MUM Indonesia

October 24–25, 2019

KUTA, BALI, Indonesia

MikroTik IPSec IKEv2 VPN site-to-site: easy step-by-step guide by Nikita Tarikin (MikroTik PRO, Russia)

Nikita Tarikin / nikita@tarikin.com

Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia

MikroTik CERTIFIED

Nikita Tarikin / nikita@tarikin.com

Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia

MTCNA 99%

MTCRE 95%

MTCTCE 96%

MTCWE 84%

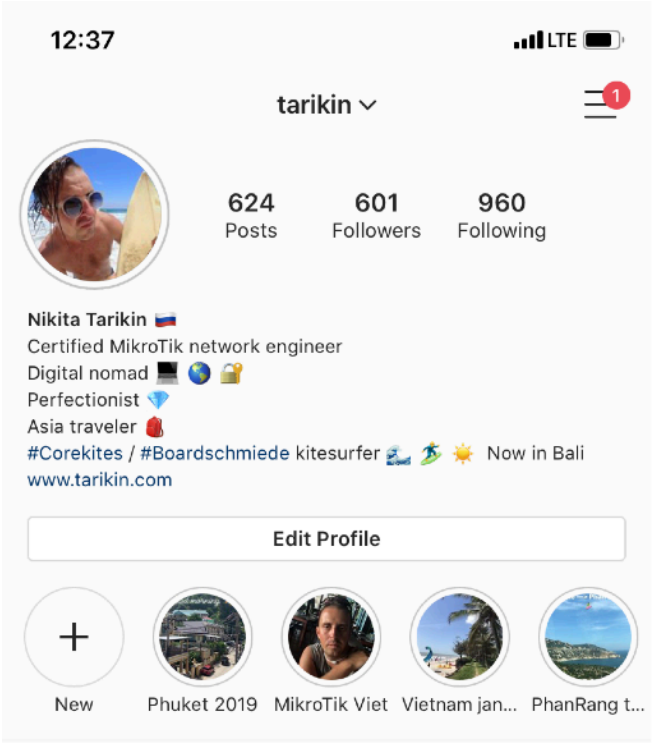
MTCUME 90%

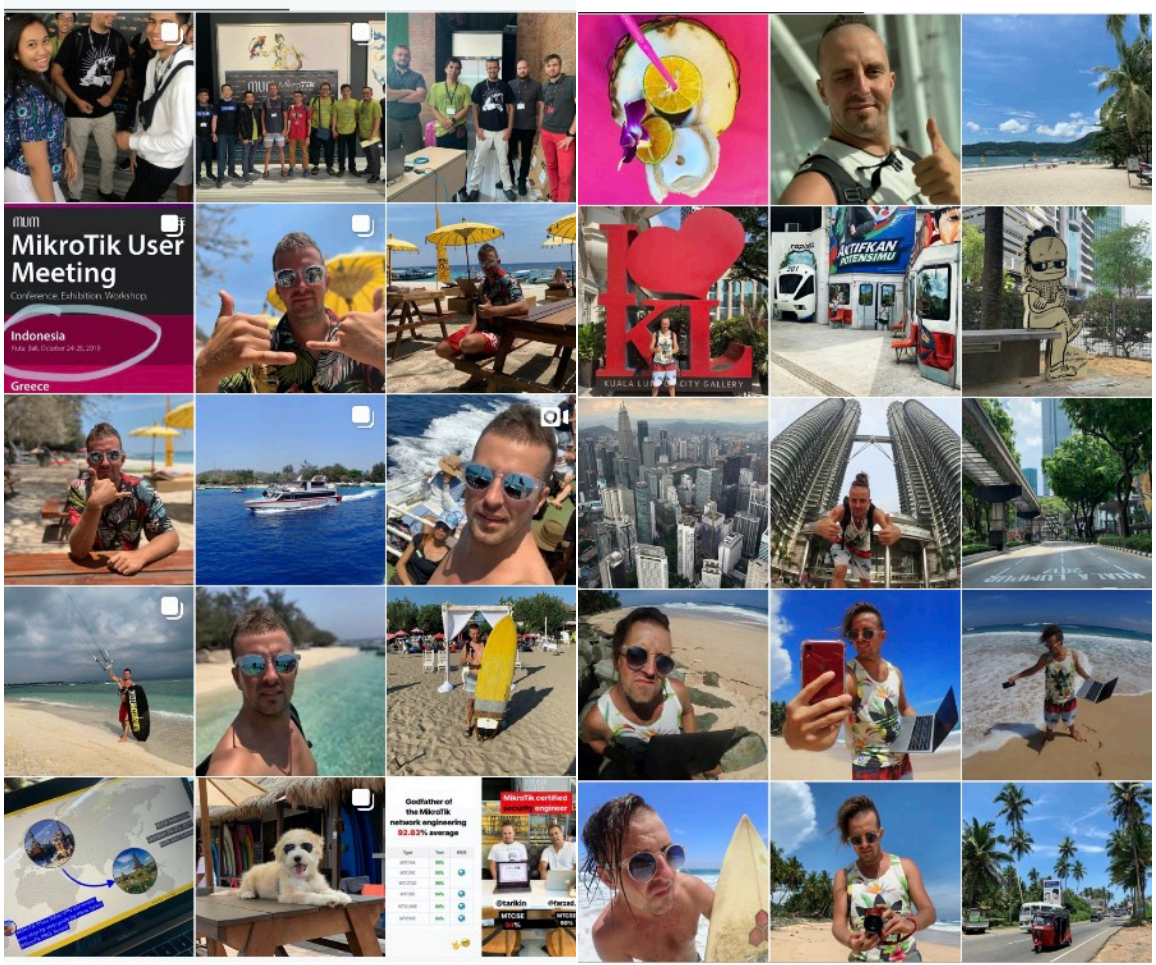
MTCSE 94%

MTCIPv6E 74%


BOARDSCHMIEDE
MikroTik
MALAYSIA

@tarikin


12:37
LTE
tarikin
624
Posts
601
Followers
960
Following
Nikita Tarikin
Certified MikroTik network engineer
Digital nomad
Perfectionist
Asia traveler
#Corekites / #Boardschmiede kitesurfer
Now in Bali
www.tarikin.com
Edit Profile
New
Phuket 2019
MikroTik Viet
Vietnam jan...
PhanRang t...


MikroTik User Meeting
Conference. Exhibition. Workshop.
Indonesia
Greece

@tropicalengineer

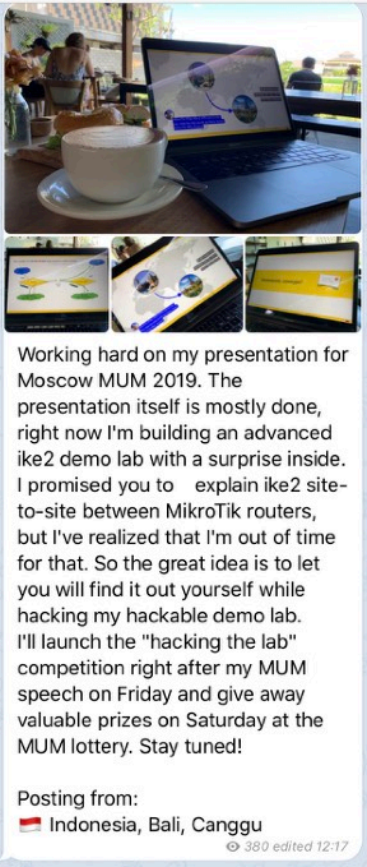
Tropical engineer
388 subscribers

share link
https://t.me/tropicalengineer

about
Stories of MikroTik network engineer.
Tropical lifestyle, remote networking, virtualization, kitesurfing, traveling, freelancing, sharing 📸 🌍 🏝

—

Nikita Tarikin @tarikin
Instagram: instagram.com/tarikin



Let’s keep in touch

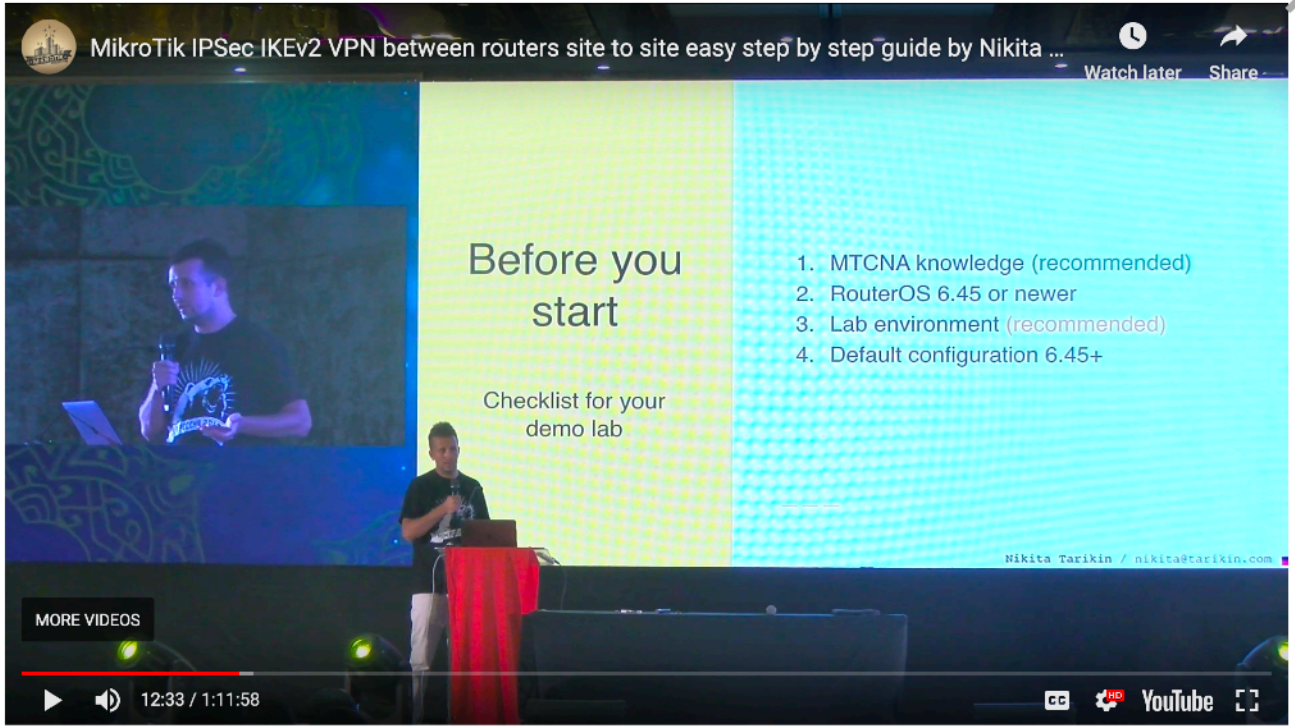
Send me e-mail:
nikita@tarikin.com

Find me in Facebook:
Nikita Tarikin

Subscribe my channels:
@tarikin
@tropicalengineer

Direct message me via:

Telegram t.me/tarikin
Messenger Nikita Tarikin



Watch this presentation on YouTube

https://www.youtube.com/watch?v=n5_Af2vllOA

Why IPSec IKE2?

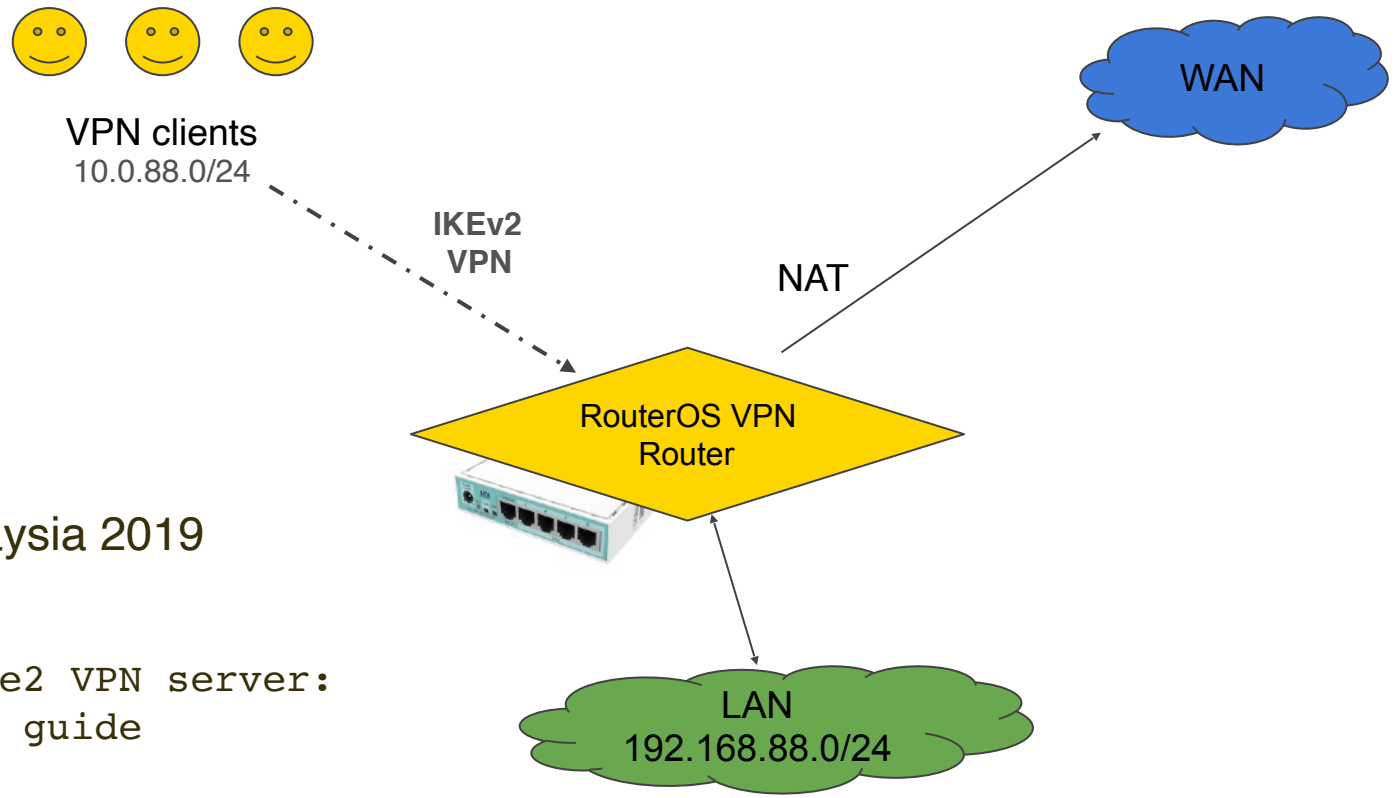
Compare VPN types (RouterOS)

	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

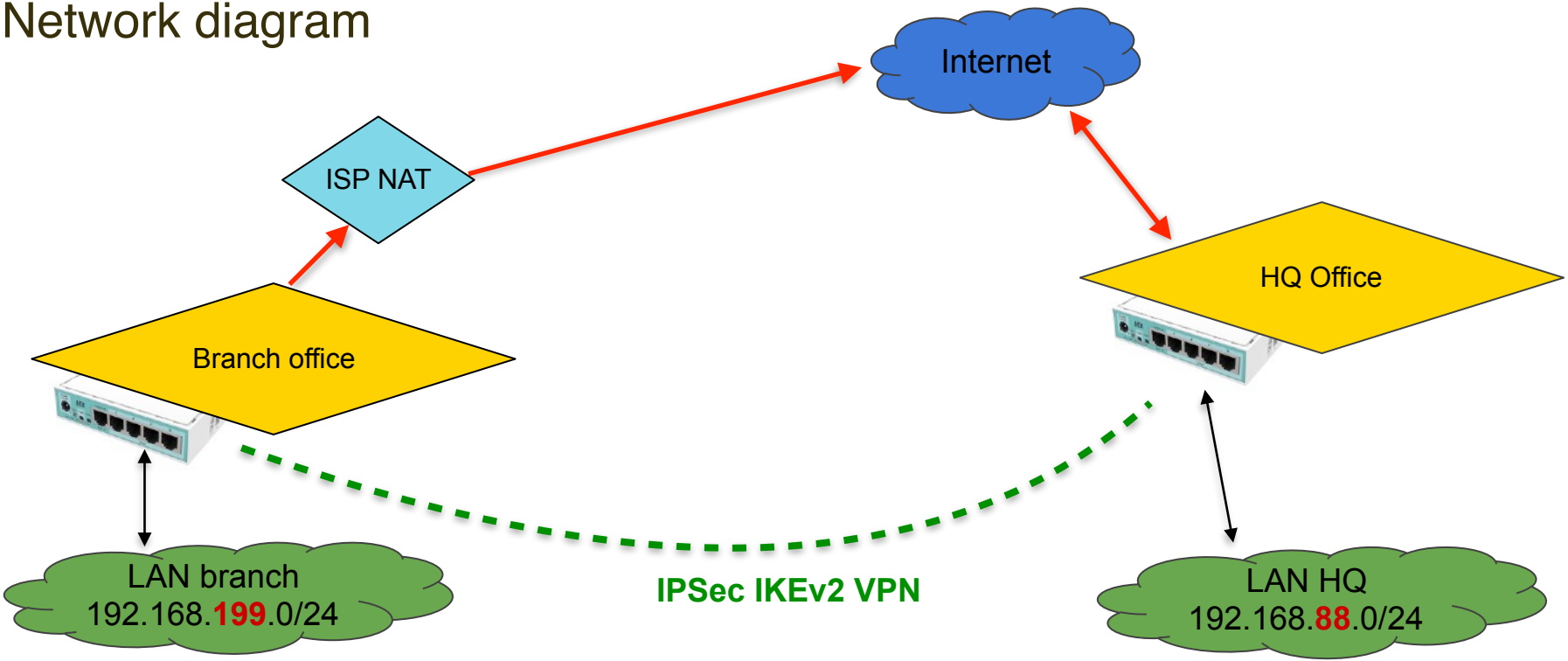


Archive: MUM Malaysia 2019 network diagram

MikroTik IPSec ike2 VPN server: easy step-by-step guide

https://mum.mikrotik.com/2019/MY/agenda/EN#475_7008

Network diagram



Headlines

1. Before you start
2. Build SSL certificates
3. Setting up ipsec vpn server
4. Setting up ipsec vpn client
5. Site-to-site via **interface over ipsec**
6. Site-to-site via **ipsec policy**
7. ~~Setting up firewall~~ (see MUM Malaysia 2019)
8. Adjust TCP-MSS
9. Demo lab + hacking quiz

Nikita Tarikin / nikita@tarikin.com

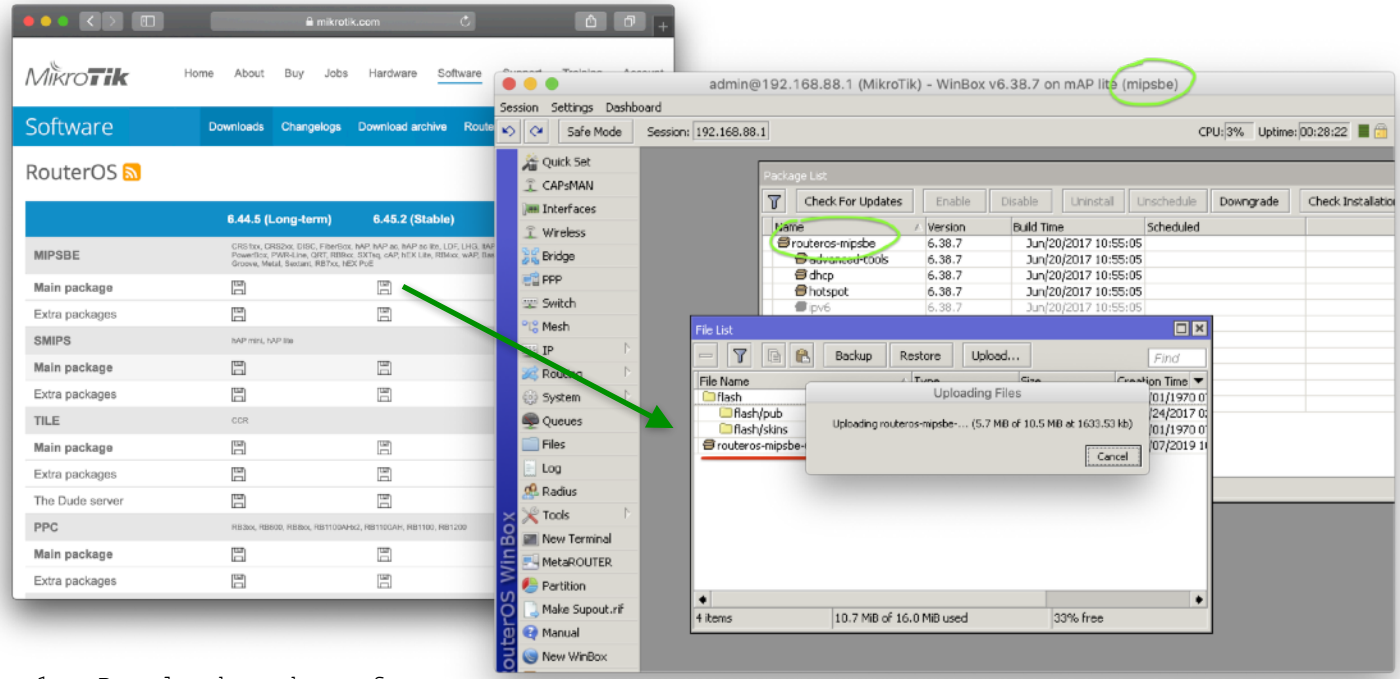
Before you start

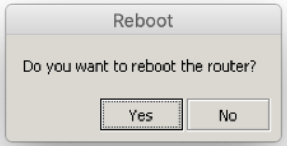
Checklist for your demo lab

1. MTCNA knowledge (recommended)
2. RouterOS 6.45 or newer
3. Lab environment (recommended)
4. Default configuration 6.45+

Nikita Tarikin / nikita@tarikin.com

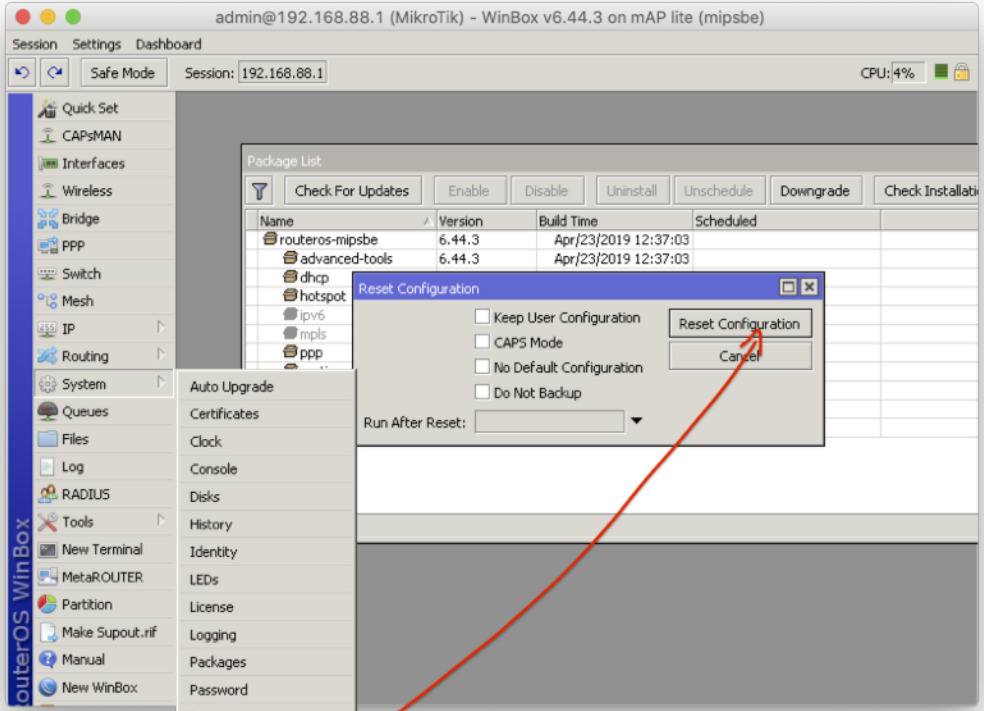
Upgrade RouterOS to 6.45+



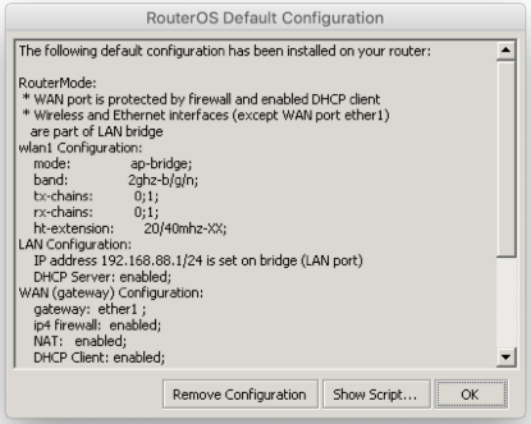


1. Download package from www.mikrotik.com/download
2. Upload package to / of your RouterBoard
3. System -> Reboot

Reset RouterBoard to default v6.45+ configuration



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



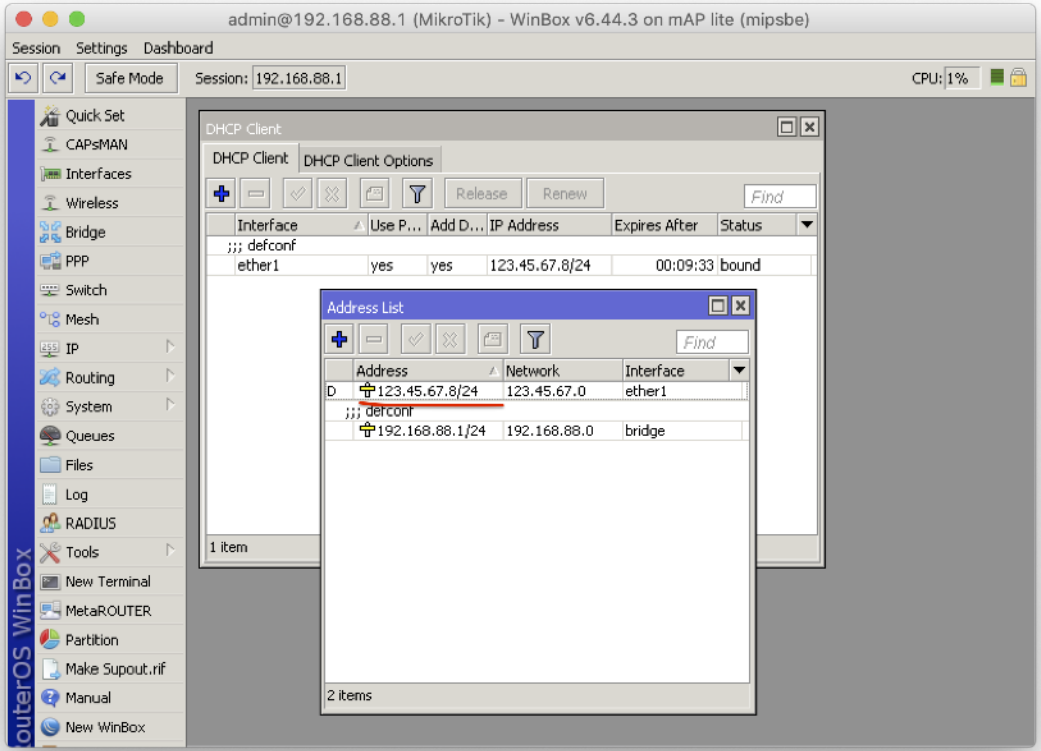
`System -> Reset configuration`

General system settings

Agenda for next slides:

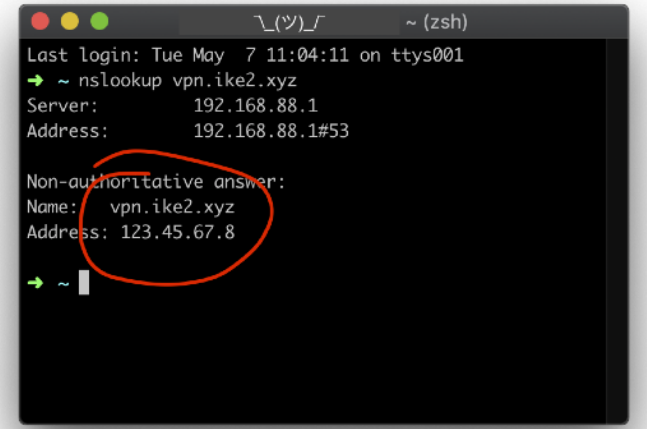
1. WAN IP/DNS addresses
2. Timezone
3. Date/time via NTP
4. Loopback bridge
5. IP pool

WAN IP and DNS addresses for IKE2 VPN server



123.45.67.8 is on WAN interface

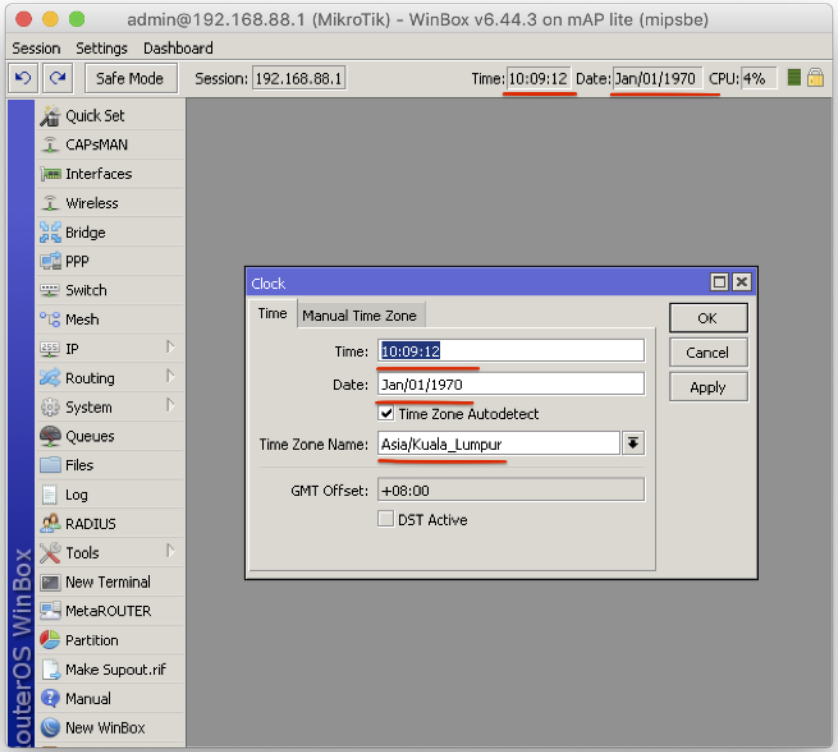
Check DNS records:
Name: **vpn.ike2.xyz**
Address: **123.45.67.8**



* Set DNS records with your domain name registrar control panel

Setup correct timezone

Important

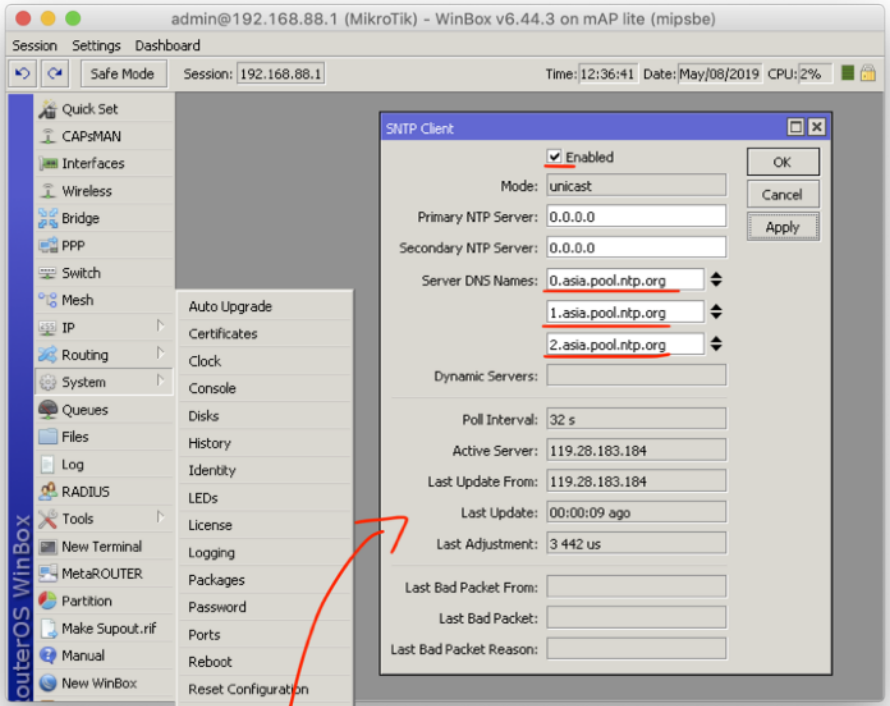


System -> Clock

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

Setup auto date/time

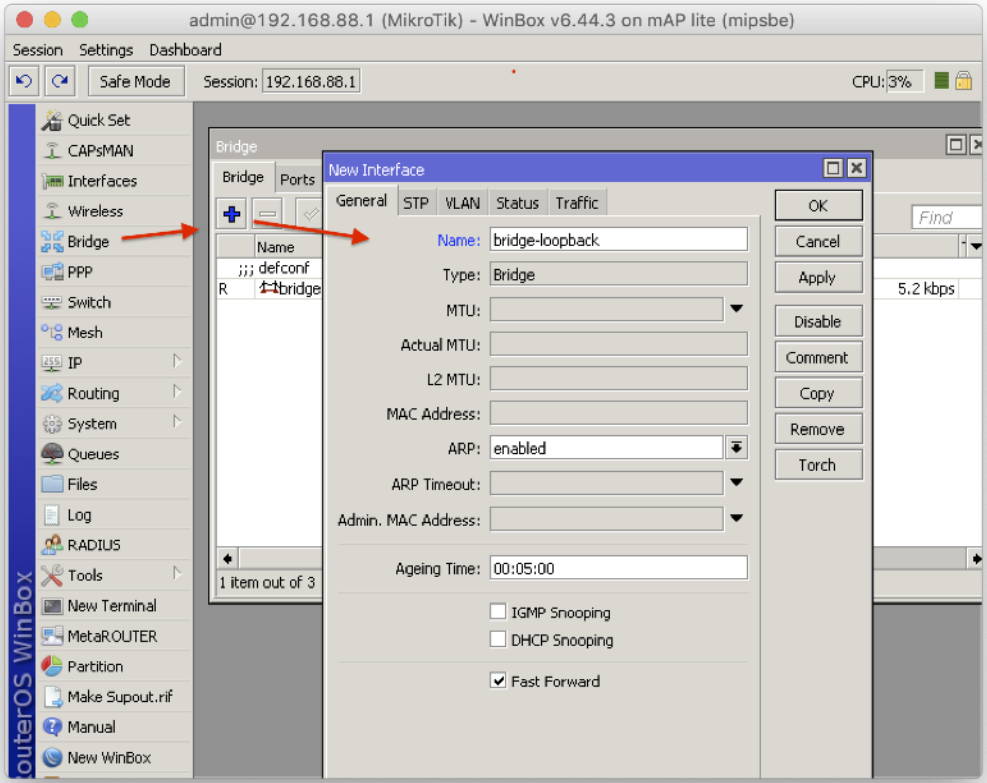
Important



Activate NTP client

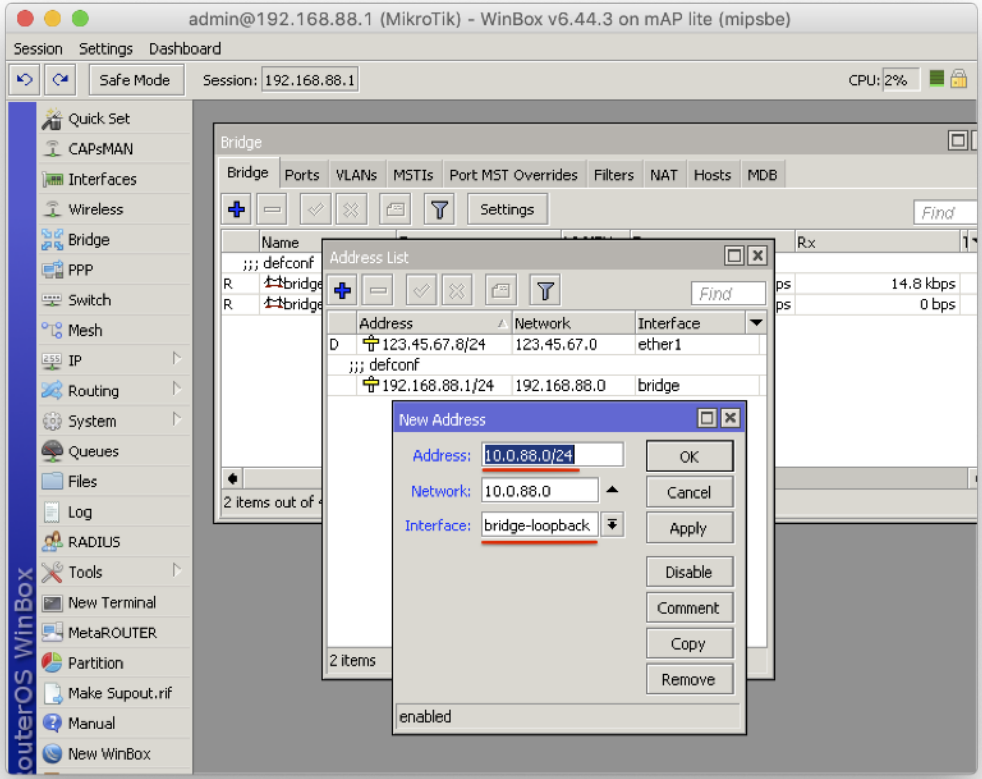
```
/system ntp client set enabled=yes
server-dns-
names=0.asia.pool.ntp.org,1.asia.pool.n
tp.org,2.asia.pool.ntp.org
```

Add new loopback bridge



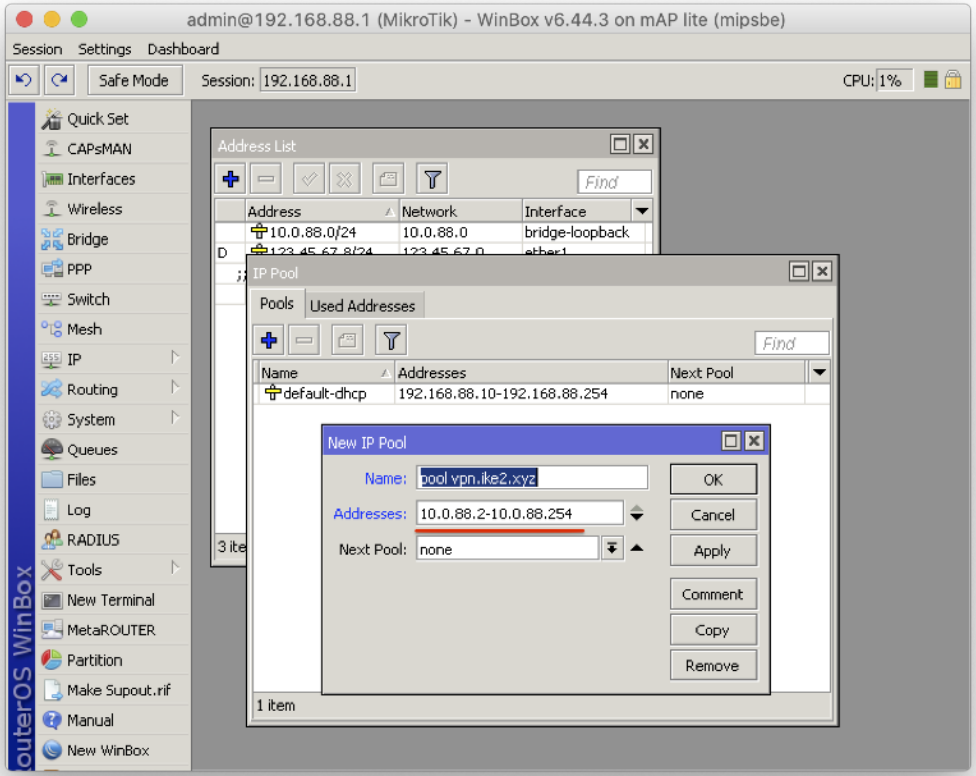

```
/interface bridge add
name=bridge-loopback
```

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



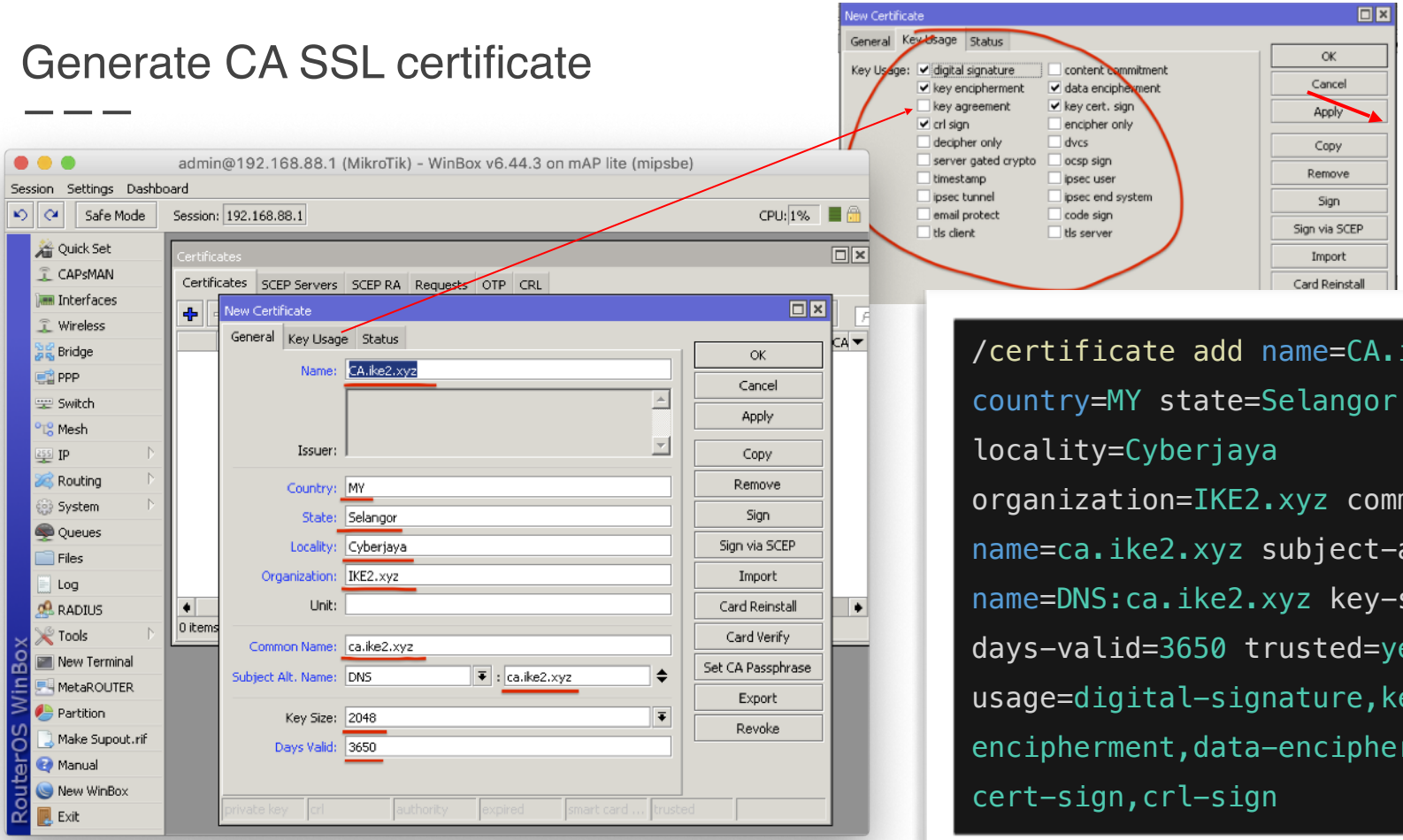

```
/ip pool add name="pool
vpn.ike2.xyz"
ranges=10.0.88.2-10.0.88.254
```

Generate SSL certificates

Agenda for next slides

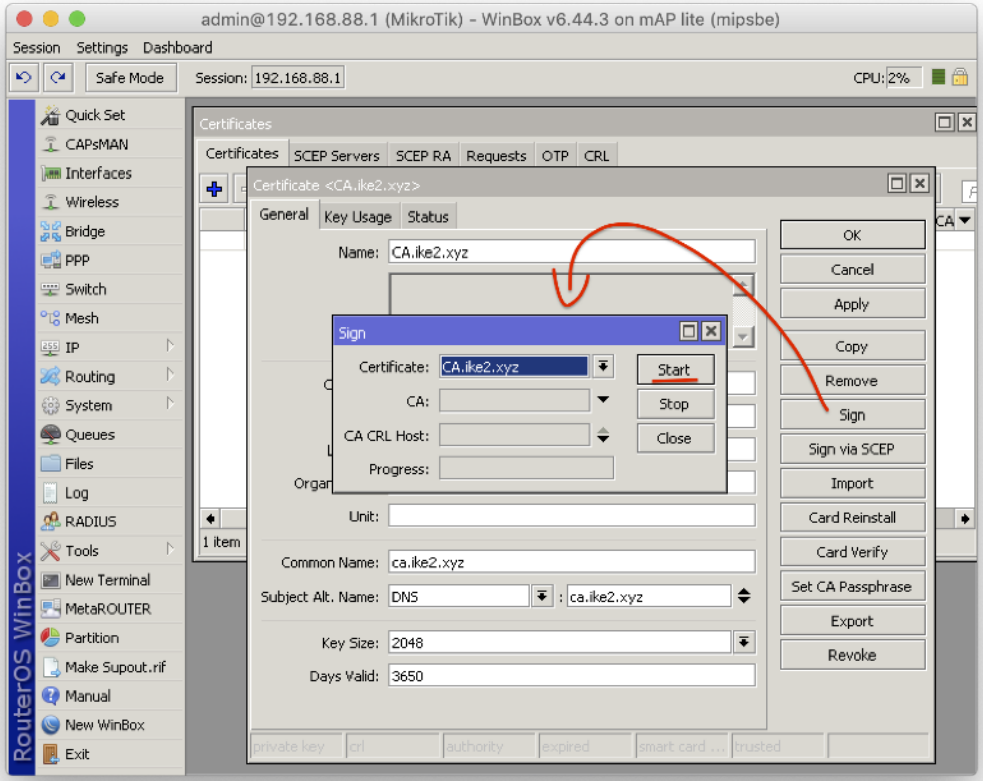
1. Generate CA
2. Generate server SSL
3. Generate client SSL
4. Export client SSL

Generate CA SSL certificate



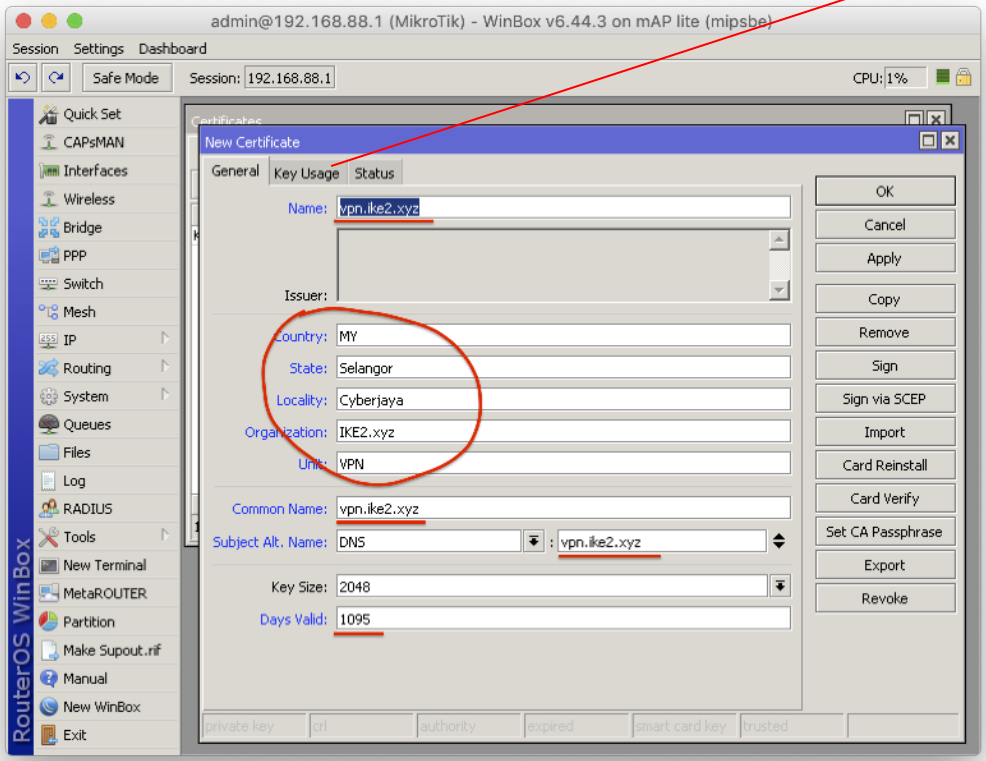

```
/certificate add name=CA.ike2.xyz
country=MY state=Selangor
locality=Cyberjaya
organization=IKE2.xyz common-
name=ca.ike2.xyz subject-alt-
name=DNS:ca.ike2.xyz key-size=2048
days-valid=3650 trusted=yes key-
usage=digital-signature,key-
encipherment,data-encipherment,key-
cert-sign,crl-sign
```

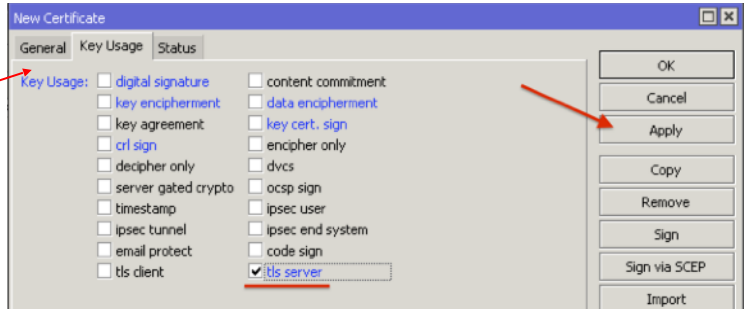
Self-sign CA SSL certificate *(Certificate Authority)*




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

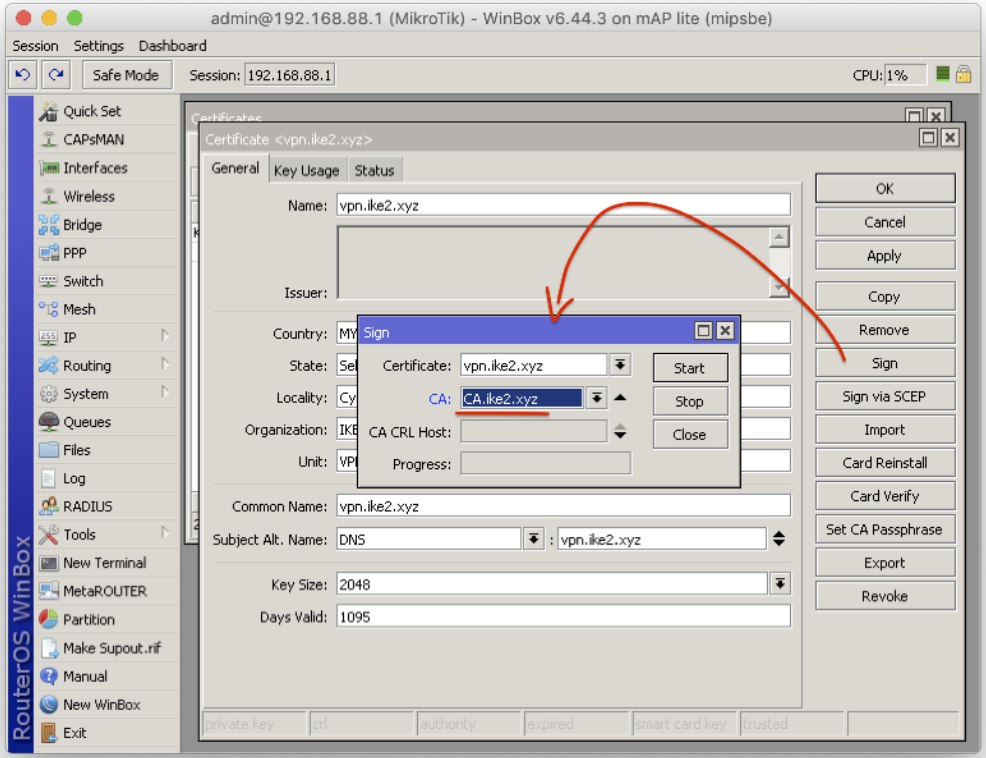
Generate server SSL certificate





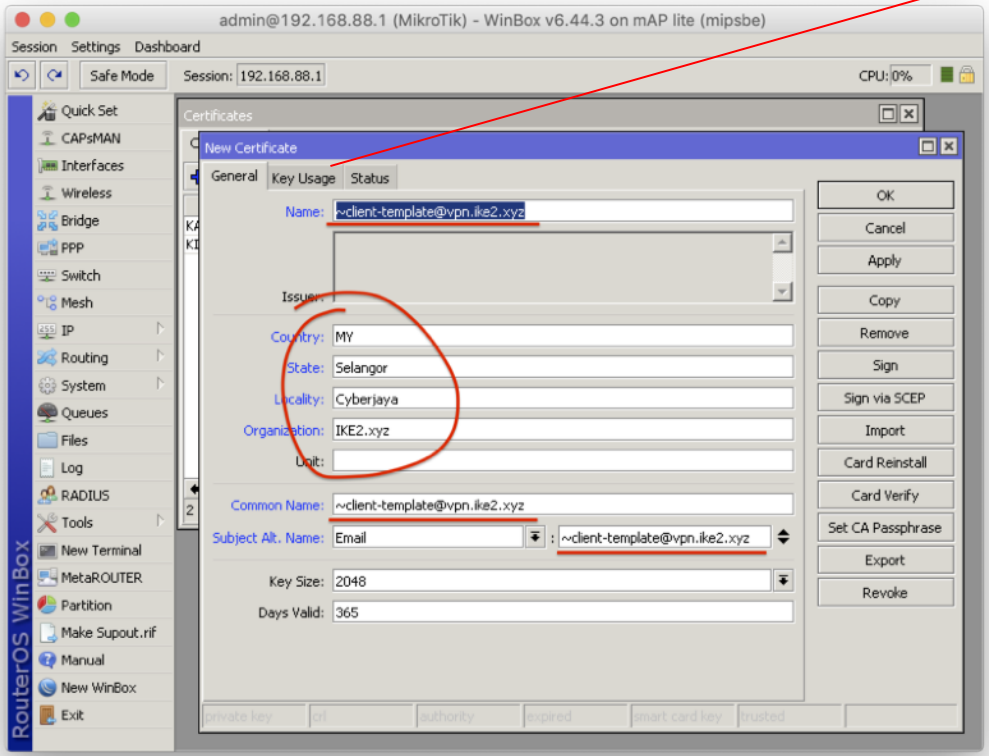

```
/certificate add name=vpn.ike2.xyz
country=MY state=Selangor
locality=Cyberjaya
organization=IKE2.xyz unit=VPN
common-name=vpn.ike2.xyz subject-
alt-name=DNS:vpn.ike2.xyz key-
size=2048 days-valid=1095
trusted=yes key-usage=tls-server
```

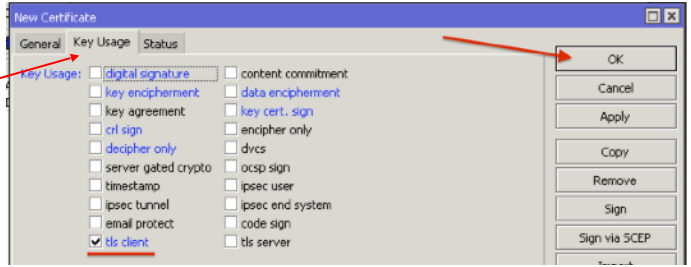
Sign server SSL certificate with CA.ike2.xyz authority




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

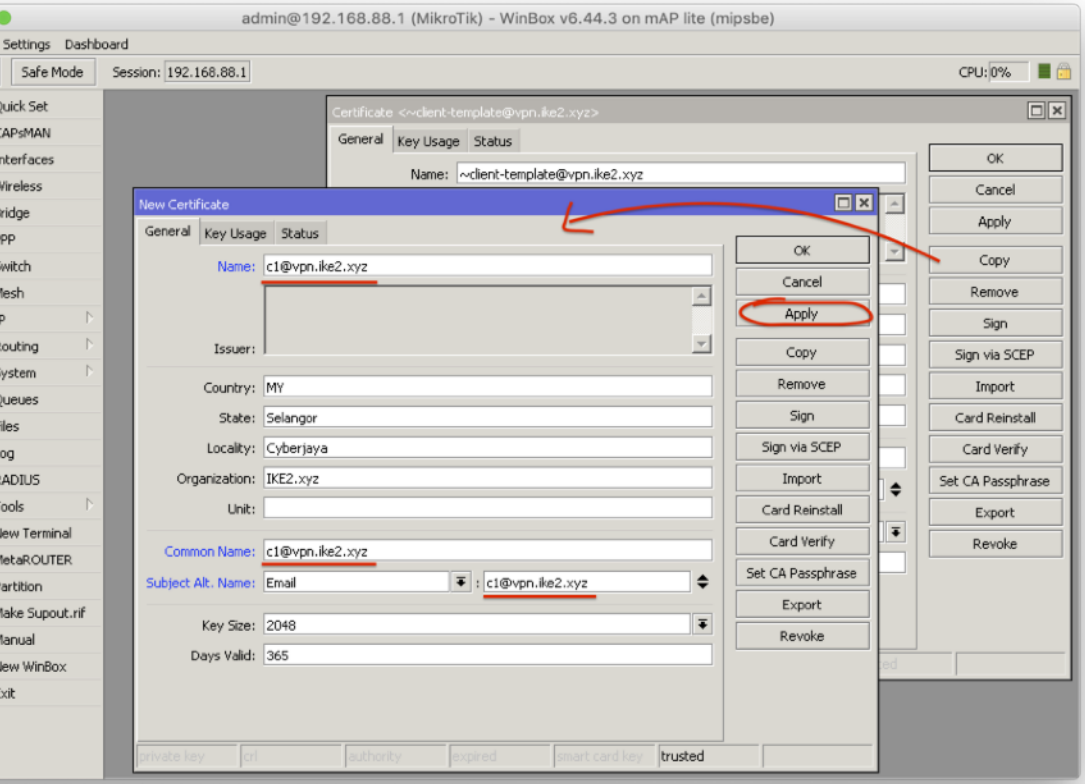
Client certificate template





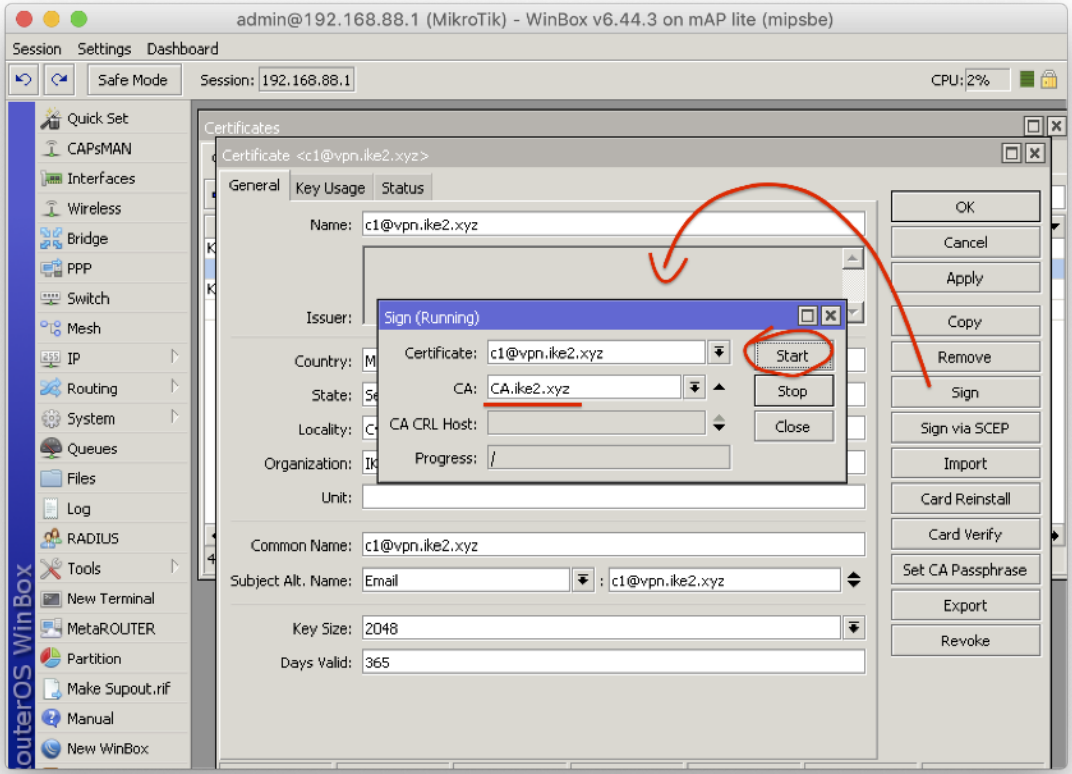

```
/certificate add name=~client-
template@vpn.ike2.xyz country=MY
state=Selangor locality=Cyberjaya
organization=IKE2.xyz common-
name=~client-template@vpn.ike2.xyz
subject-alt-name=email:~client-
template@vpn.ike2.xyz key-size=2048
days-valid=365 trusted=yes key-
usage=tls-client
```

Generate client SSL certificate from template



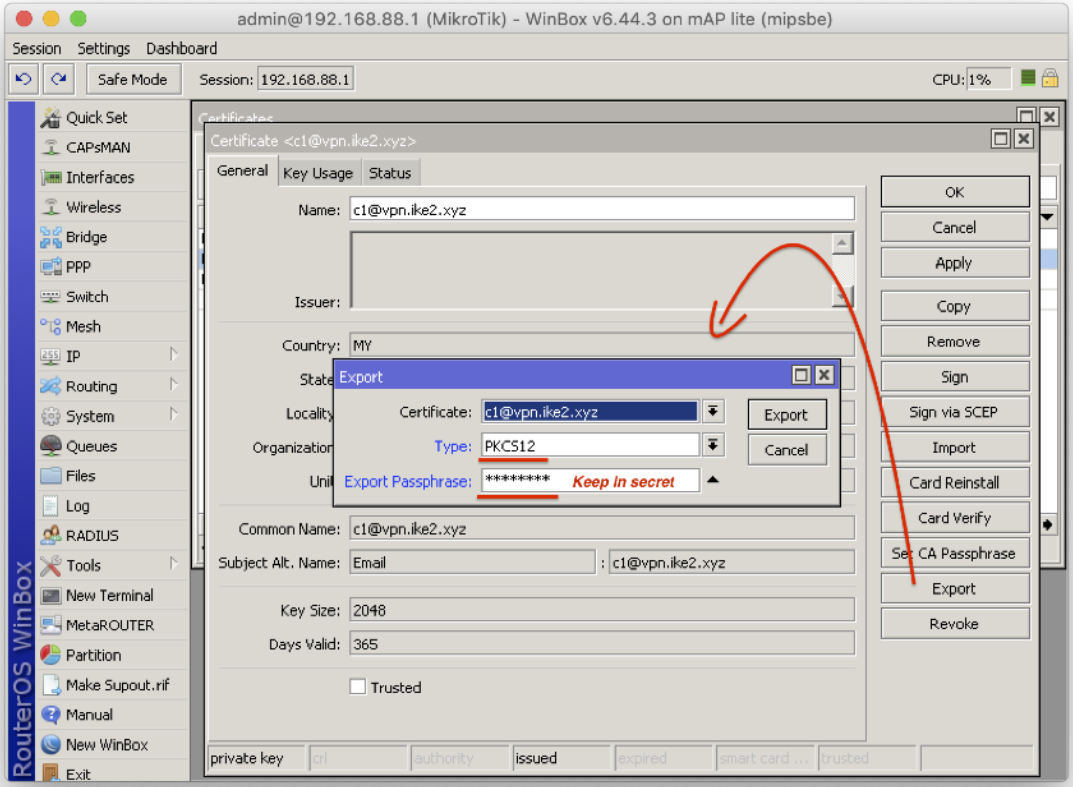

```
/certificate add copy-from=~client-
template@vpn.ike2.xyz
name=c1@vpn.ike2.xyz common-
name=c1@vpn.ike2.xyz subject-alt-
name=email:c1@vpn.ike2.xyz
```

Sign client SSL certificate with CA.ike2.xyz authority



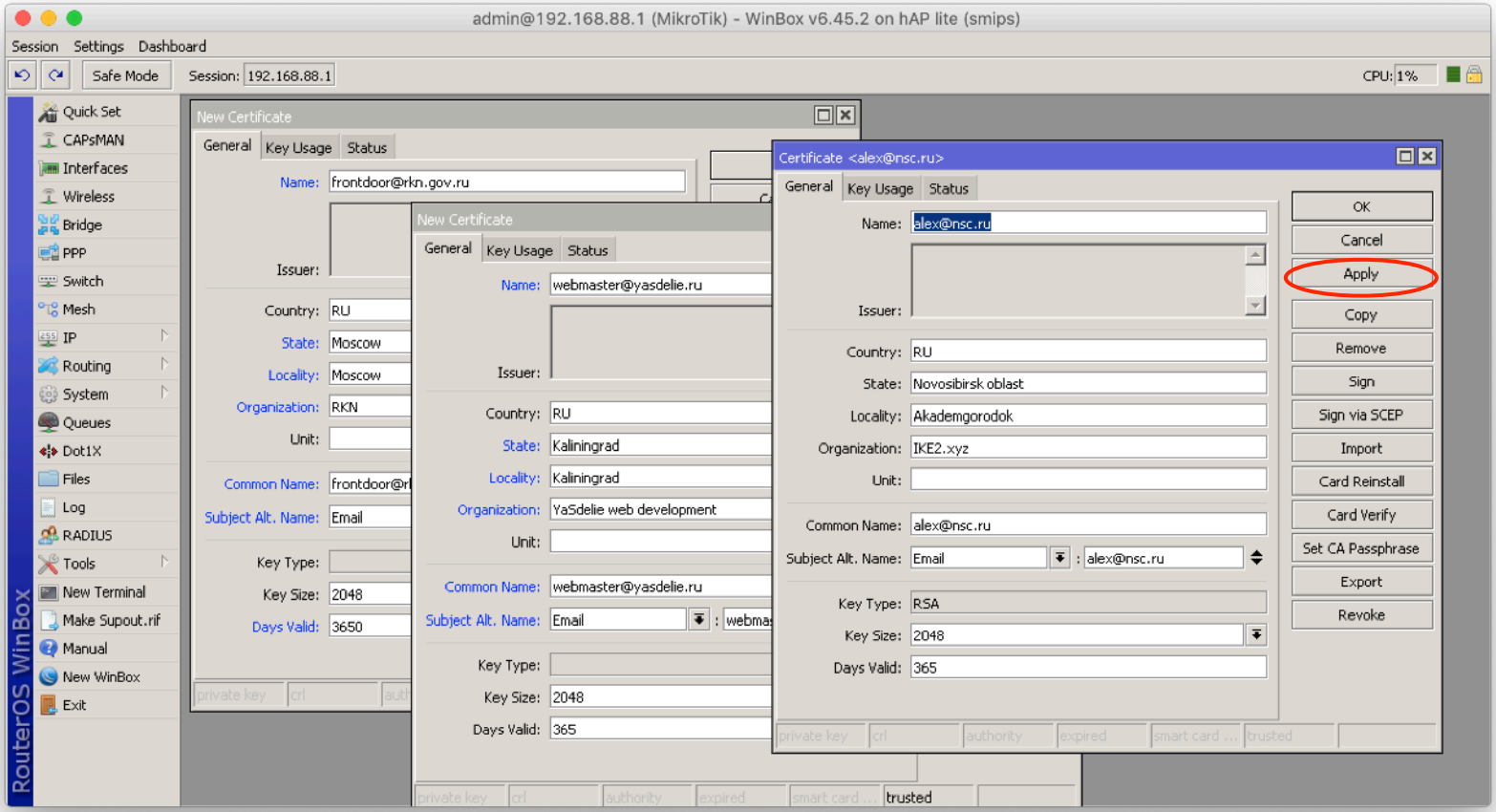

```
/certificate sign
c1@vpn.ike2.xyz ca=CA.ike2.xyz
```

Export client SSL certificate + private key to .p12 file

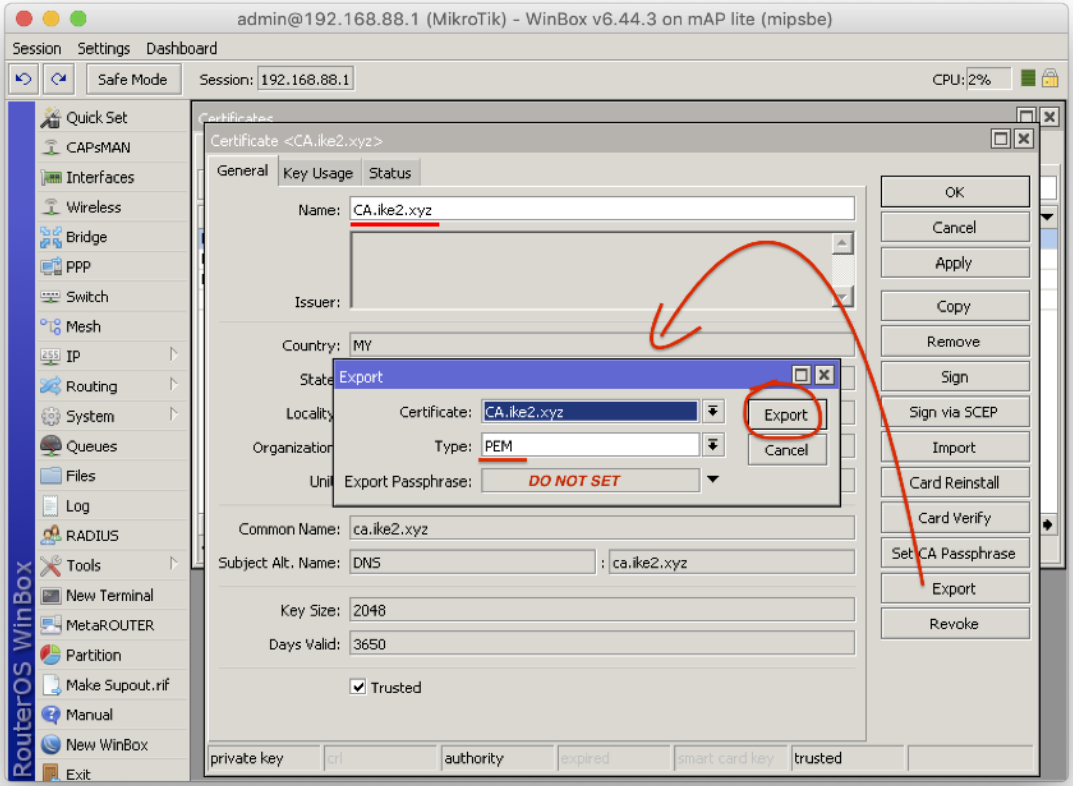



```
/certificate export-certificate
c1@vpn.ike2.xyz type=pkcs12
export-passphrase=keepinsecret
```

Generate various client SSL certificates from template (example)

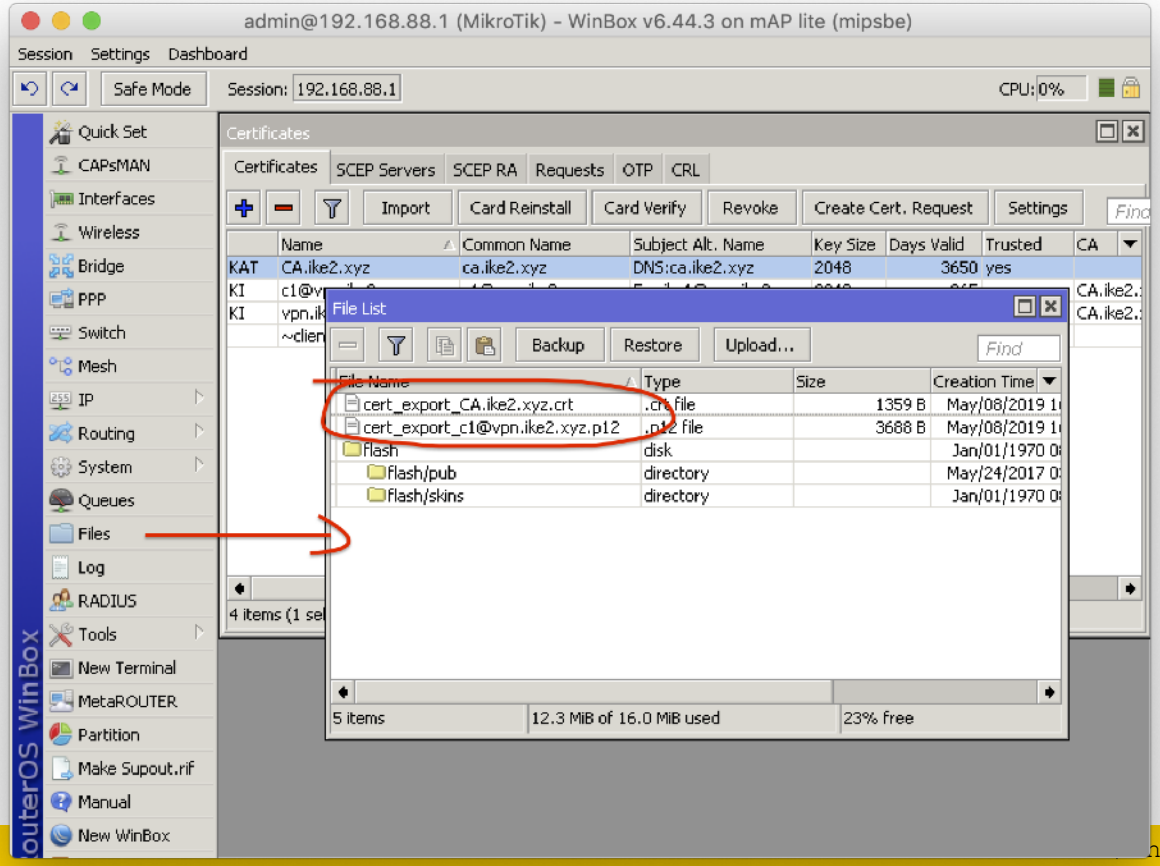


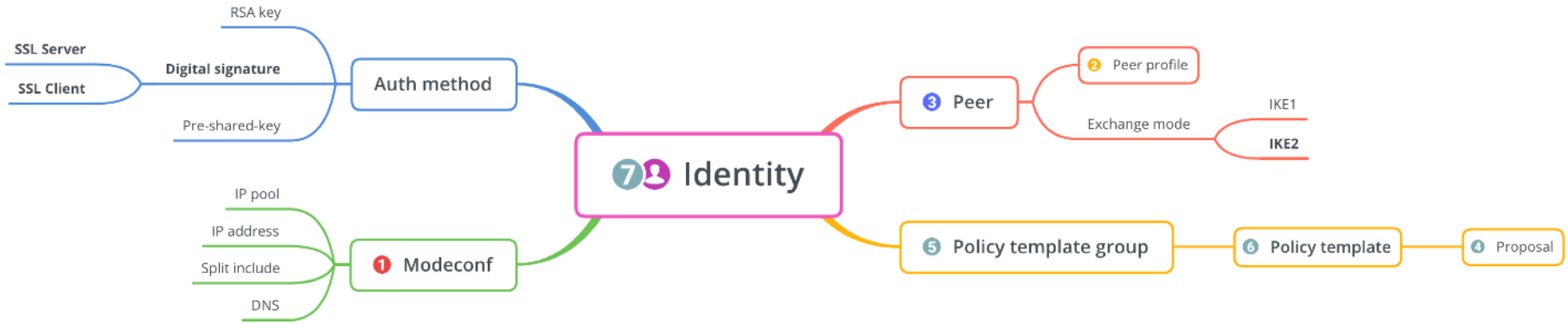
Export CA SSL certificate .crt file




```
/certificate
export-certificate CA.ike2.xyz
type=pem
```

Download exported SSL certificates





Setting up IPSec

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

Nikita Tarikin / nikita@tarikin.com

What's new in 6.44

*) ipsec - added account log message when user is successfully authenticated;
*) ipsec - added basic pre-shared-key strength checks;
*) ipsec - added new "remote-id" peer matcher;
*) ipsec - allow to specify single address instead of IP pool under "mode-config";
*) ipsec - fixed active connection killing when changing peer configuration;
*) ipsec - fixed all policies not getting installed after startup (introduced in v6.43.8);
*) ipsec - fixed stability issues after changing peer configuration (introduced in v6.43);
*) ipsec - hide empty prefixes on "peer" menu;
*) ipsec - improved invalid policy handling when a valid policy is uninstalled;
*) ipsec - made dynamic "src-nat" rule more specific;
*) ipsec - made peers autosort themselves based on reachability status;
*) ipsec - moved "profile" menu outside "peer" menu;
*) ipsec - properly detect AES-NI extension as hardware AEAD;
*) ipsec - removed limitation that allowed only single "auth-method" with the same "exchange-mode" as responder;
*) ipsec - require write policy for key generation;
*) ike2 - added option to specify certificate chain;
*) ike2 - added peer identity validation for RSA auth (disabled after upgrade);
*) ike2 - allow to match responder peer by "my-id=fqdn" field;
*) ike2 - fixed local address lookup when initiating new connection;
*) ike2 - improved subsequent phase 2 initialization when no childs exist;
*) ike2 - properly handle certificates with empty "Subject";
*) ike2 - retry RSA signature validation with deduced digest from certificate;
*) ike2 - send split networks over DHCP (option 249) to Windows initiators if DHCP Inform is received;
*) ike2 - show weak pre-shared-key warning;

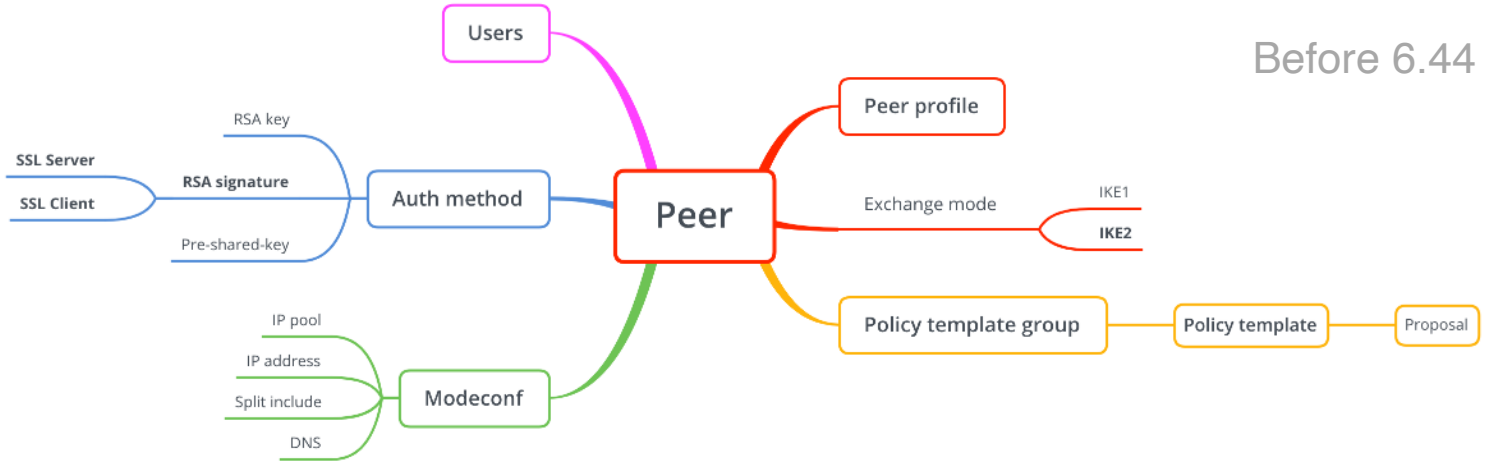
Key **ipsec** changes in RouterOS 6.44

*) ipsec - added new "remote-id" peer matcher;
*) ipsec - allow to specify single address instead of IP pool under "mode-config";
*) ipsec - moved "profile" menu outside "peer" menu;
*) ipsec - removed limitation that allowed only single "auth-method" with the same "exchange-mode" as responder;

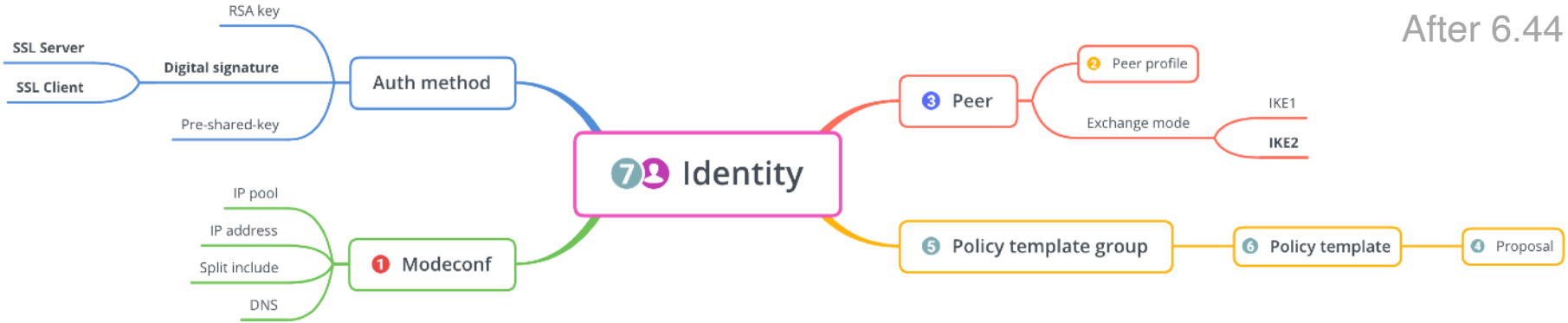
*) ike2 - added option to specify certificate chain;
*) ike2 - added peer identity validation for RSA auth (disabled after upgrade);
*) ike2 - allow to match responder peer by "my-id=fqdn" field;
*) ike2 - send split networks over DHCP (option 249) to Windows initiators if DHCP Inform is received;

IPSec structure

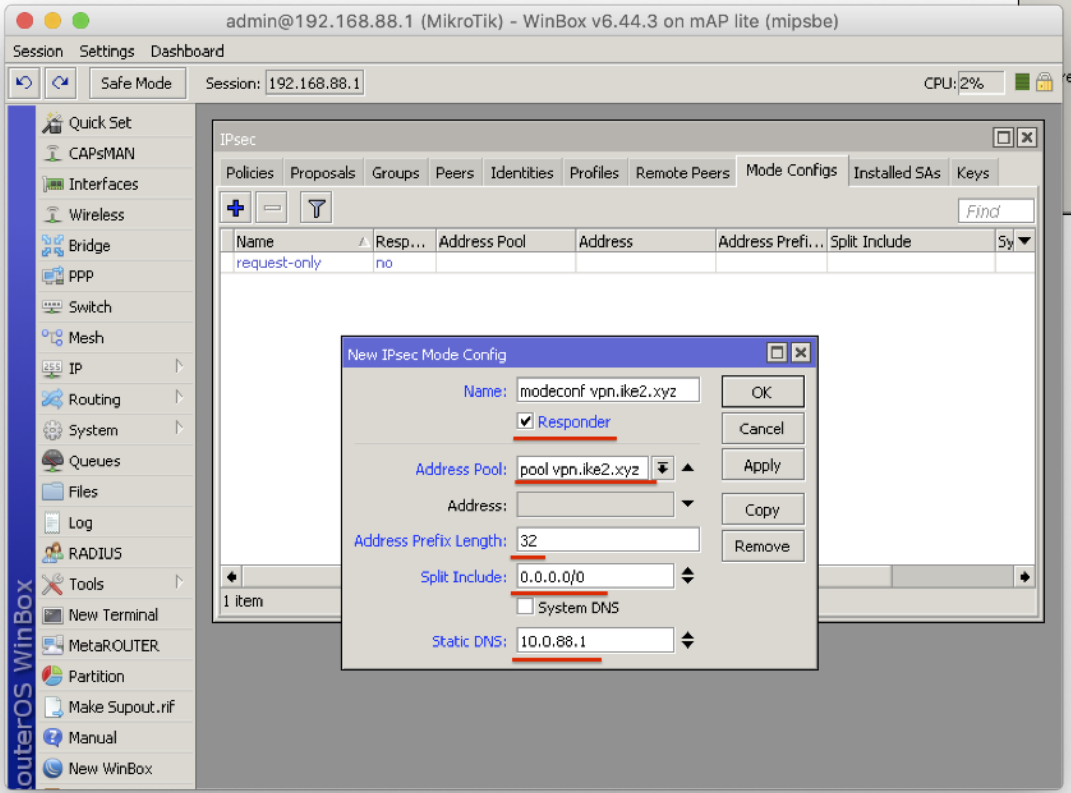
Before 6.44

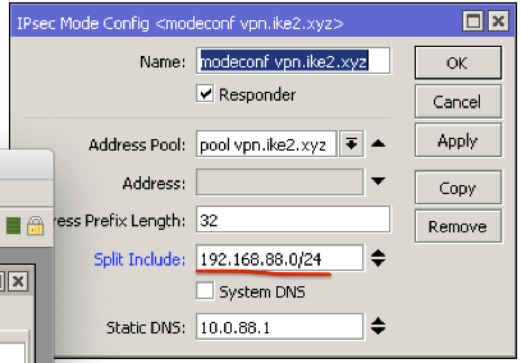


After 6.44



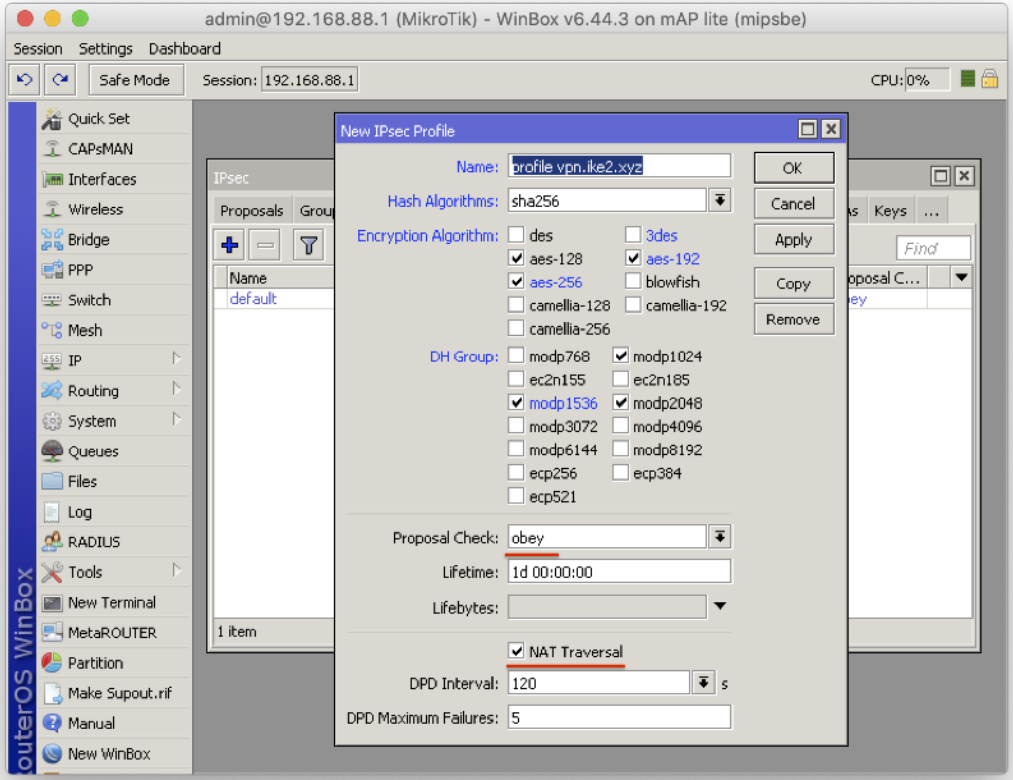
1. Setting up new IPSec mode config





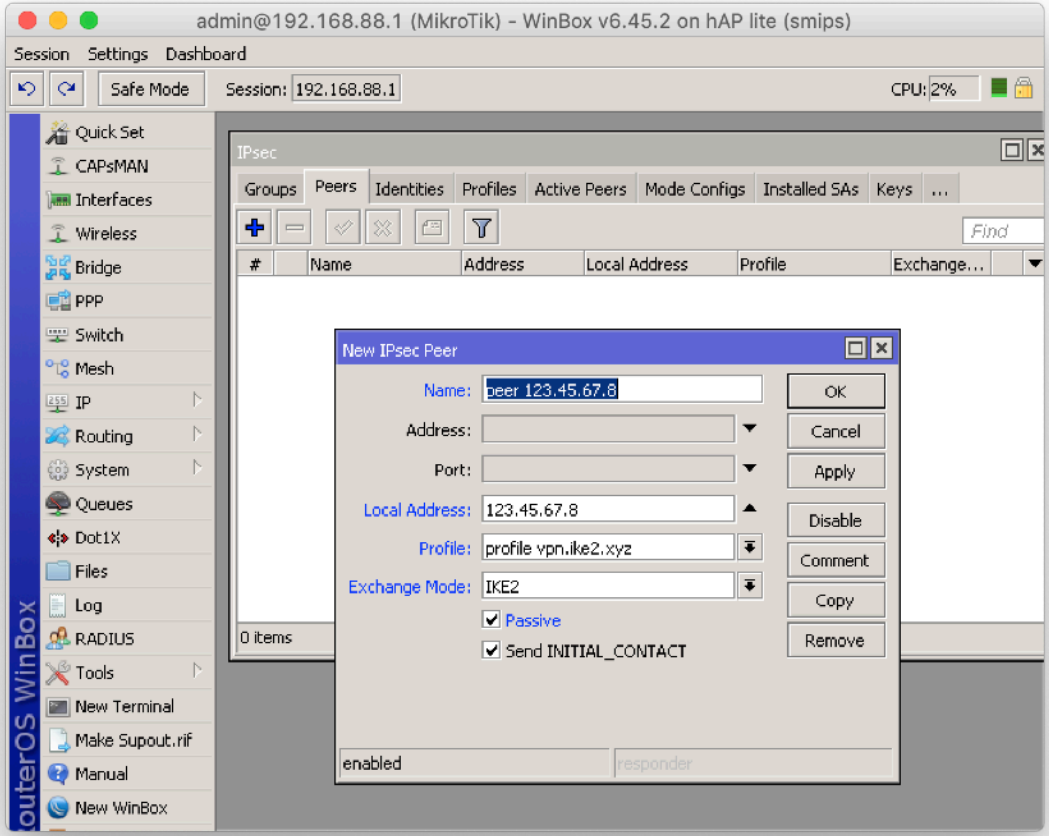

```
/ip ipsec mode-config
add address-pool="pool
vpn.ike2.xyz" address-prefix-
length=32 name="modeconf
vpn.ike2.xyz" split-
include=0.0.0.0/0 static-
dns=10.0.88.1 system-dns=no
```

2. Setting up new IPSec peer profile *(phase 1)*




```
/ip ipsec profile add dh-
group=modp2048,modp1536,modp10
24 enc-
algorithm=aes-256,aes-192,aes-
128 hash-algorithm=sha256
name="profile vpn.ike2.xyz"
nat-traversal=yes proposal-
check=obey
```

3. Setting up new IPSec peer on public IP address (IKE2 mode)

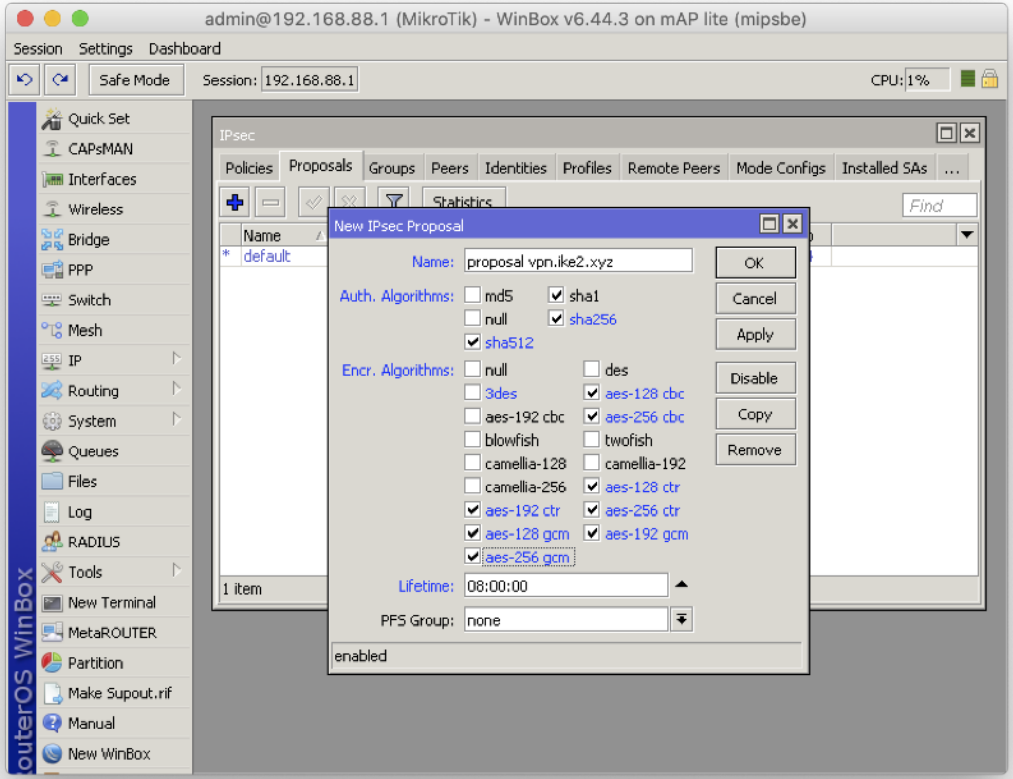


Accepting clients from all IP addresses **0.0.0.0/0**

Accepting clients on public IP address **123.45.67.8**

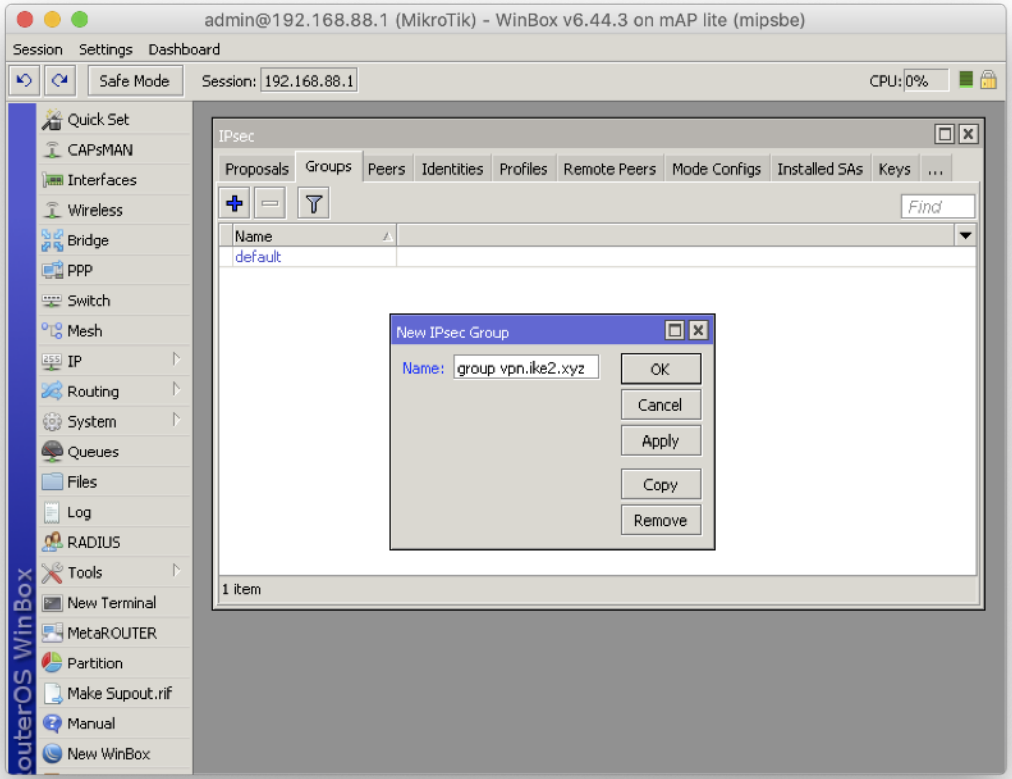
```
/ip ipsec peer add exchange-
mode=ike2 address=0.0.0.0/0
local-address=123.45.67.8
name="peer 123.45.67.8"
passive=yes send-initial-
contact=yes profile="profile
vpn.ike2.xyz"
```

4. Setting up new IPSec proposal *(phase 2)*



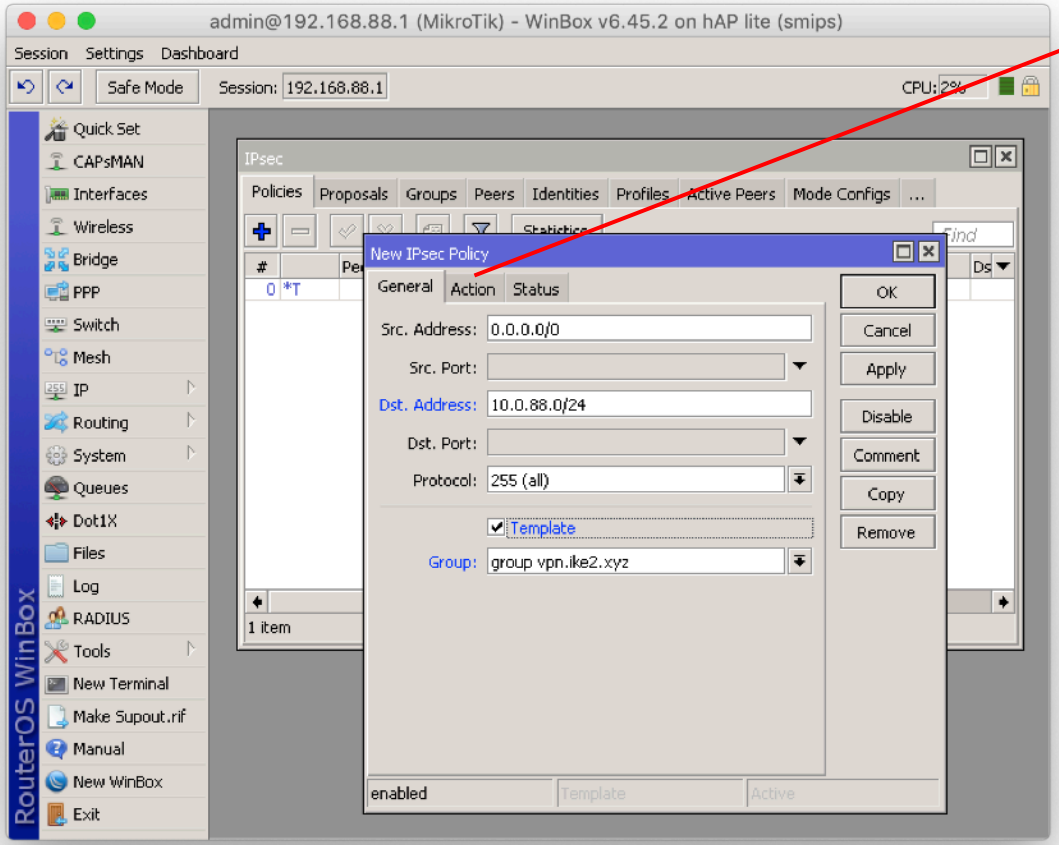

```
/ip ipsec proposal add auth-
algorithms=sha512,sha256,sha1
enc-algorithms=aes-256-
cbc,aes-256-ctr,aes-256-
gcm,aes-192-ctr,aes-192-
gcm,aes-128-cbc,aes-128-
ctr,aes-128-gcm lifetime=8h
name="proposal vpn.ike2.xyz"
pfs-group=none
```

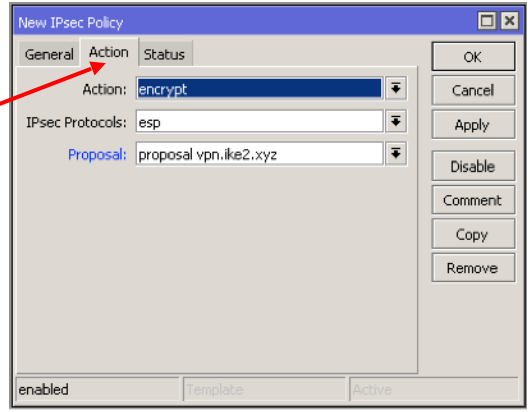
5. Setting up new IPSec policy group




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

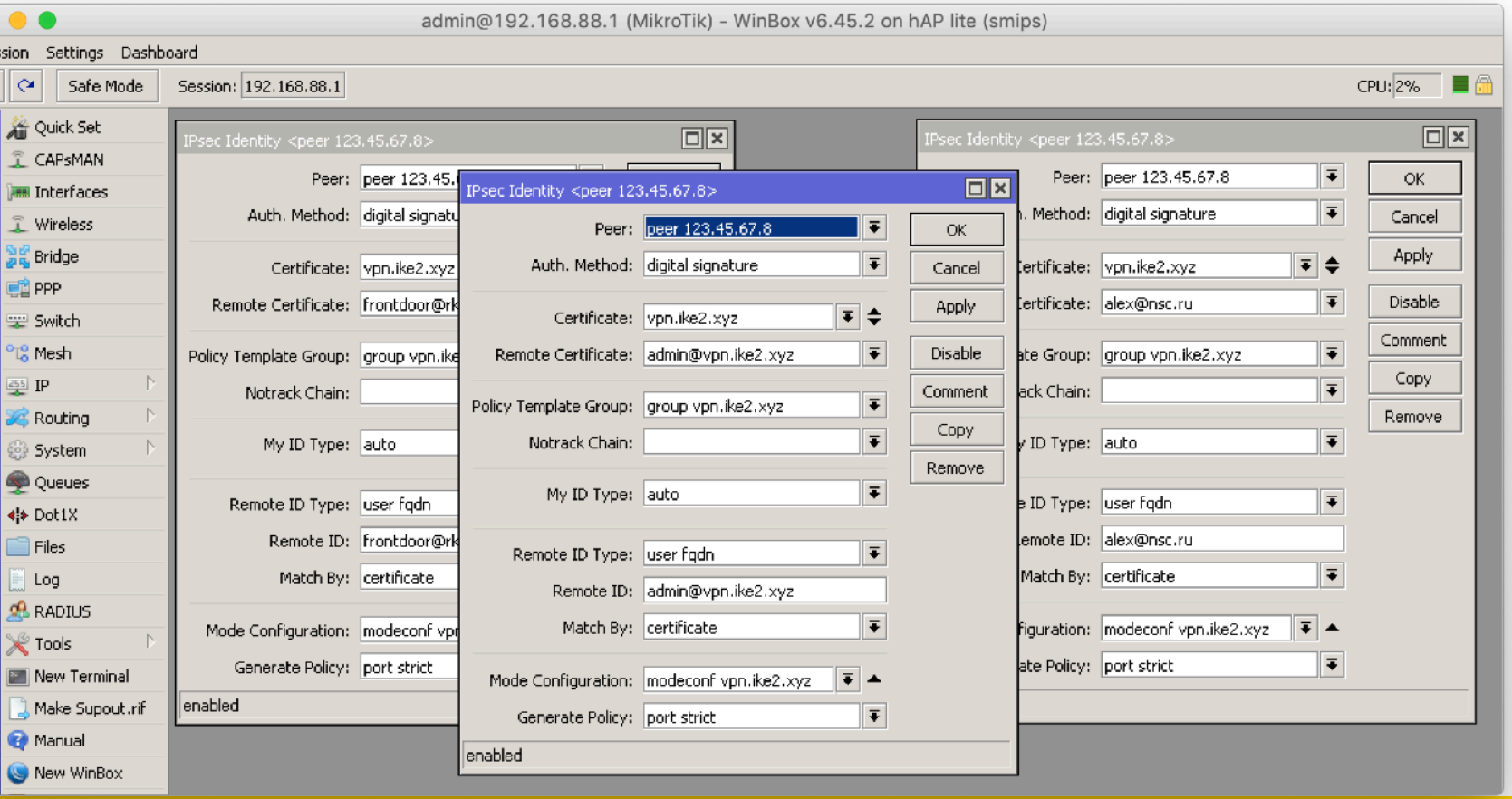
6. Setting up new IPSec policy template





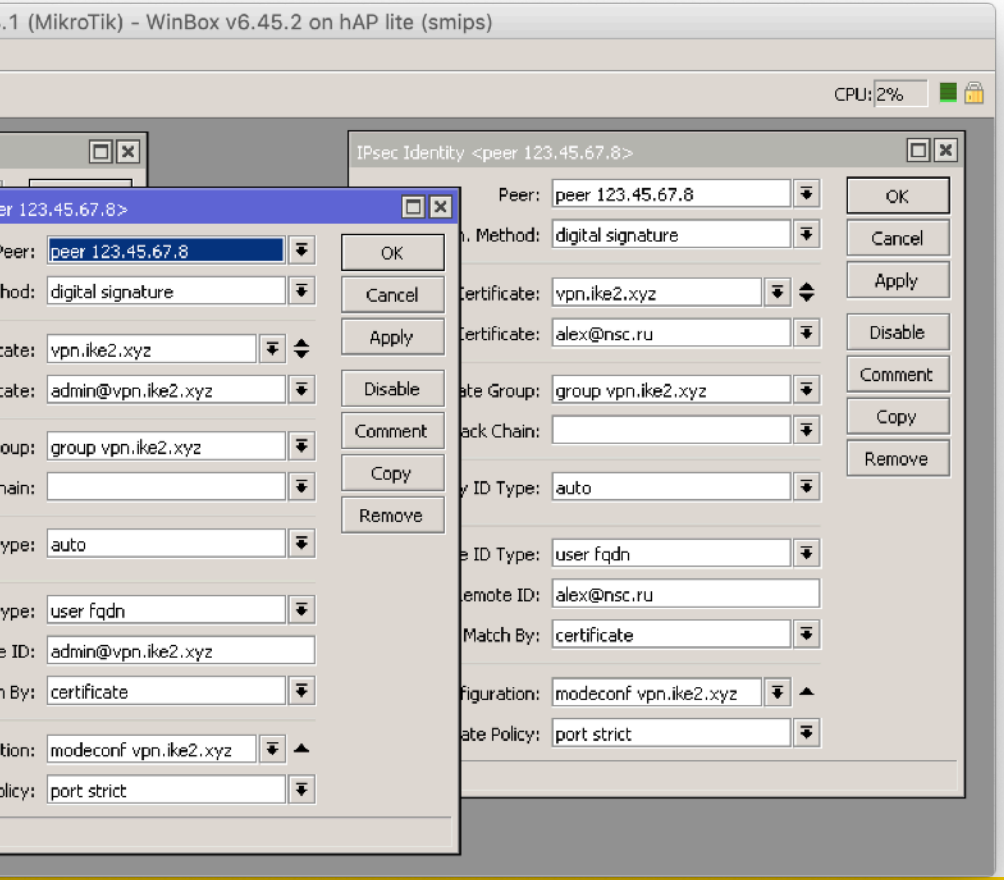

```
/ip ipsec policy add template=yes
dst-address=10.0.88.0/24
protocol=all src-address=0.0.0.0/0
group="group vpn.ike2.xyz"
proposal="proposal vpn.ike2.xyz"
ipsec-protocols=esp action=encrypt
```

7. Carefully assembling IPSec identities for each client




```
/ip ipsec identity add auth-method=digital-
  signature certificate=vpn.ike2.xyz remote-
  certificate=admin@vpn.ike2.xyz generate-
```

7. Carefully assembling IPSec identities for each client




```
/ip ipsec identity add auth-method=digital-
signature certificate=vpn.ike2.xyz remote-
certificate=admin@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:admin@vpn.ike2.xyz

/ip ipsec identity add auth-method=digital-
signature certificate=vpn.ike2.xyz remote-
certificate=alex@nsc.ru 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:alex@nsc.ru
```

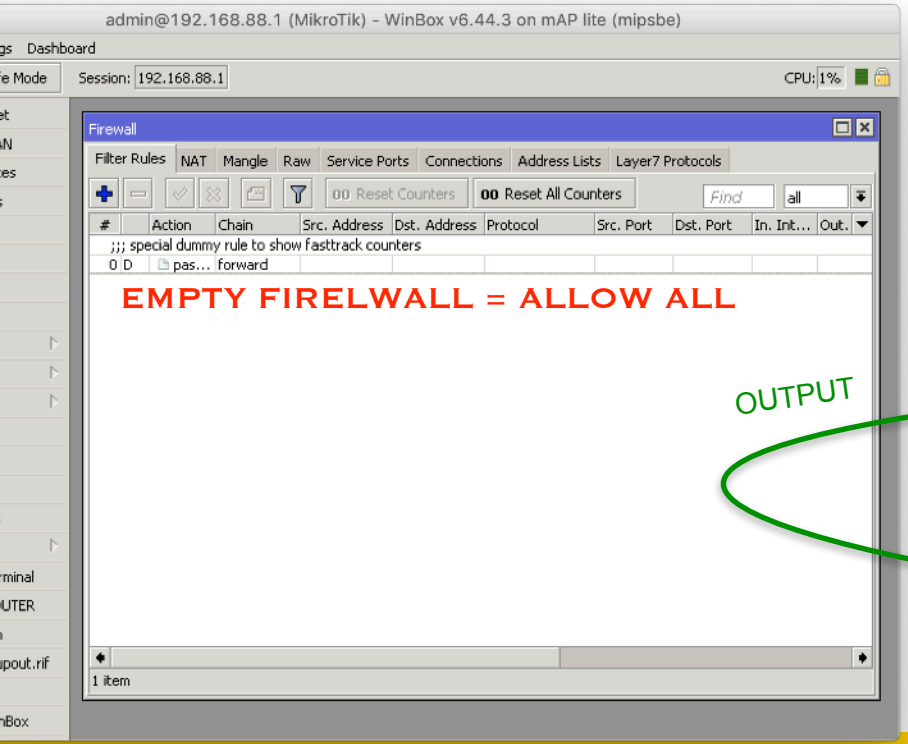
Setting up Firewall

Understanding the default firewall filter

Nikita Tarikin / nikita@tarikin.com

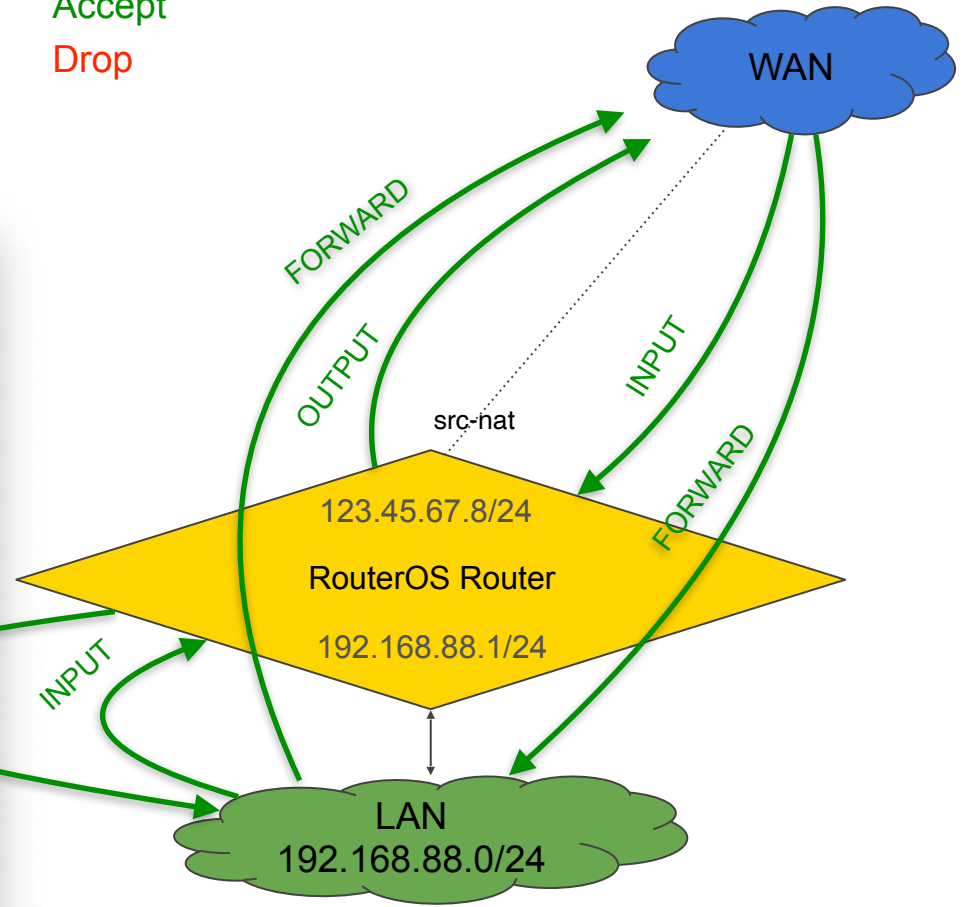
Important

Empty FIREWALL filter

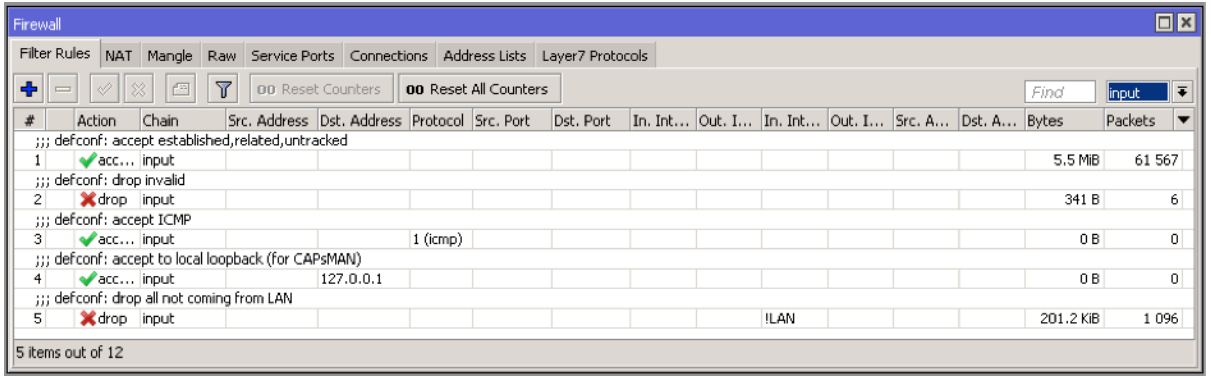


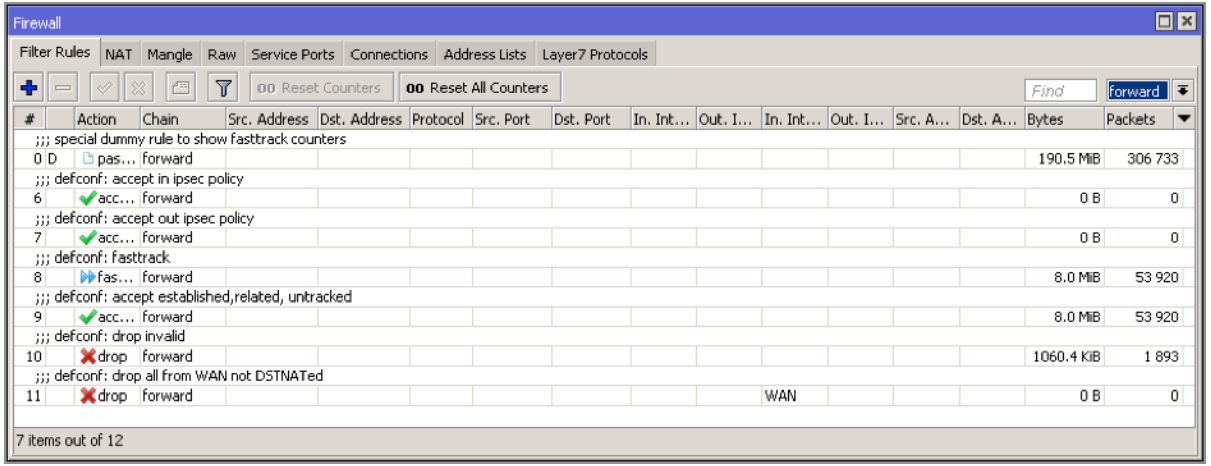
Accept

Drop



RouterOS 6.45+ default configuration firewall overview



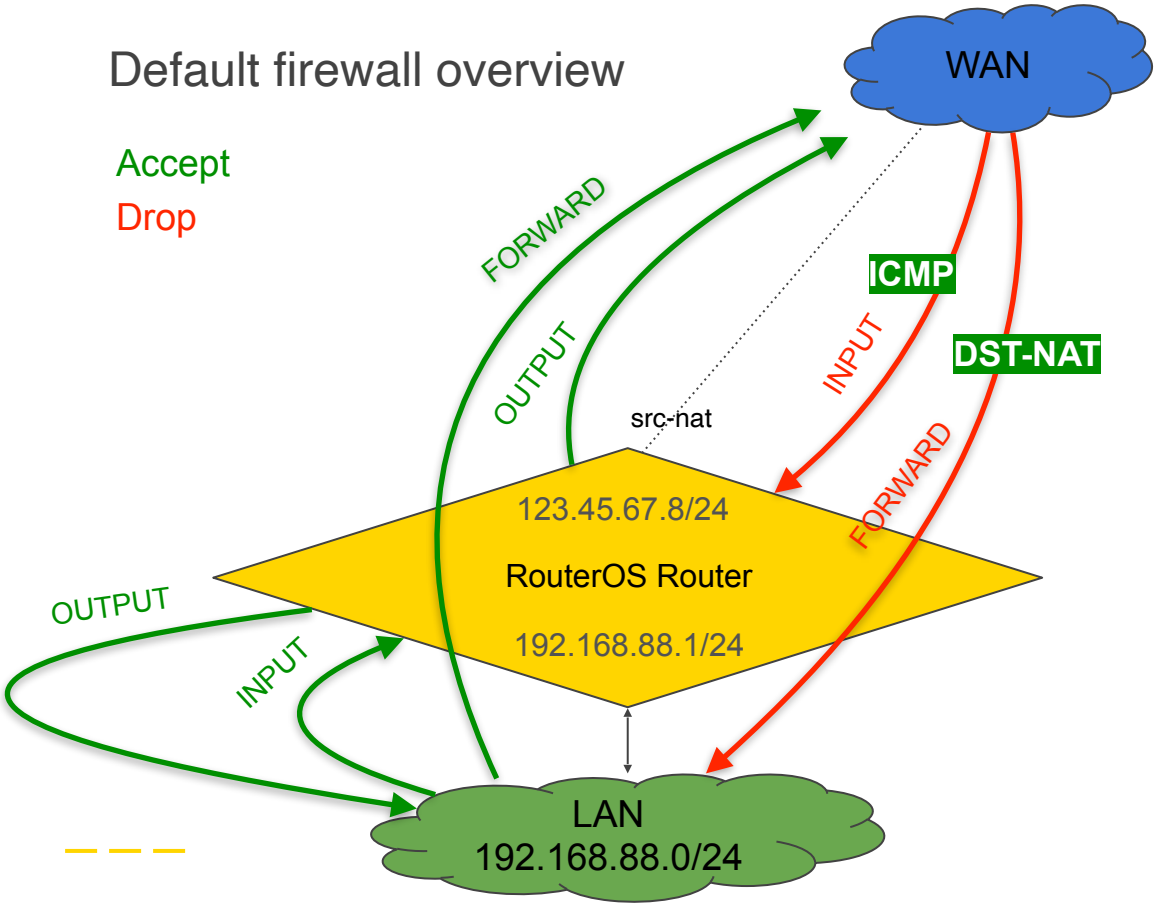


```
#Input Chain Rules
/ip firewall filter
add action=accept chain=input comment="defconf: accept established,related,untracked" connection-
state=established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=accept chain=input comment="defconf: accept to local loopback (for CAPsMAN)" dst-address=127.0.0.1
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-list=!LAN

#Forward Chain Rules
/ip firewall filter
add action=accept chain=forward comment="defconf: accept in ipsec policy" ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec policy" ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" connection-state=established,related
add action=accept chain=forward comment="defconf: accept established,related, untracked" connection-
state=established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
add action=drop chain=forward comment="defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat
connection-state=new in-interface-list=WAN
```

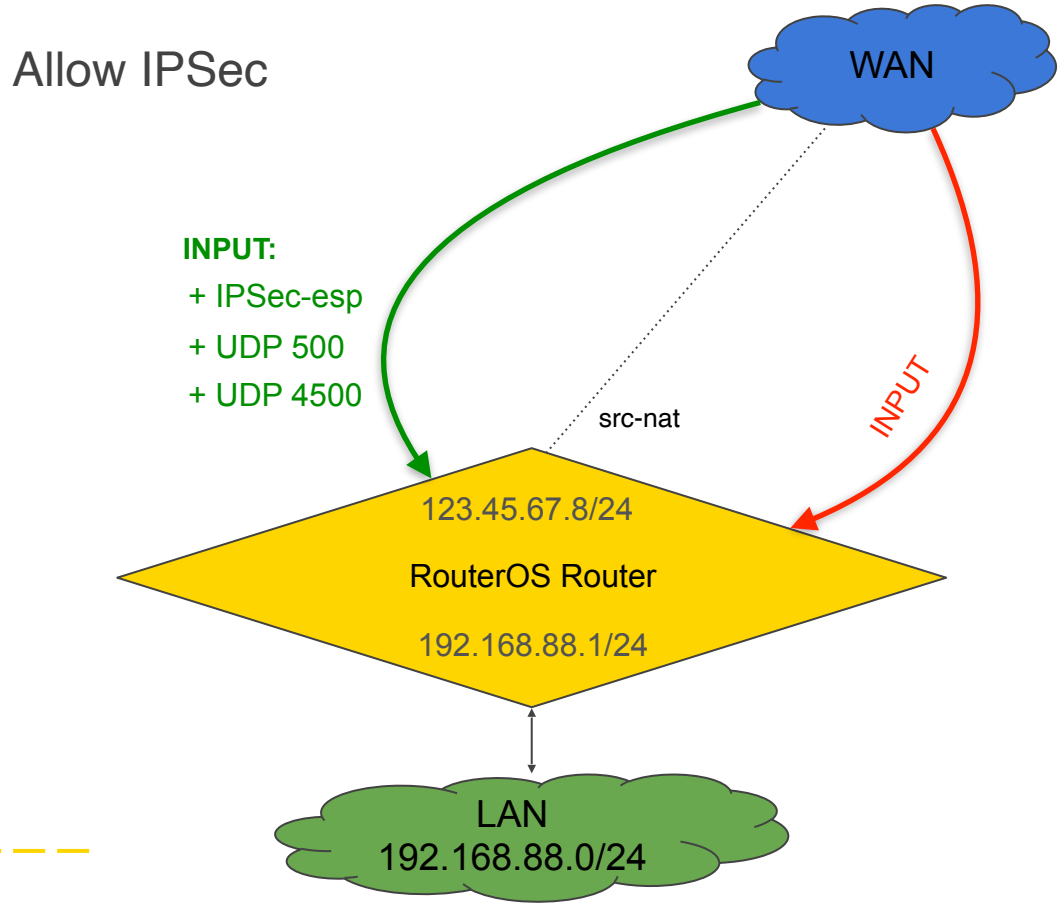
Setting up Firewall

1. **Default firewall overview**
2. Allow IPSec



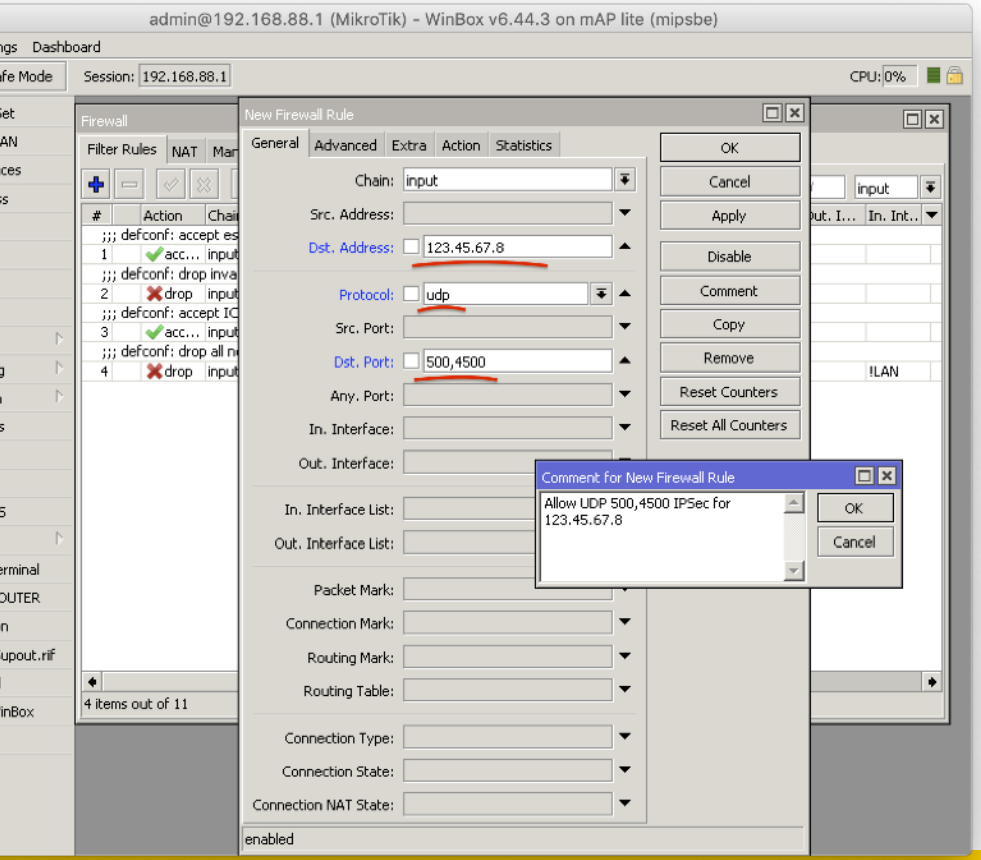
Setting up Firewall

1. Default firewall overview
2. **Allow IPSec**



Firewall filter rules for IPSec packets (defconf)

INPUT chain

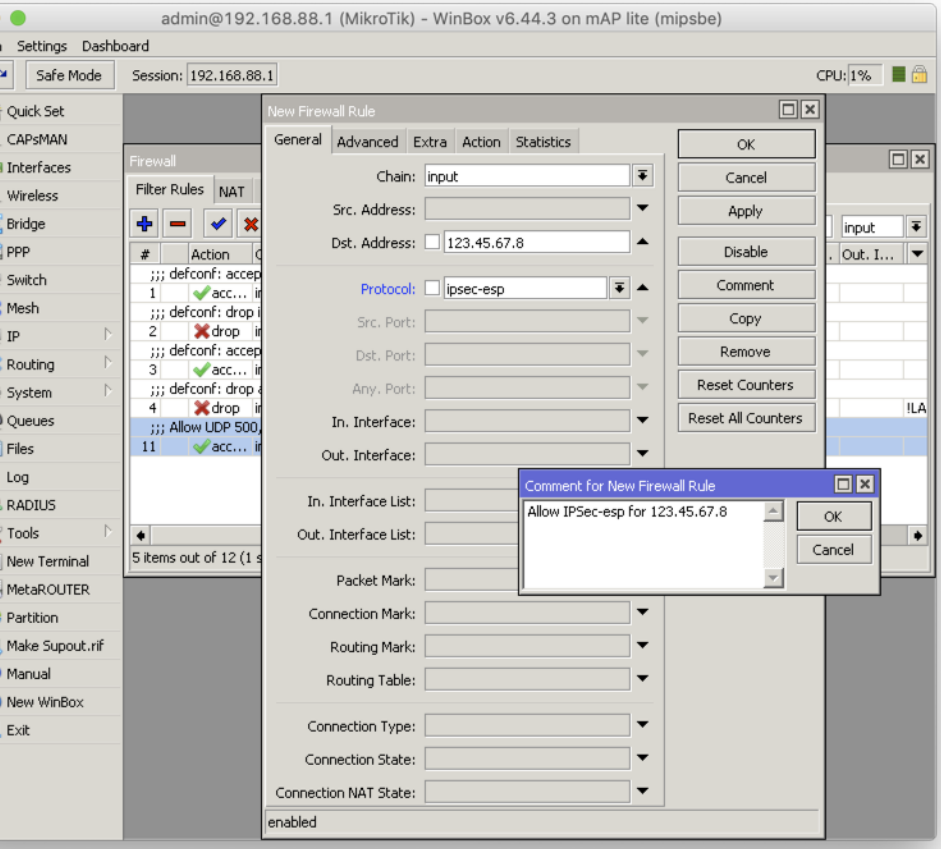


+ UDP 500
+ UDP 4500

```
/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 packets (defconf)

INPUT chain



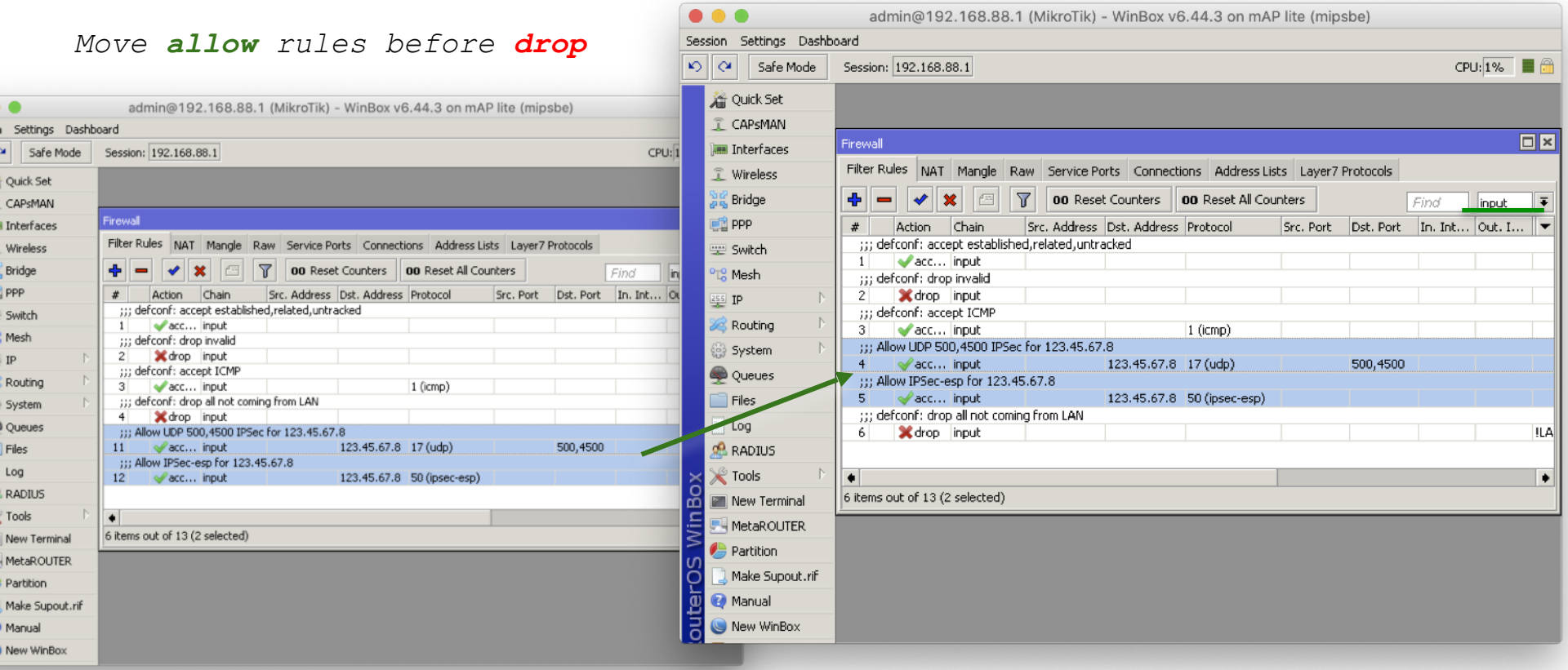
+ IPSec-esp (protocol 50)

```
/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"
```

REorder firewall filter rules for IPSec packets (defconf)

INPUT chain

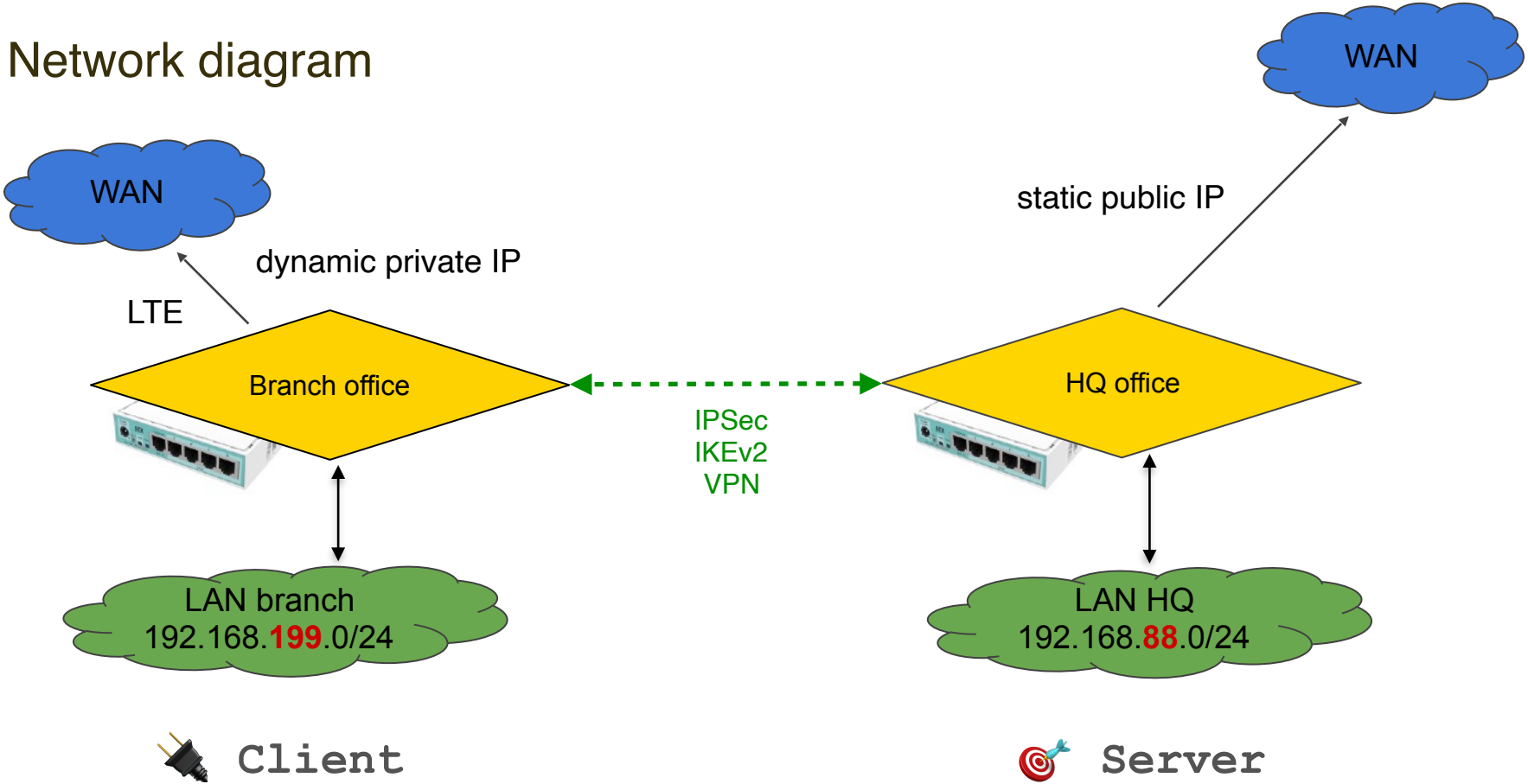
*Move **allow** rules before **drop***



🎯 RouterOS IPSec IKEv2 server ready

Nikita Tarikin / nikita@tarikin.com

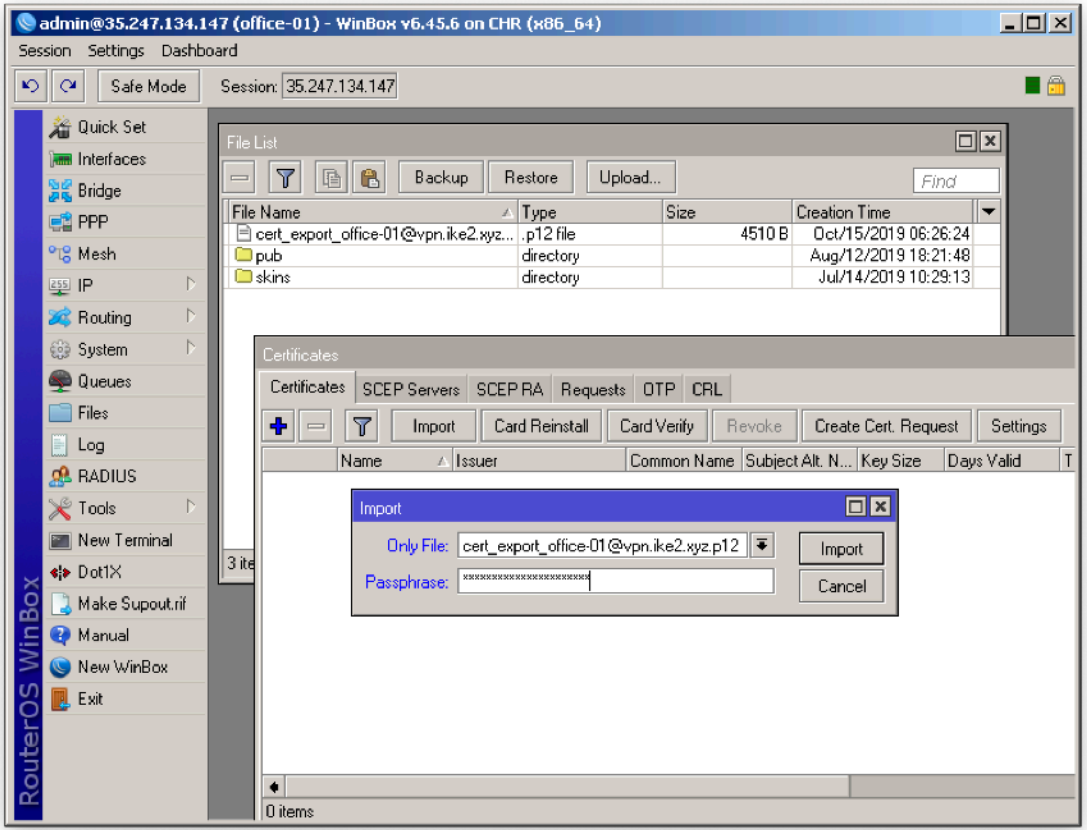
Network diagram



Setting up client RouterOS 🔌

Upload and install client SSL certificate

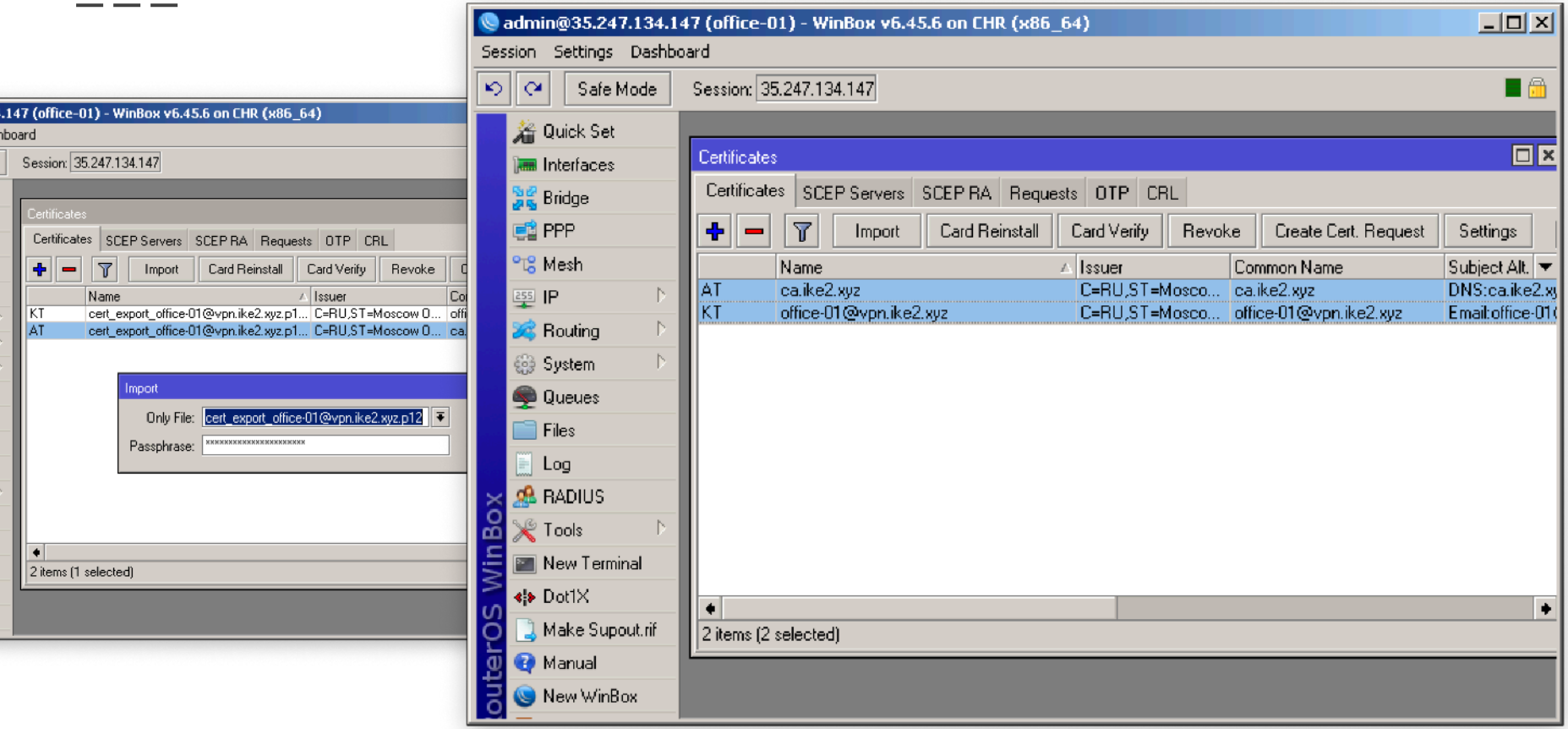
Client




```
/certificate import file-
name=cert_export_office-01@v
pn.ike2.xyz.p12
```

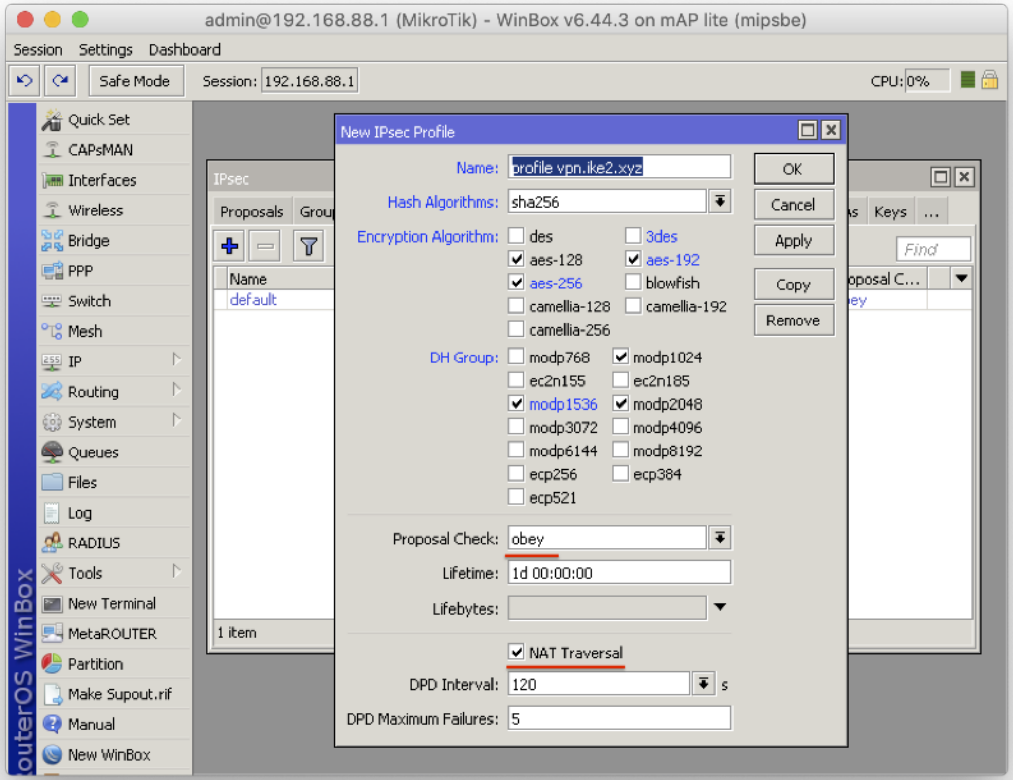
Rename installed SSL certificates: CA and client

Client



Setting up new IPSec peer profile *(phase 1)*

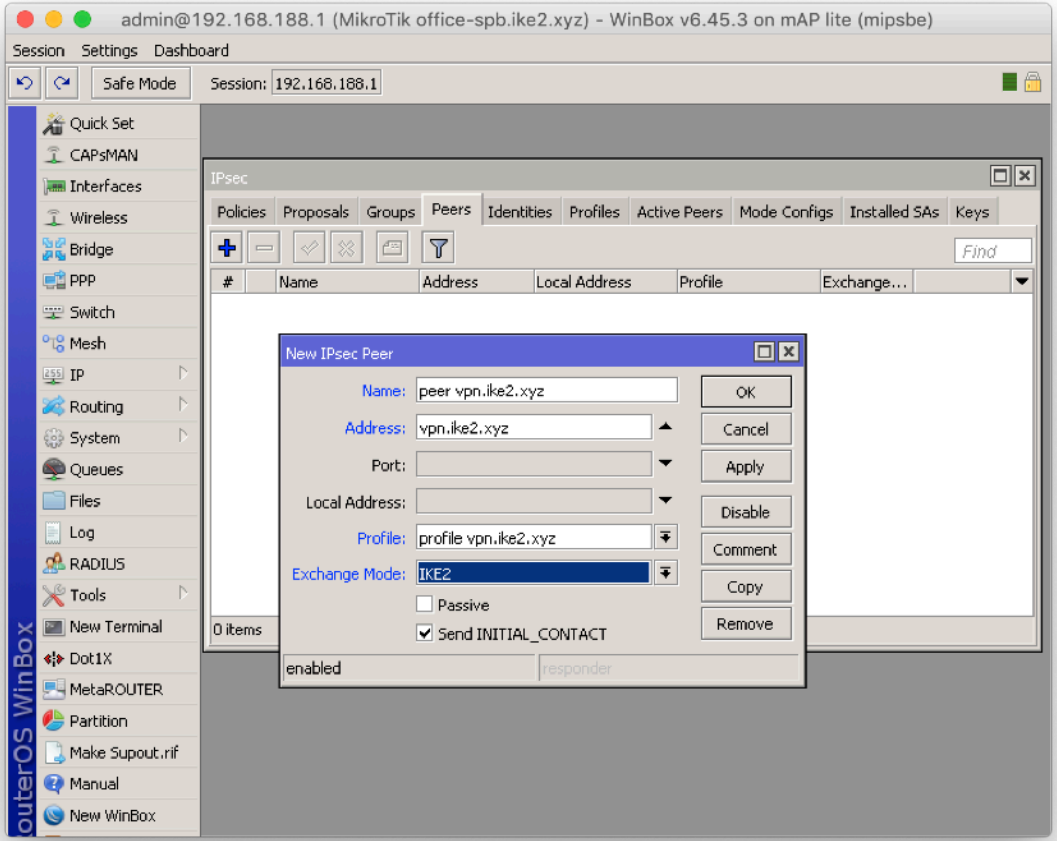
Client




```
/ip ipsec profile add dh-
group=modp2048,modp1536,modp10
24 enc-
algorithm=aes-256,aes-192,aes-
128 hash-algorithm=sha256
name="profile vpn.ike2.xyz"
nat-traversal=yes proposal-
check=obey
```

Adding new client IPSec peer (initiator)

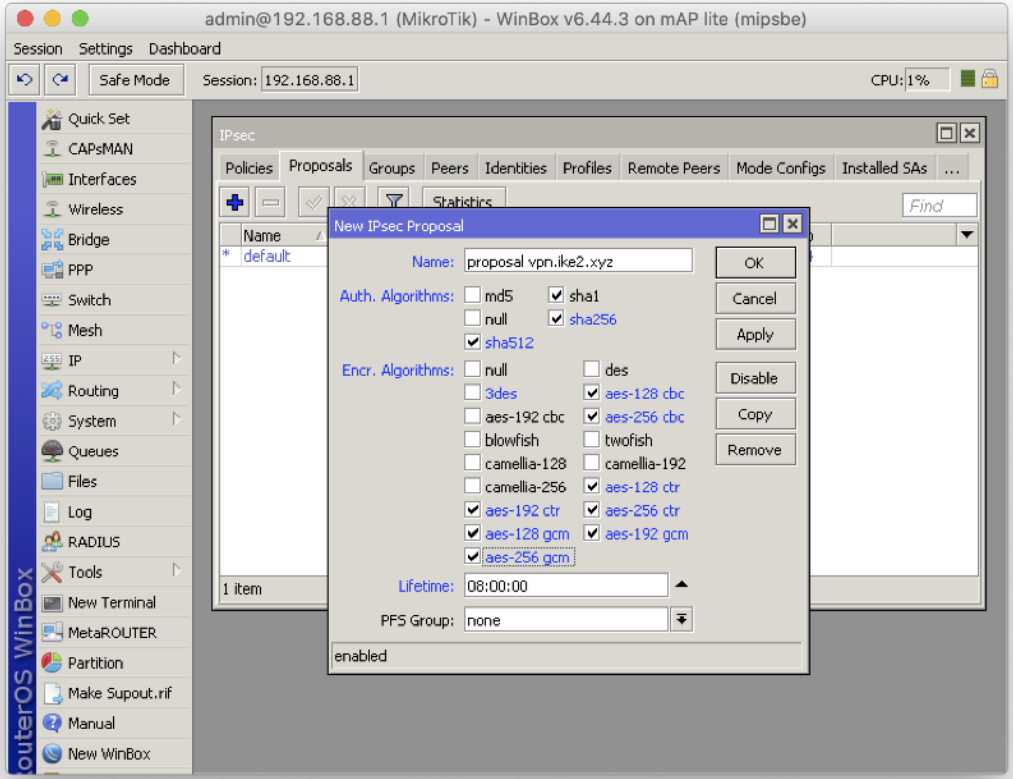
Client




```
/ip ipsec peer
add address=vpn.ike2.xyz exchange-
mode=ike2 name="peer vpn.ike2.xyz"
profile="profile vpn.ike2.xyz"
```

Setting up new IPSec proposal *(phase 2)*

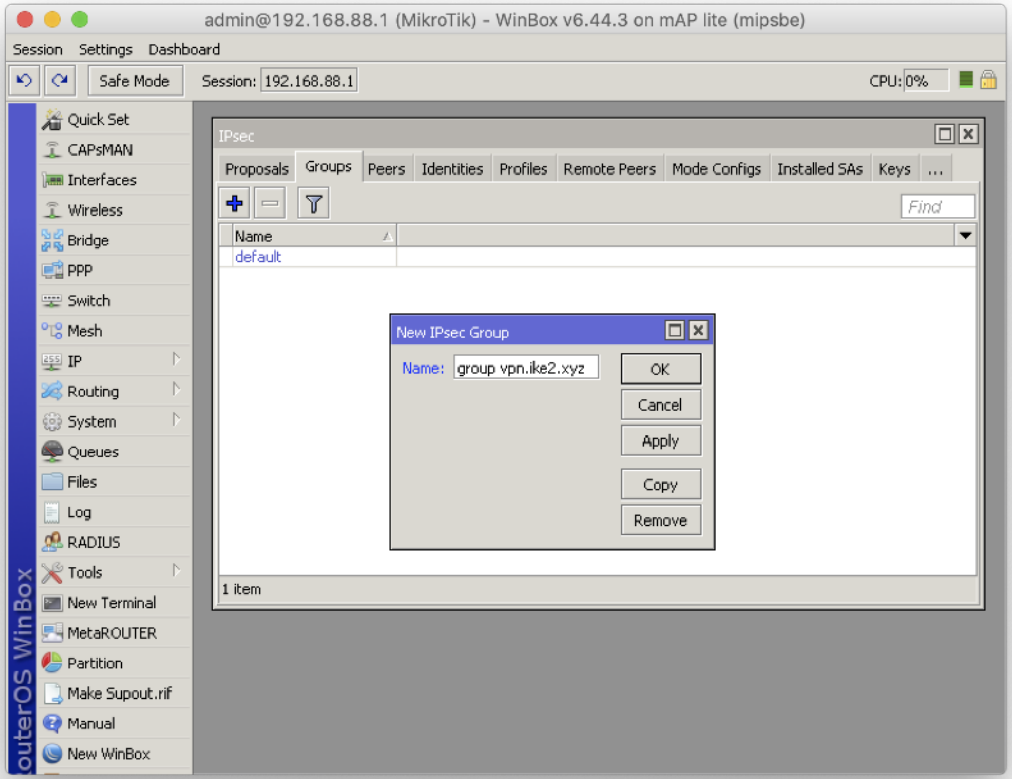
Client




```
/ip ipsec proposal add 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
```

Adding new IPSec policy group

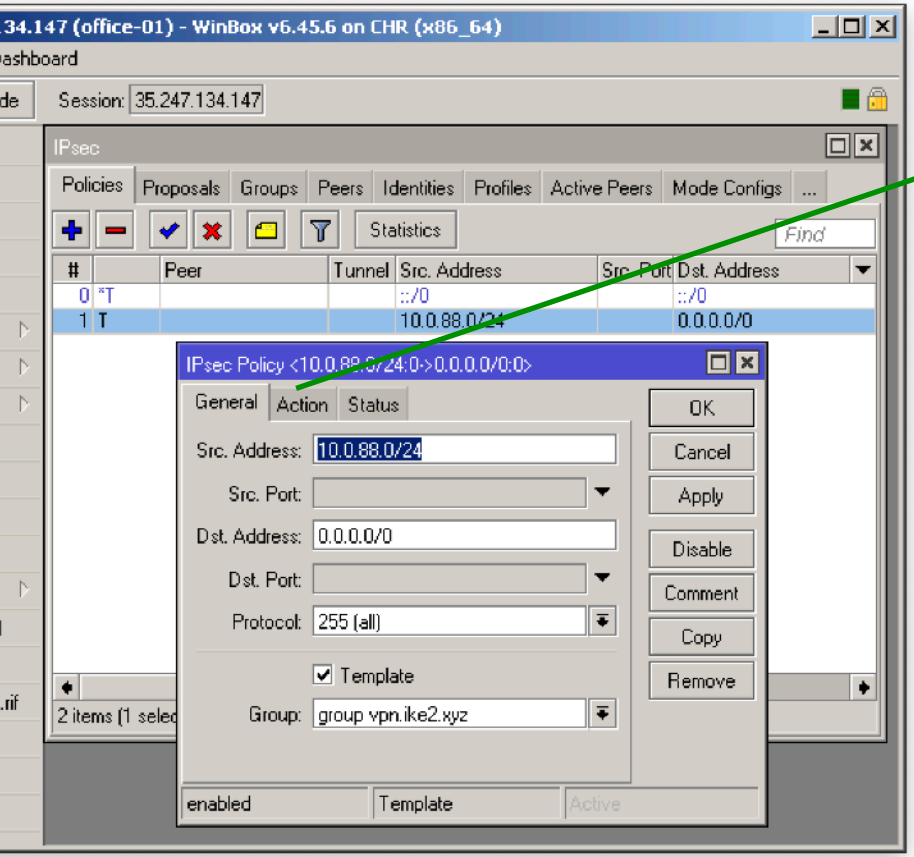
Client

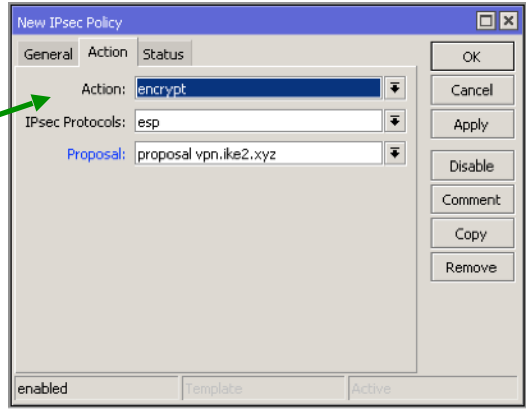



```
/ip ipsec policy group
add name="group vpn.ike2.xyz"
```

Adding new IPSec policy template

Client

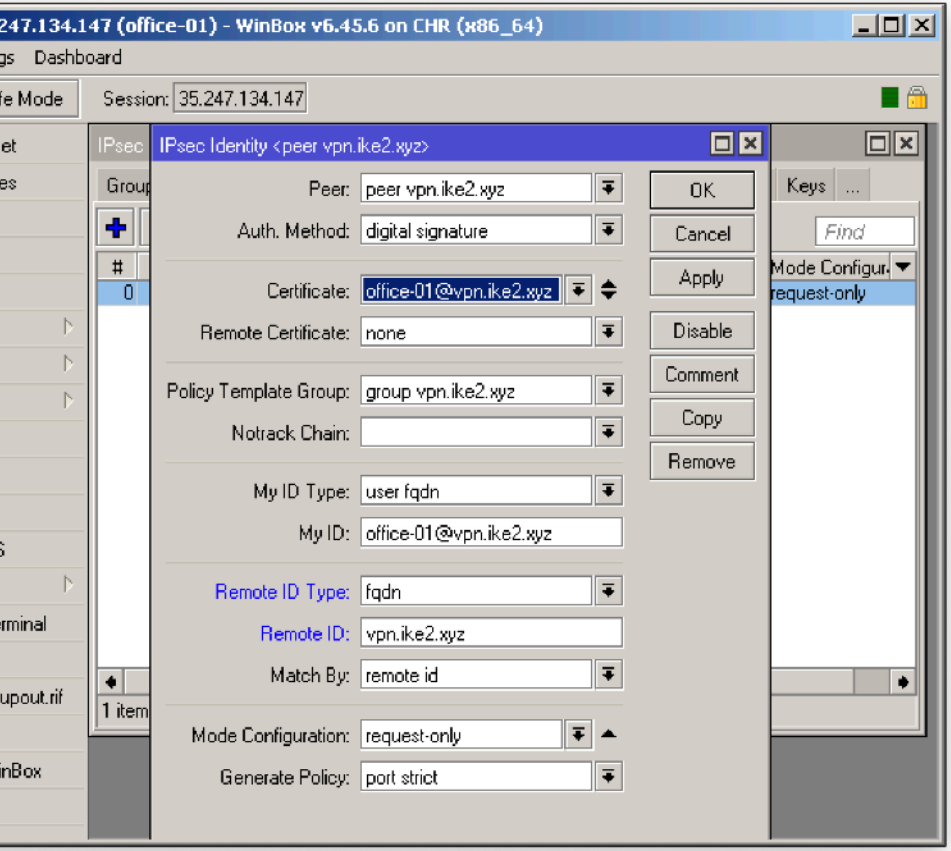





```
/ip ipsec policy
add comment="policy template vpn.ike2.xyz"
dst-address=0.0.0.0/0 group="group
vpn.ike2.xyz" proposal="proposal vpn.ike2.xyz"
src-address=10.0.88.0/24 template=yes
```

Carefully assembling client's IPSec identity

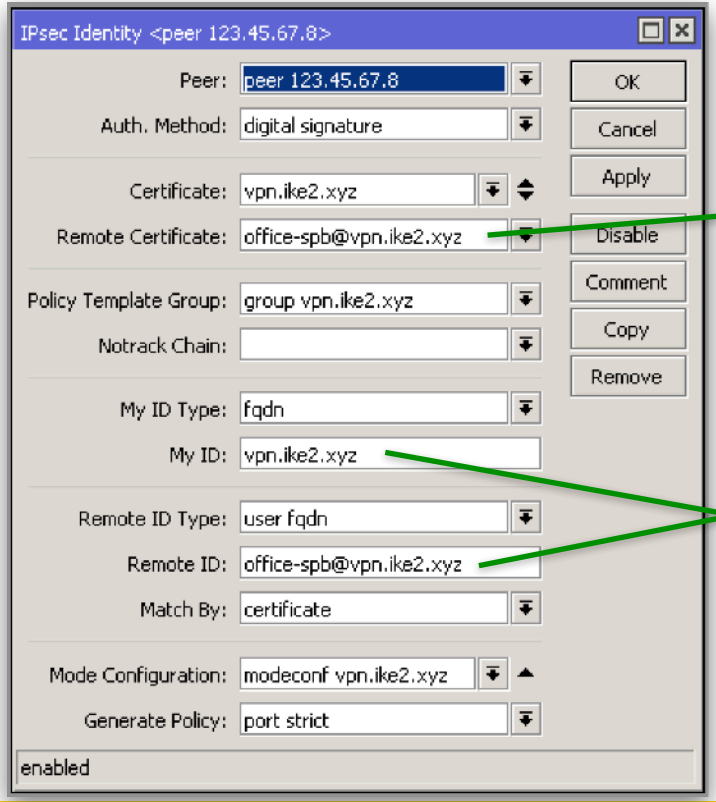
Client



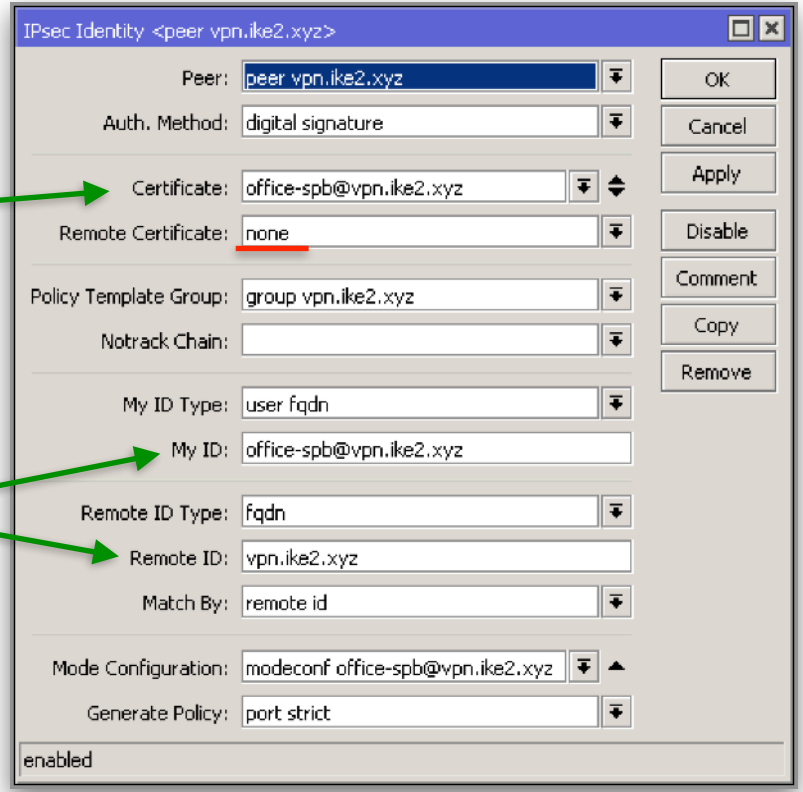

```
/ip ipsec identity
add auth-method=digital-signature
certificate=office-spb@vpn.ike2.xyz
generate-policy=port-strict mode-
config="modeconf office-01@vpn.ike2.xyz"
my-id=user-fqdn:office-01@vpn.ike2.xyz
peer="peer vpn.ike2.xyz" policy-template-
group="group vpn.ike2.xyz" remote-
id=fqdn:vpn.ike2.xyz
```

Cross-check IPSec identity (example)

🎯 Server



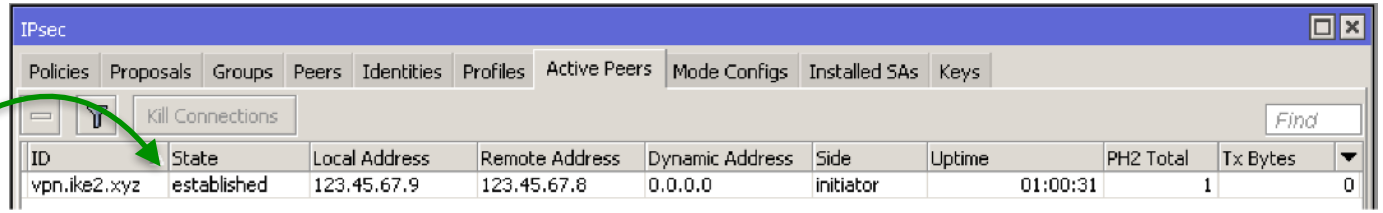
🔌 Client



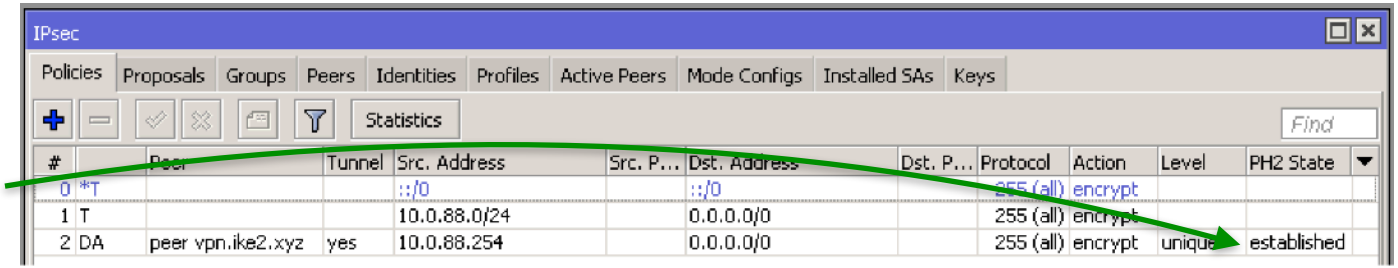
Testing the IKEv2 connectivity

Client

Active peers
state: established



Dynamic Active(**DA**) IPSec policy generated from Template (**T**)
PH2 state: established

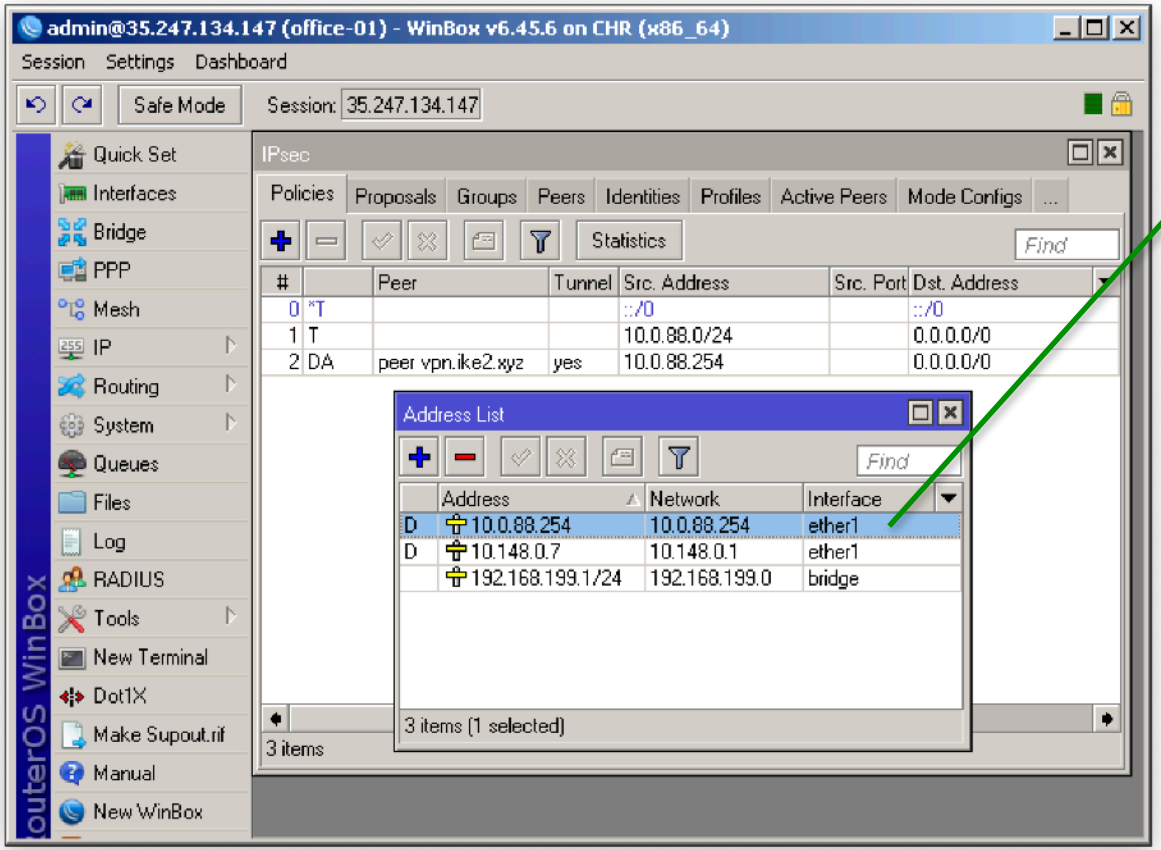


Peer: authorized
Address: acquired

Aug/08/2019 15:51:58	memory	ipsec, info	new ike2 SA (R): 123.45.67.8[4500]-123.45.67.9[4500] spi:39d4a4bf6c5f4e2b:099b4c2c836ffe5d
Aug/08/2019 15:51:58	memory	ipsec, info, account	peer authorized: 123.45.67.8[4500]-123.45.67.9[4500] spi:39d4a4bf6c5f4e2b:099b4c2c836ffe5d
Aug/08/2019 15:51:58	memory	ipsec, info	acquired 10.0.88.254 address for 123.45.67.9, office-spb@vpn.ike2.xyz

Testing the IKEv2 connectivity

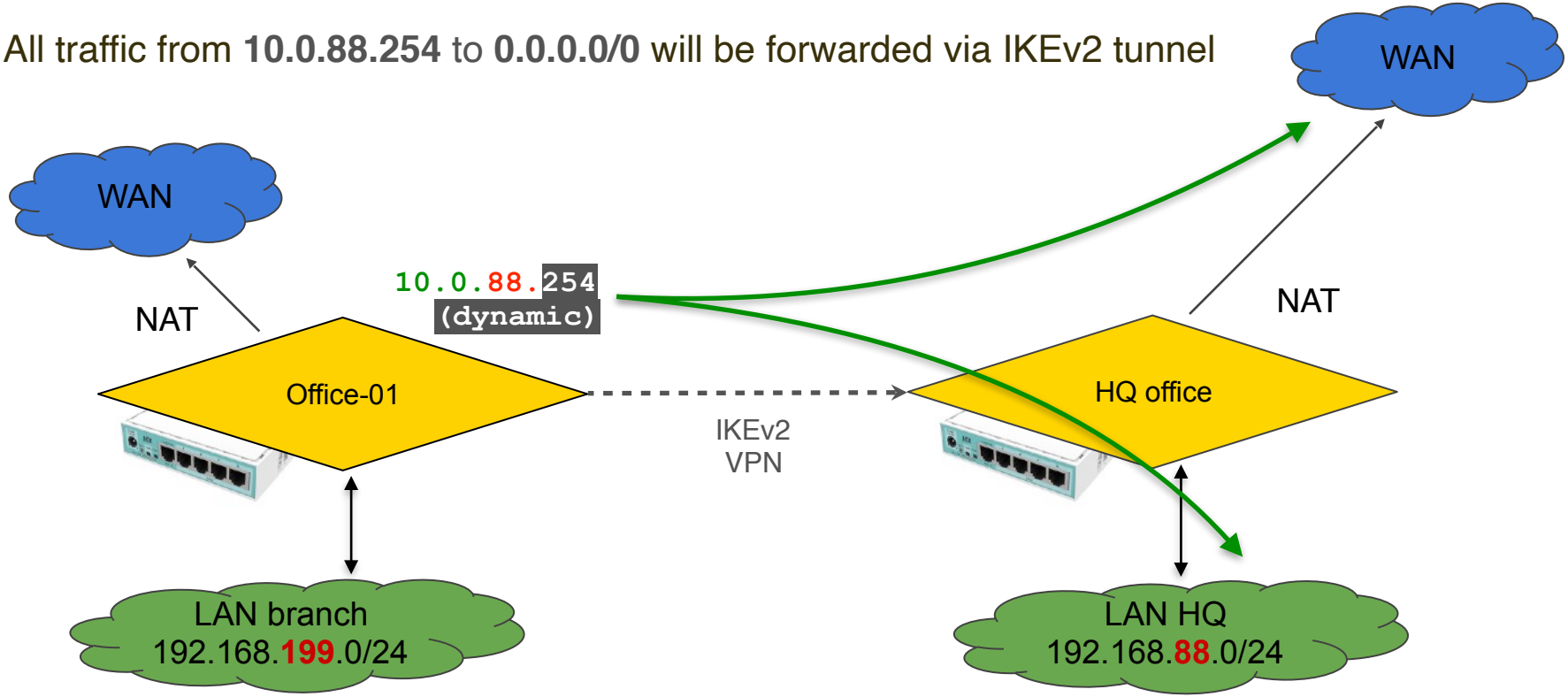
Client



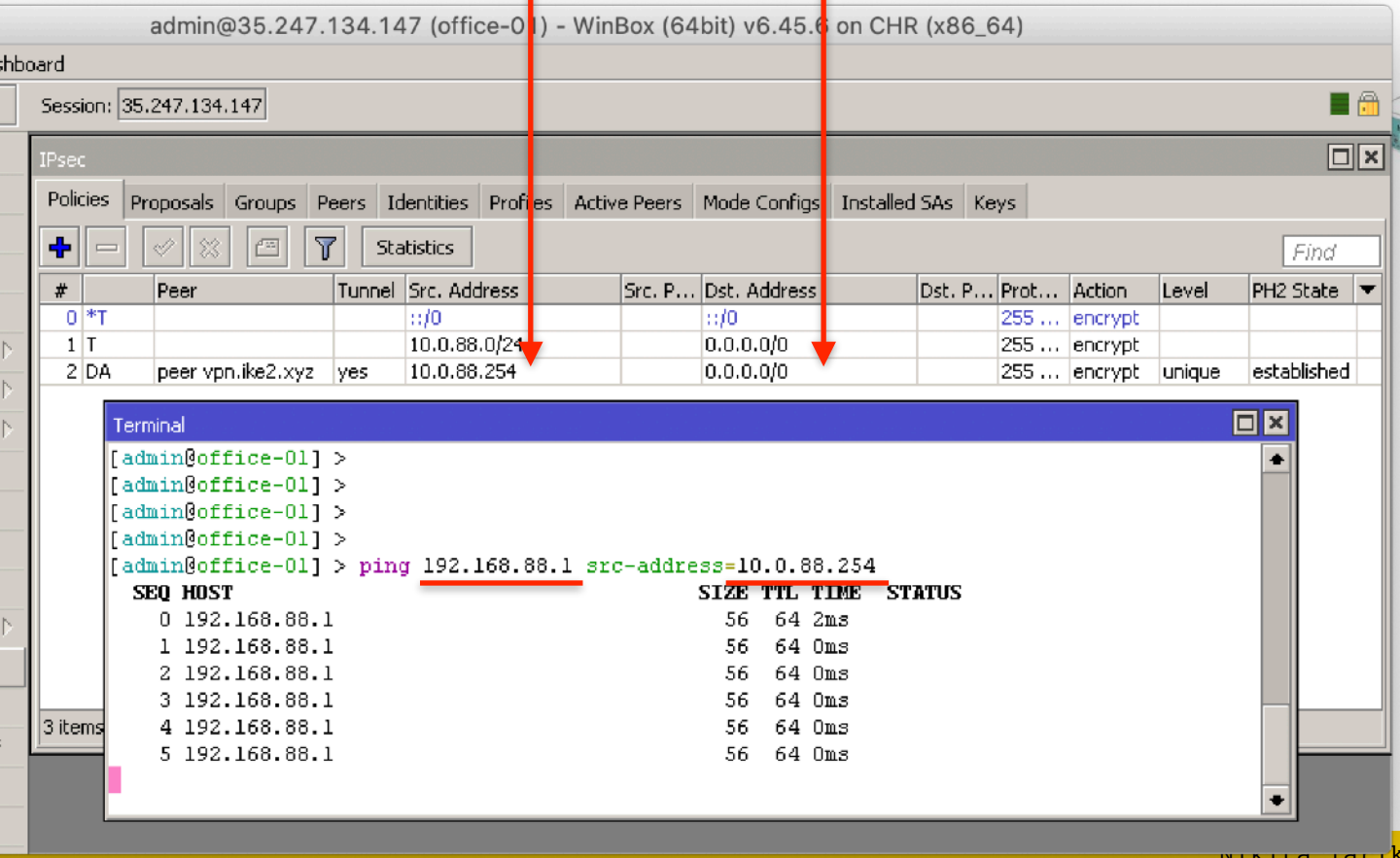
IP address **10.0.88.254**

Interface **ether1**

All traffic from **10.0.88.254** to **0.0.0.0/0** will be forwarded via IKEv2 tunnel



All traffic from 10.0.88.254 to 0.0.0.0/0 will be forwarded via IKEv2 tunnel



10.0.88.254
(dynamic)

LAN HQ
192.168.88.0/24

Pros:

Easy to configure and understand

OSPF works

Routable

No TCP MSS issues

Has interface

Option 1 (easy)

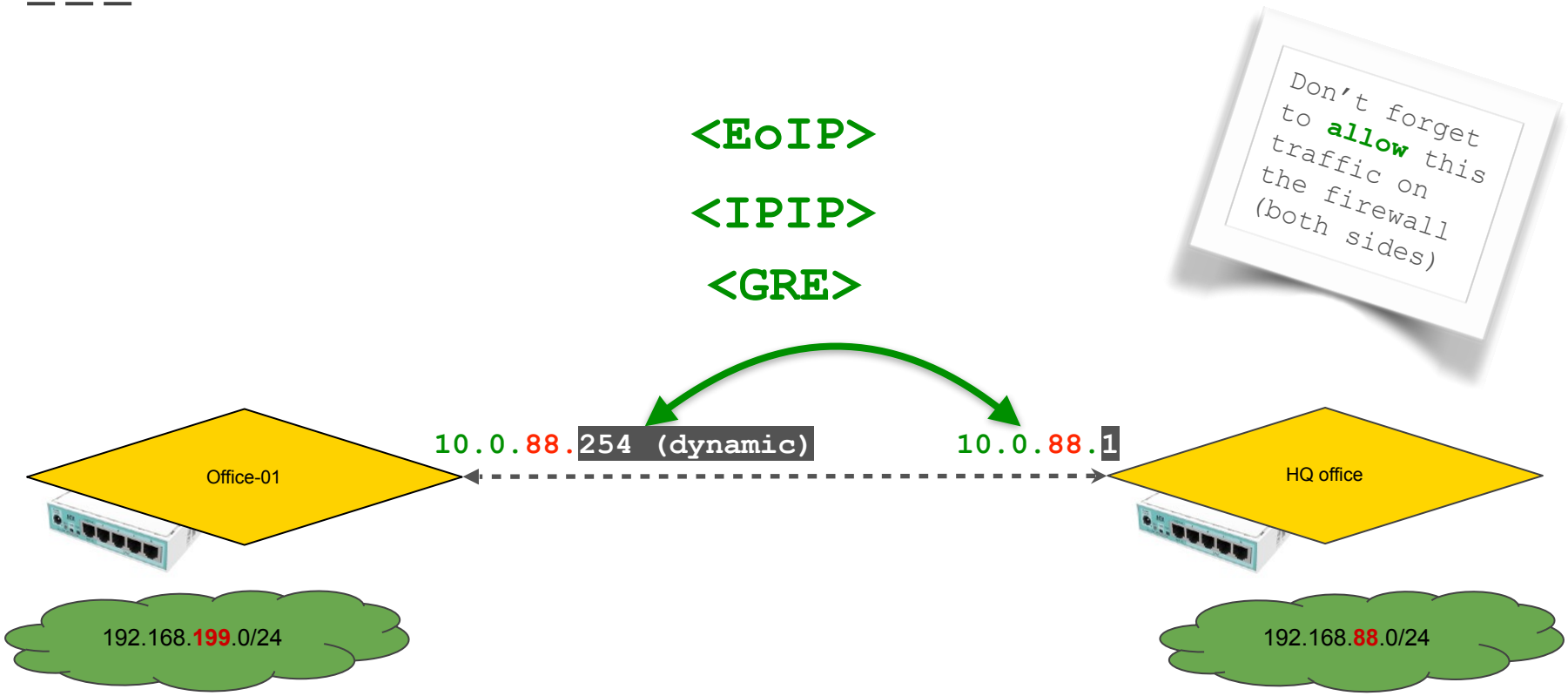
<interface> over ipsec ike2

Cons:

Decreased MTU due to extra encapsulation overhead

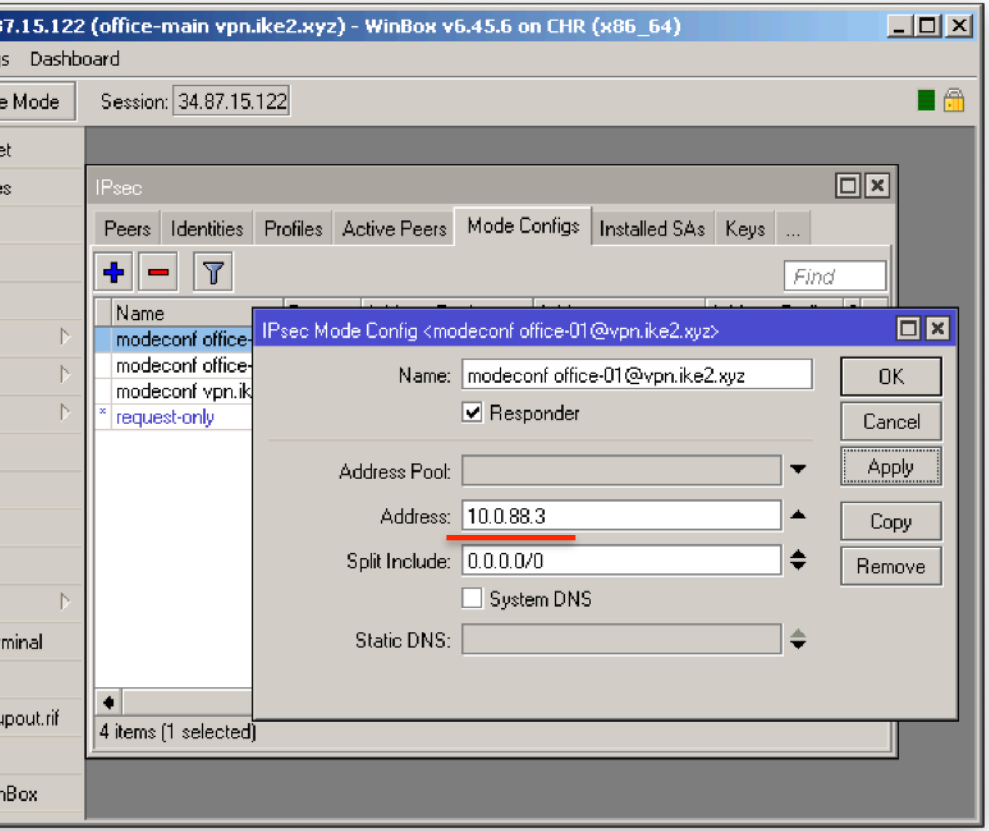
Takes longer to connect and reconnect

Option #1: **routable** using your favourite <interface> over IKEv2



Create new ipsec modeconf with static IP address

Server

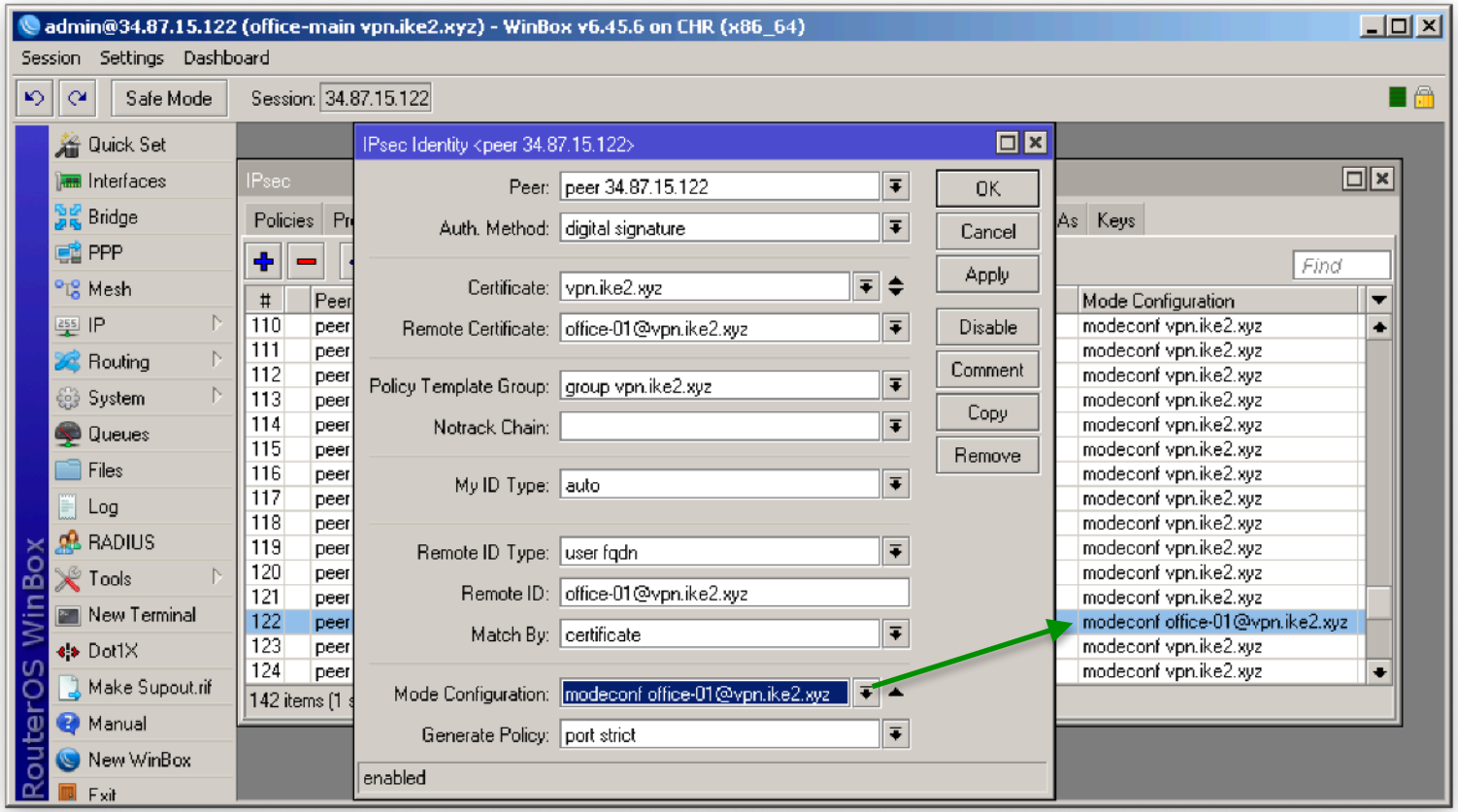


10.0.88.3

```
/ip ipsec add
name="modeconf office-01@vpn.ike2.xyz"
 address=10.0.88.3 address-prefix-
length=32 split-
include=0.0.0.0/0 system-dns=no
```

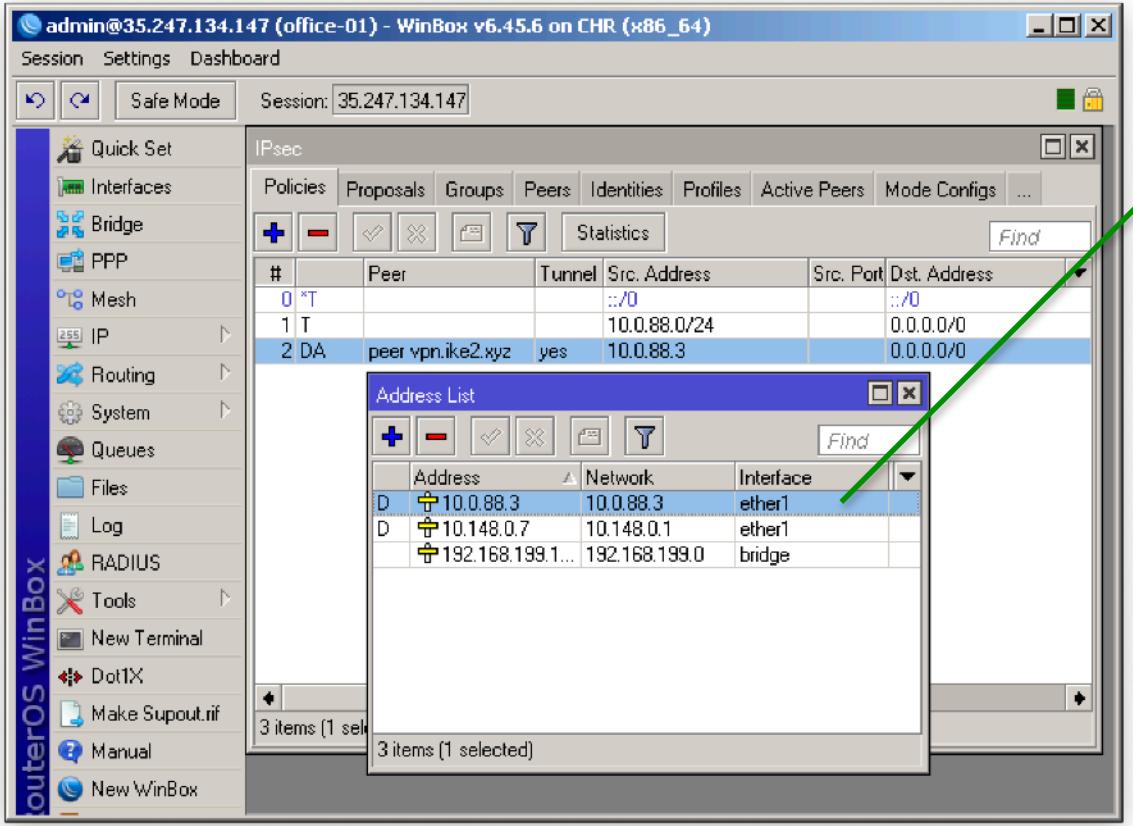
Select new ipsec **static** modeconf for the client identity

Server



Reconnect ipsec peer and check new **static** IP address

Client



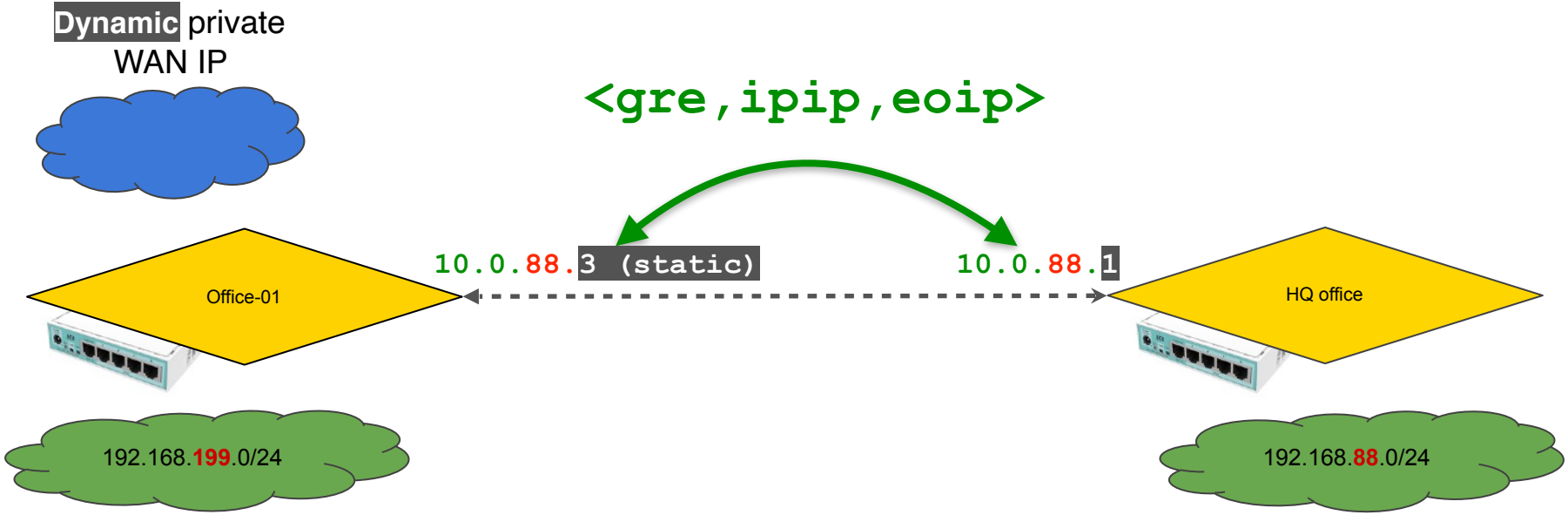
IP address **10.0.88.3**

Interface **ether1**

10.0.88.3

You can establish <interface> connection between **static** endpoint IP addresses

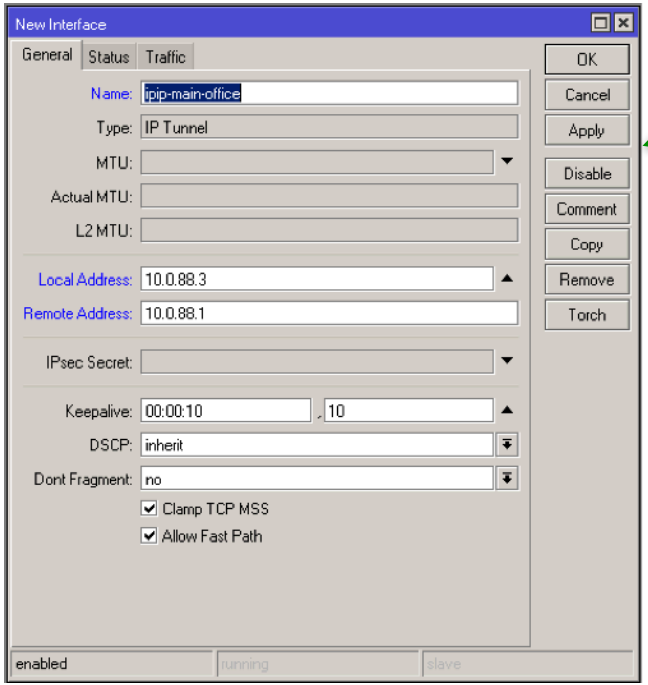
*Even if you have **dynamic** address on your ether1*



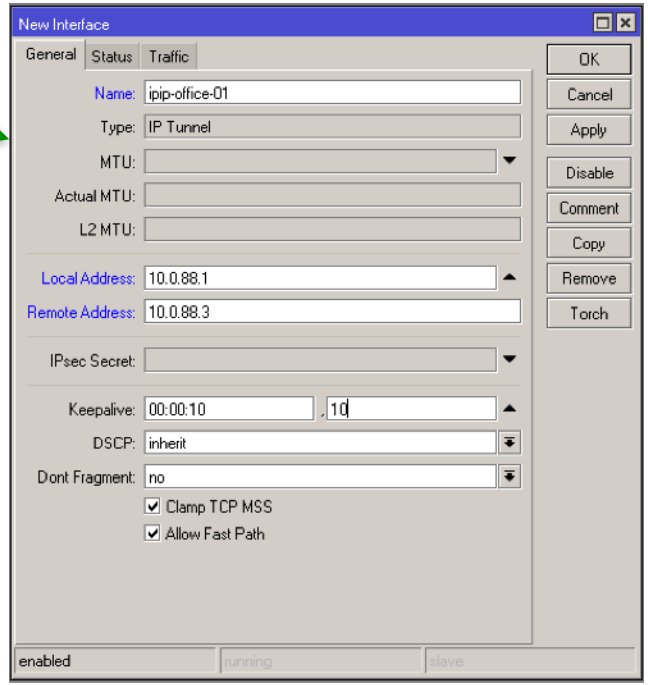
Creating <IPIP interface> on top of static endpoint IP addresses

Client

Server

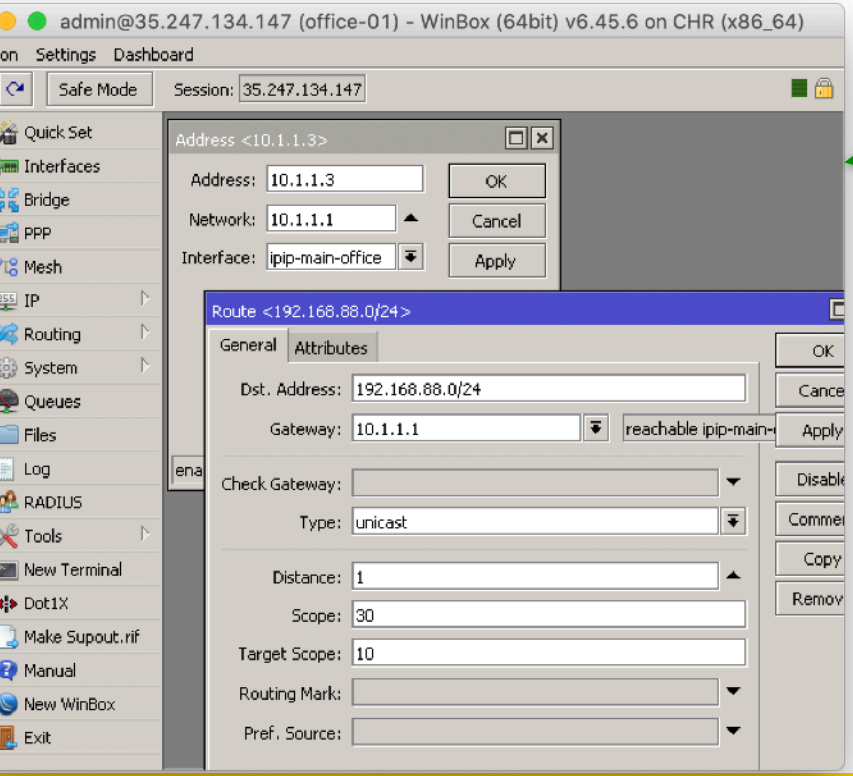


<ipip>

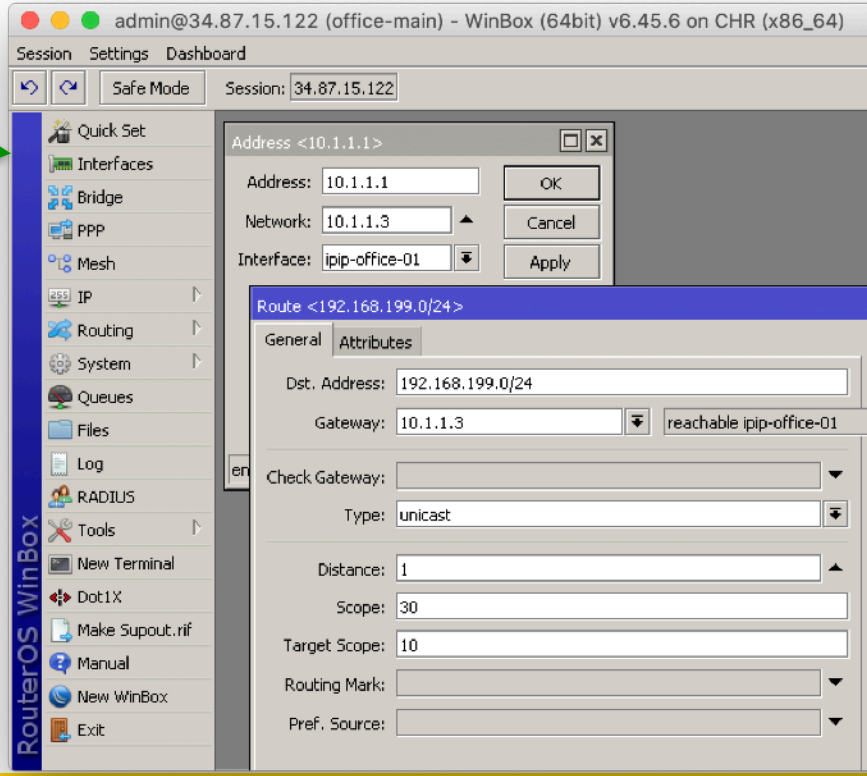


Setup IP addresses on <IPIP interfaces> and static routes (classic vpn)

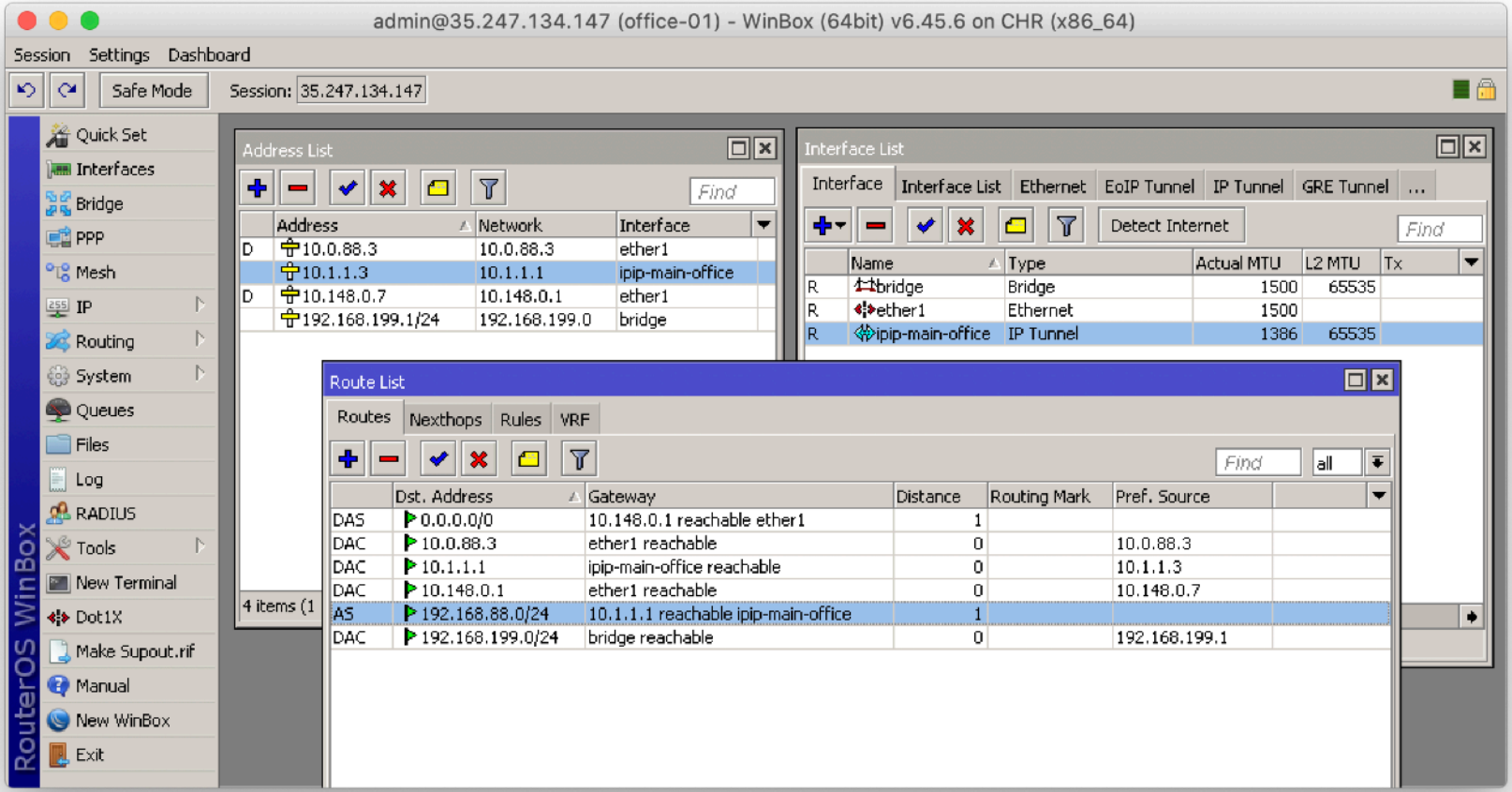
Client



Server



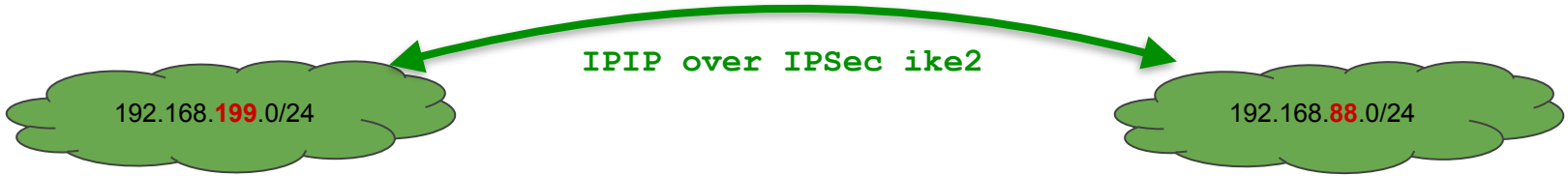
Let's overview <interfaces>, IP addresses and routes



Let’s test our site-to-site <interface> over ipsec based connectivity

```
n@office-01] > ping 192.168.88.1 src-address=192.168.199.1
 HOST                                     SIZE TTL TIME  STATUS
 192.168.88.1                               56  64 1ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
ent=12 received=12 packet-loss=0% min-rtt=0ms avg-rtt=0ms
x-rtt=1ms
```

```
[admin@office-main] > ping 192.168.199.1 src-address=192.168.88.1
  SEQ HOST                                     SIZE TTL TIME  STAT
    0 192.168.199.1                            56  64 0ms
    1 192.168.199.1                            56  64 0ms
    2 192.168.199.1                            56  64 0ms
    3 192.168.199.1                            56  64 0ms
    4 192.168.199.1                            56  64 0ms
    5 192.168.199.1                            56  64 0ms
    6 192.168.199.1                            56  64 0ms
    7 192.168.199.1                            56  64 0ms
    8 192.168.199.1                            56  64 0ms
    sent=9 received=9 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-r
```



Pros:

No MTU overhead -> **performs faster**

Connects and reconnects much faster

Much more **stable**, less reconnects

Option 2 (advanced)

100% policy based ipsec ike2

Cons:

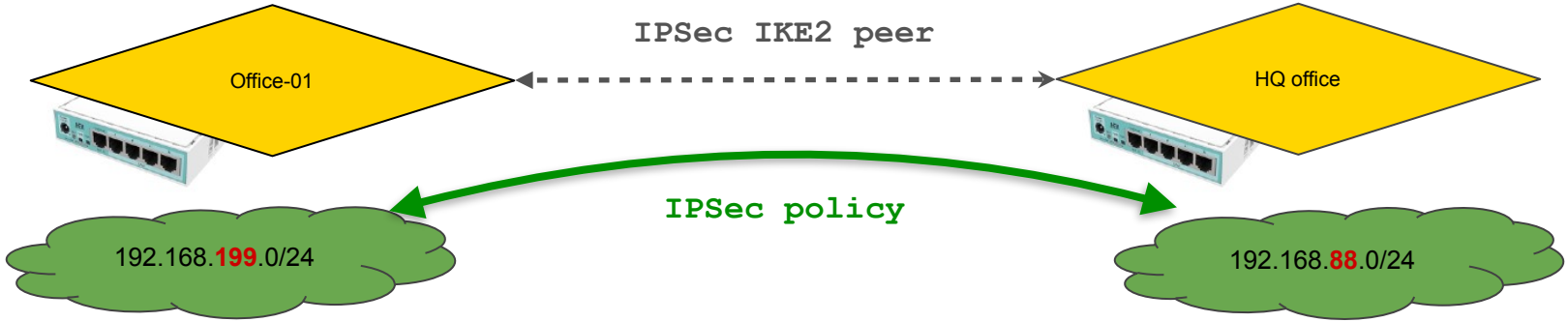
OSPF ~~works~~

Harder to configure and understand

Has no routable interface

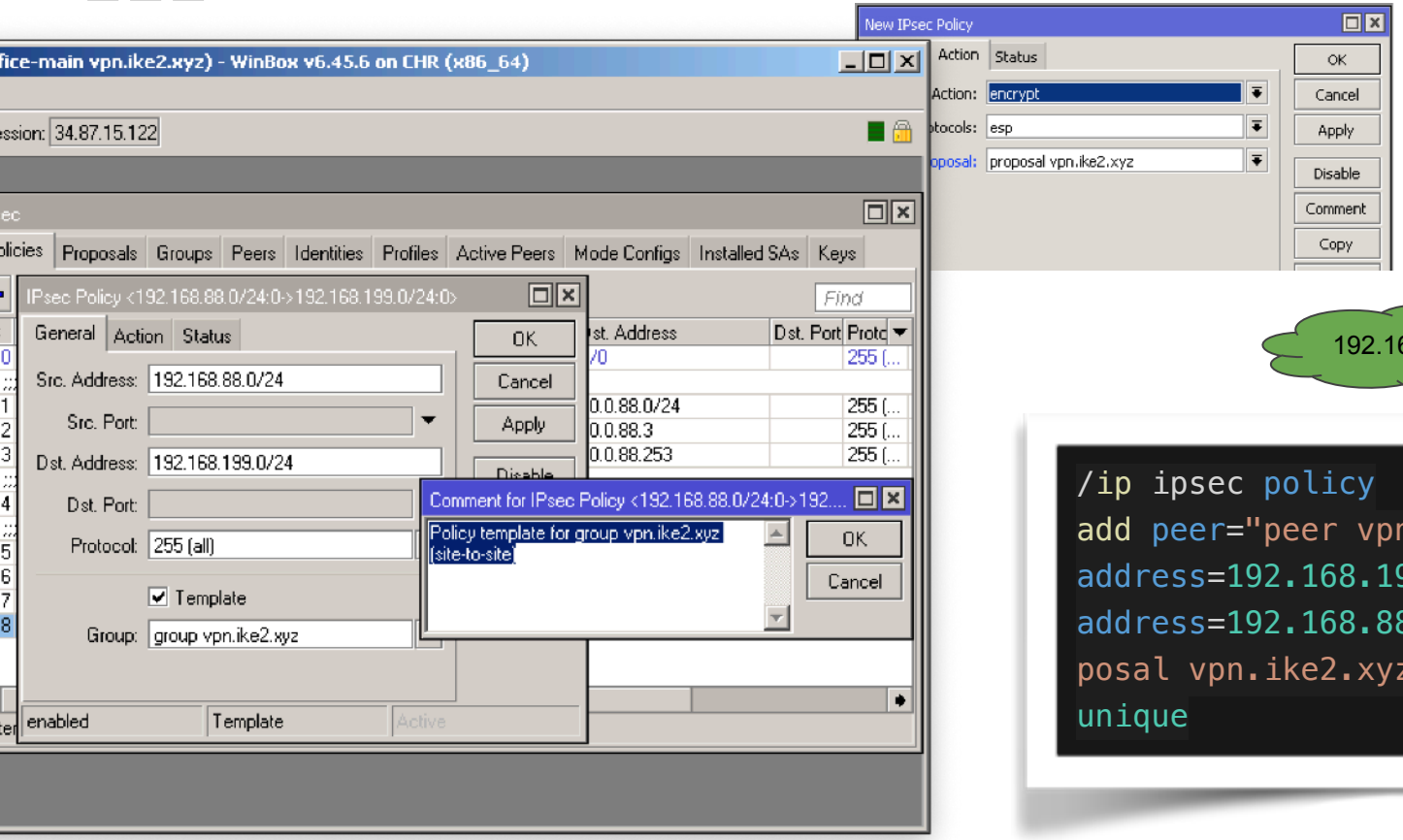
Need to adjust TCP MSS manually

Option #2: **policy** based ipsec IKEv2



Create new ipsec policy template for <group vpn.ike2.xyz>

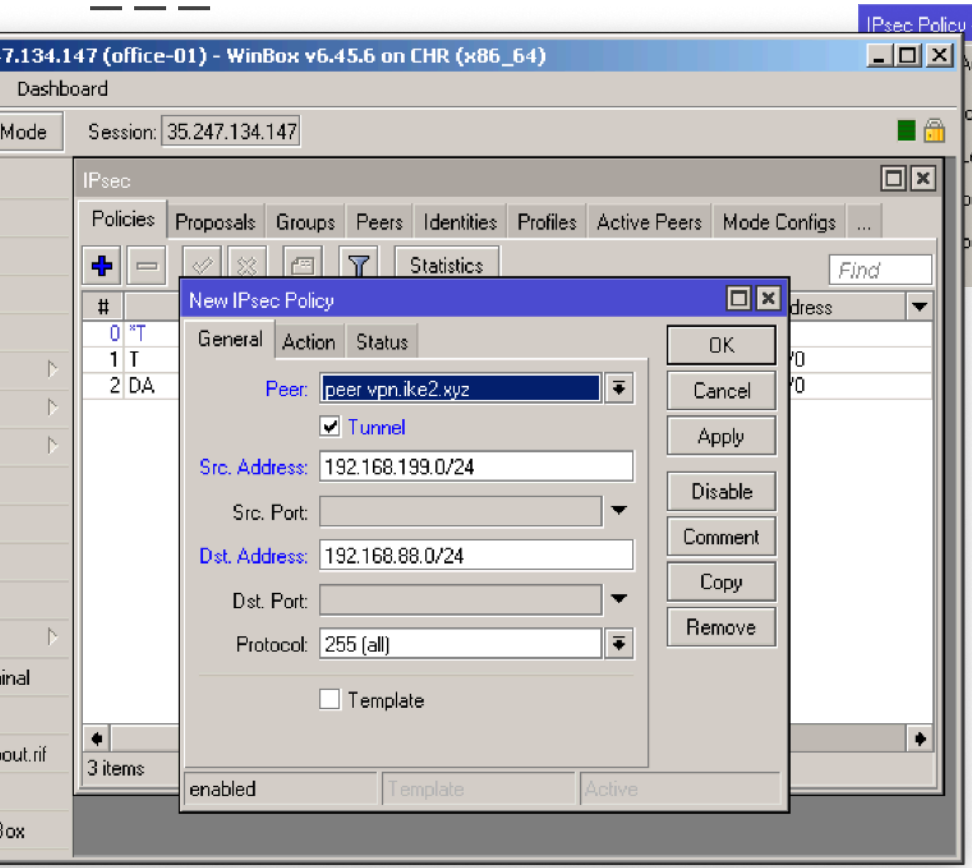
Server

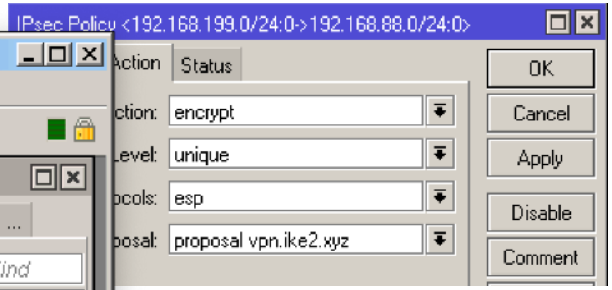



```
/ip ipsec policy
add peer="peer vpn.ike2.xyz" src-
address=192.168.199.0/24 dst-
address=192.168.88.0/24 proposal="pro
posal vpn.ike2.xyz" tunnel=yes level=
unique
```

Create new static **tunnel** policy on <peer vpn.ike2.xyz>

Client



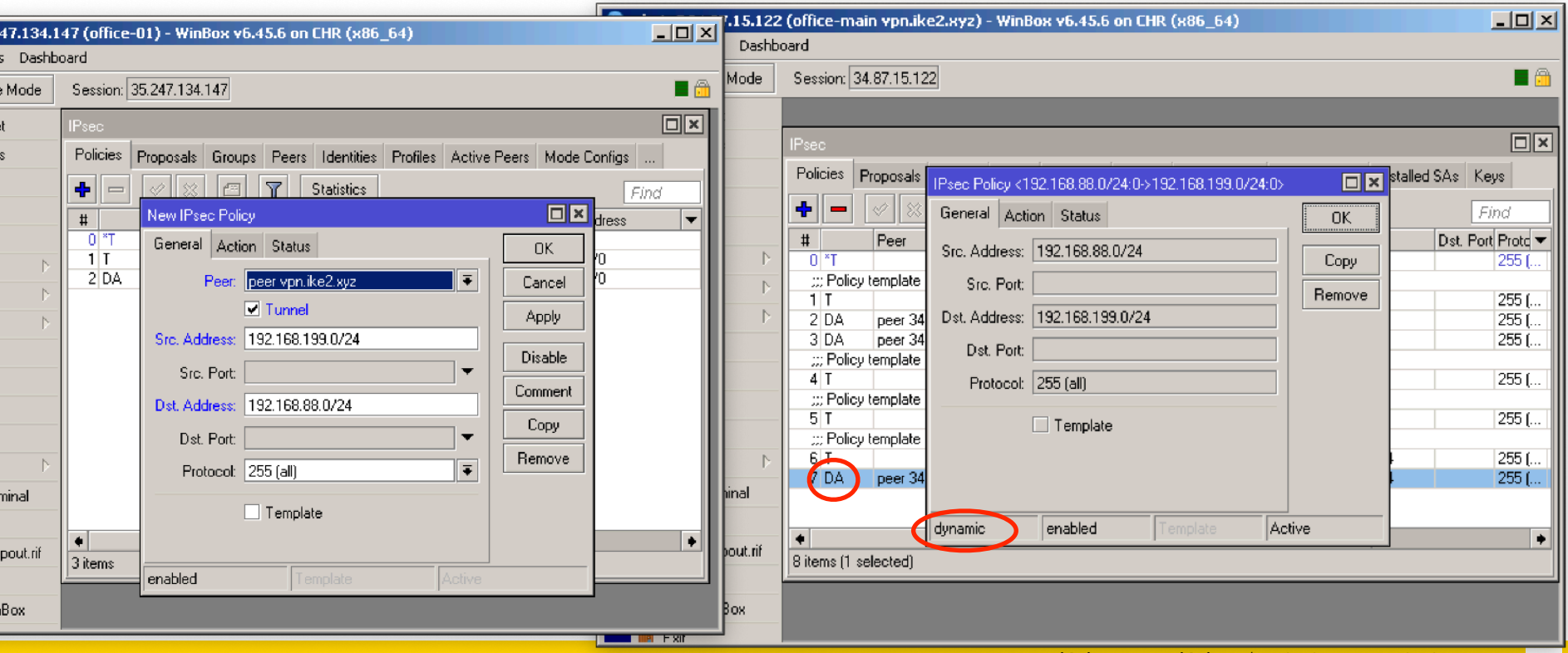


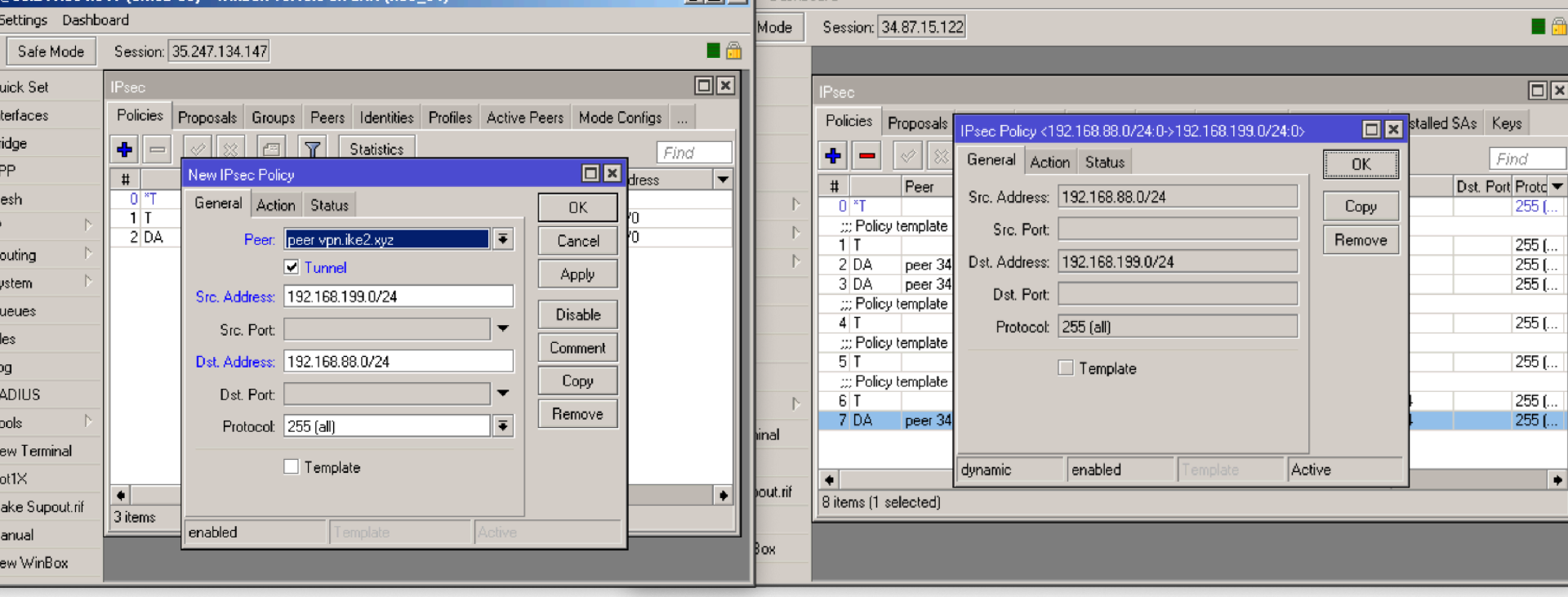

```
/ip ipsec policy
add peer="peer vpn.ike2.xyz" src-
address=192.168.199.0/24 dst-
address=192.168.88.0/24 tunnel=yes
proposal="proposal vpn.ike2.xyz"
```

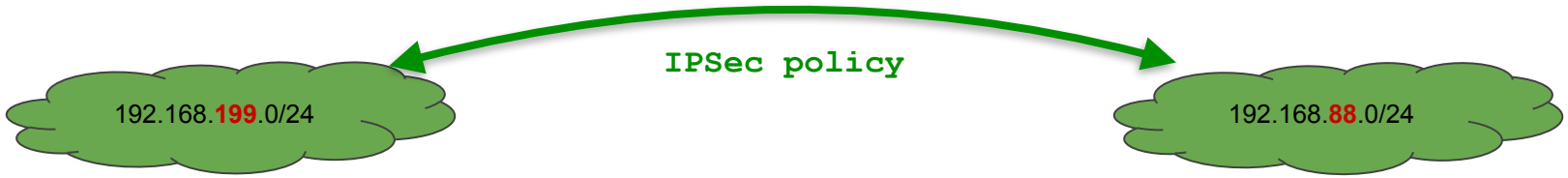
… this will trigger dynamic policy generation on server (if matches policy template)

Client

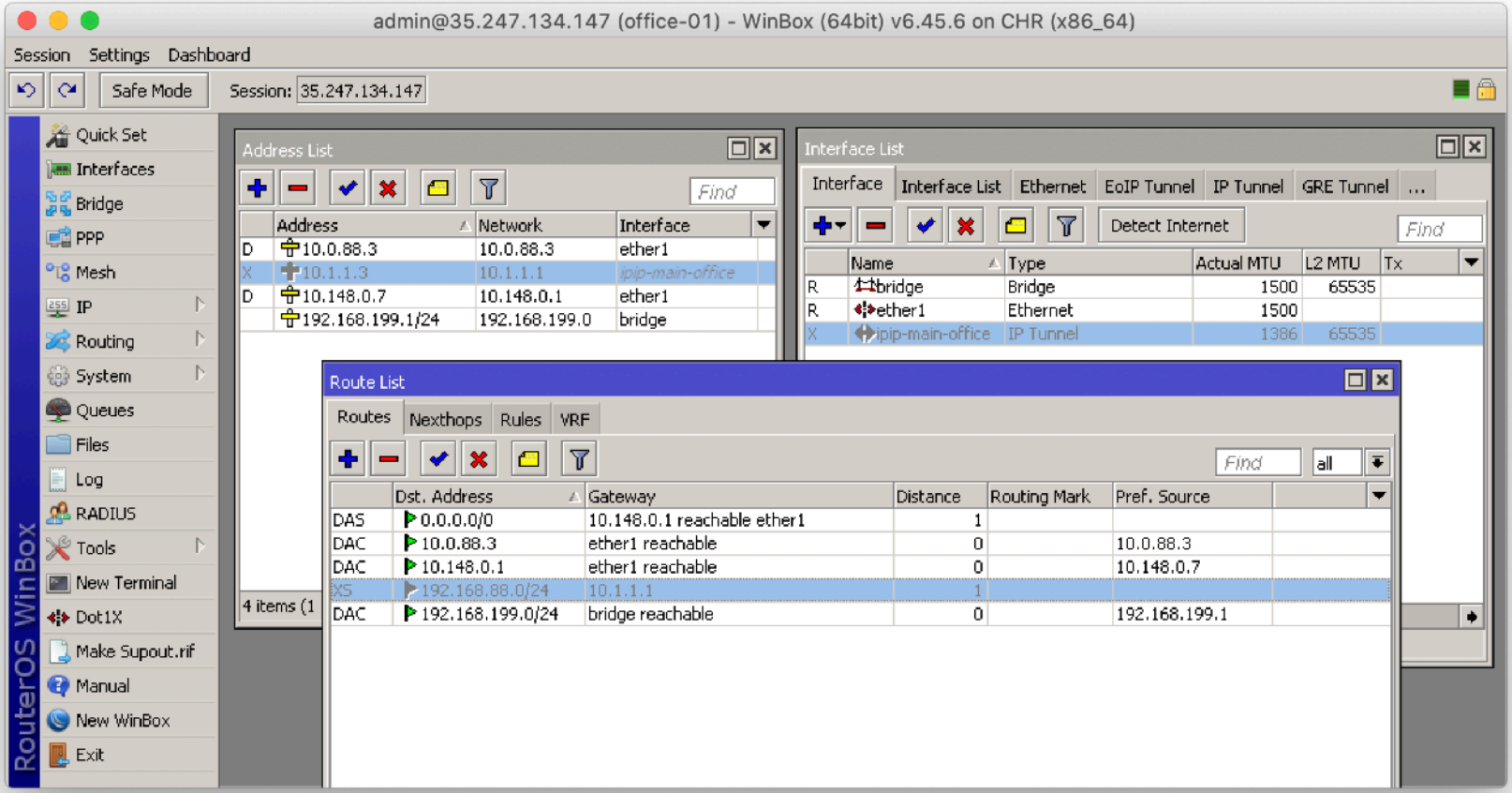
Server



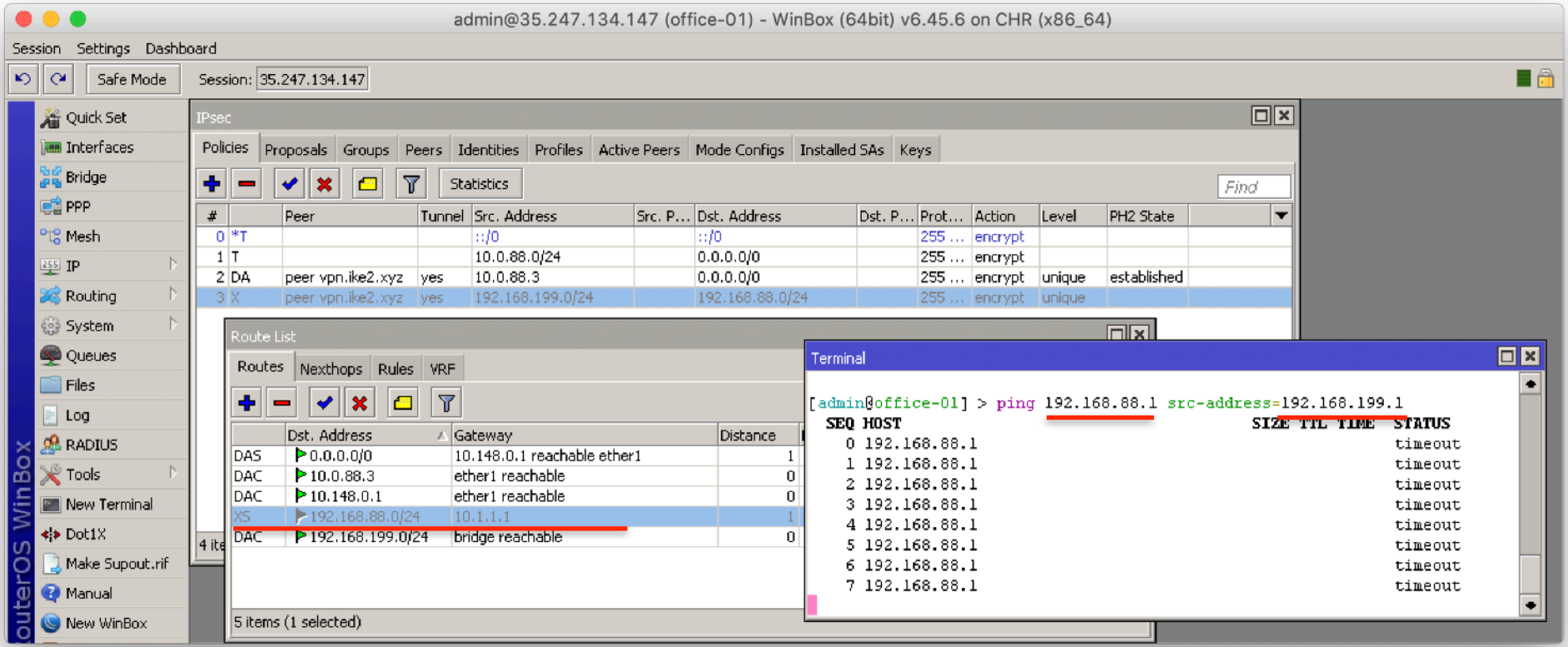

Settings
Dashboard
Safe Mode
Session: 35.247.134.147
IPsec
Policies
Proposals
Groups
Peers
Identities
Profiles
Active Peers
Mode Configs
Statistics
New IPsec Policy
General
Action
Status
Peer: peer vpn.ike2.xyz
Tunnel
Src. Address: 192.168.199.0/24
Src. Port:
Dst. Address: 192.168.88.0/24
Dst. Port:
Protocol: 255 (all)
Template
OK
Cancel
Apply
Disable
Comment
Copy
Remove
3 items
enabled
Template
Active
Mode
Session: 34.87.15.122
IPsec
Policies
Proposals
Keys
IPsec Policy <192.168.88.0/24:0->192.168.199.0/24:0>
General
Action
Status
Src. Address: 192.168.88.0/24
Src. Port:
Dst. Address: 192.168.199.0/24
Dst. Port:
Protocol: 255 (all)
Template
OK
Copy
Remove
dynamic
enabled
Template
Active
8 items (1 selected)


IPSec policy
192.168.199.0/24
192.168.88.0/24

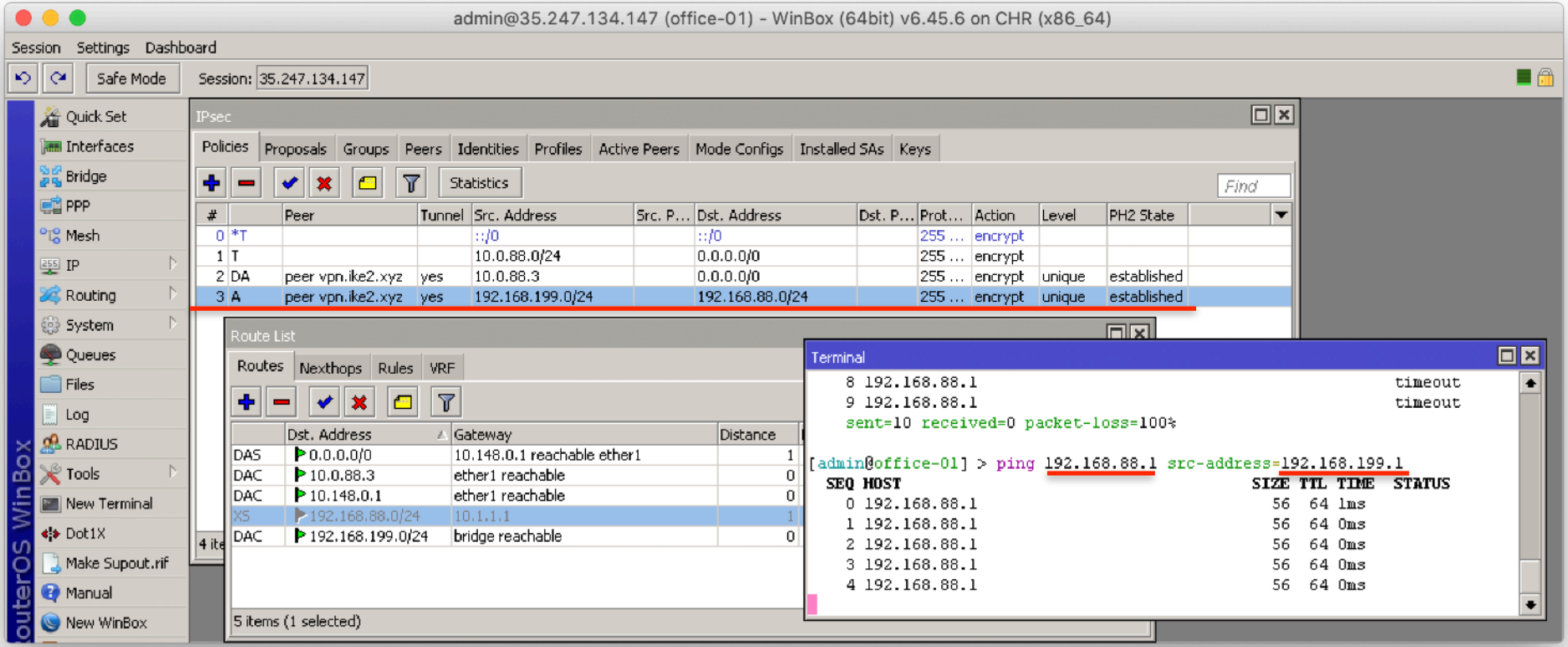
Let's review our <interfaces>, IP addresses and routes



Let's look **very carefully** at our ipsec policies and ip routes



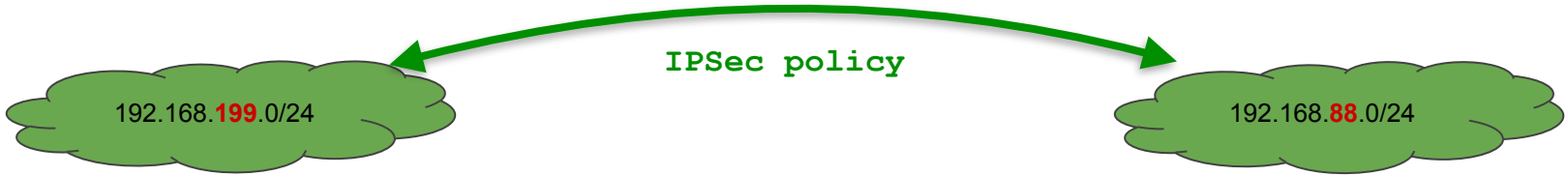
Let's **enable** ipsec policy and keep ip route **disabled**



Testing site-to-site ipsec policy based connectivity

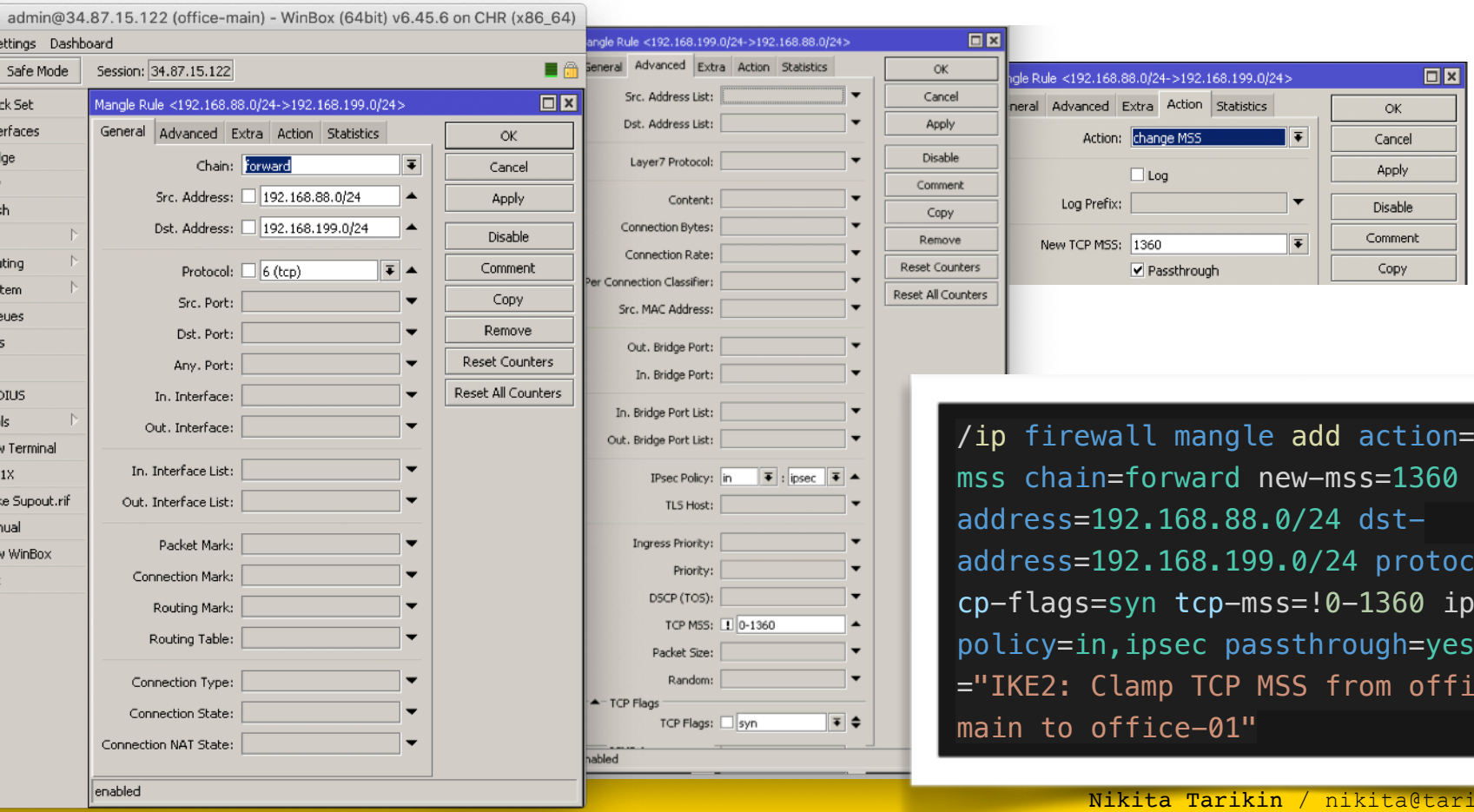
```
n@office-01] > ping 192.168.88.1 src-address=192.168.199.1
 HOST                                     SIZE TTL TIME  STATUS
 192.168.88.1                               56  64 1ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
ent=12 received=12 packet-loss=0% min-rtt=0ms avg-rtt=0ms
x-rtt=1ms
```

```
[admin@office-main] > ping 192.168.199.1 src-address=192.168.88.1
  SEQ HOST                                     SIZE TTL TIME  STAT
    0 192.168.199.1                            56  64 0ms
    1 192.168.199.1                            56  64 0ms
    2 192.168.199.1                            56  64 0ms
    3 192.168.199.1                            56  64 0ms
    4 192.168.199.1                            56  64 0ms
    5 192.168.199.1                            56  64 0ms
    6 192.168.199.1                            56  64 0ms
    7 192.168.199.1                            56  64 0ms
    8 192.168.199.1                            56  64 0ms
    sent=9 received=9 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-r
```



Setting up TCP MSS 🎯

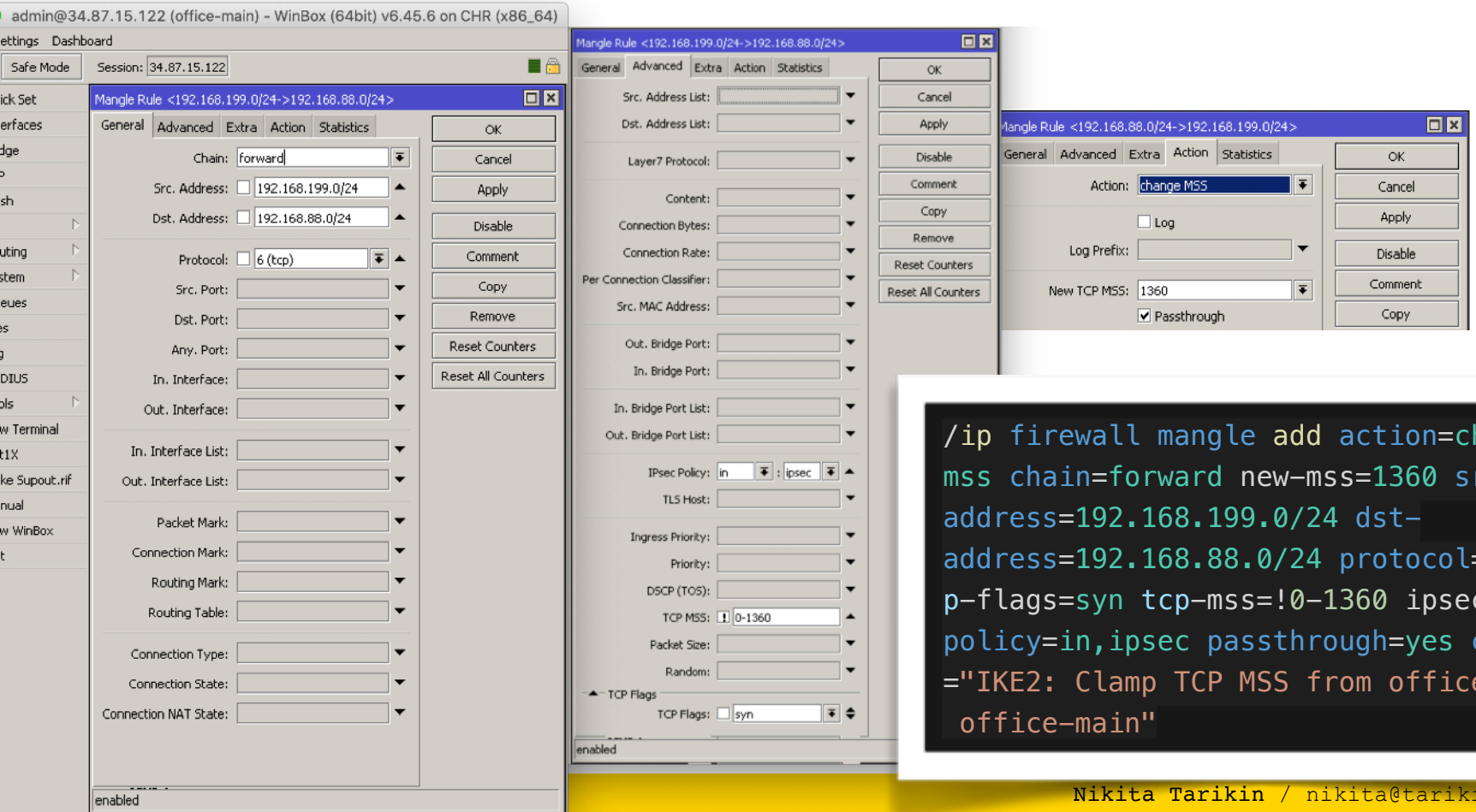
Adjust TCP MSS from office-main to office-01 over ipsec policy connection




```
/ip firewall mangle add action=change-
mss chain=forward new-mss=1360 src-
address=192.168.88.0/24 dst-
address=192.168.199.0/24 protocol=tcp t
cp-flags=syn tcp-mss=!0-1360 ipsec-
policy=in,ipsec passthrough=yes comment
="IKE2: Clamp TCP MSS from office-
main to office-01"
```

Nikita Tarikin / nikita@tarikin.com

Adjust TCP MSS from office-01 to office-main over ipsec policy connection




```
/ip firewall mangle add action=change-
mss chain=forward new-mss=1360 src-
address=192.168.199.0/24 dst-
address=192.168.88.0/24 protocol=tcp tc
p-flags=syn tcp-mss=!0-1360 ipsec-
policy=in,ipsec passthrough=yes comment
="IKE2: Clamp TCP MSS from office-01 to
 office-main"
```

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/TTmKeHe8W2u9YZ3c7

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

`vpn.ike2.xyz`

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

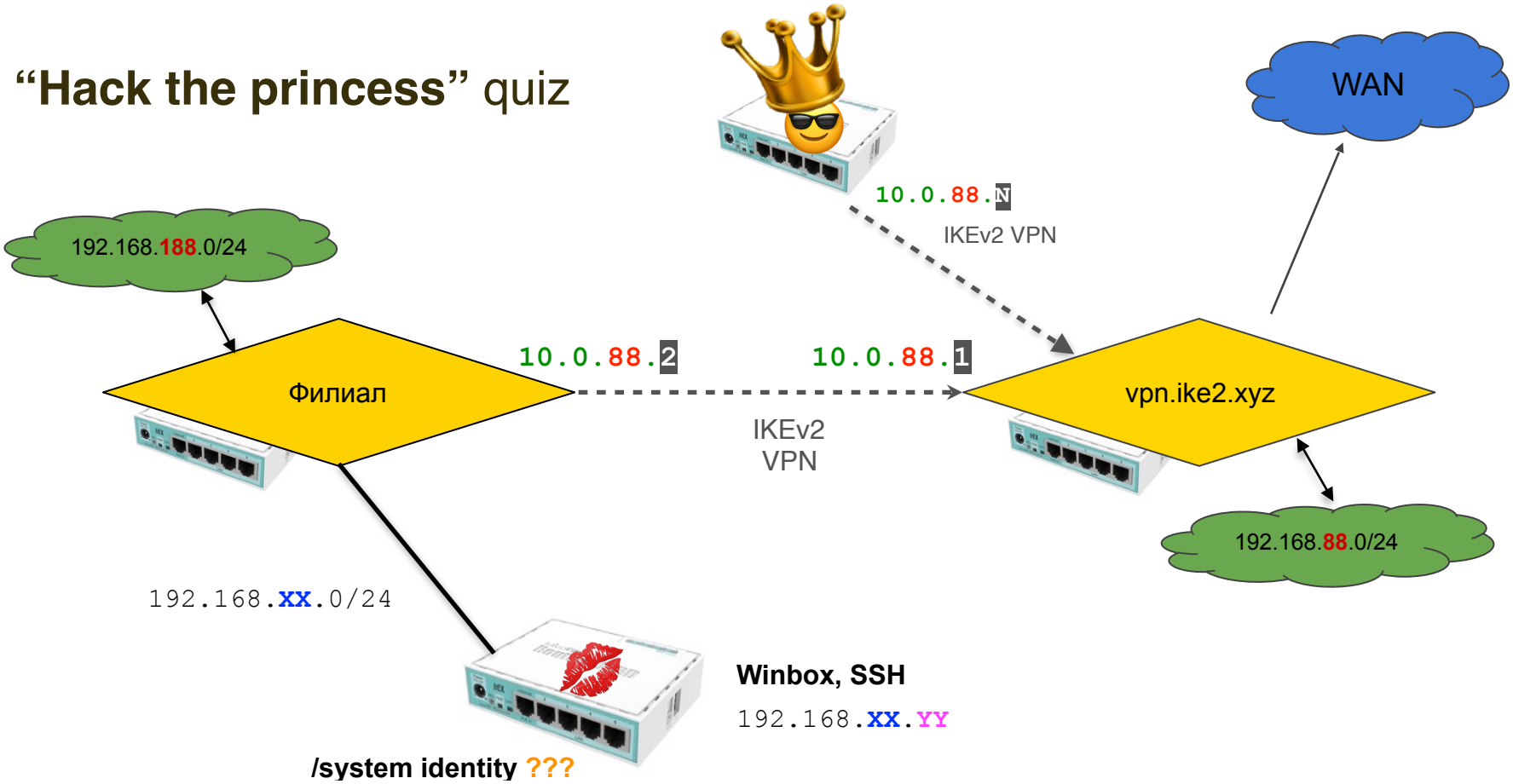
IPSec quiz time!

“ Hack the princess ”

Will be open until 31 December 2019

Nikita Tarikin / nikita@tarikin.com

“Hack the princess” quiz

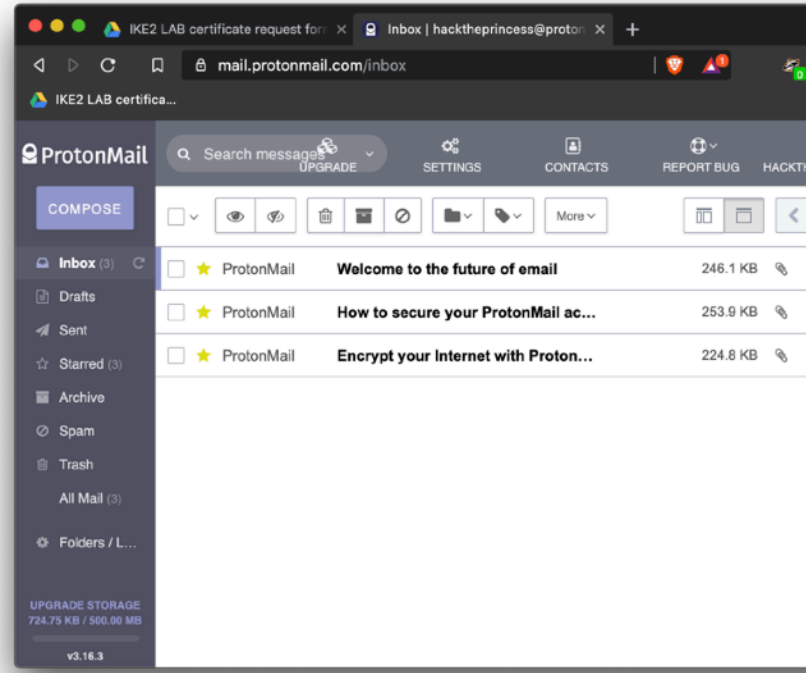


hacktheprincess@protonmail.com

192.168.**XX**.0/24

192.168.**XX**.**YY**

/system identity **???**



Send results to e-mail

Let’s keep in touch

Send me e-mail:
nikita@tarikin.com

Find me in Facebook:
Nikita Tarikin

Subscribe my channels:
@tarikin
@tropicalengineer

Direct message me via:

Telegram t.me/tarikin
Messenger Nikita Tarikin