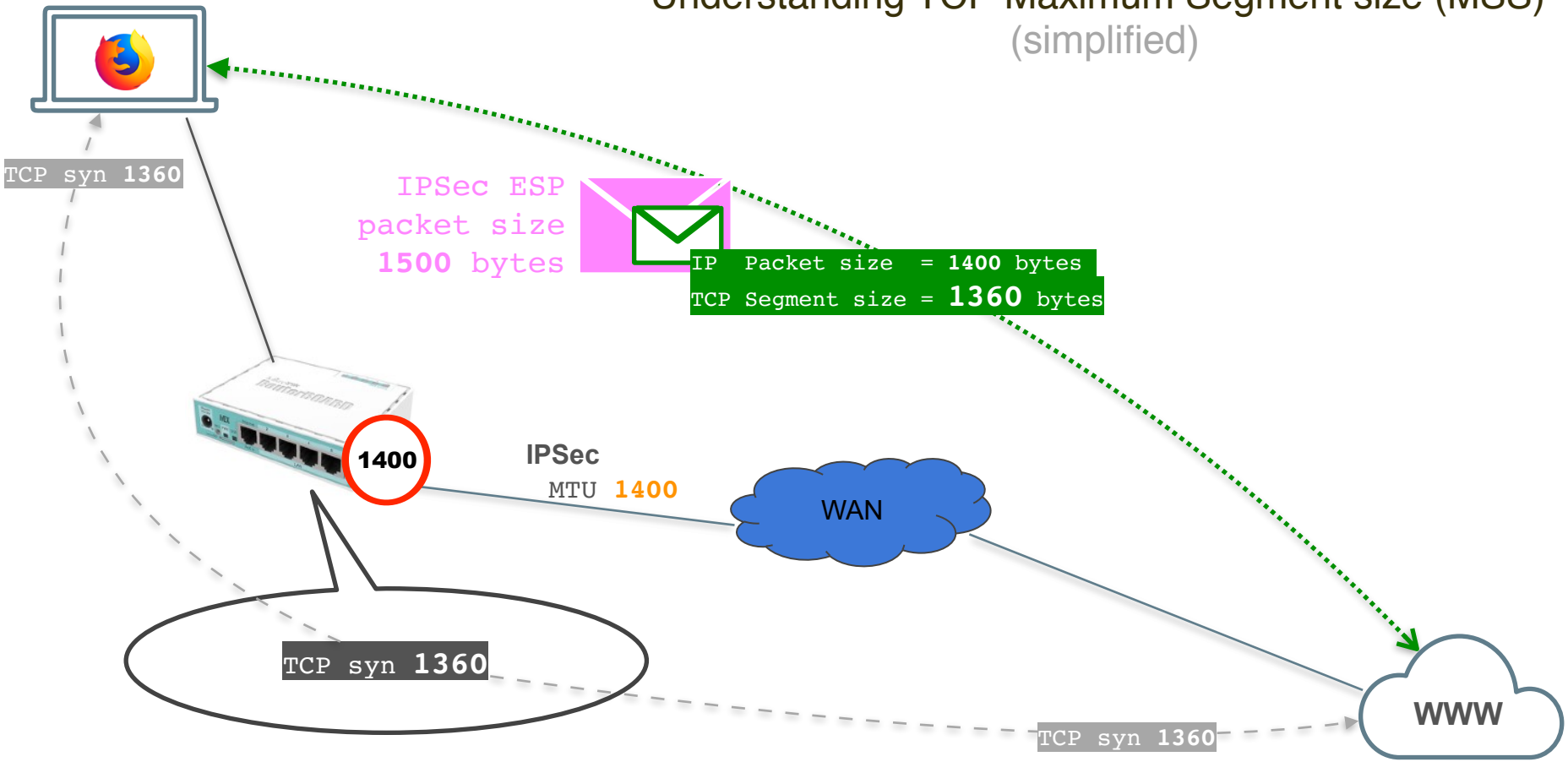
Understanding TCP Maximum Segment size (MSS)

(simplified)

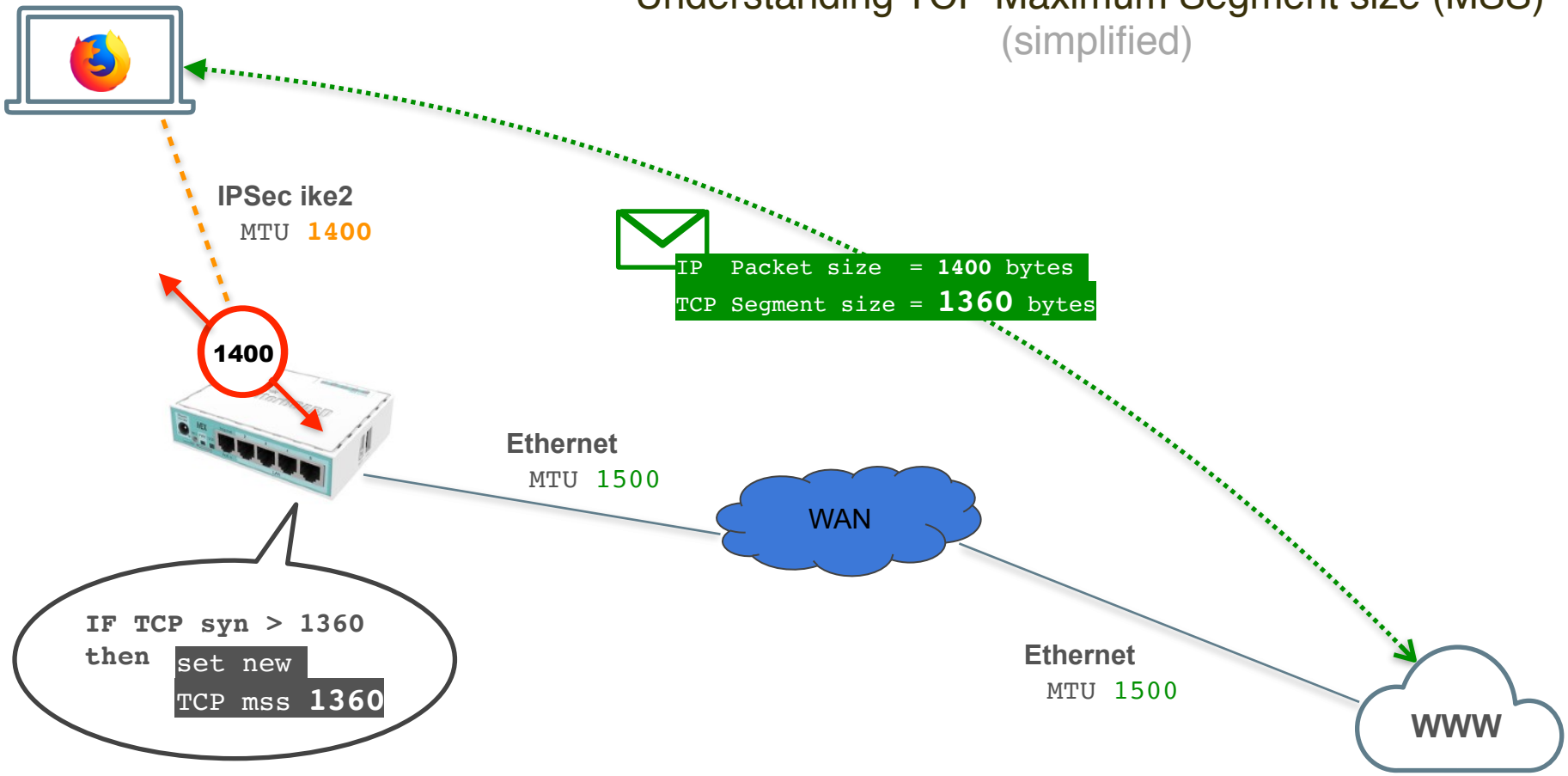


Understanding TCP Maximum Segment size (MSS)

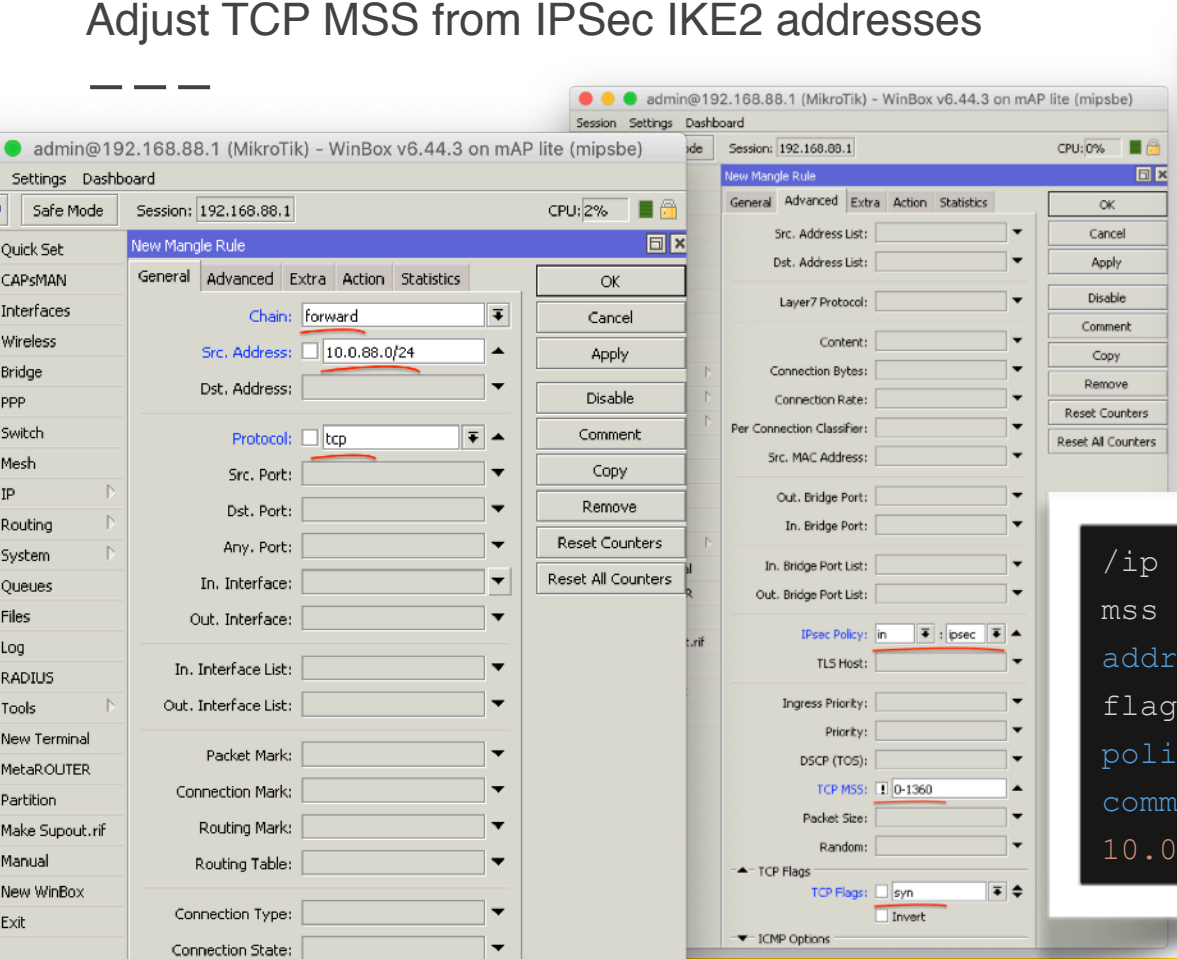
(simplified)

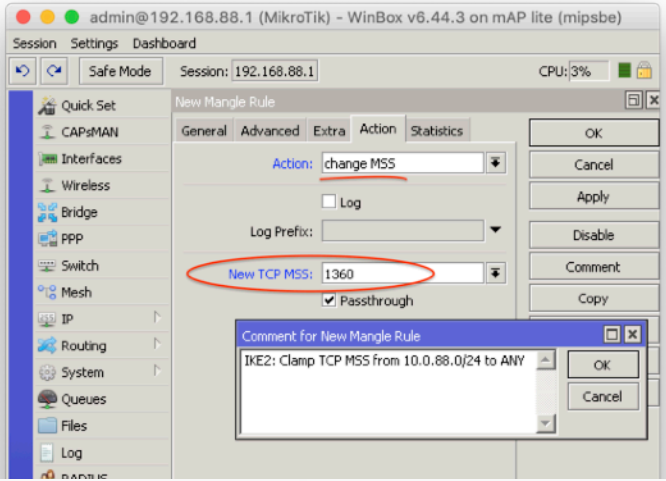


Understanding TCP Maximum Segment size (MSS)
(simplified)



Adjust TCP MSS from IPSec IKE2 addresses

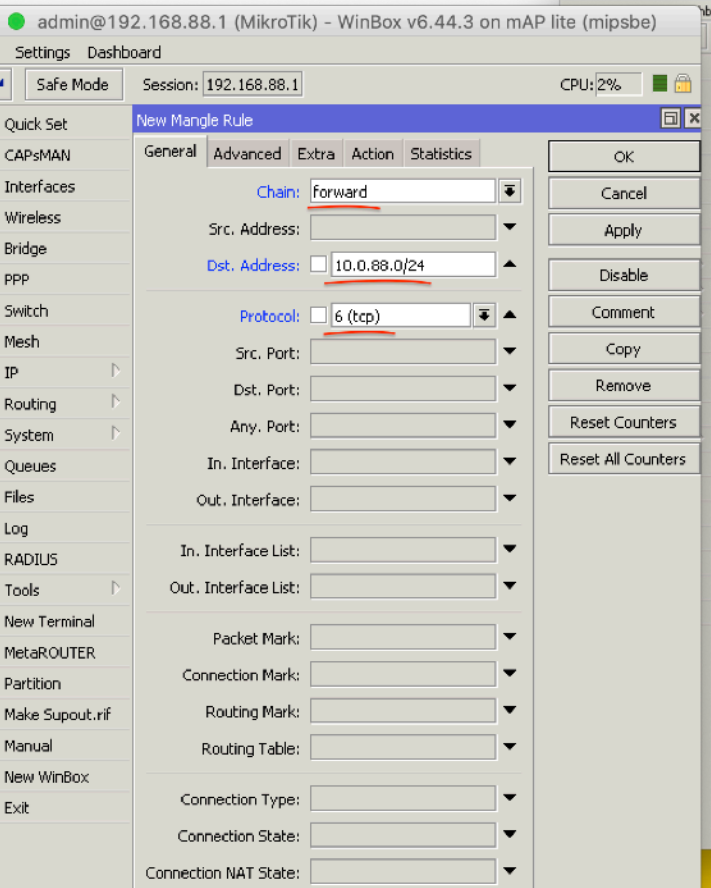


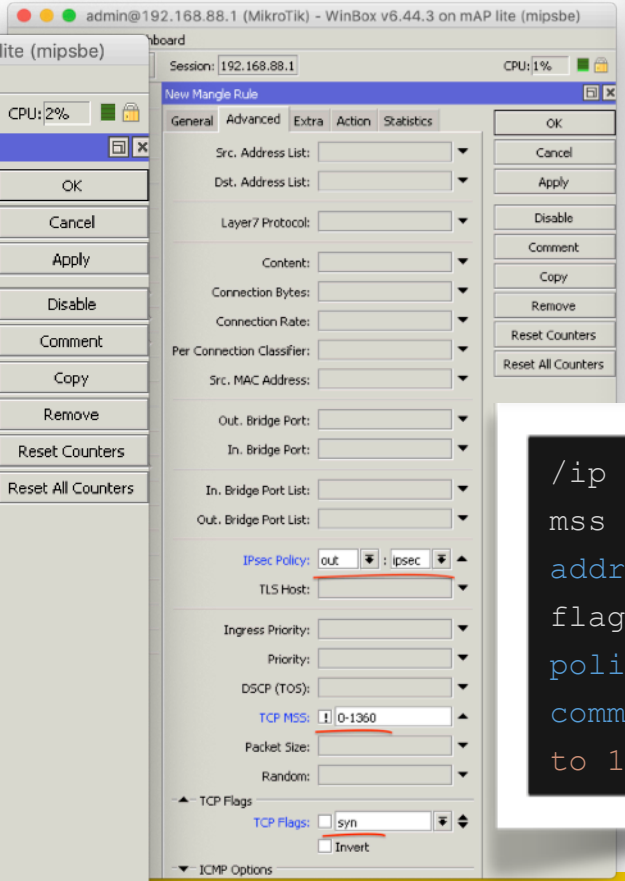


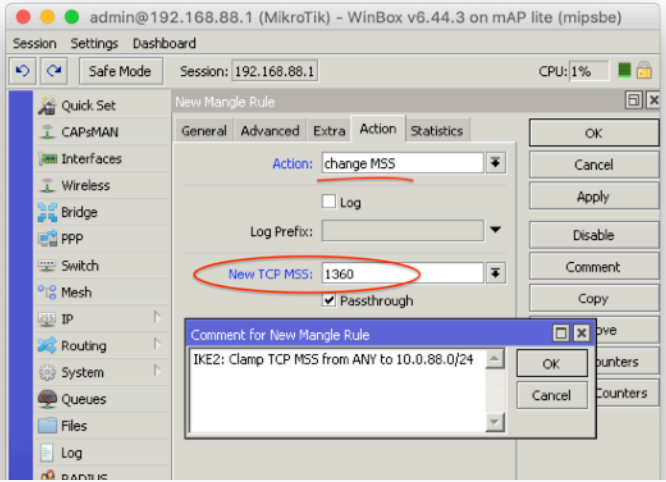

```
/ip firewall mangle add action=change-
mss chain=forward new-mss=1360  src-
address=10.0.88.0/24 protocol=tcp tcp-
flags=syn tcp-mss=!0-1360 ipsec-
policy=in,ipsec passthrough=yes
comment="IKE2: Clamp TCP MSS from
10.0.88.0/24 to ANY"
```

Nikita Tarikin / nikita@tarikin.com

Adjust TCP MSS to IPSec IKE2 addresses








```
/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"
```

Nikita Tarikin / nikita@tarikin.com

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

Nikita Tarikin / nikita@tarikin.com

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

Nikita Tarikin / nikita@tarikin.com

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 :)
```

Nikita Tarikin / nikita@tarikin.com

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>

Nikita Tarikin / nikita@tarikin.com

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

Nikita Tarikin / nikita@tarikin.com

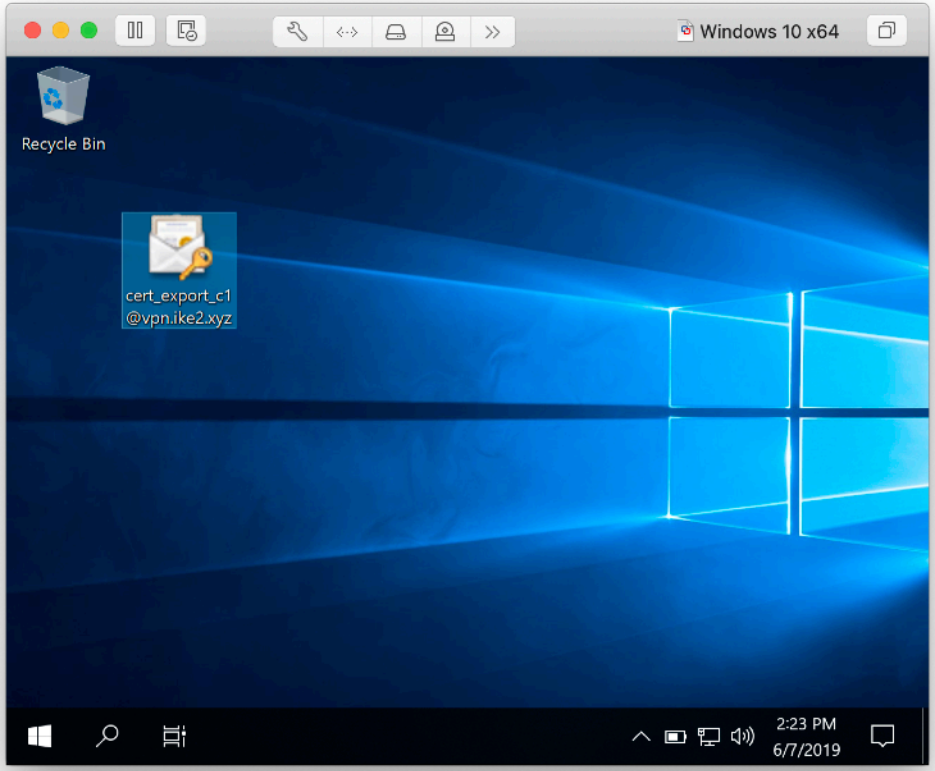
Configure clients

Windows 10

Agenda for next slides

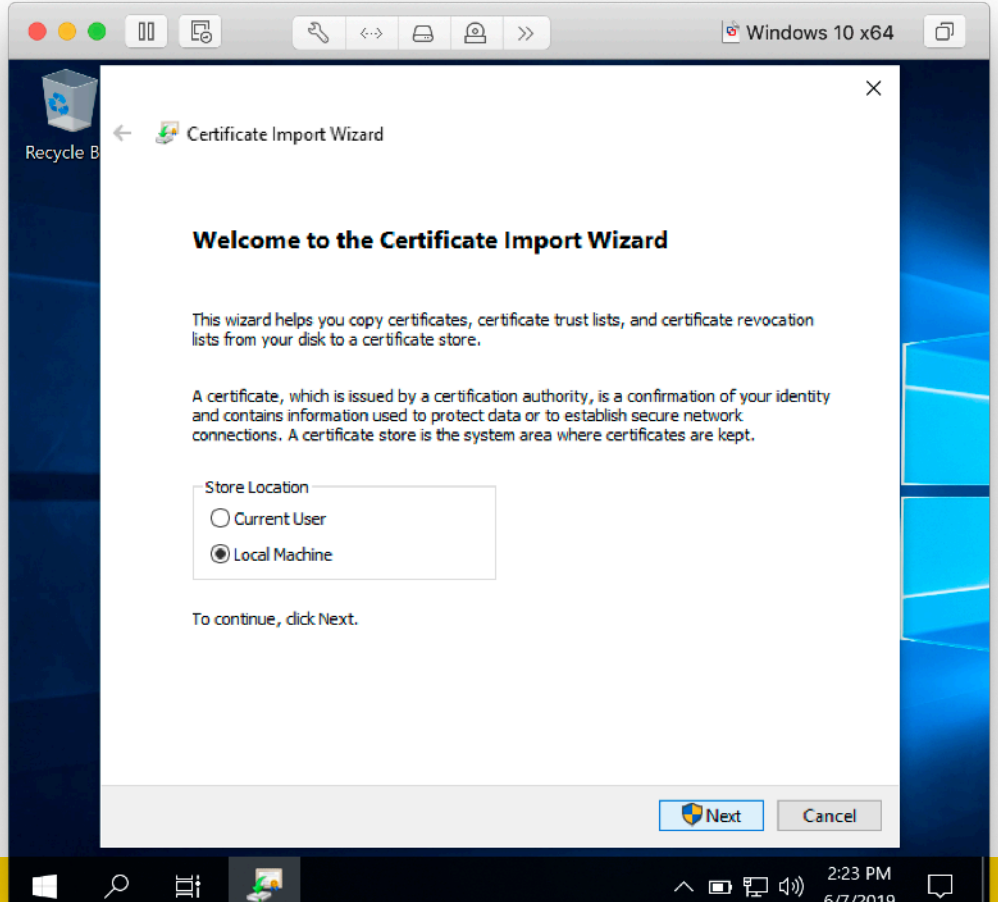
1. Import SSL certificate
2. Setup IKEv2 connection
3. Testing IKEv2 VPN routing

Windows 10: Import SSL certificates



Download .p12 certificate

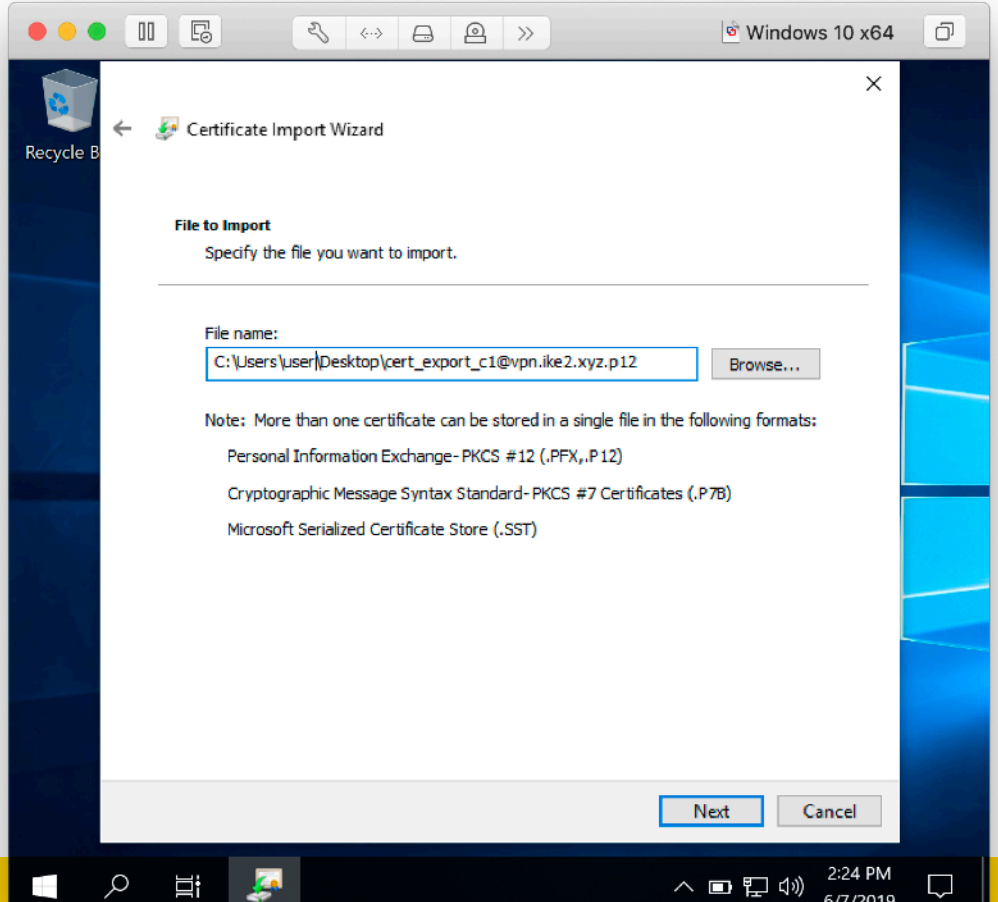
Windows 10: Import SSL certificates



Select **Local Machine** store location

—> **Next**

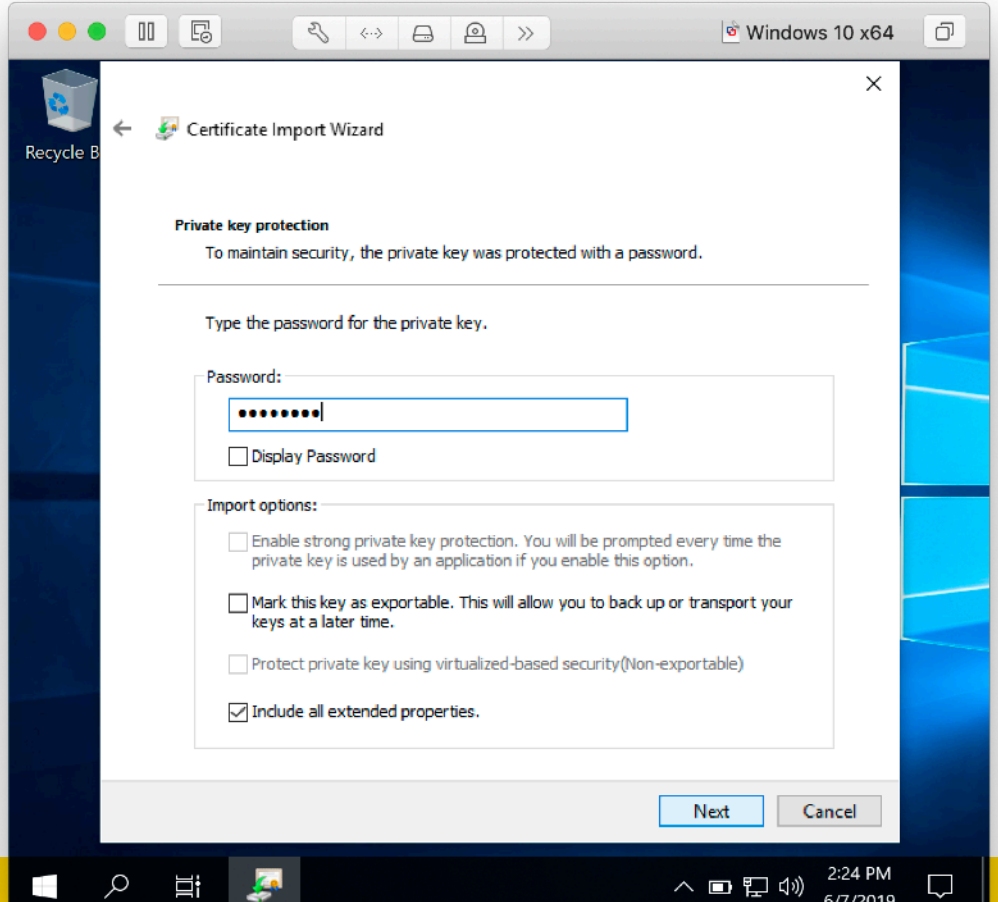
Windows 10: Import SSL certificates

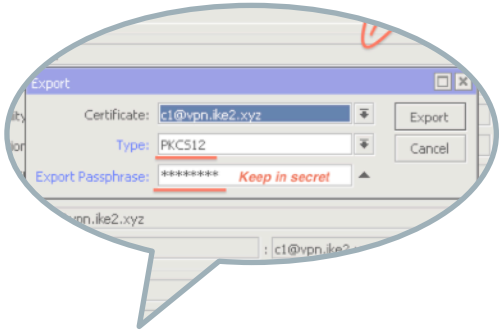


File name already selected

—> **Next**

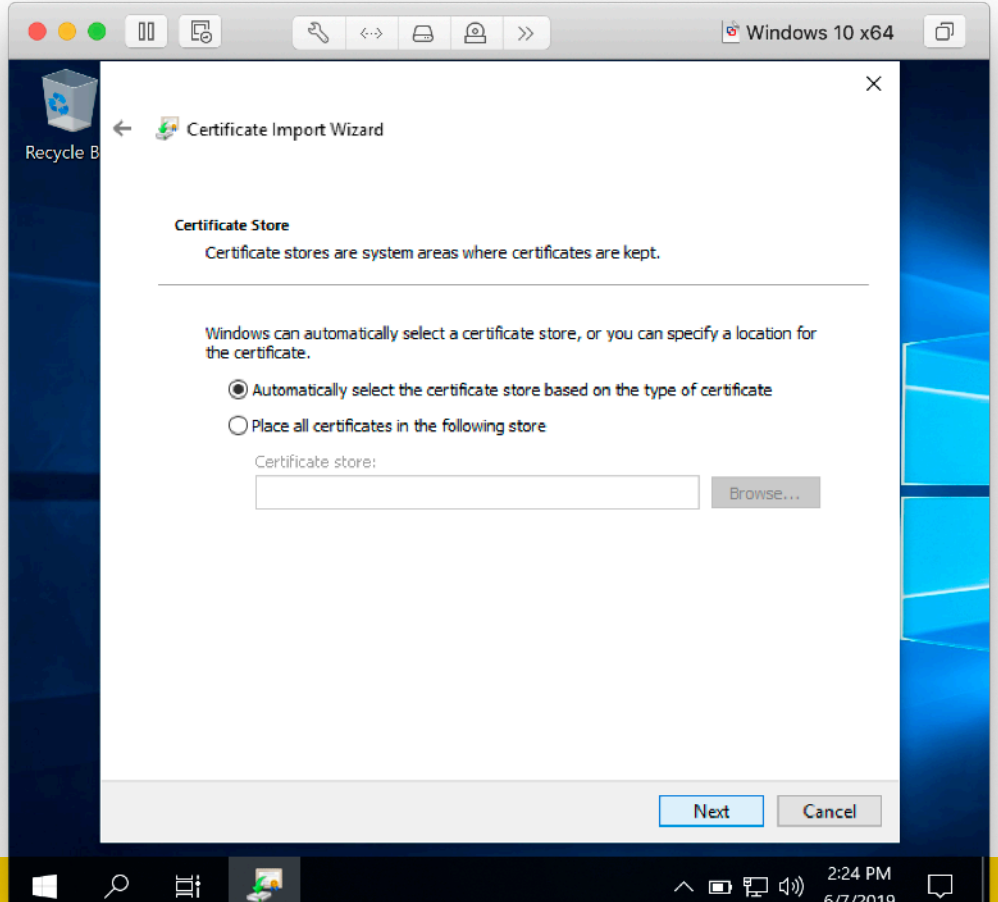
Windows 10: Import SSL certificates





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

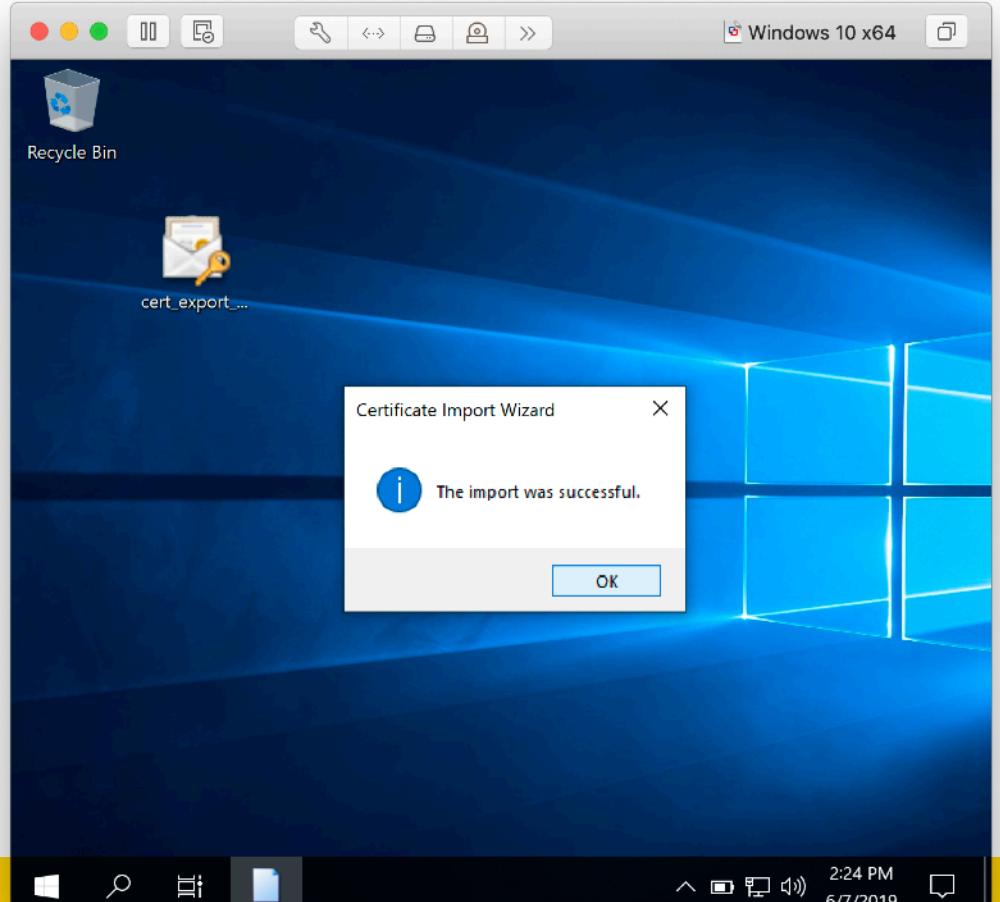
Windows 10: Import SSL certificates



Automatic

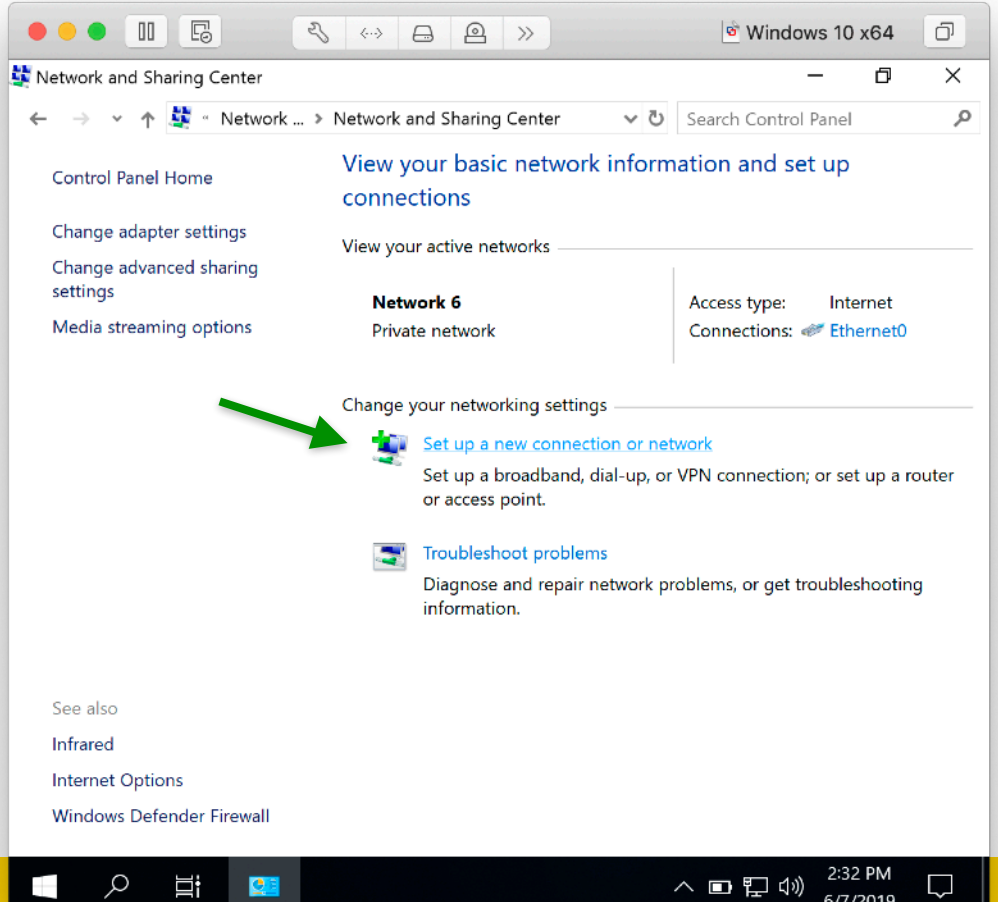
—> **Next**

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

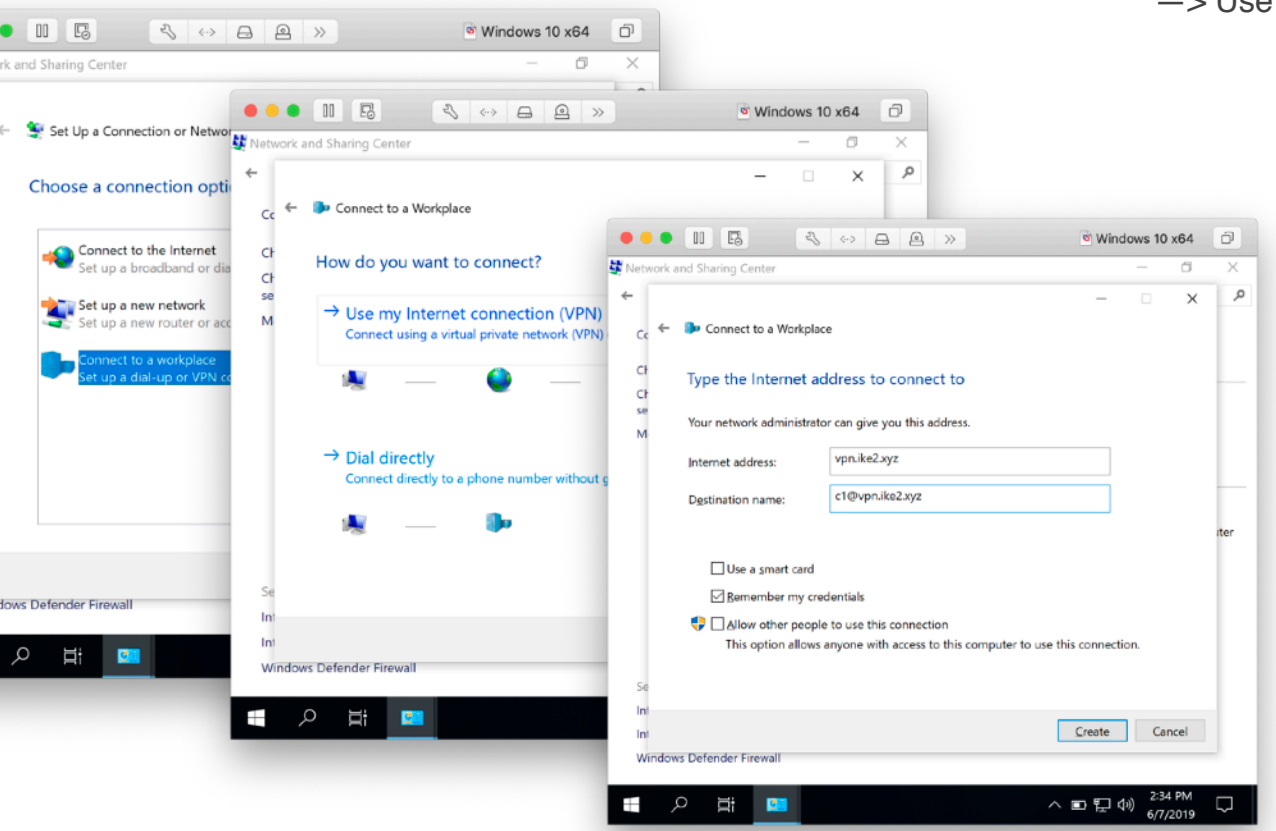
Set up a new connection or network

Windows 10: Setup IKEv2 VPN connection

—> Connect to a workspace

—> Use my Internet connection (VPN)

—> **Next**



Internet address:

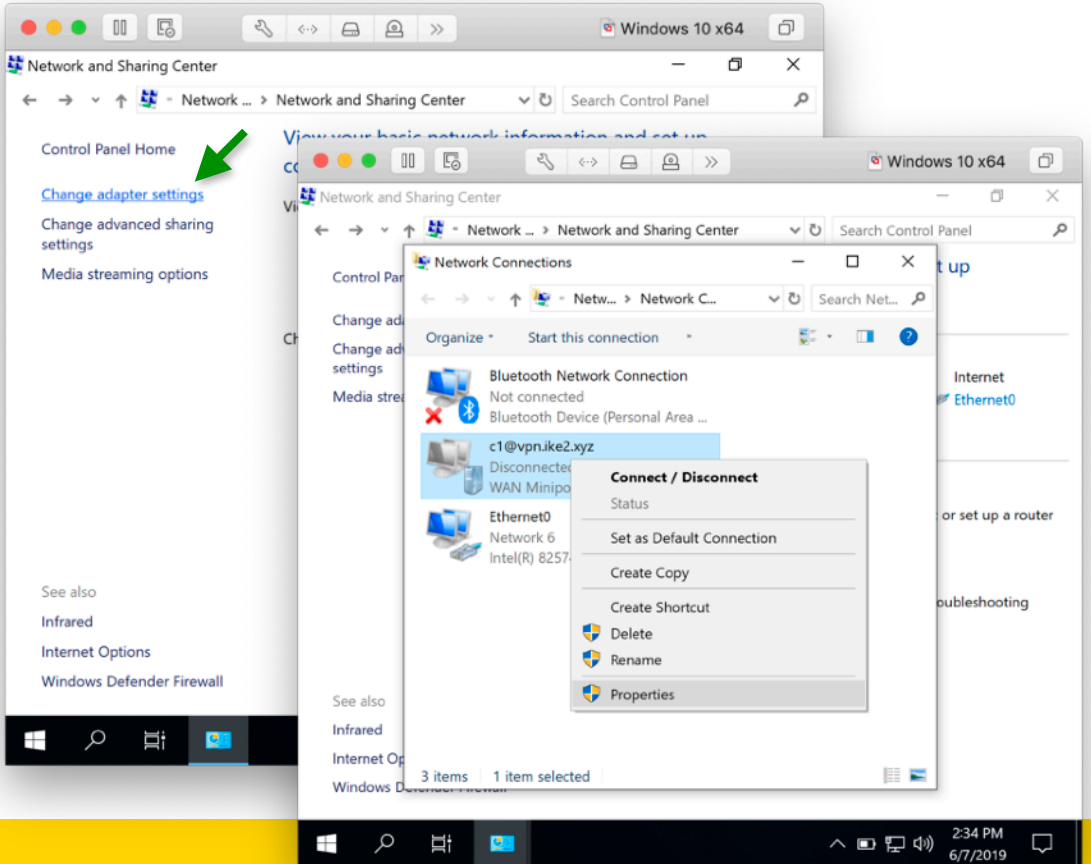
`vpn.ike2.xyz`

Destination name:

`c1@vpn.ike2.xyz`

—> **Create**

Windows 10: Setup IKEv2 VPN connection

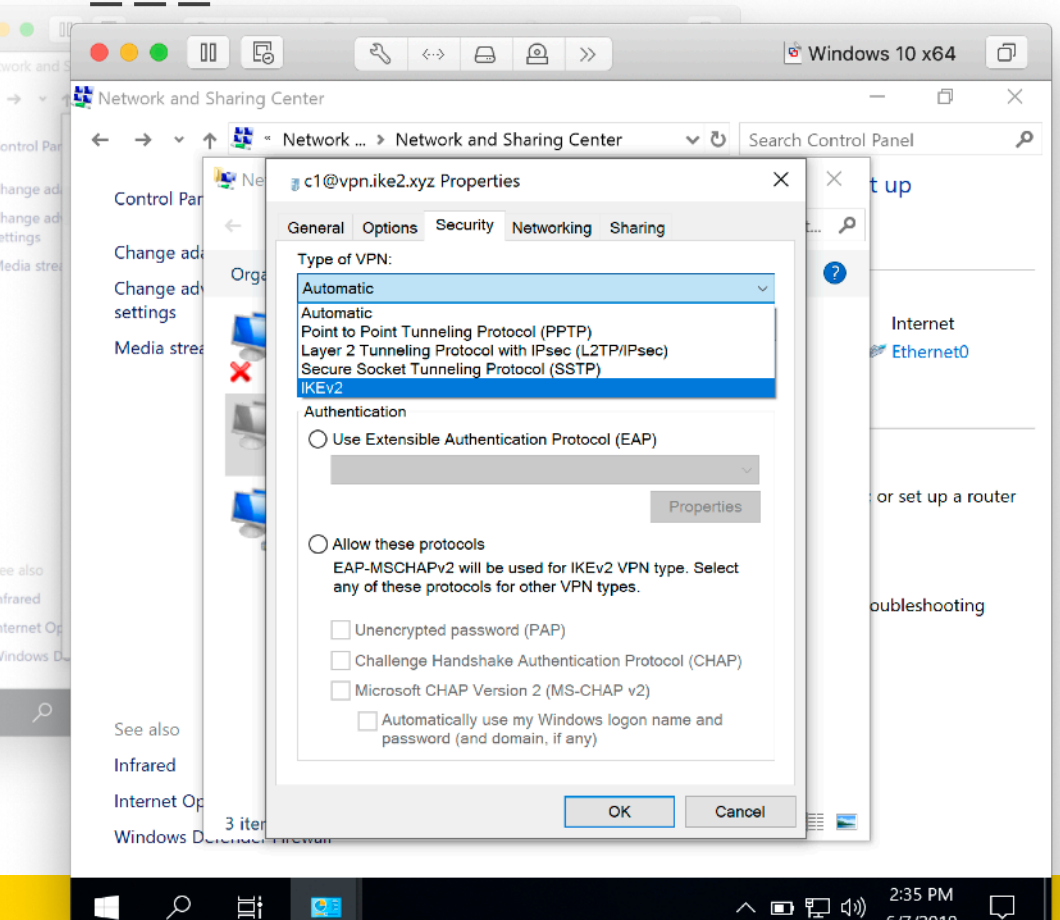


—> Change adapter settings

`c1@vpn.ike2.xyz`

—> **Properties**

Windows 10: Setup IKEv2 VPN connection

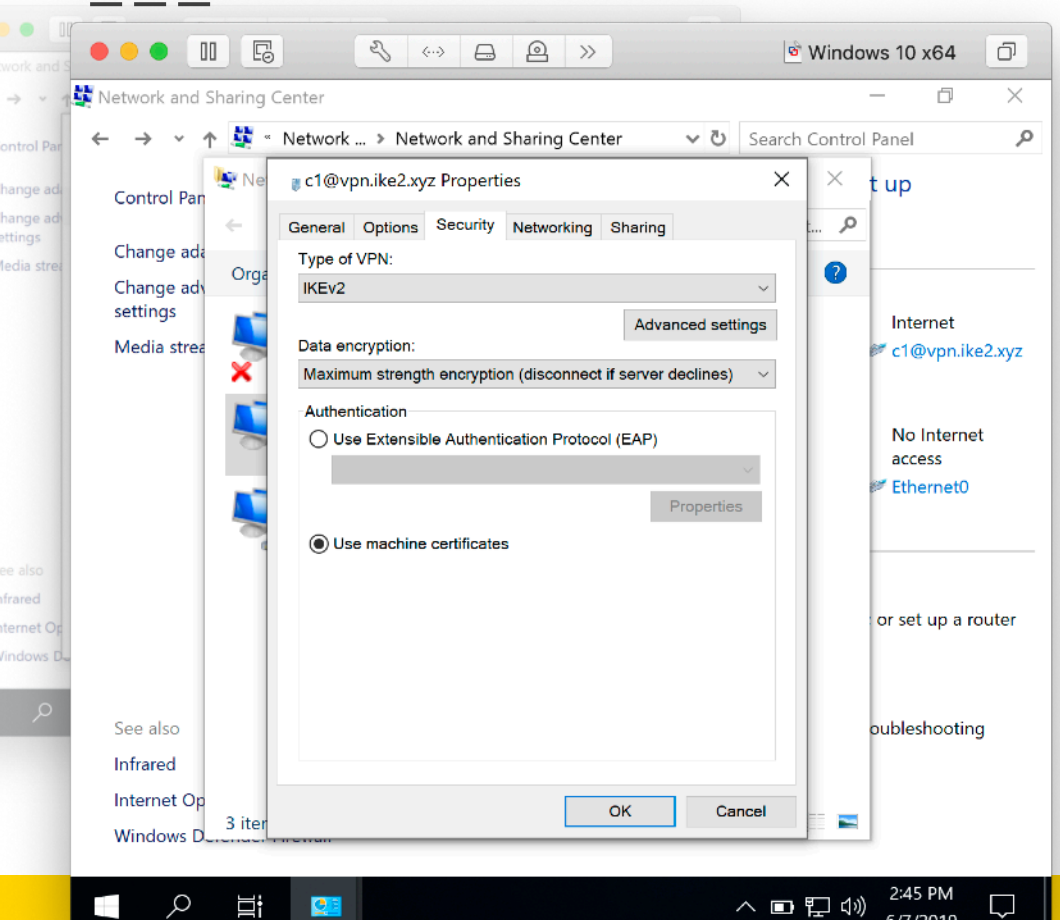


Properties -> Security tab

Type of VPN:

`IKEv2`

Windows 10: Setup IKEv2 VPN connection



Properties -> Security tab

Data encryption:

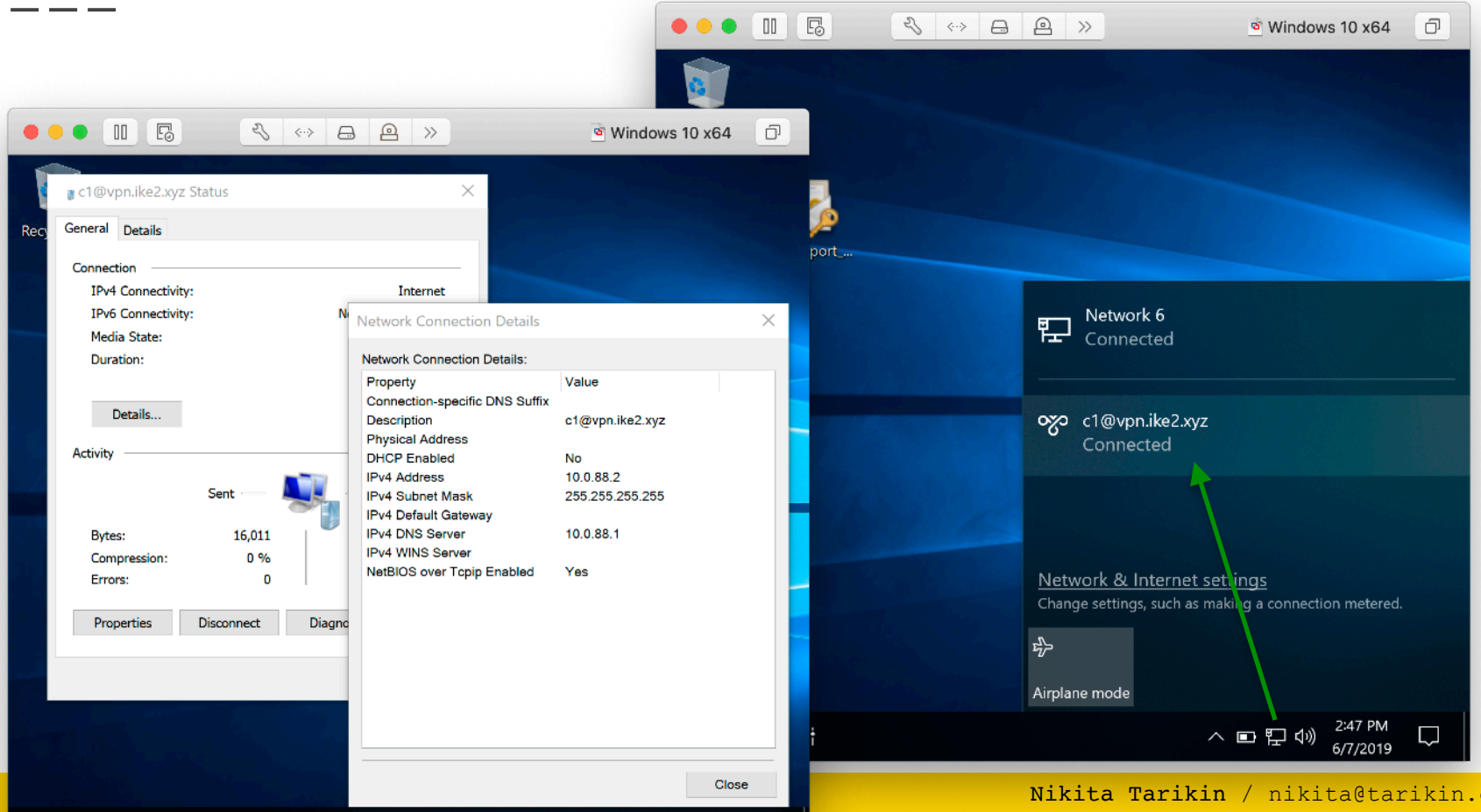
`Maximum strength encryption`

Authentication:

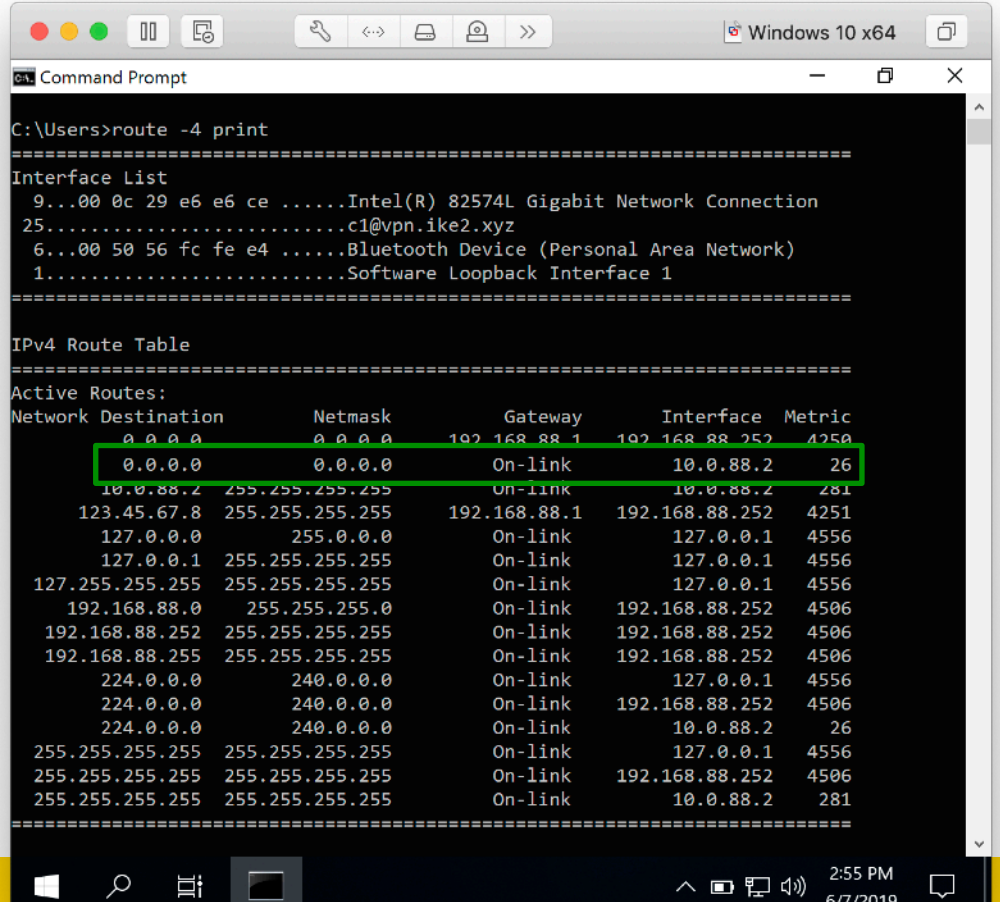
`Use machine certificates`

—> OK

Windows 10: Testing IKEv2 VPN connection



Windows 10: Testing IKEv2 VPN routes



`route -4 print`

Destination

`0.0.0.0/0` (default)

Gateway:

`On-link`

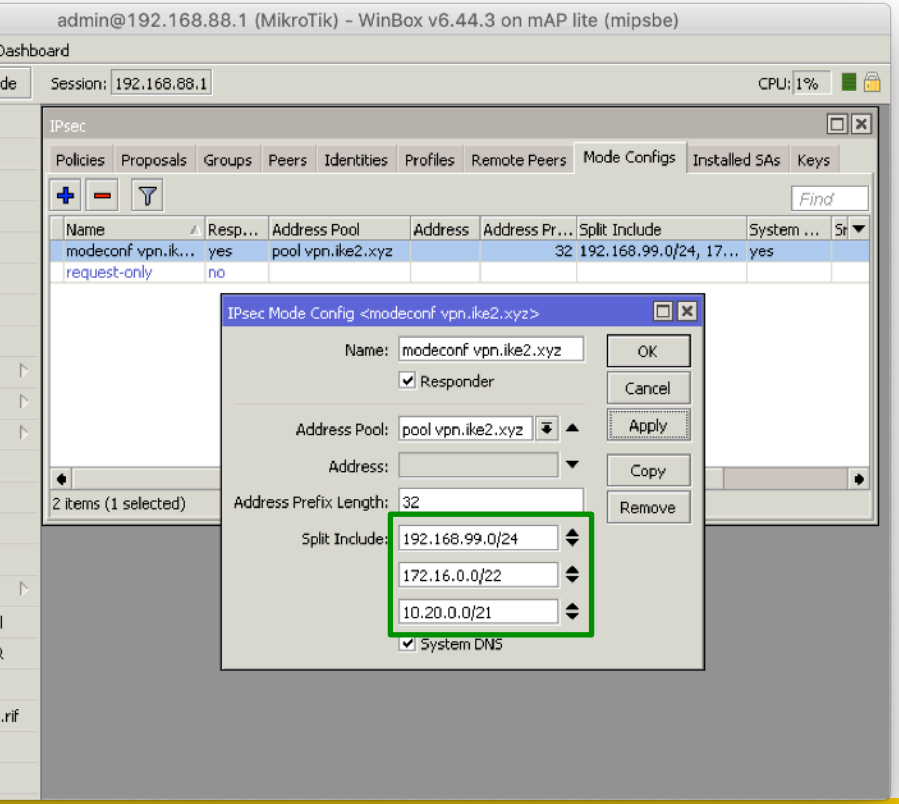
Interface:

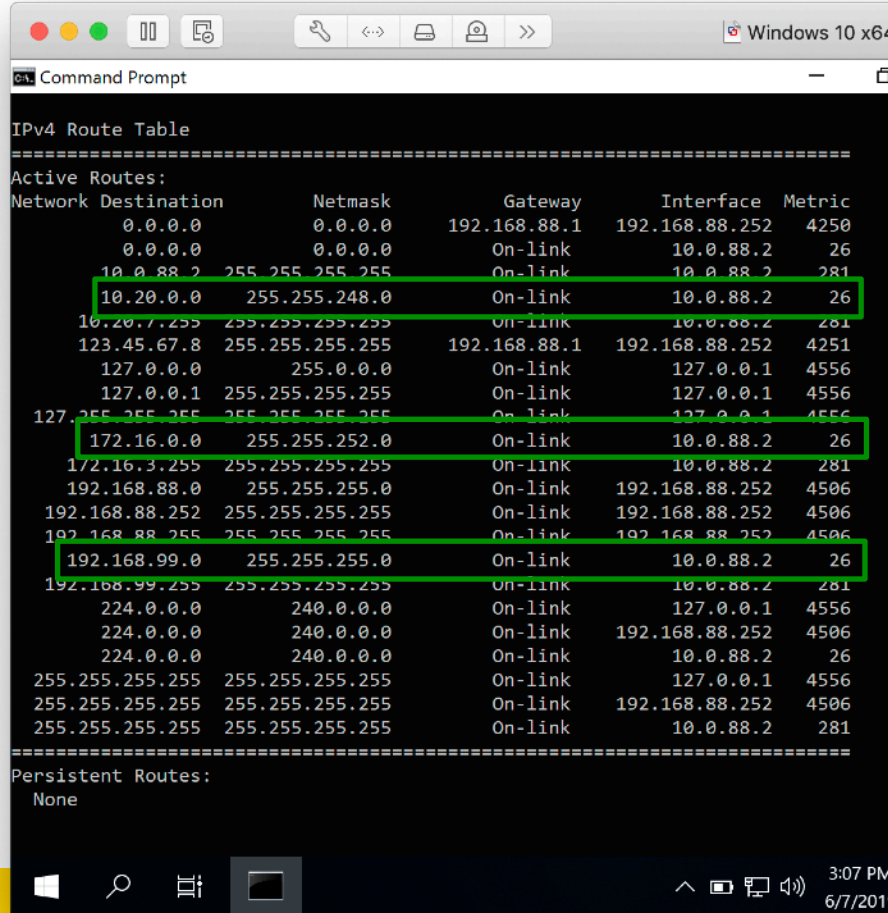
`10.0.88.2`

Metric (distance):

`26`

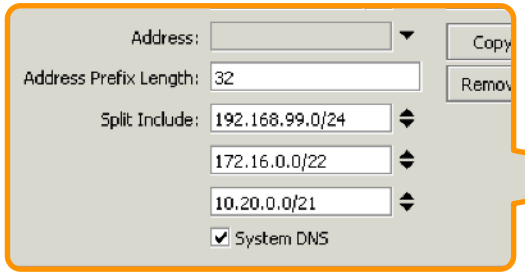
Windows 10: Testing IKEv2 VPN routes

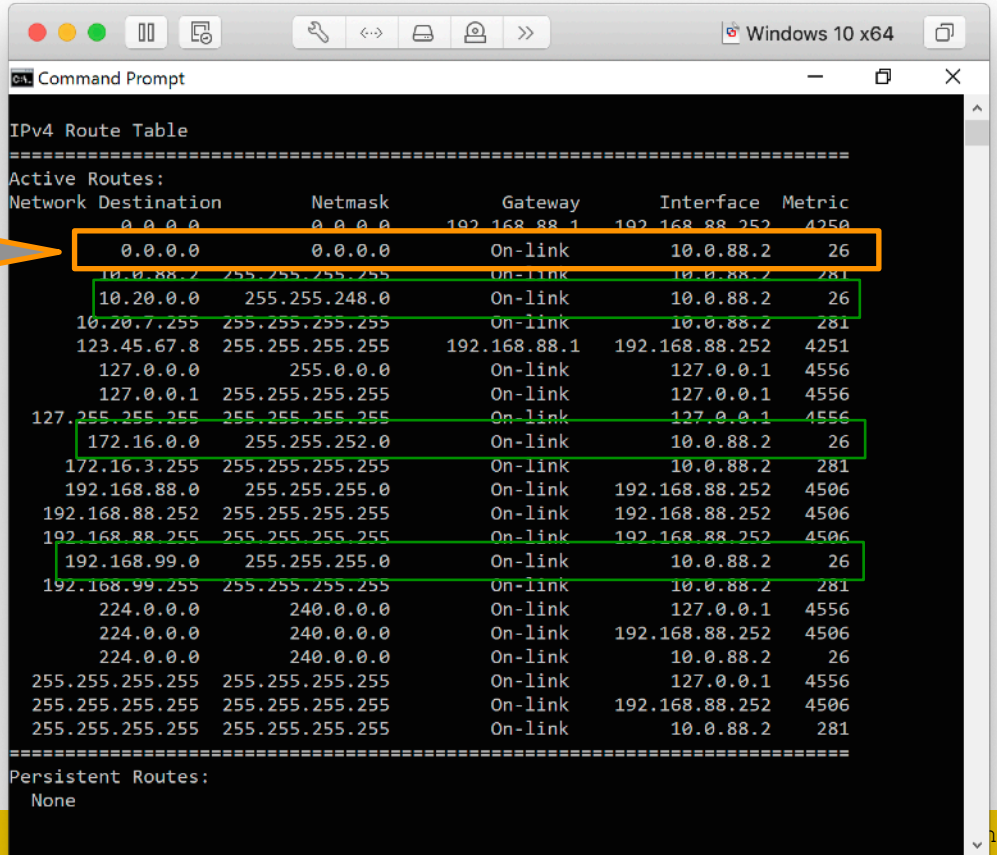




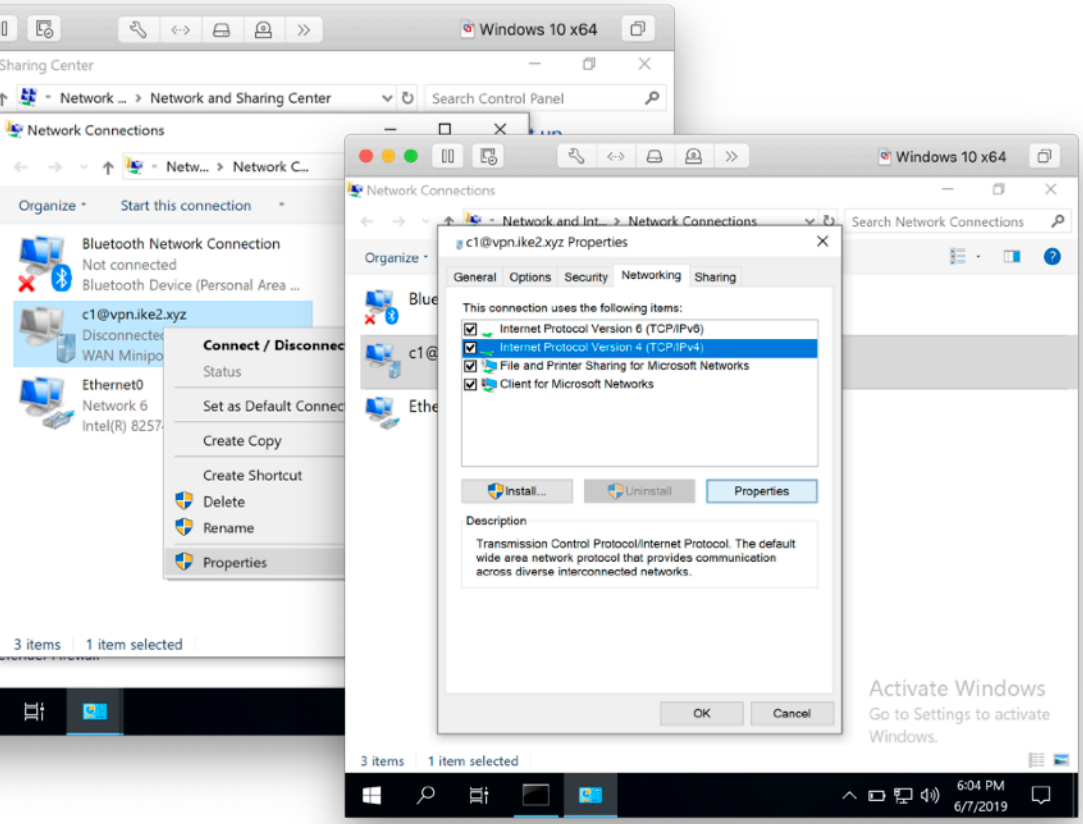
Windows 10: Testing IKEv2 VPN routes

— 0.0.0.0/0 ???





Windows 10: Disable IKEv2 VPN default gateway

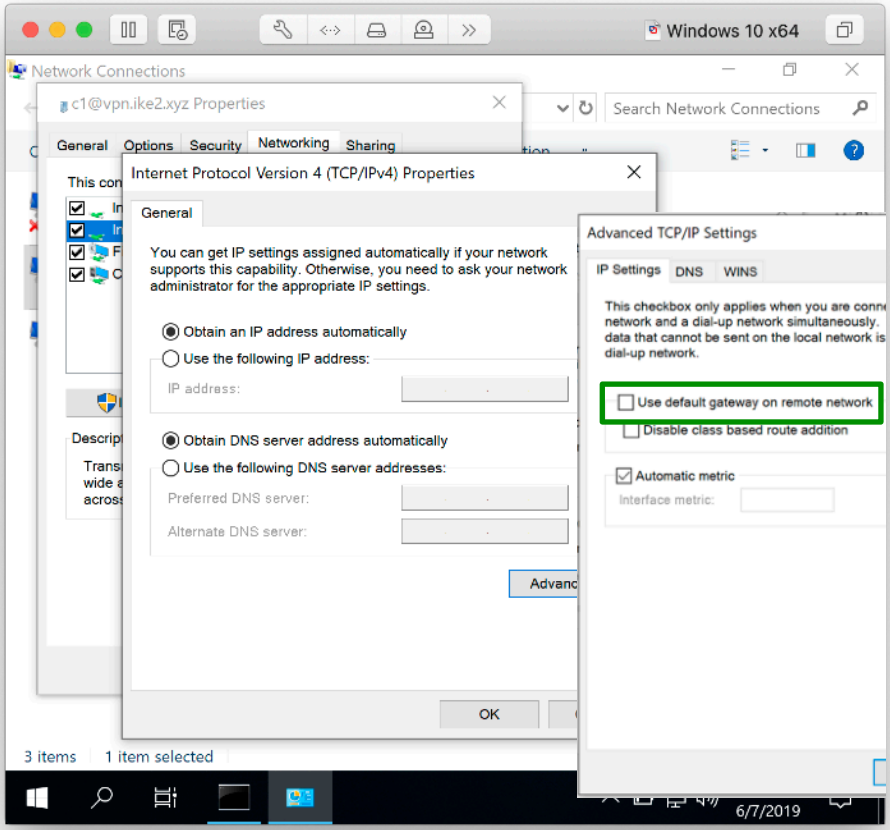


Properties -> Networking tab

✓ 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

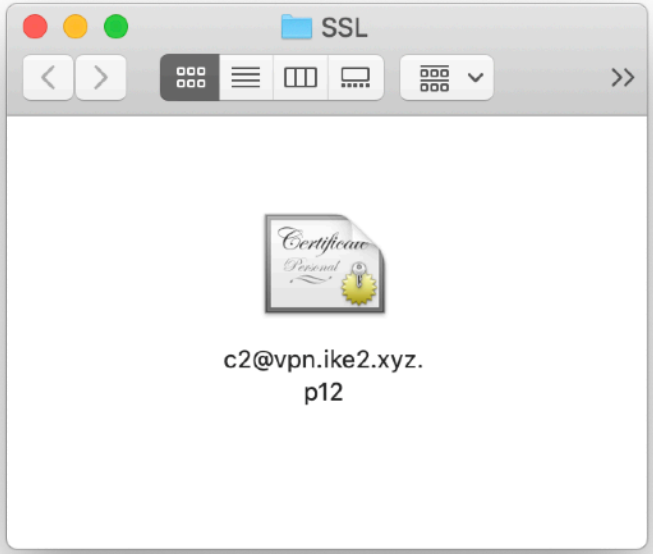
≥ 10.11 El Capitan

Agenda for next slides

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

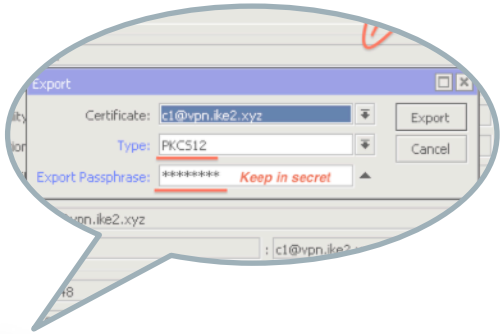
Nikita Tarikin / nikita@tarikin.com

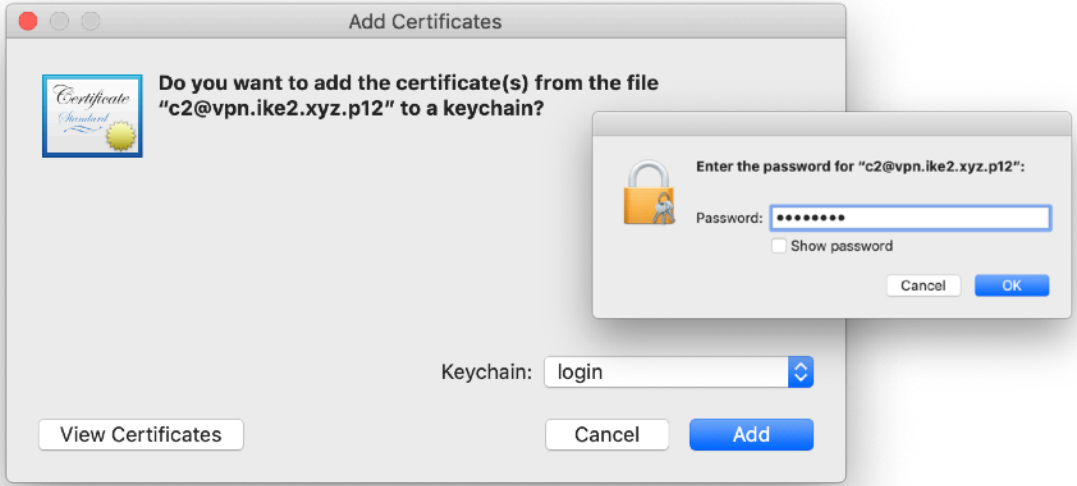
MacOS: Import SSL certificates



Download .p12 certificate

MacOS: Import SSL certificates





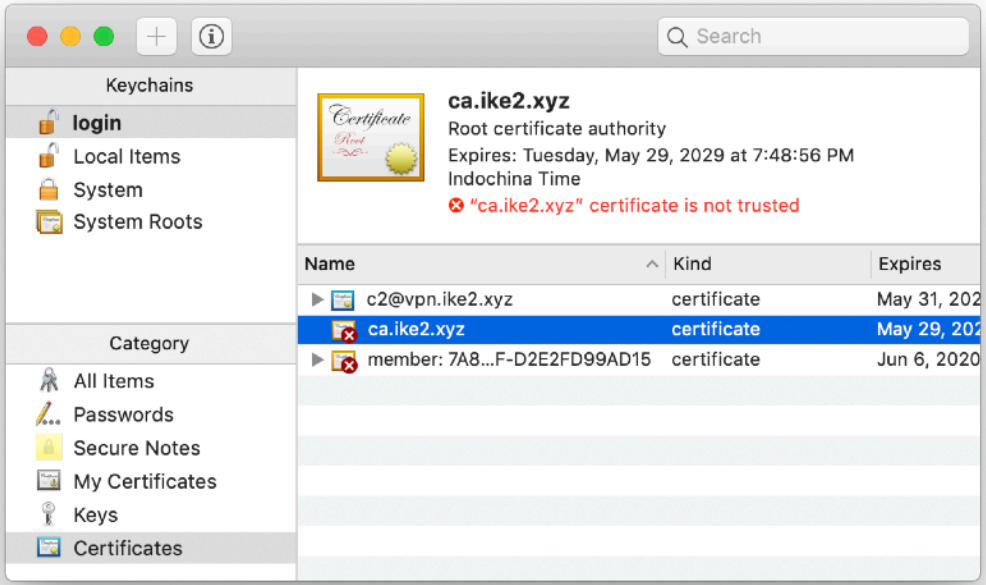
Keychain:
login (default)

—> **Add**

Type your
SSL certificate password

—> **OK**

MacOS: Manage SSL certificates

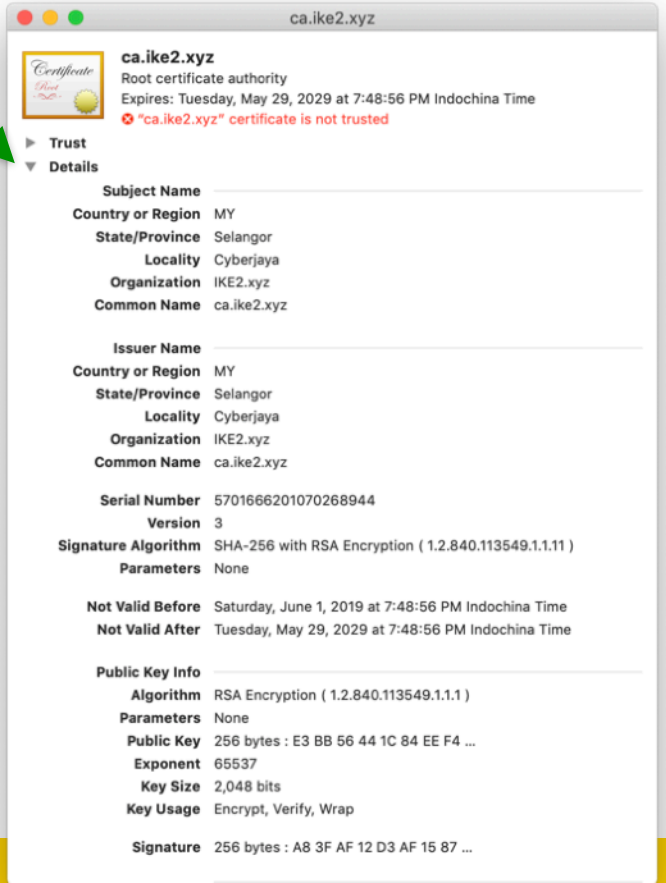


Keychain access

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

MacOS: Manage SSL certificates

Important



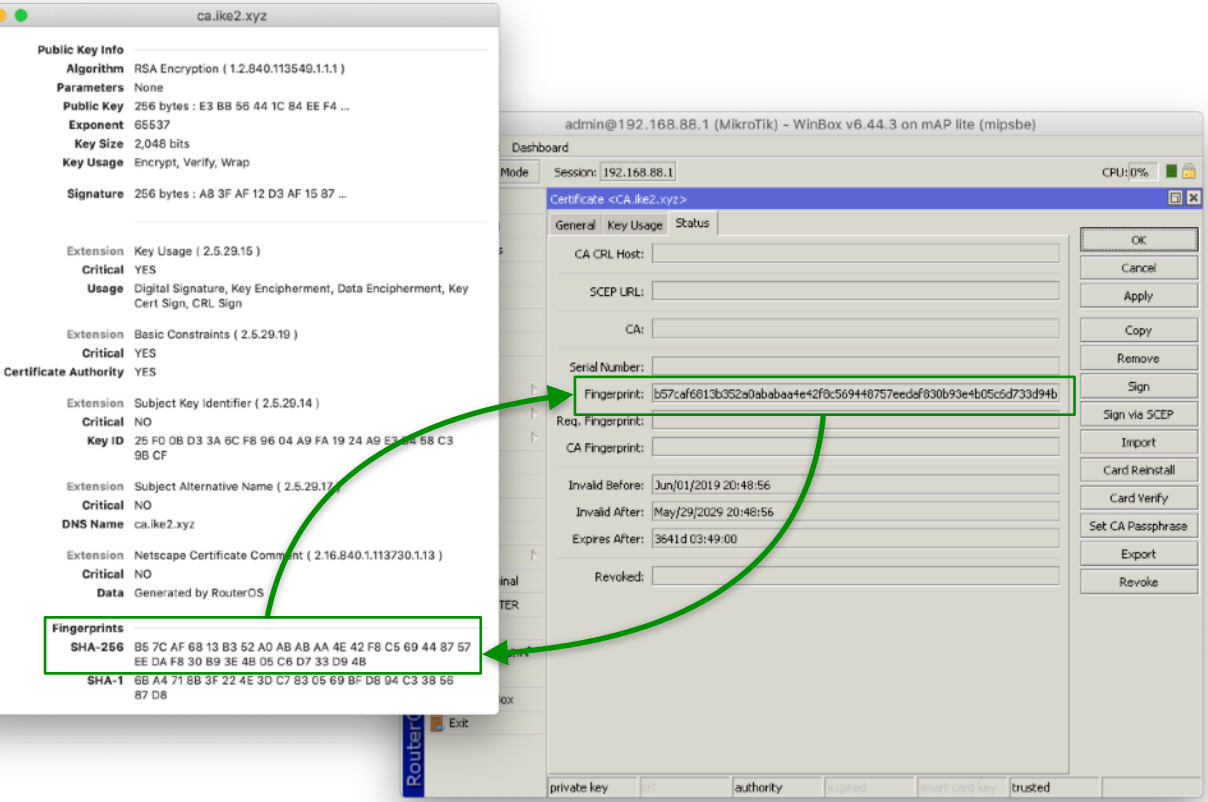
Keychain access

Verify CA certificate details

MacOS: Manage SSL certificates

Important

Keychain access

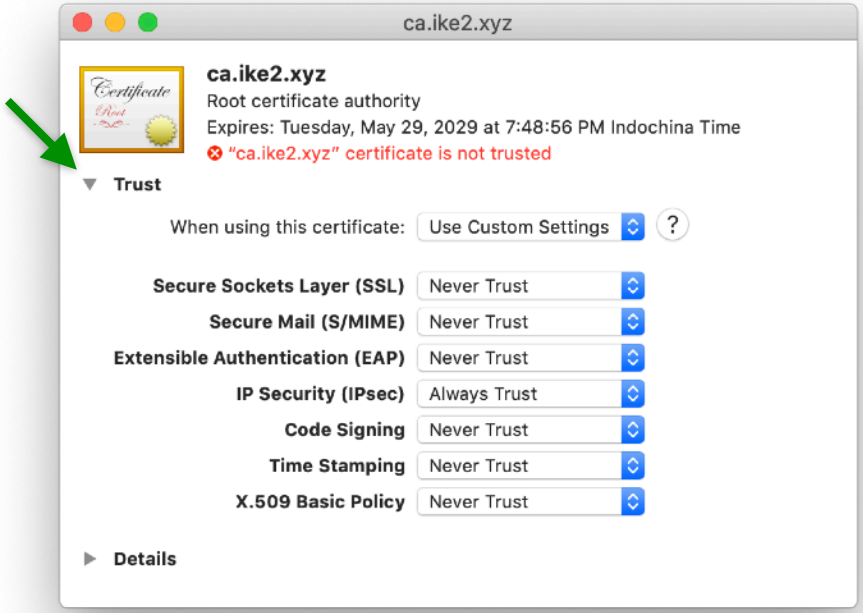


Compare CA certificate **fingerprints**

MacOS: Manage SSL certificates

Important

Keychain access

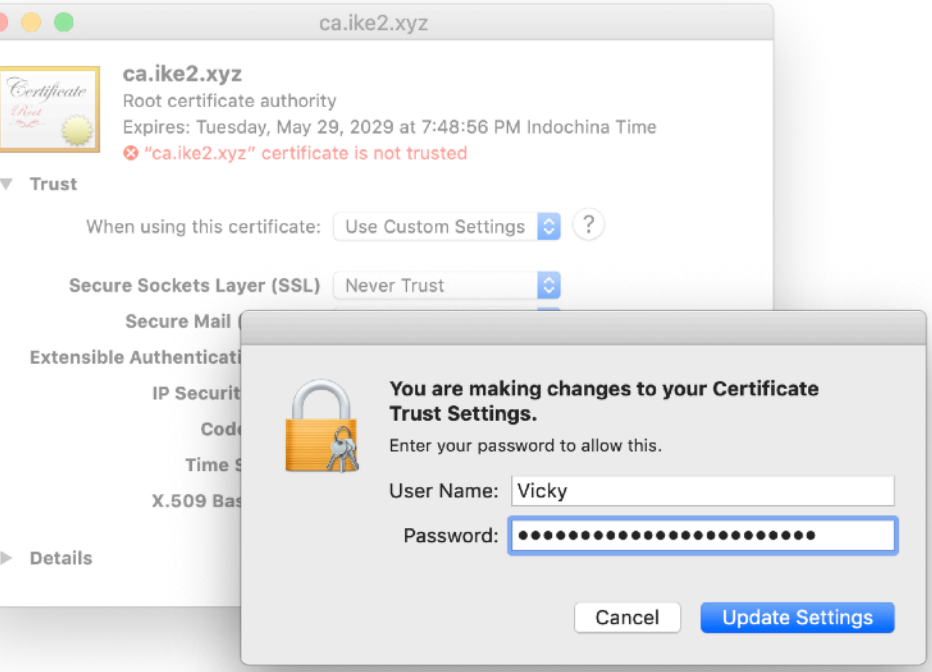


✅ IP Security (IPSec)

❌ Everything else

MacOS: Manage SSL certificates

Important



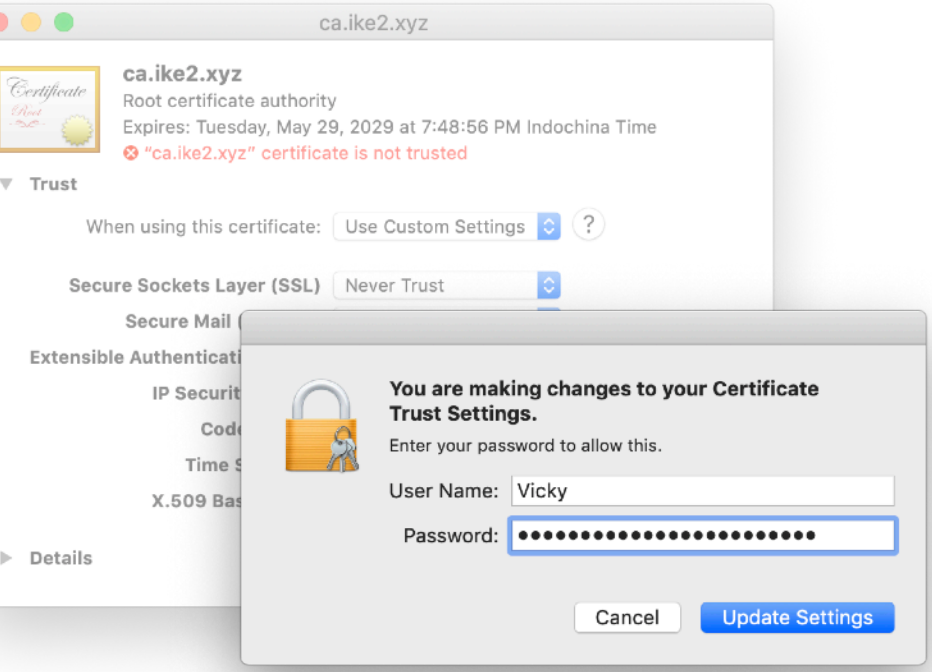
Keychain access

Type your
MacOS password

—> **Update settings**

MacOS: Manage SSL certificates

Important

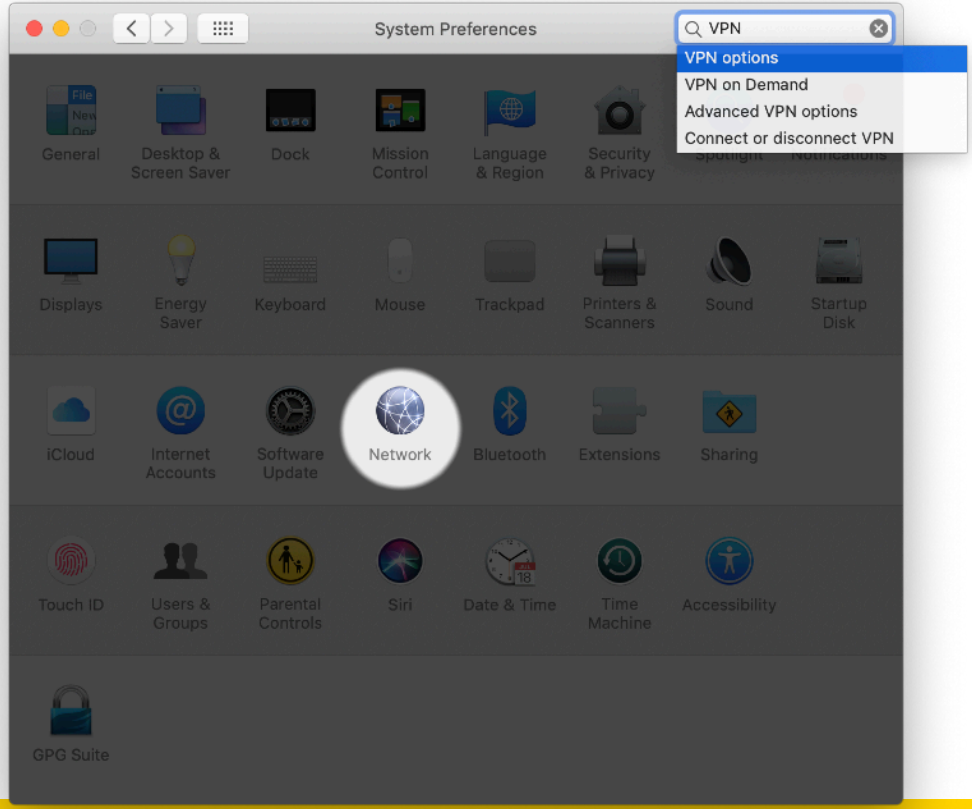


Keychain access

Type your
MacOS password

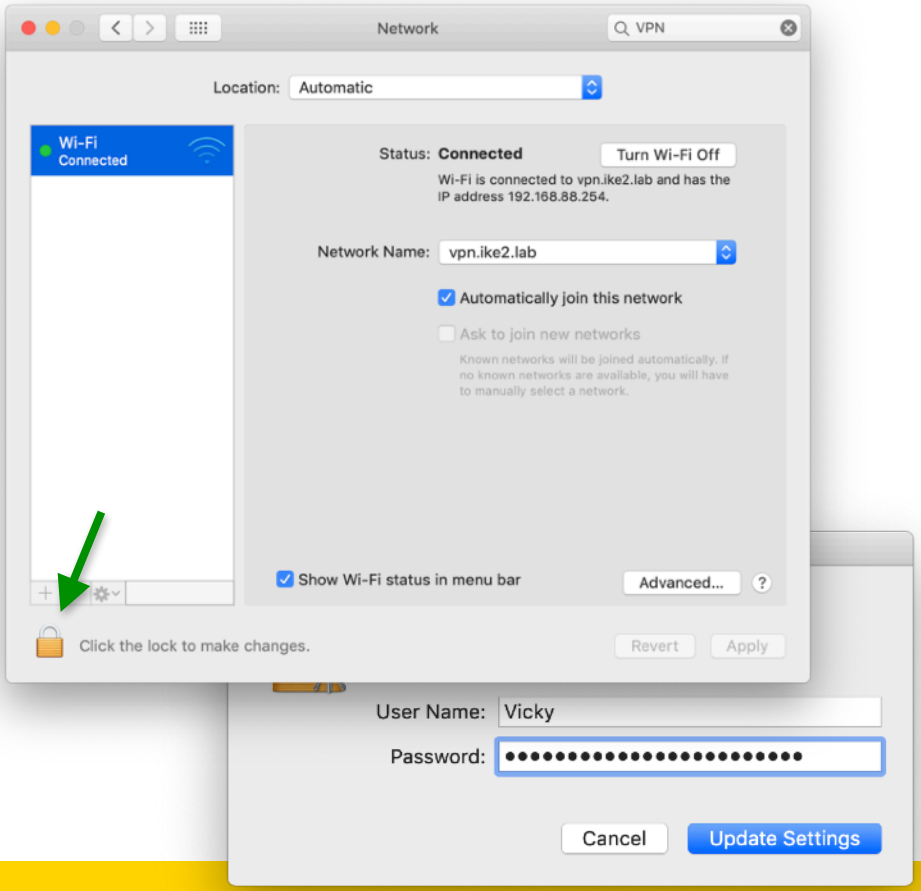
—> **Update settings**

MacOS: Setup IKEv2 VPN connection



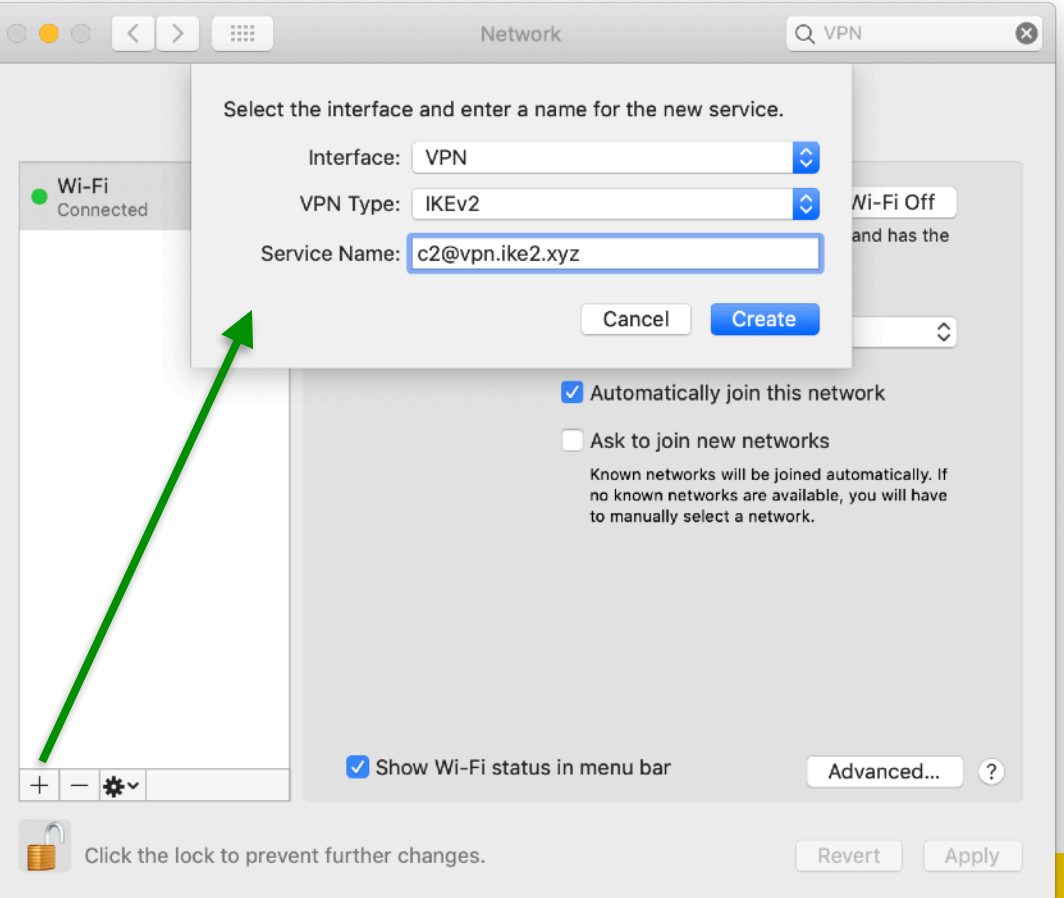
System preferences ->
Network

MacOS: Setup IKEv2 VPN connection



Unlock to make changes

MacOS: Setup IKEv2 VPN connection



Create new connection

Interface:

VPN

VPN Type:

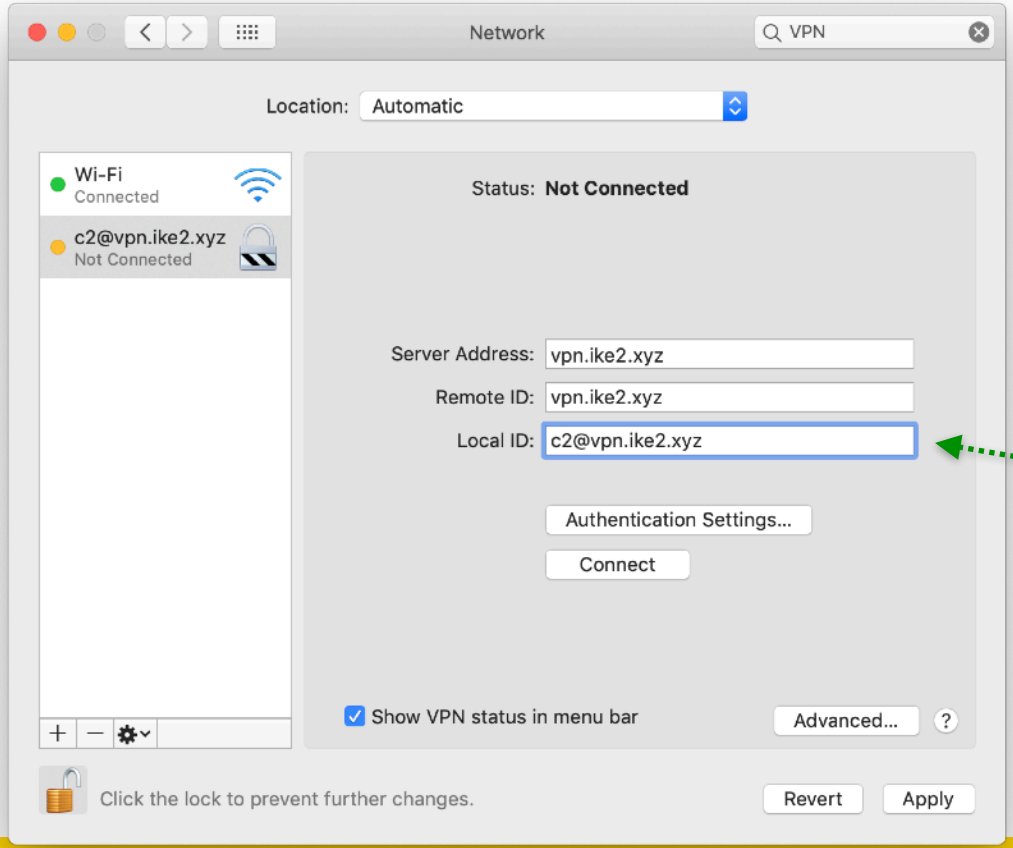
IKEv2

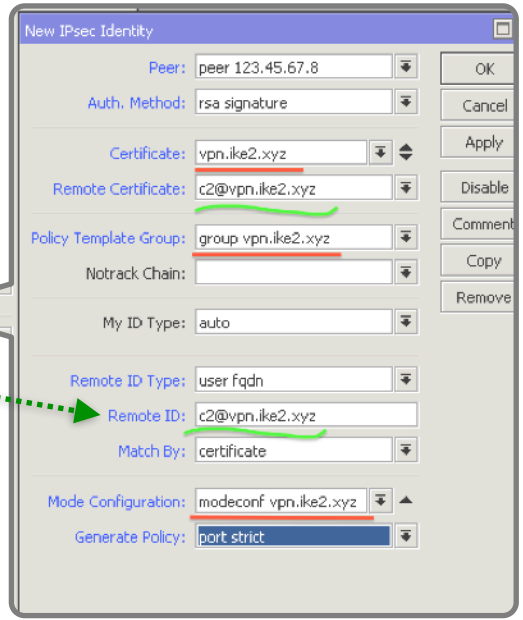
Service name:

c2@vpn.ike2.xyz

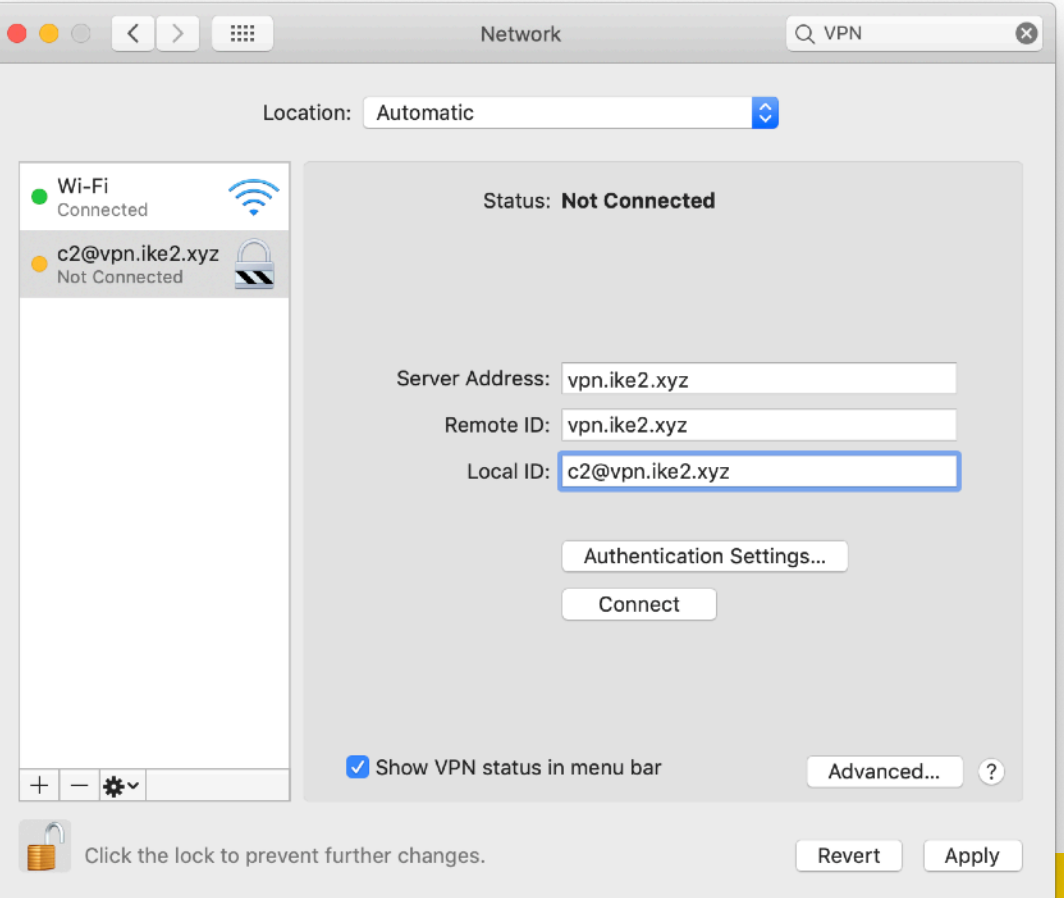
–> Create

MacOS: Setup IKEv2 VPN connection





MacOS: Setup IKEv2 VPN connection



Create new connection

Server Address:

`vpn.ike2.xyz`

Remote ID:

`vpn.ike2.xyz`

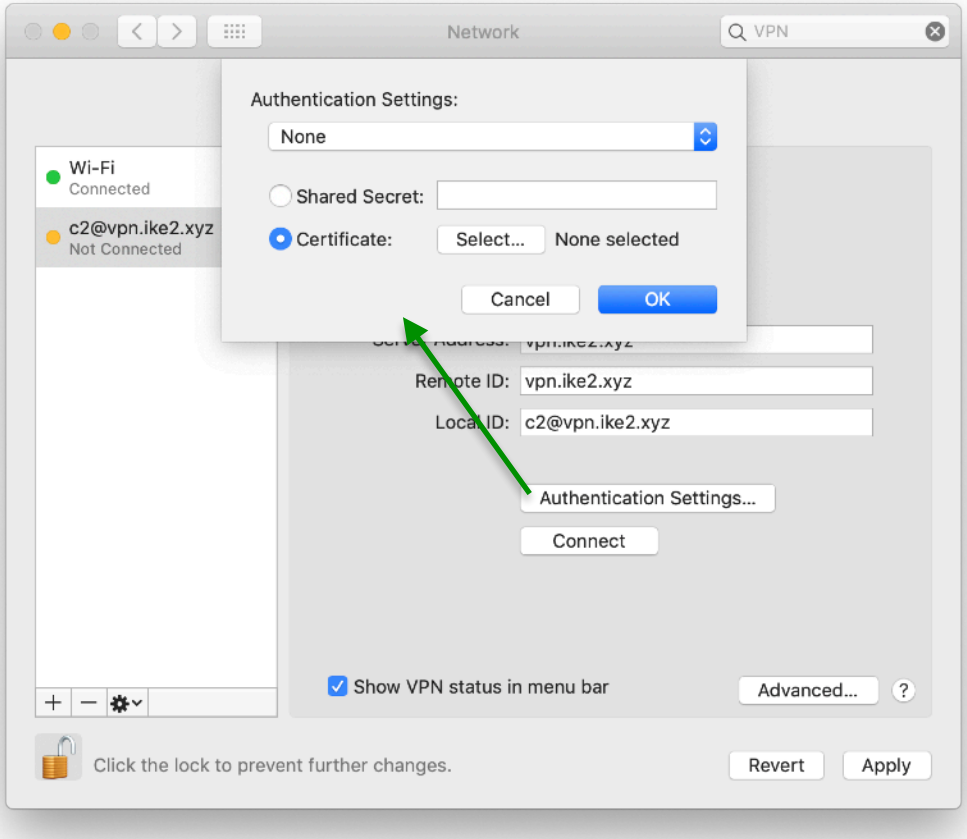
Local ID:

`c2@vpn.ike2.xyz`

✓ Show VPN status in menu bar

`–> Apply`

MacOS: Setup IKEv2 VPN connection



Authentication Settings

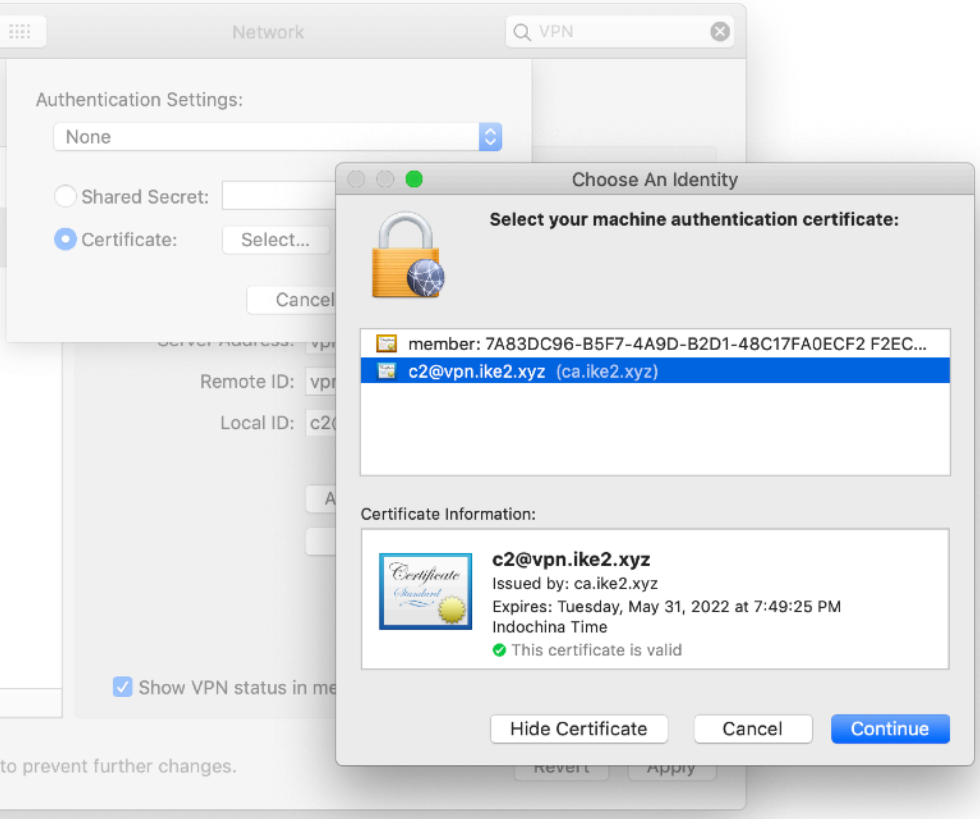
Authentication Settings:

None

Certificate:

–> Select

MacOS: Setup IKEv2 VPN connection



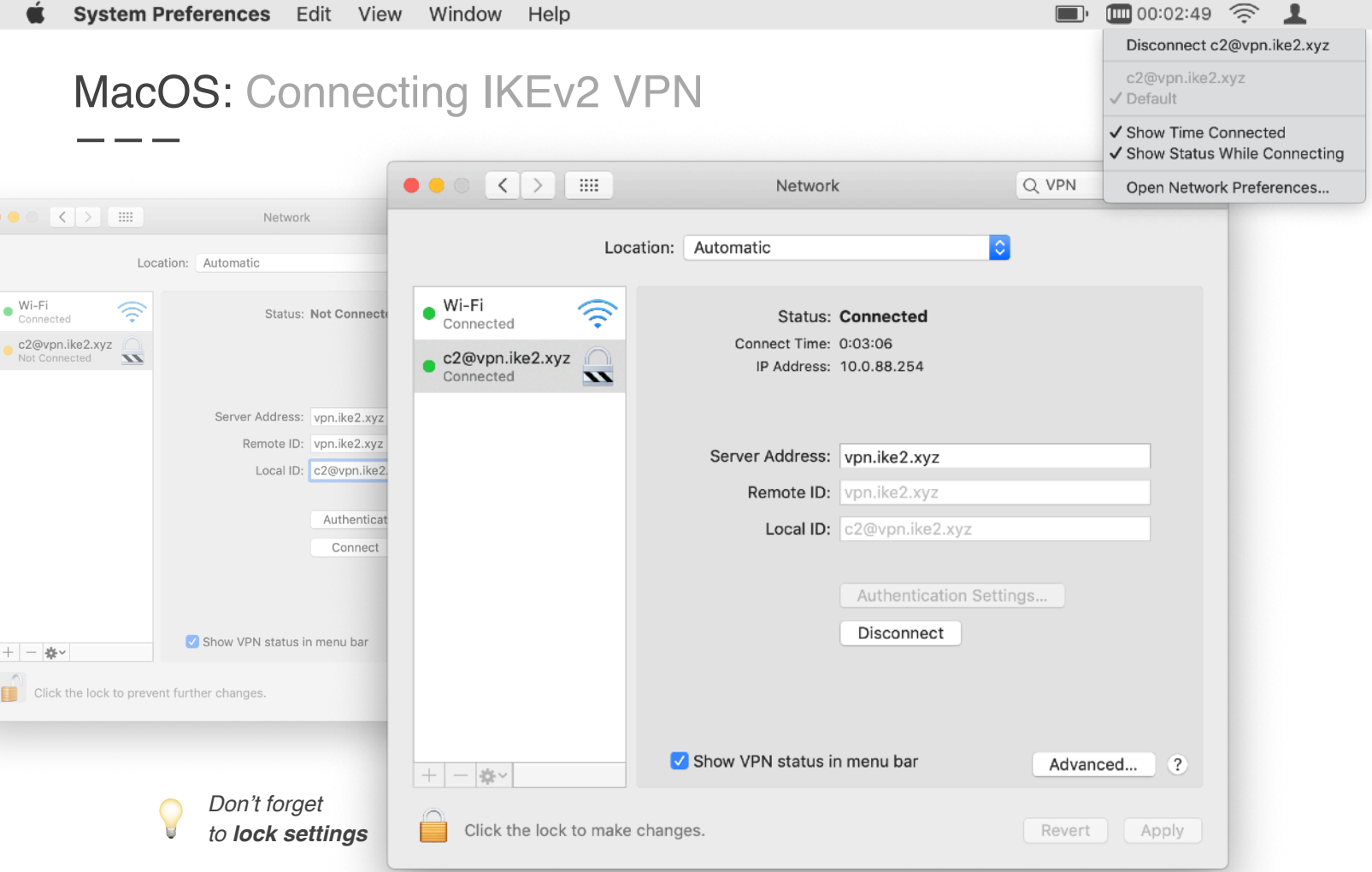
Authentication Settings

Select machine auth certificate:

`c2@vpn.ike2.xyz`

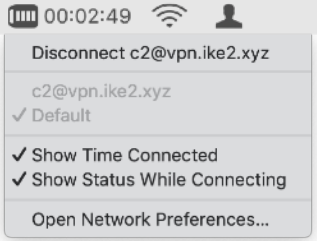
`–> Continue`

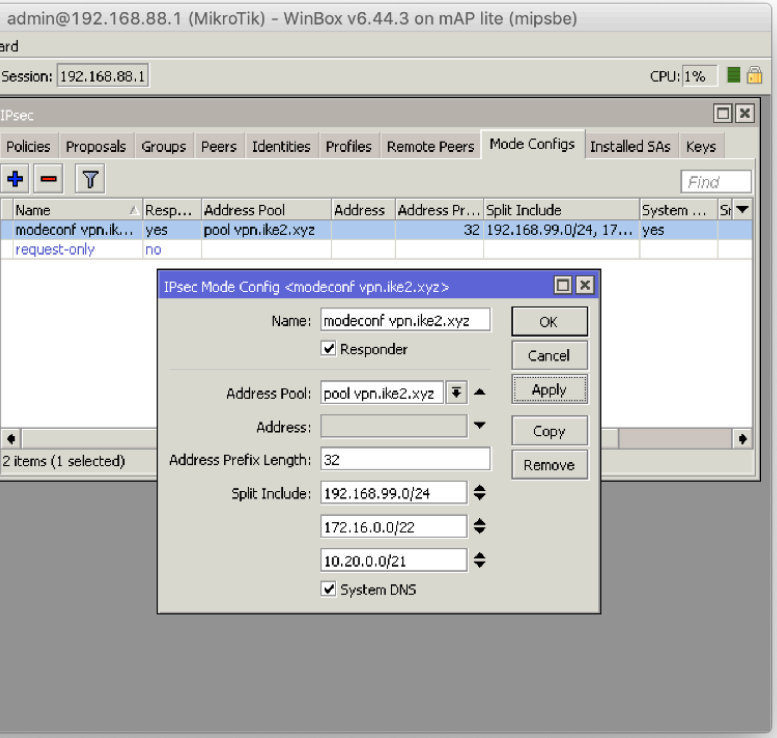
MacOS: Connecting IKEv2 VPN

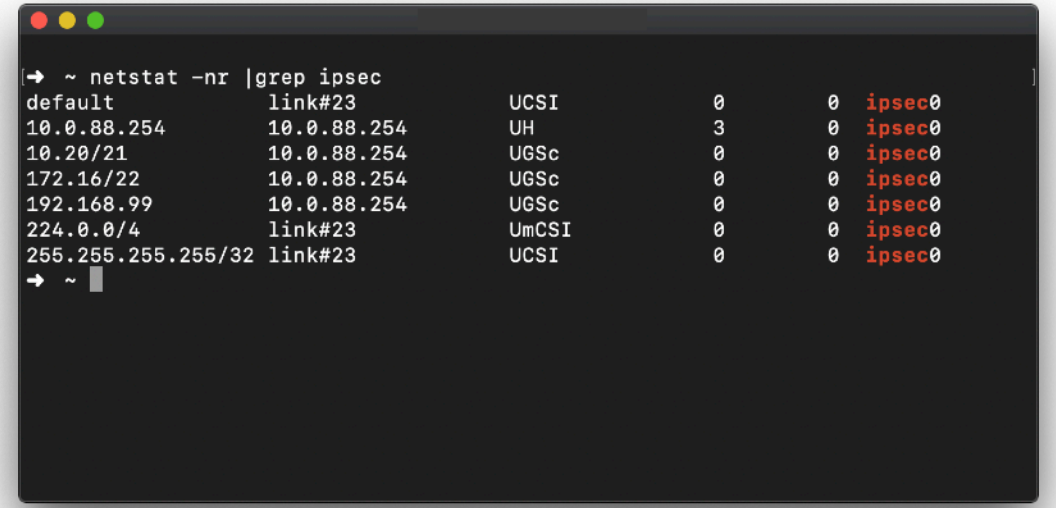


*Don't forget to **lock settings***

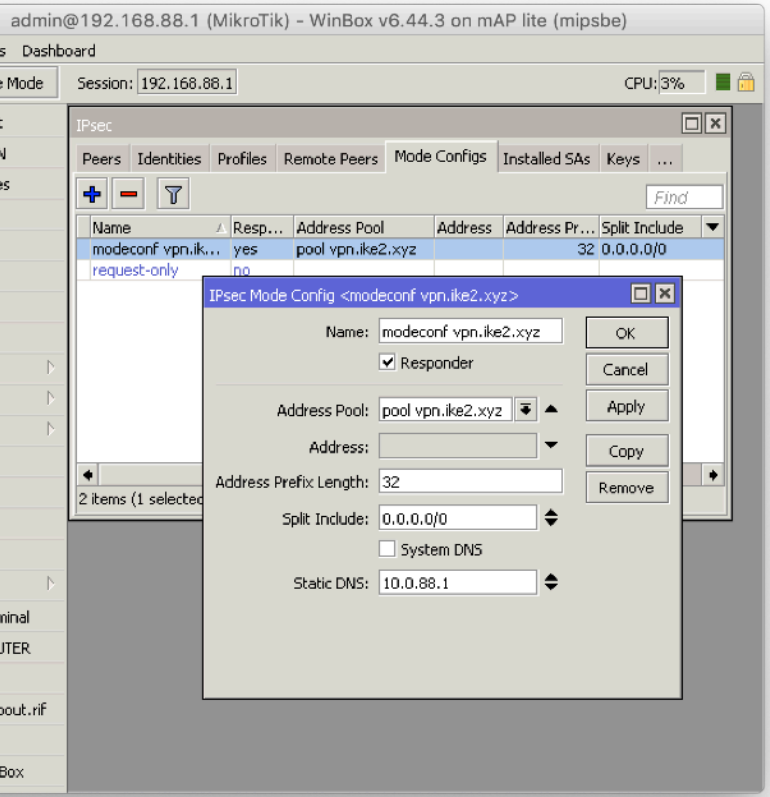
MacOS: Check IKEv2 VPN routes







MacOS: Check IKEv2 VPN routes




```
➜  ~ 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
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      1
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      1
2.       .62       link#23            UHW3I           0        1  ipsec0      !
2.       100       link#23            UHW3I           0        1  ipsec0      2
2.       95        link#23            UHW3I           0        1  ipsec0      !
```

Apple iOS

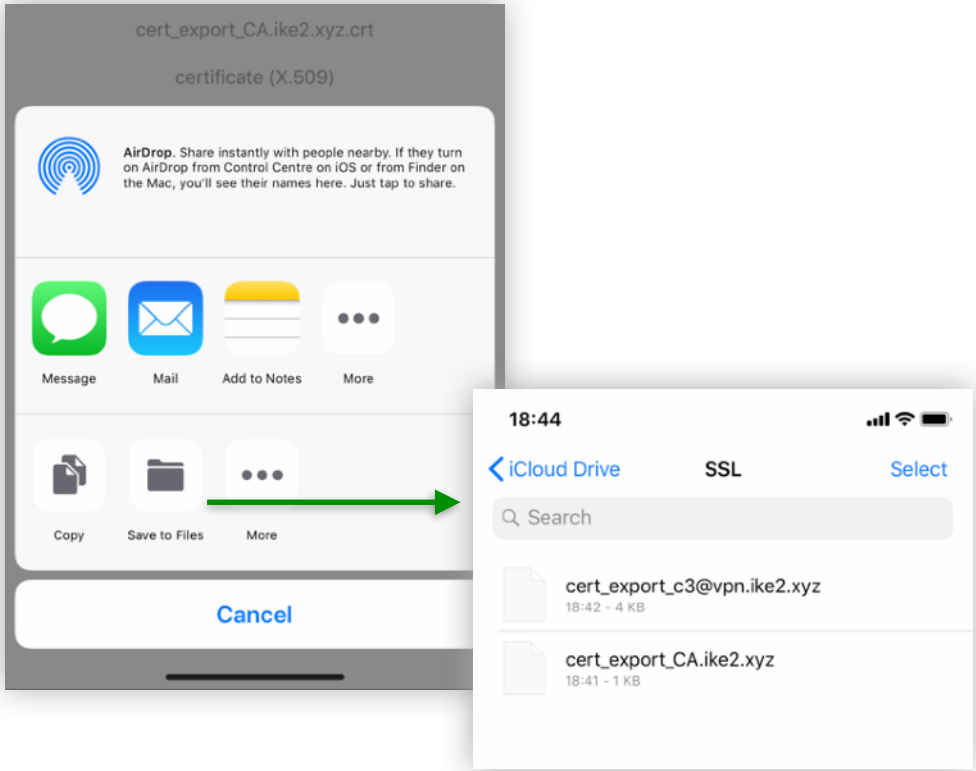
≥ version 9

Agenda for next slides

1. Import SSL certificates
2. Setup IKEv2 VPN connection

Nikita Tarikin / nikita@tarikin.com

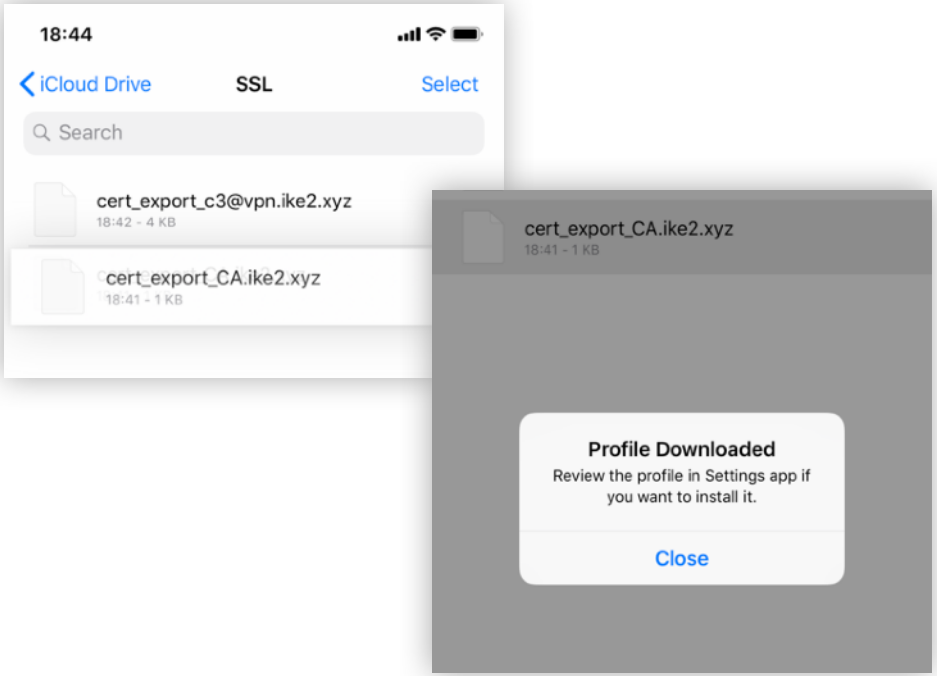
iOS: Import SSL certificates



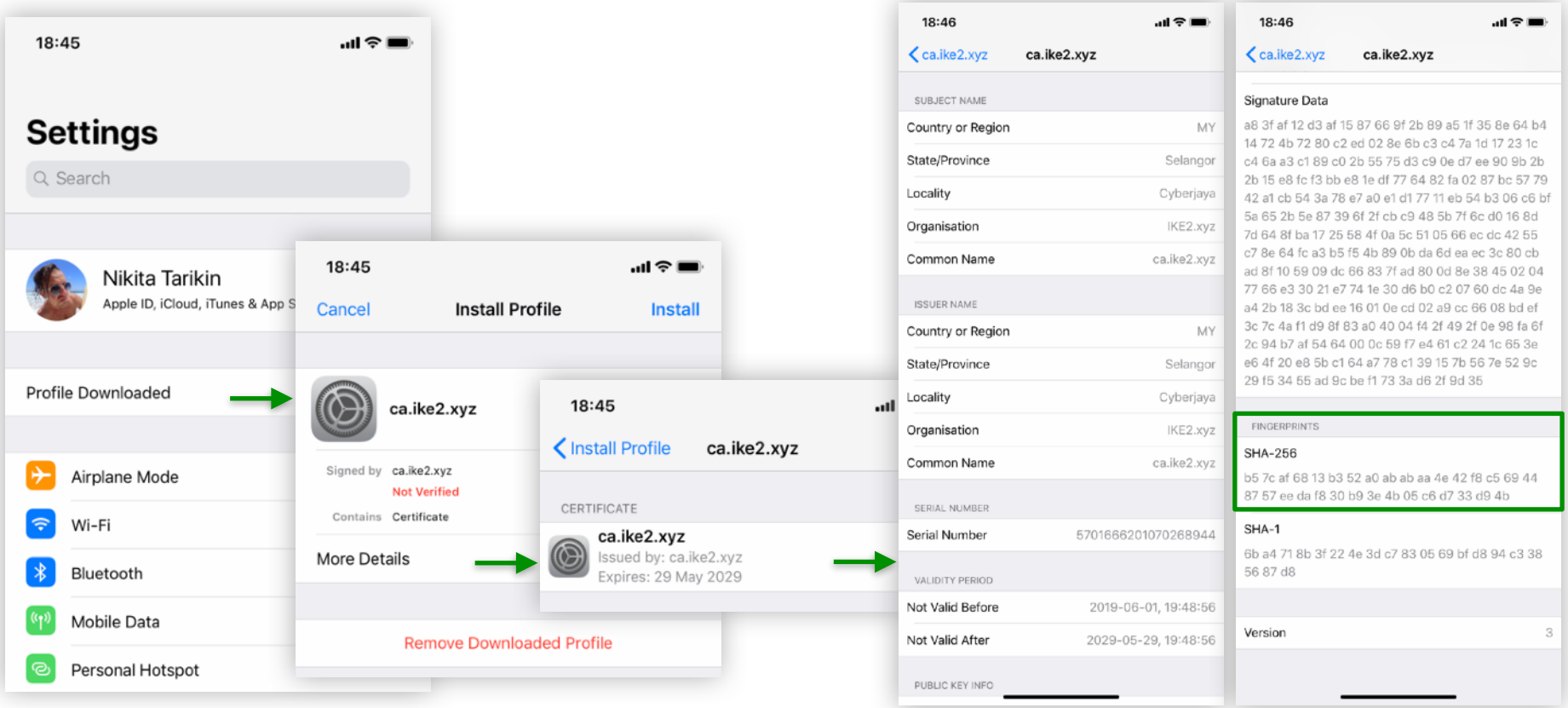
Download **CA** certificate .crt

Download **client** certificate .p12

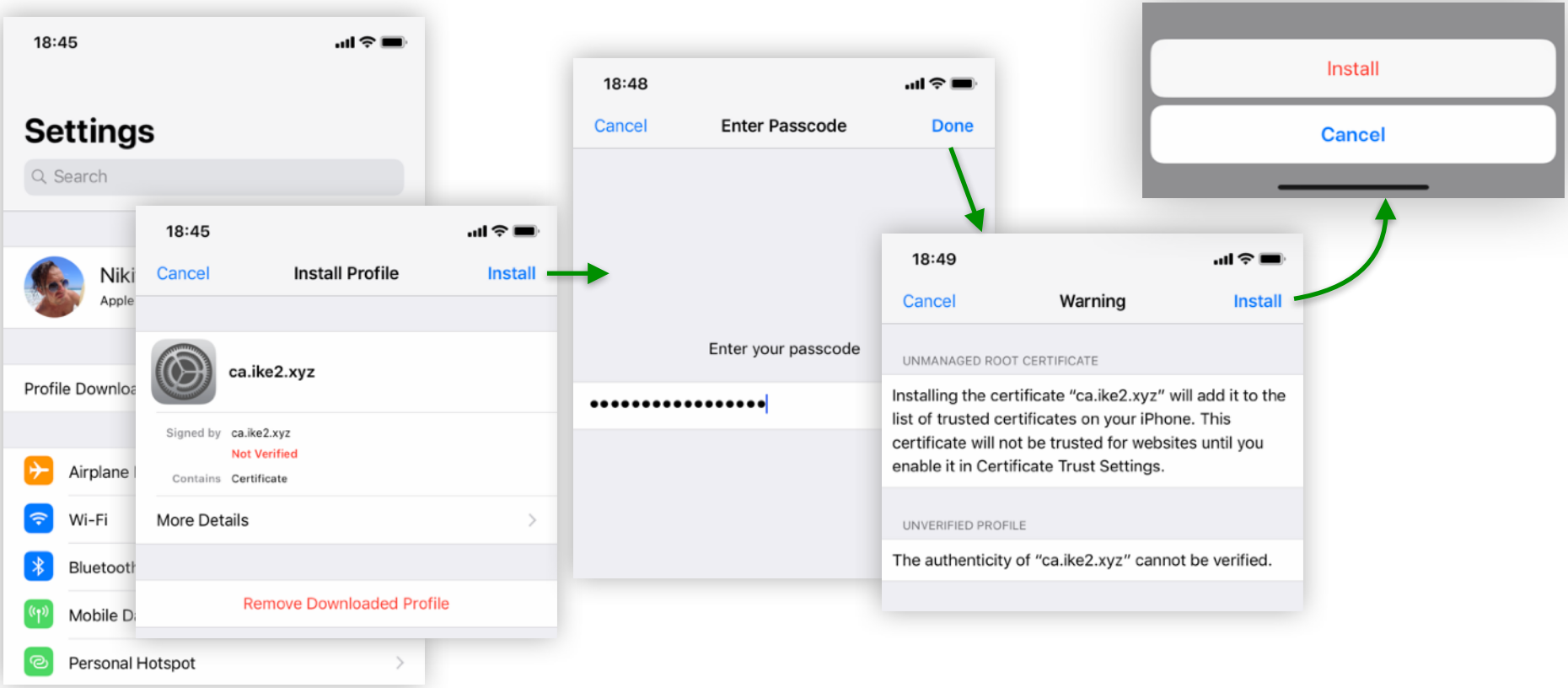
iOS: Import CA SSL certificate



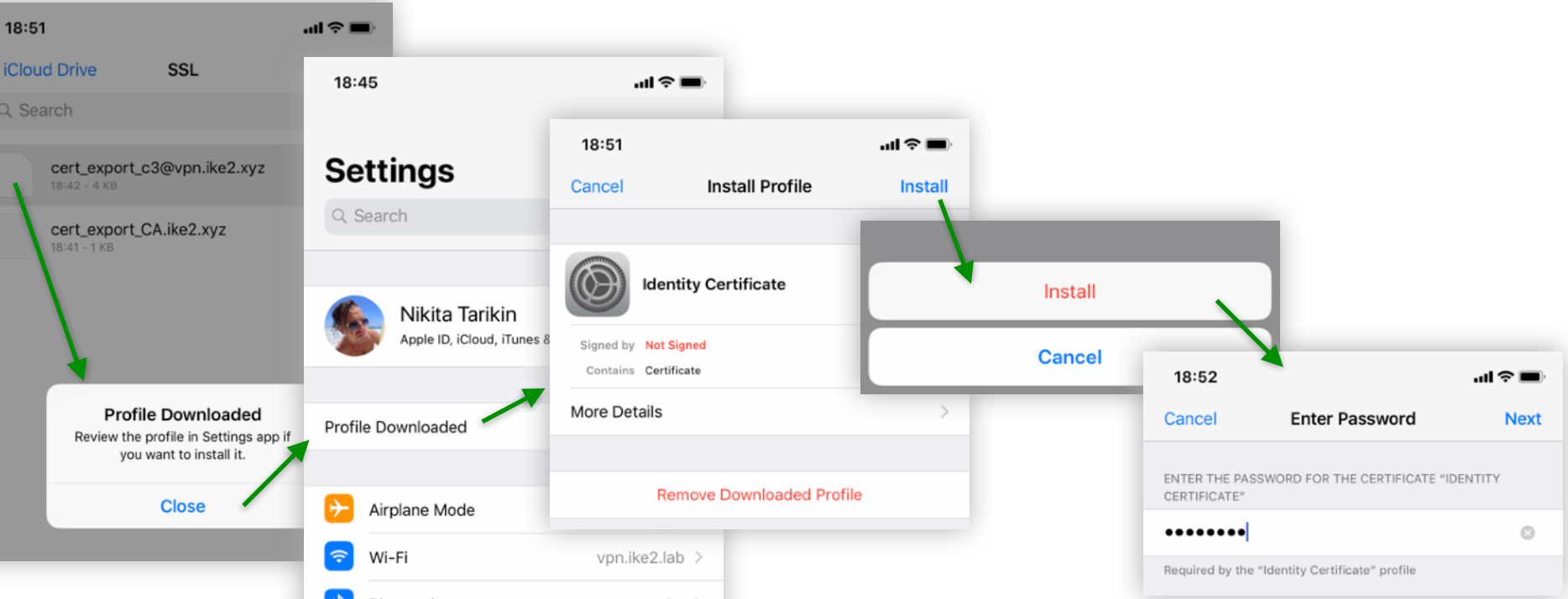
iOS: Import CA SSL certificate



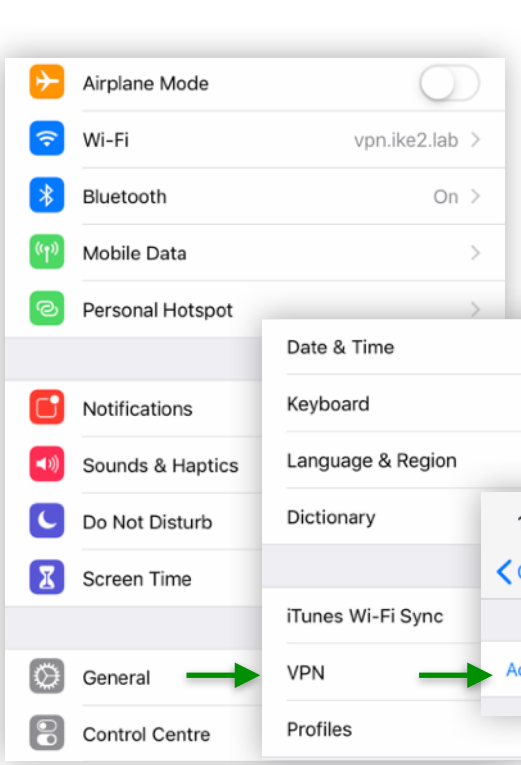
iOS: Import CA SSL certificate

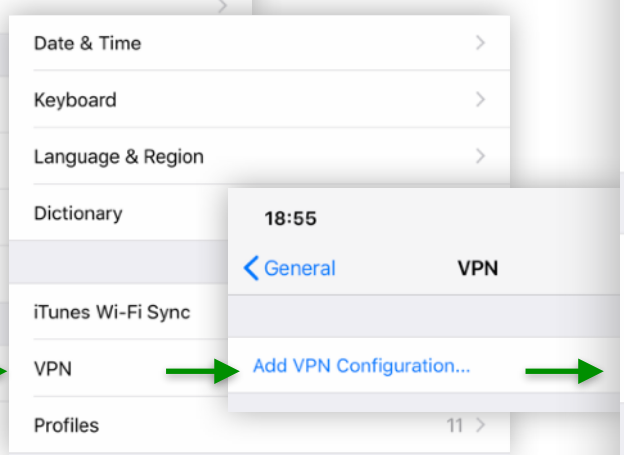


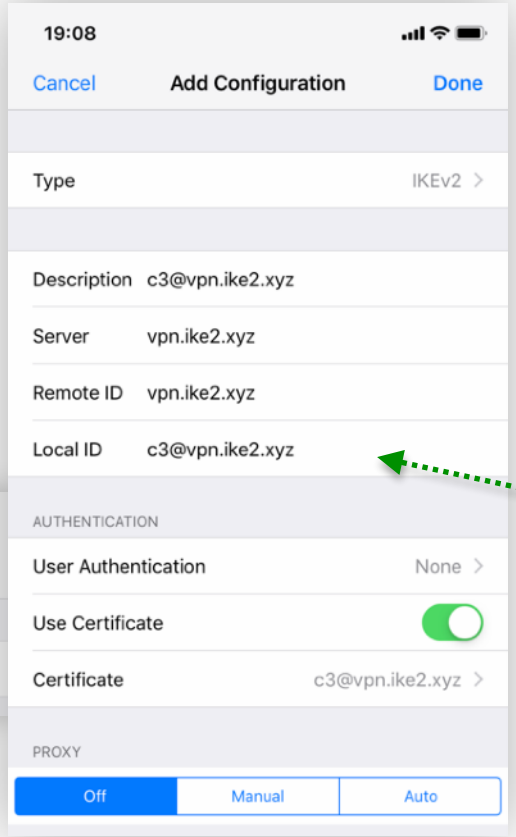
iOS: Import client SSL certificate

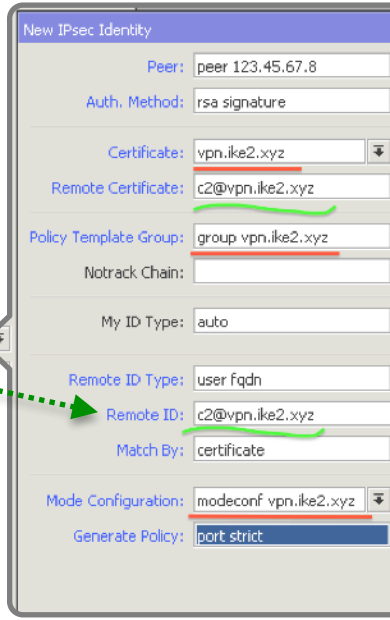


iOS: Setup IKEv2 VPN connection

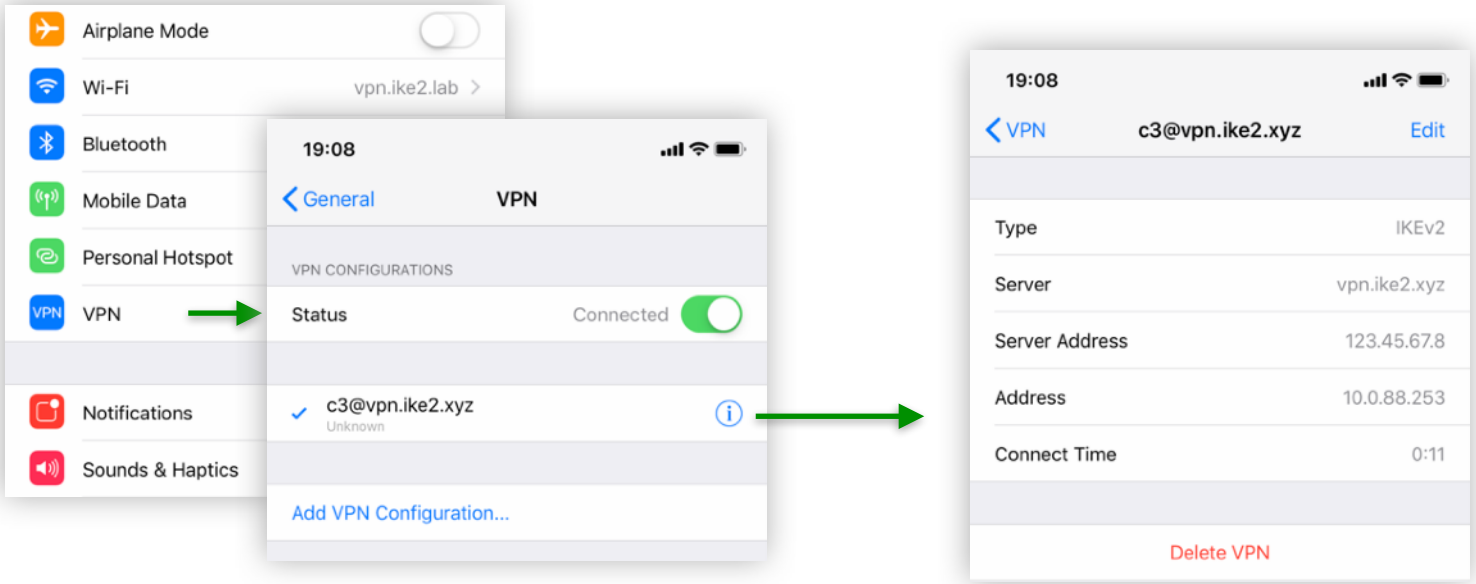








iOS: Connect IKEv2 VPN

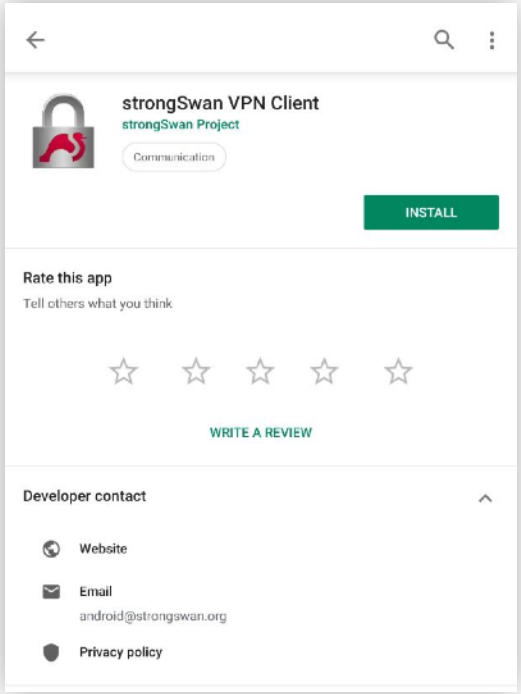


Android

Agenda for next slides

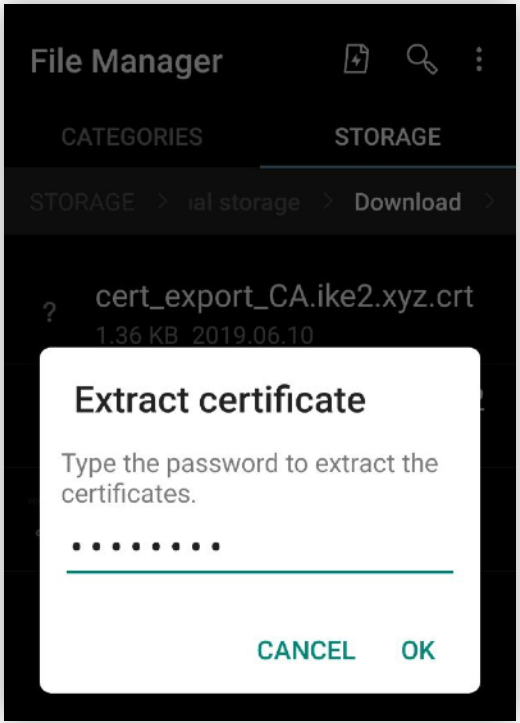
1. Install 3rd party app StrongSwan
2. Import SSL certificates
3. Setup IKEv2 VPN connection

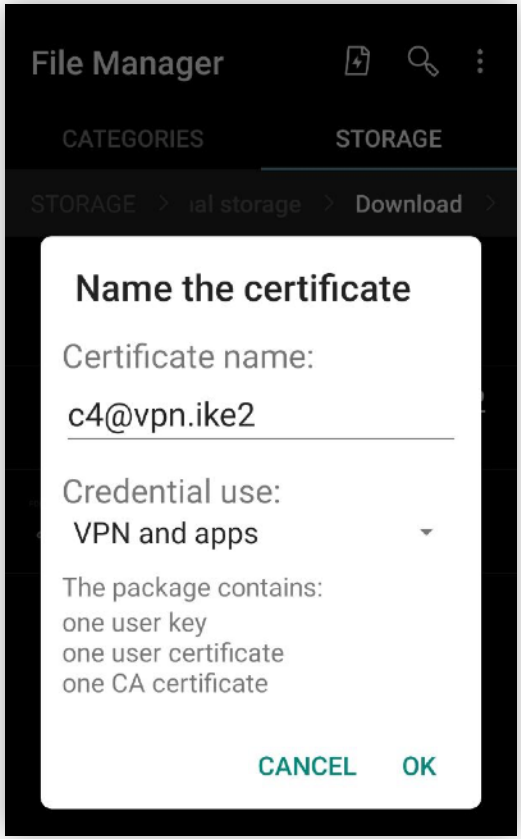
Android: Install StrongSwan



Find **StrongSwan** app on the Google Play

Android: Import SSL certificates

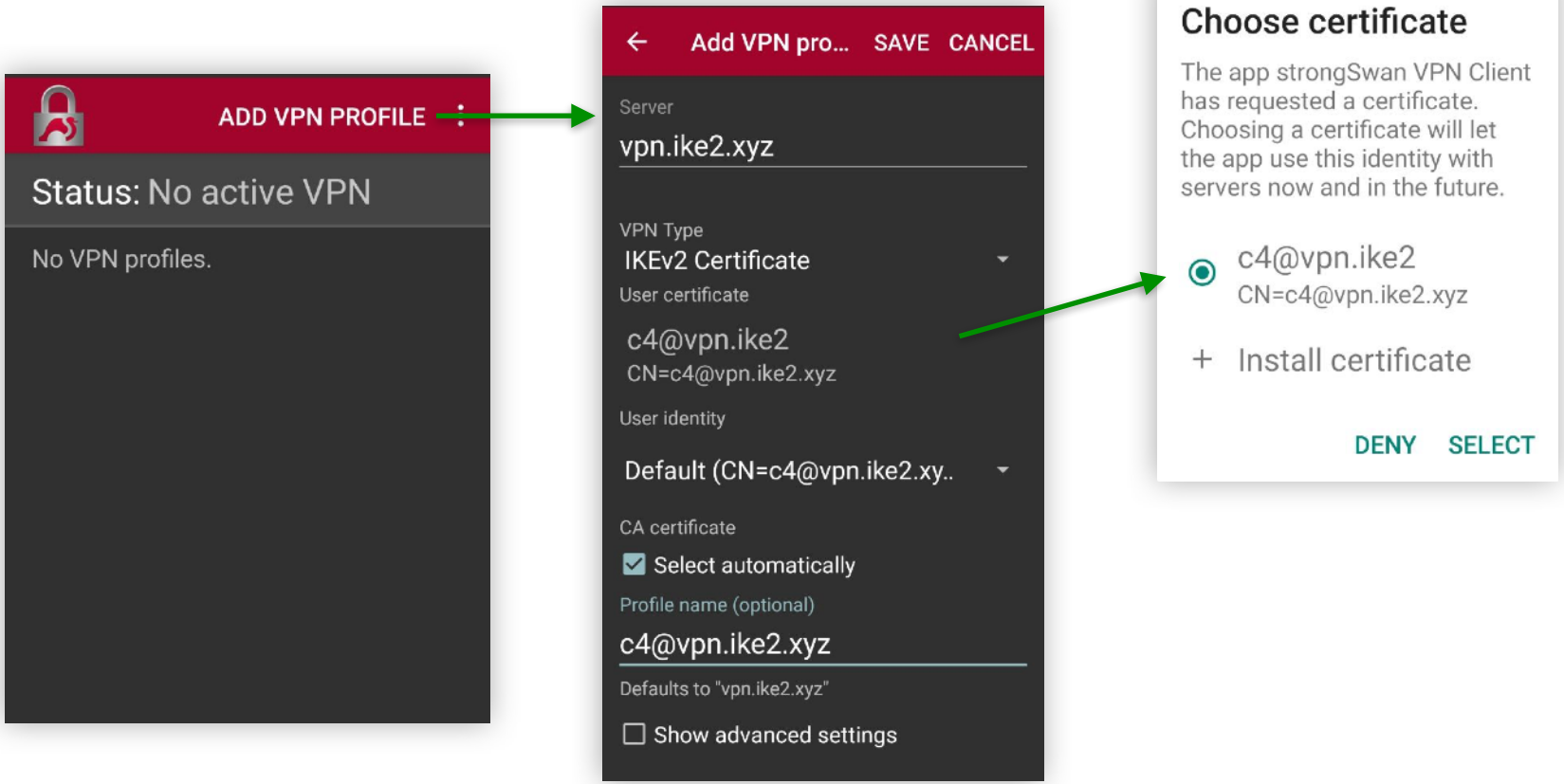




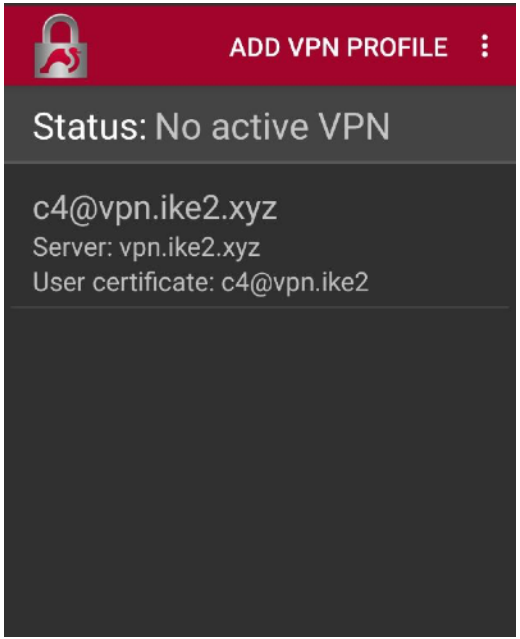
Download and install

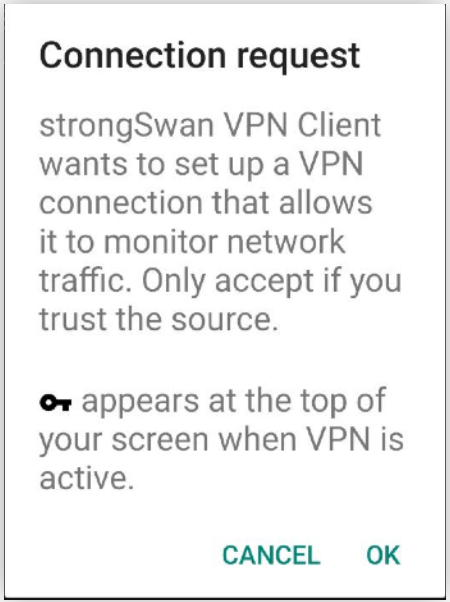
user certificate .p12

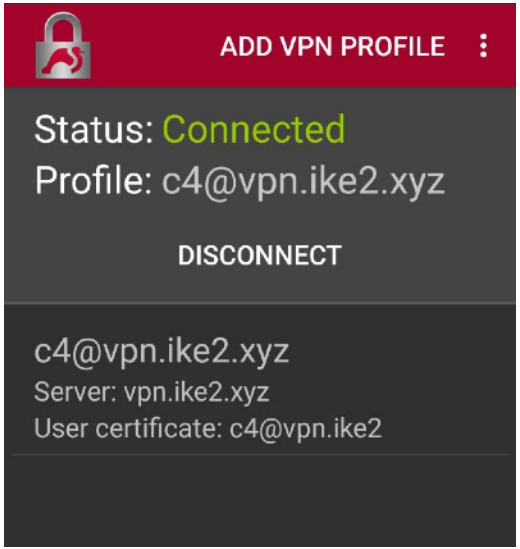
Android: Setup IKEv2 VPN connection



Android: Connect IKEv2 VPN







The end ¯_(ツ)_/¯

Nikita Tarikin / nikita@tarikin.com

YouTube video for this presentation in 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

Messenger Nikita Tarikin

Please contact me

Nikita Tarikin

nikita@tarikin.com

Demo lab

Request your certificate via form

https://forms.gle/nZTDK2wex5nneqo6A

Nikita Tarikin / nikita@tarikin.com