



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

Certified network engineer
MikroTik PRO, Russia



MikroTik
C E R T I F I E D

Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia

MTCNA 99%

MTCRE 95%

MTCTCE 96%

MTCWE 84%

MTCUME 90%

MTCSE 94%

MTCIPv6E 74%



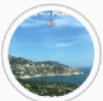




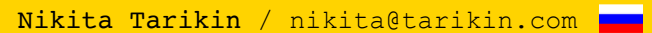
1



www.tarikin.com

[Edit Profile](#)

PhanRang t...





@tropicalengineer



Tropical engineer

388 subscribers

share link

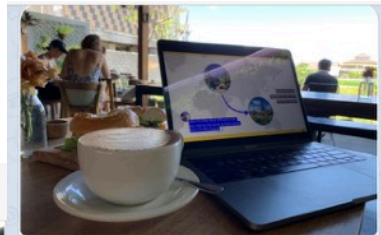
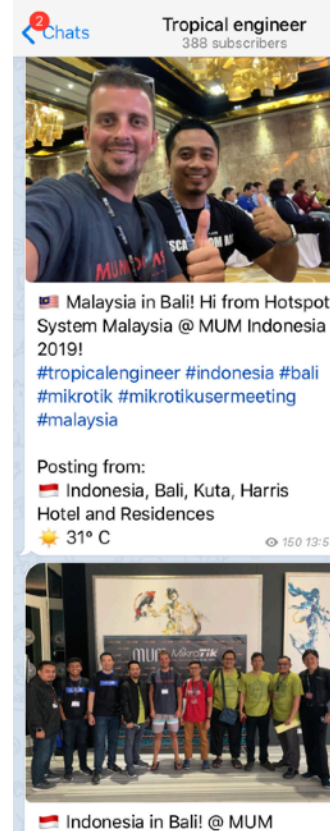
<https://t.me/tropicalengineer>

about

Stories of MikroTik network engineer.
Tropical lifestyle, remote networking, virtualization,
kitesurfing, traveling, freelancing, sharing 📷 🌍
🏖️

Nikita Tarikin @tarikin

Instagram: [instagram.com/tarikin](https://www.instagram.com/tarikin)



Working hard on my presentation for Moscow MUM 2019. The presentation itself is mostly done, right now I'm building an advanced ike2 demo lab with a surprise inside. I promised you to explain ike2 site-to-site between MikroTik routers, but I've realized that I'm out of time for that. So the great idea is to let you will find it out yourself while hacking my hackable demo lab. I'll launch the "hacking the lab" competition right after my MUM speech on Friday and give away valuable prizes on Saturday at the MUM lottery. Stay tuned!

Posting from:
Indonesia, Bali, Canggu

380 edited 12:17

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:

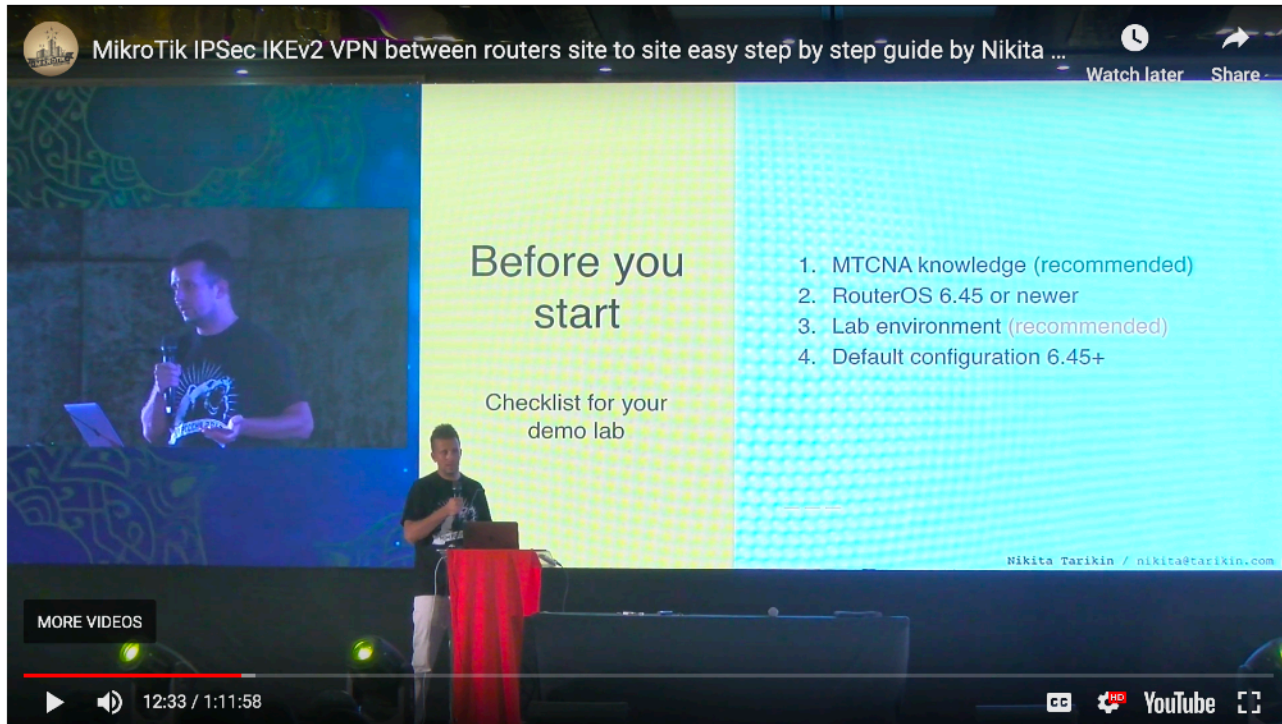


Telegram t.me/tarikin



Messenger Nikita Tarikin

— — —



Watch this presentation on YouTube

https://www.youtube.com/watch?v=n5_Af2vIIOA

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

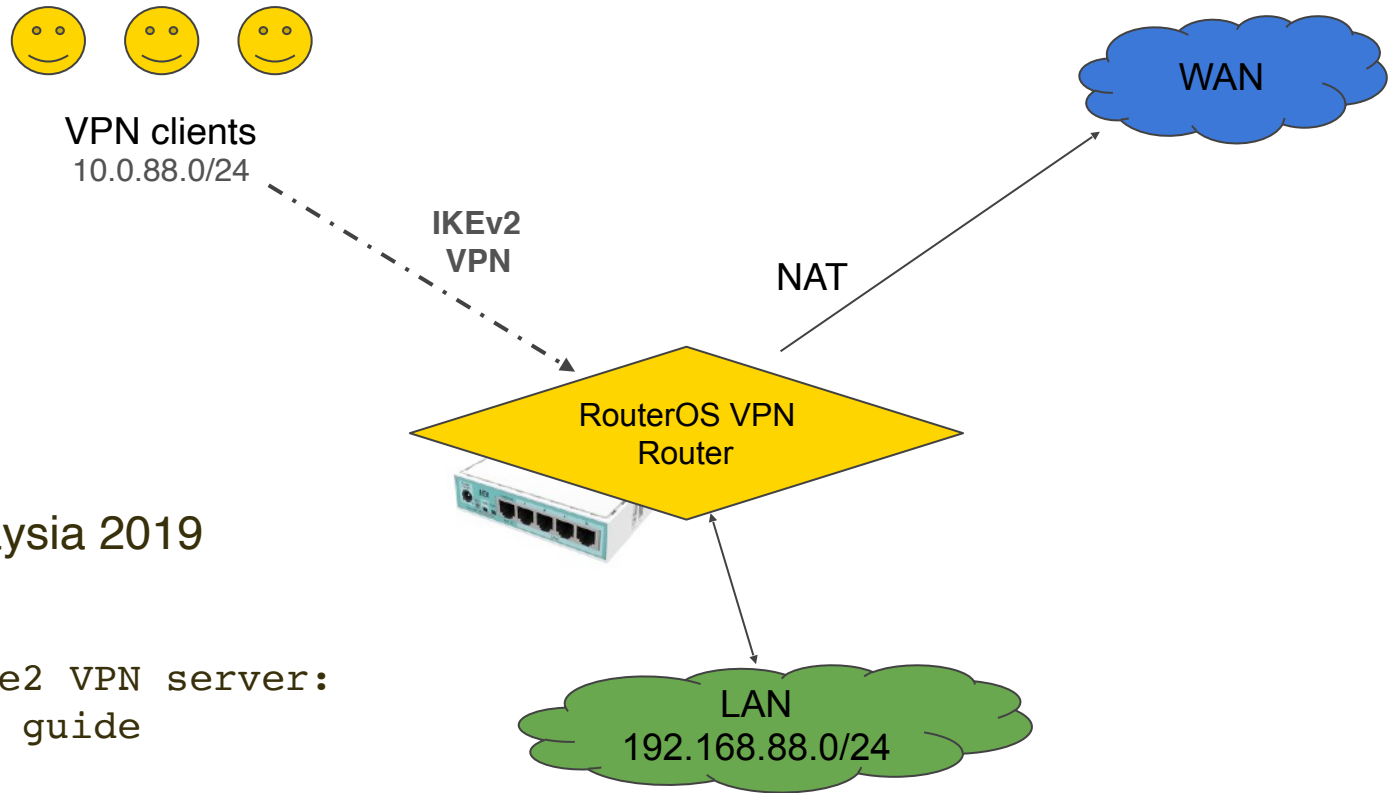


Why IKE2?

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

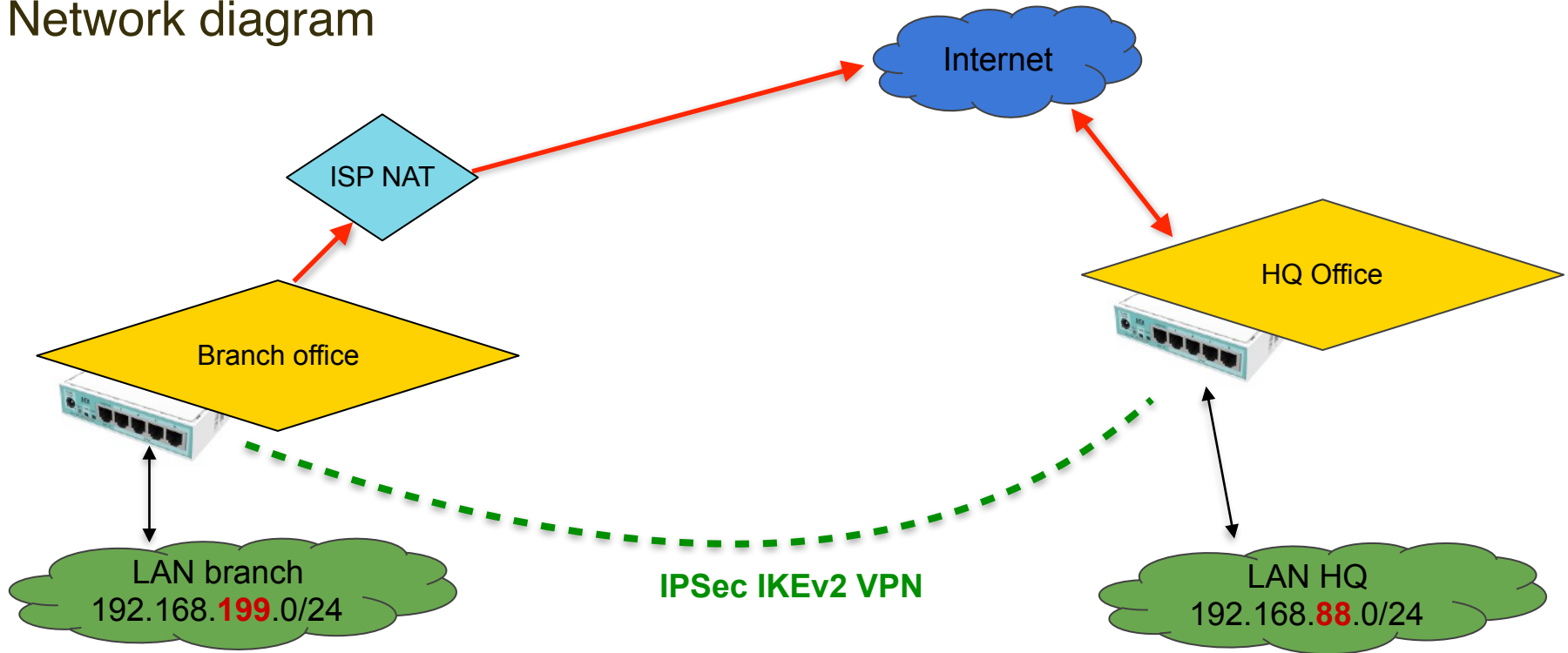


Archive: MUM Malaysia 2019
network diagram

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

— — —

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+

— — —

Upgrade RouterOS to 6.45+

The image displays two overlapping screenshots. The left screenshot shows the Mikrotik website's 'Software' page, specifically the 'RouterOS' section. It lists two versions: '6.44.5 (Long-term)' and '6.45.2 (Stable)'. A green arrow points from the '6.45.2 (Stable)' link to the WinBox interface. The right screenshot shows the WinBox interface. The top bar indicates 'admin@192.168.88.1 (MikroTik) - WinBox v6.38.7 on MAP lite (mipsbe)'. The 'Package List' table shows several packages, with 'routeros-mipsbe' highlighted. A 'File List' dialog box is open, showing the upload progress of 'routeros-mipsbe' (5.7 MB of 10.5 MB at 1633.53 kb/s). A 'Reboot' dialog box is also visible, asking 'Do you want to reboot the router?' with 'Yes' and 'No' buttons.

Name	Version	Build Time	Scheduled
routeros-mipsbe	6.38.7	Jun/20/2017 10:55:05	
advanced-tools	6.38.7	Jun/20/2017 10:55:05	
dhcp	6.38.7	Jun/20/2017 10:55:05	
hotspot	6.38.7	Jun/20/2017 10:55:05	
pvs	6.38.7	Jun/20/2017 10:55:05	

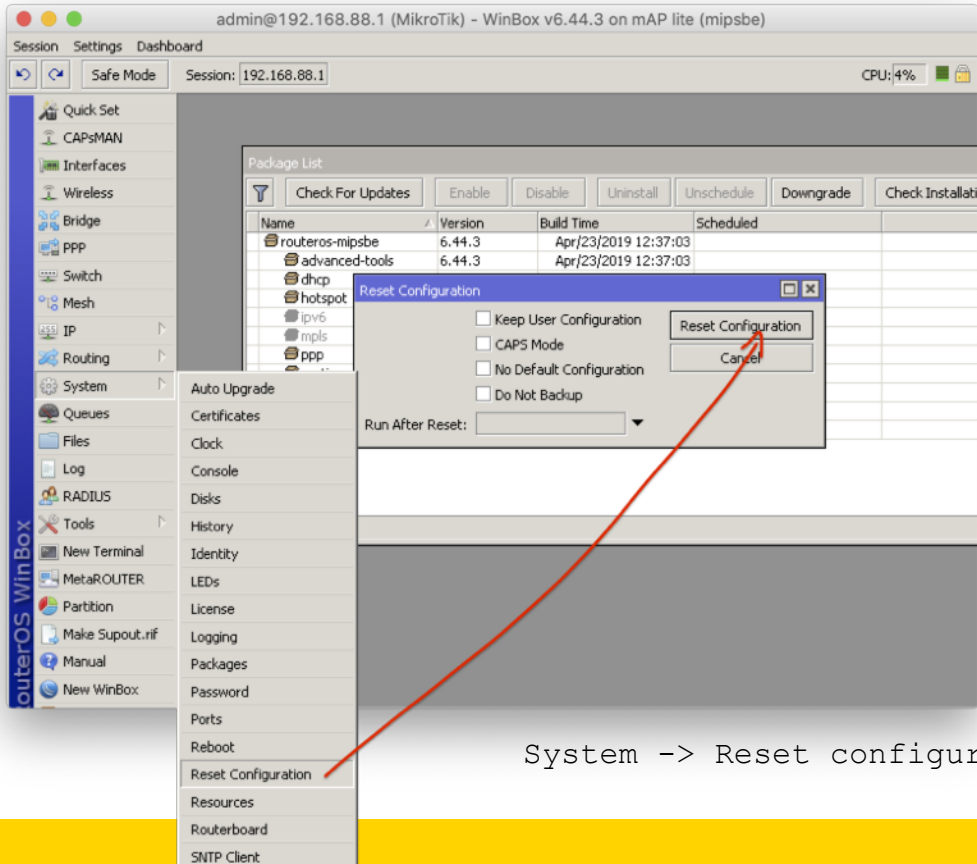
File Name	Size	Creation Time
flash		01/1970 0
flash/pub		24/2017 0
flash/skins		01/1970 0
routeros-mipsbe		07/2019 1

1. Download package from
www.mikrotik.com/download

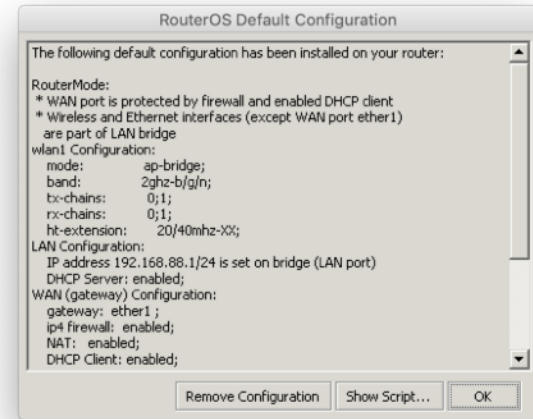
2. Upload package to / of
your RouterBoard

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

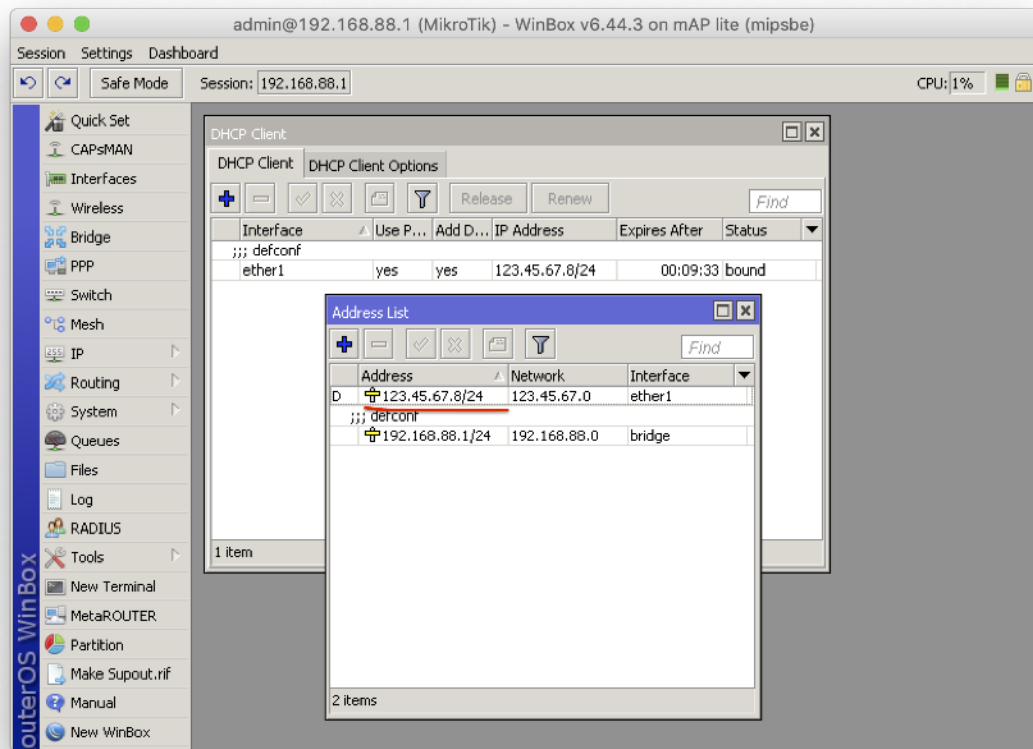
General system settings

Agenda for next slides:

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

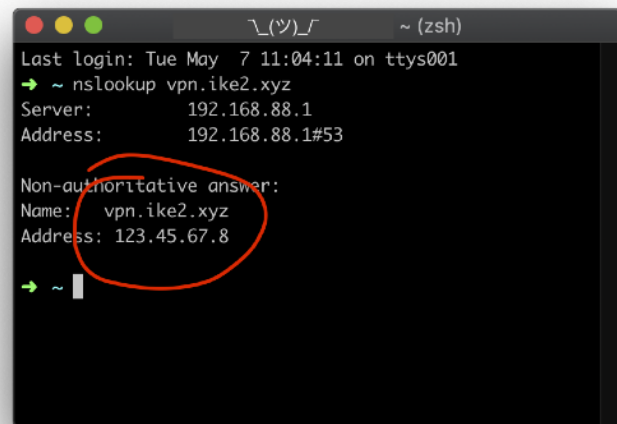
— — —

WAN IP and DNS addresses for IKE2 VPN server



123.45.67.8 is on WAN interface

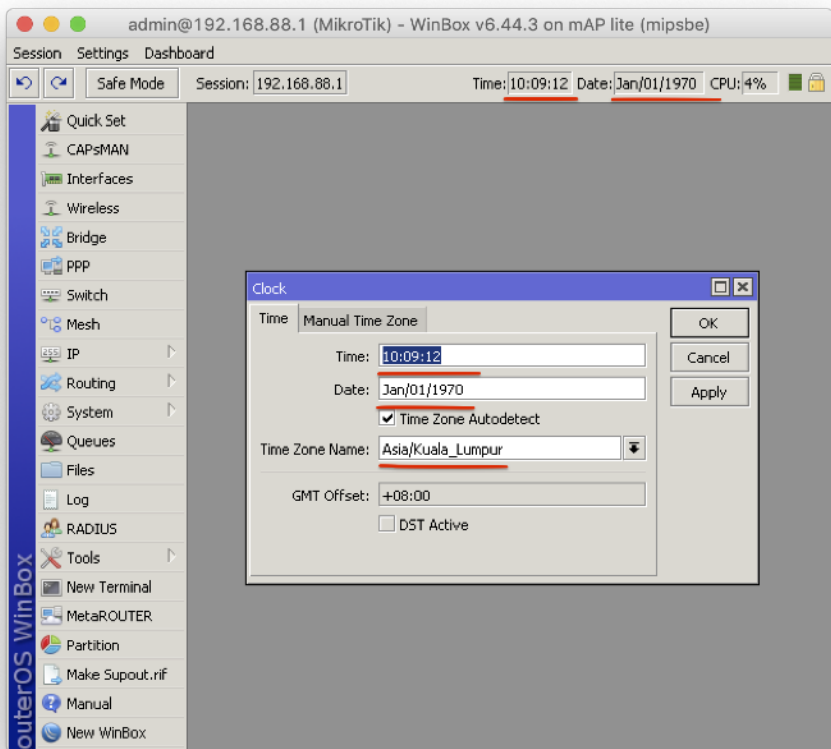
Check DNS records:
Name: **vpn.ike2.xyz**
Address: **123.45.67.8**



* Set DNS records with your domain name registrar control panel

Setup correct timezone

Important

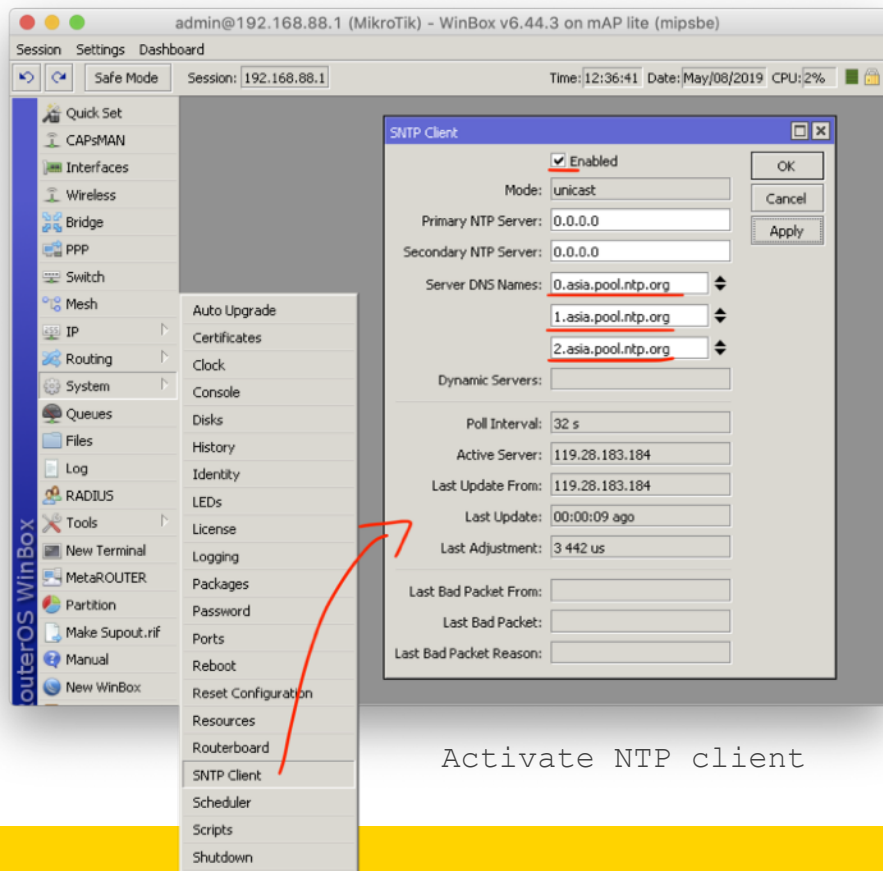


System -> Clock

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

Setup auto date/time

Important

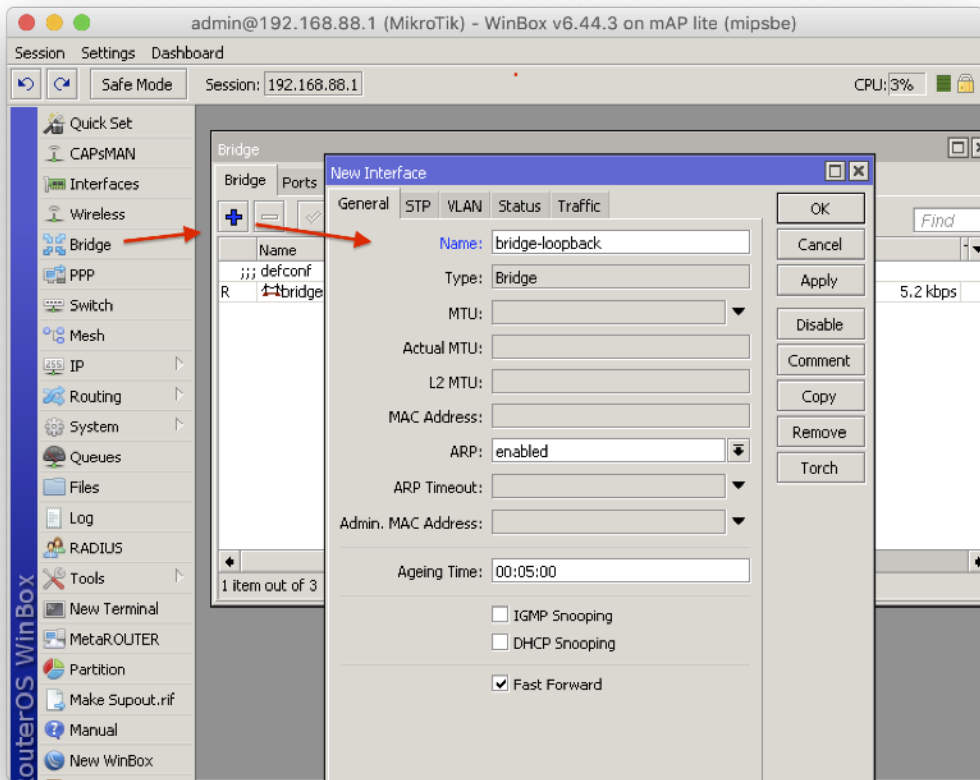


Activate NTP client

```
/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
```

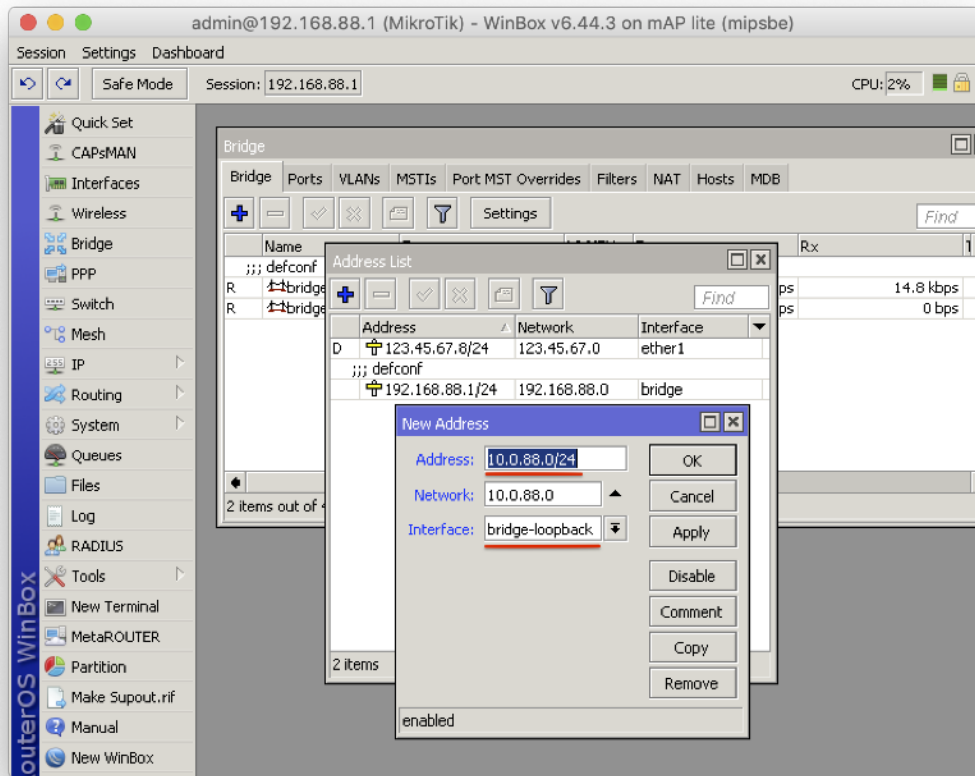
```
fb*o1d'5'92T9'booJ'uqb*o1d
```

Add new loopback bridge



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

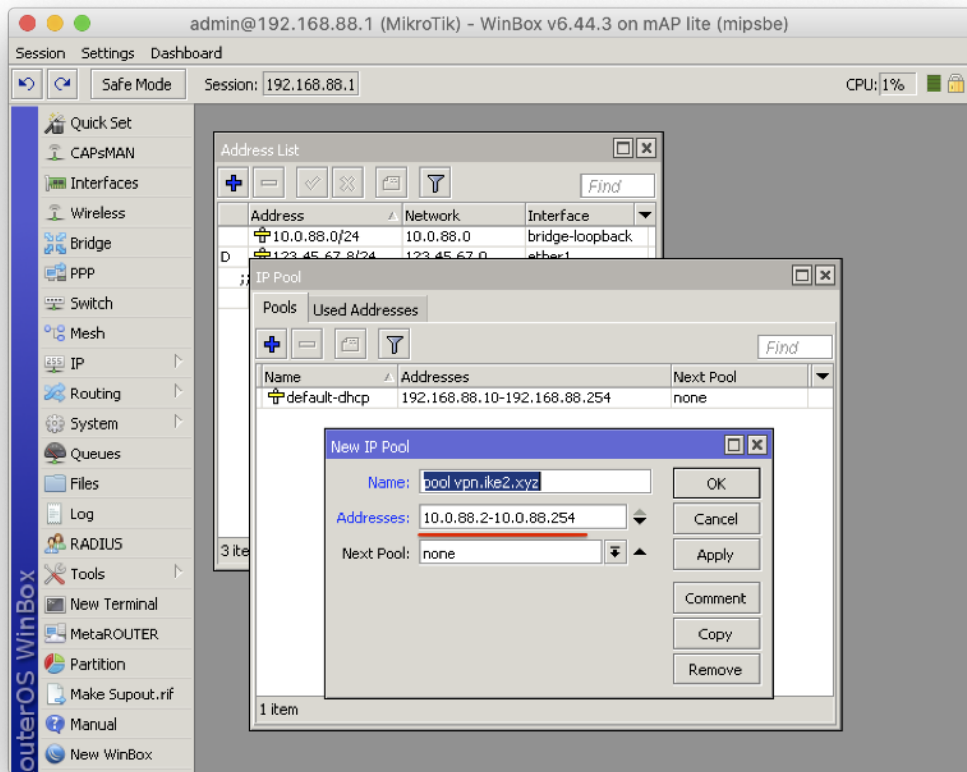
Set loopback bridge IP address



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

```
UGfMOLK=J0'0'88'0
```

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
```

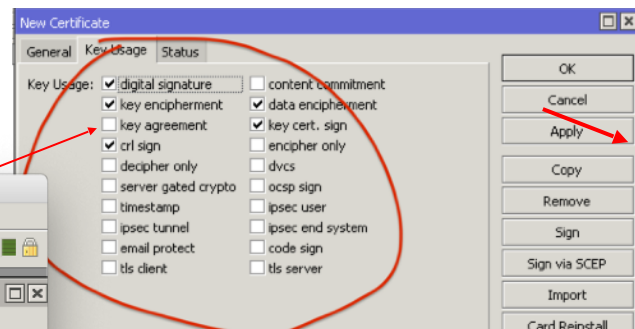
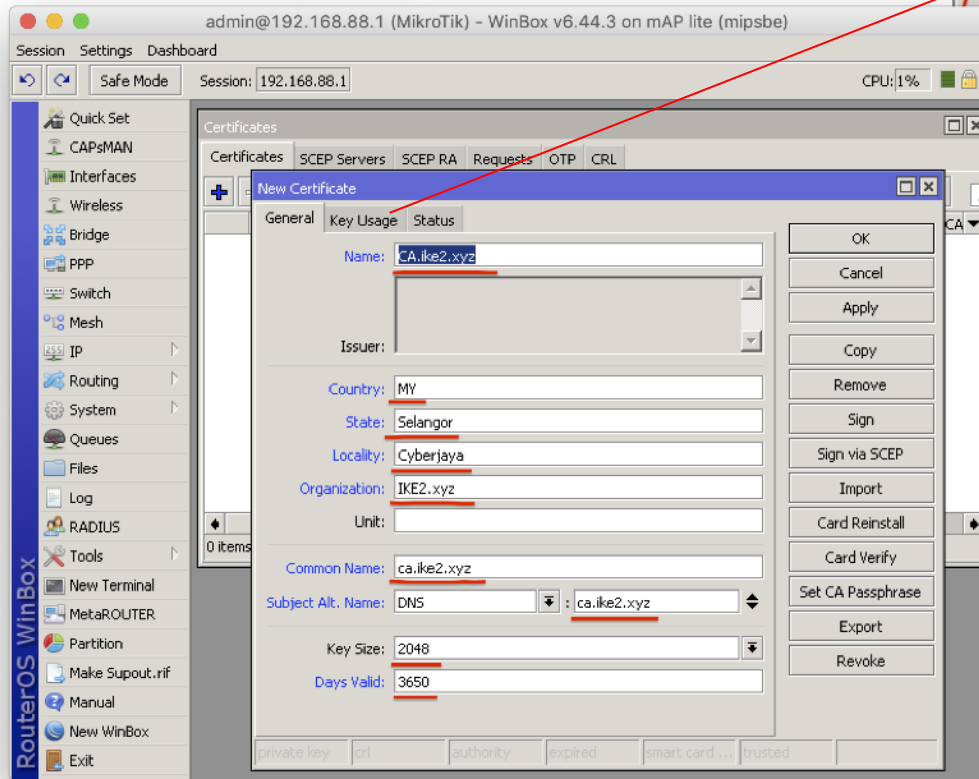

Generate SSL certificates

Agenda for next slides

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

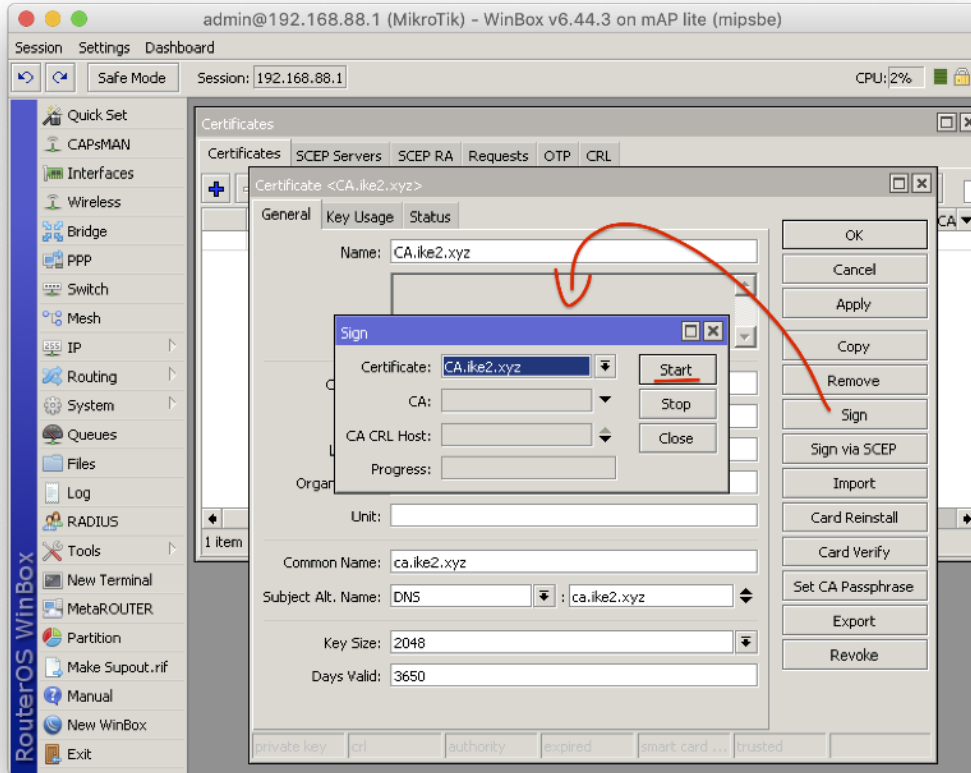
— — —

Generate CA SSL certificate



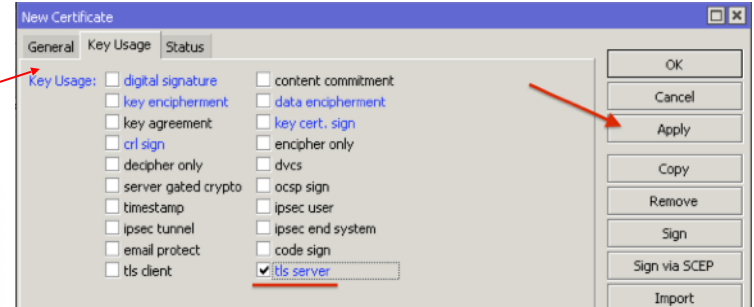
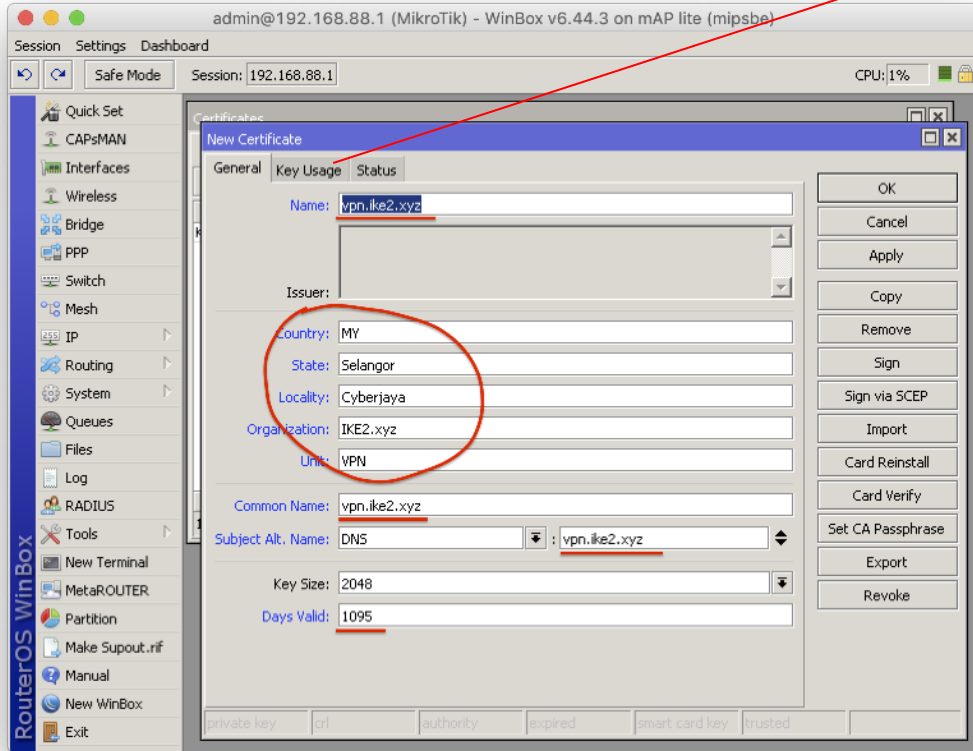
```
/certificate add name=CA.ike2.xyz  
country=MY state=Selangor  
locality=Cyberjaya  
organization=IKE2.xyz common-  
name=ca.ike2.xyz subject-alt-  
name=DNS:ca.ike2.xyz key-size=2048  
days-valid=3650 trusted=yes key-  
usage=digital-signature,key-  
encipherment,data-encipherment,key-  
cert-sign,crl-sign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

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



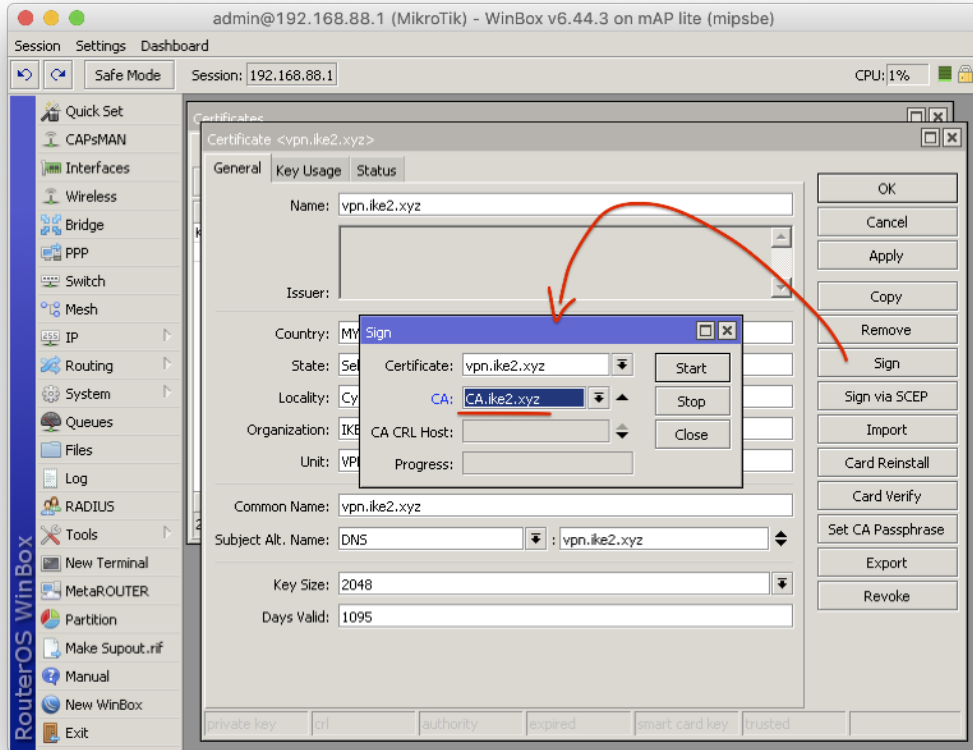
```
/certificate sign CA.ike2.xyz
```

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

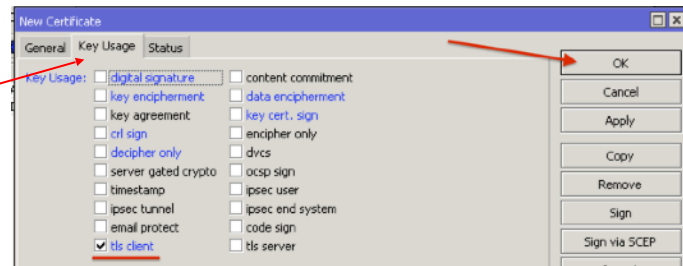
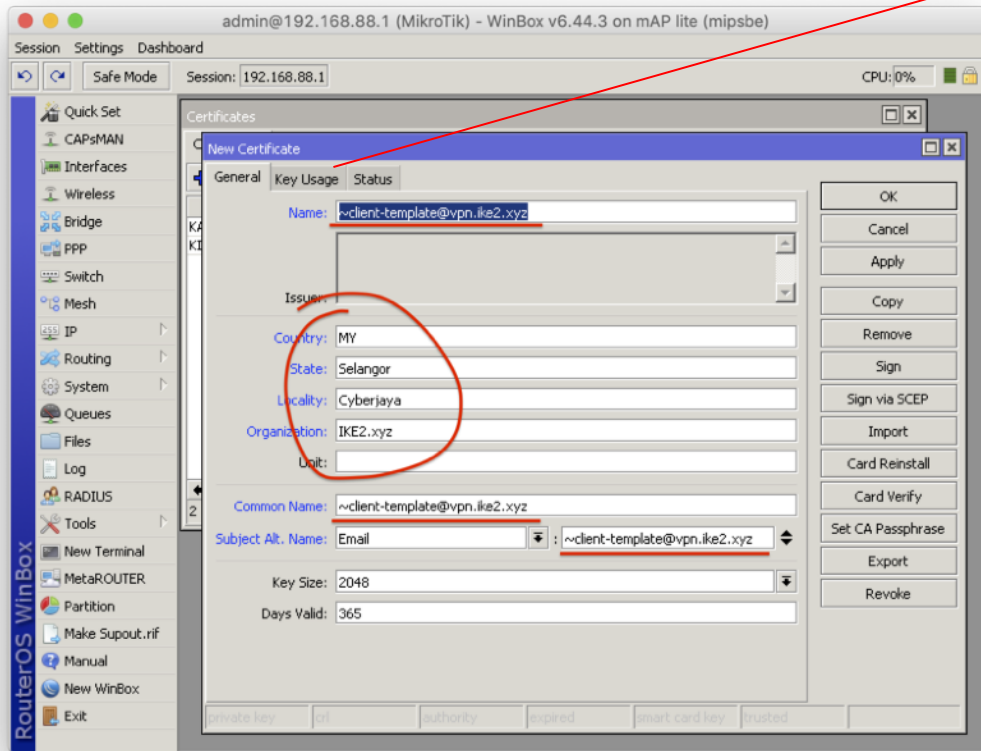


```
/certificate sign vpn.ike2.xyz
```

```
ca=CA.ike2.xyz
```

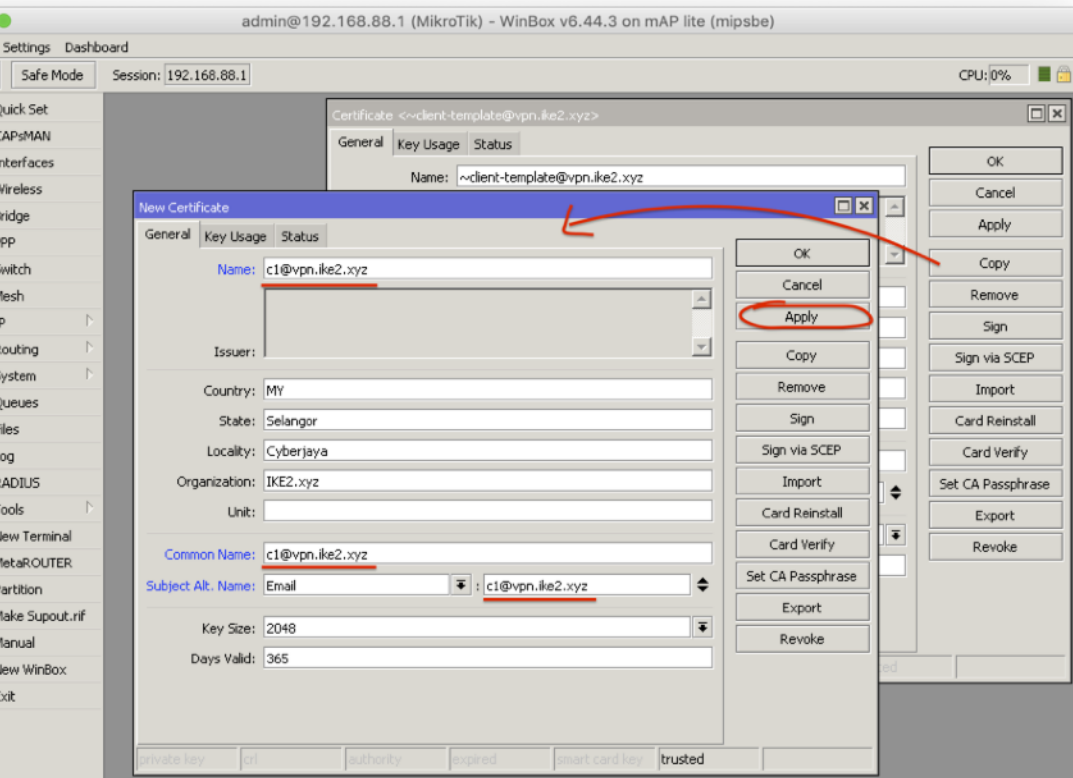
```
CN=CN*IK65*XΛΣ
```

Client certificate template



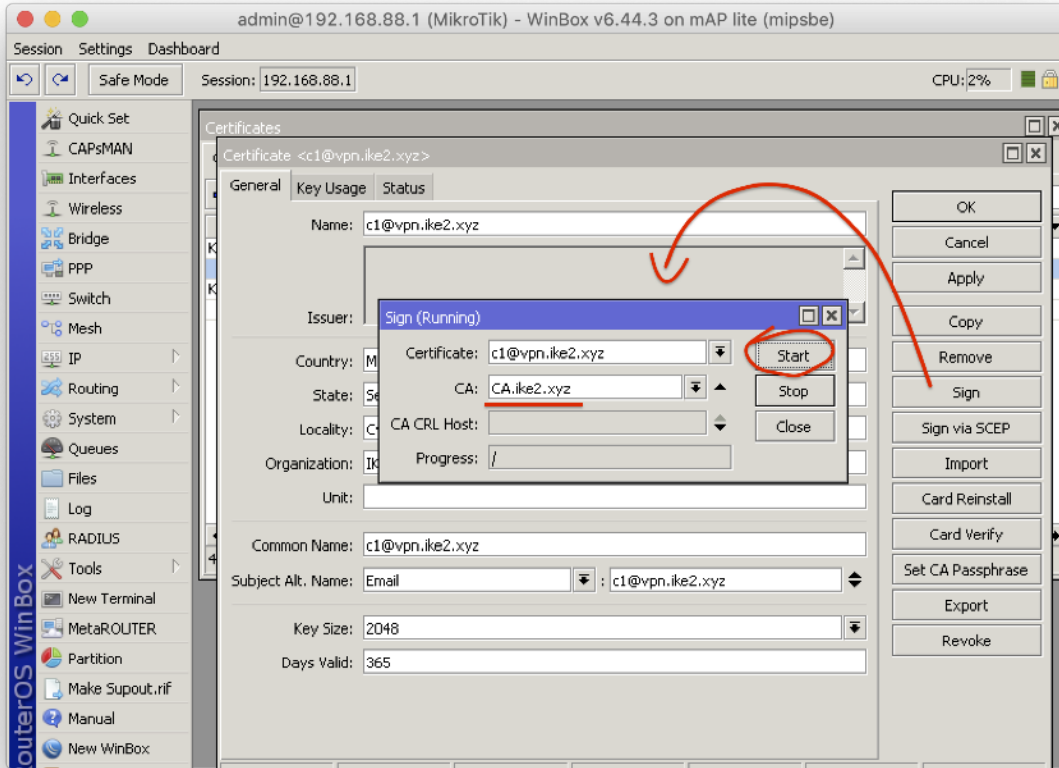
```
/certificate add name=~client-  
template@vpn.ike2.xyz country=MY  
state=Selangor locality=Cyberjaya  
organization=IKE2.xyz common-  
name=~client-template@vpn.ike2.xyz  
subject-alt-name=email::~client-  
template@vpn.ike2.xyz key-size=2048  
days-valid=365 trusted=yes key-  
usage=tls-client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

Generate client SSL certificate from template



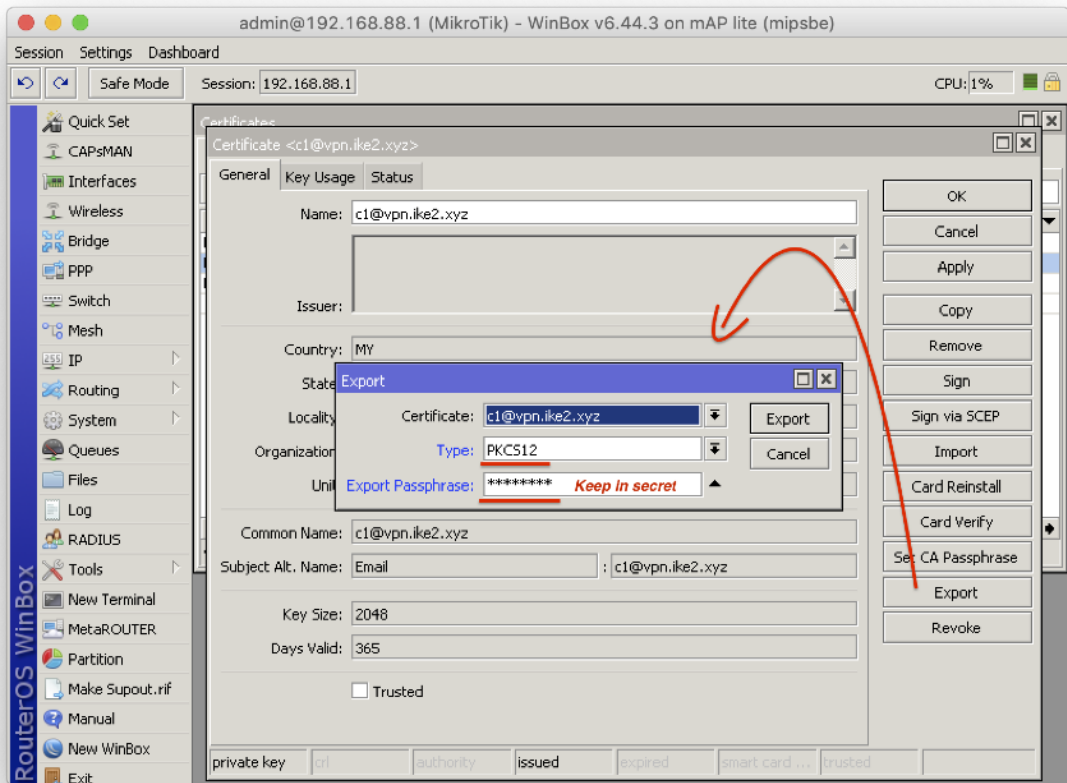
```
/certificate add copy-from=~client-  
template@vpn.ike2.xyz  
name=c1@vpn.ike2.xyz common-  
name=c1@vpn.ike2.xyz subject-alt-  
name=email:c1@vpn.ike2.xyz
```


Sign client SSL certificate with CA.ike2.xyz authority



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

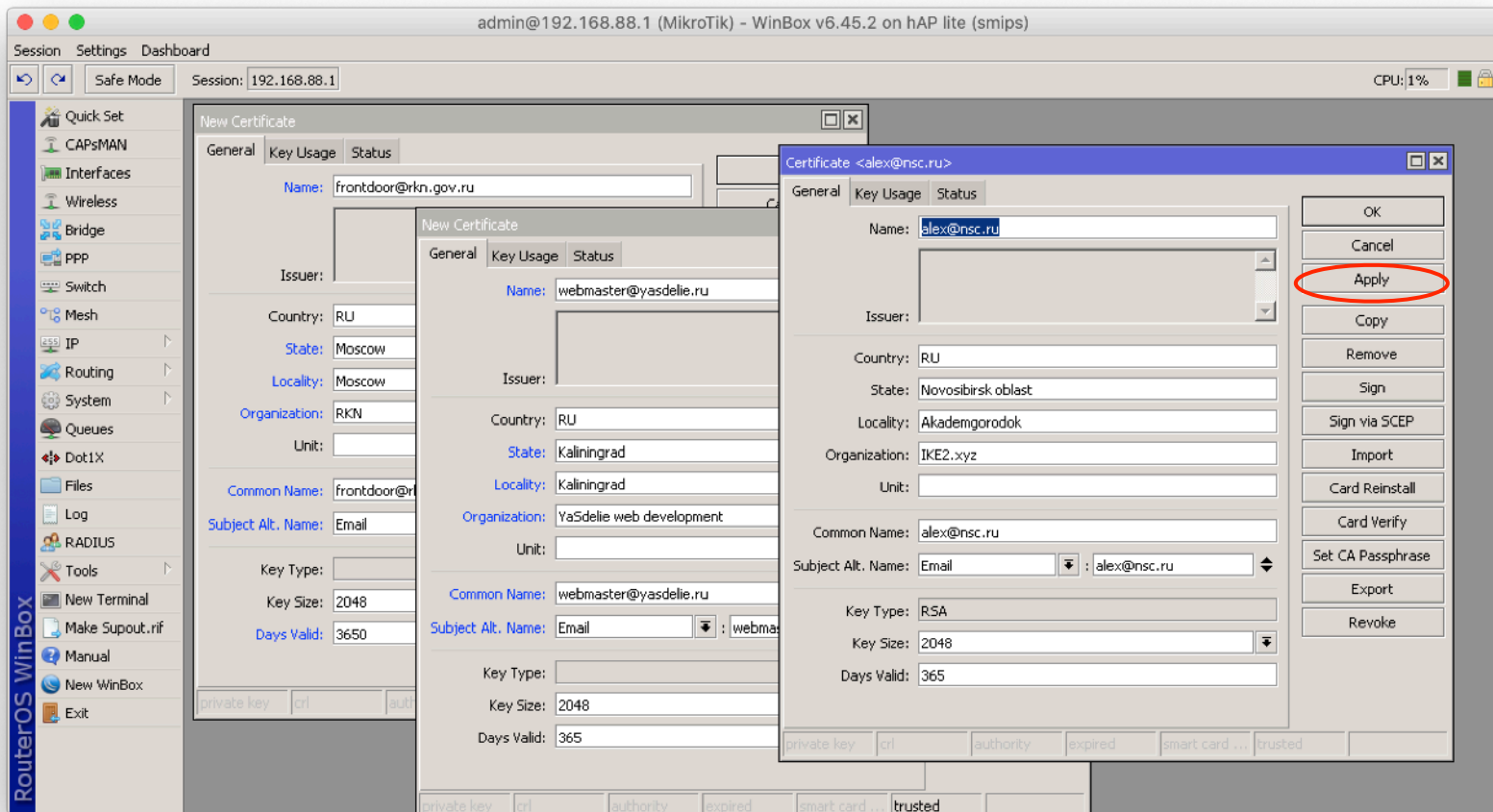
Export client SSL certificate + private key to .p12 file



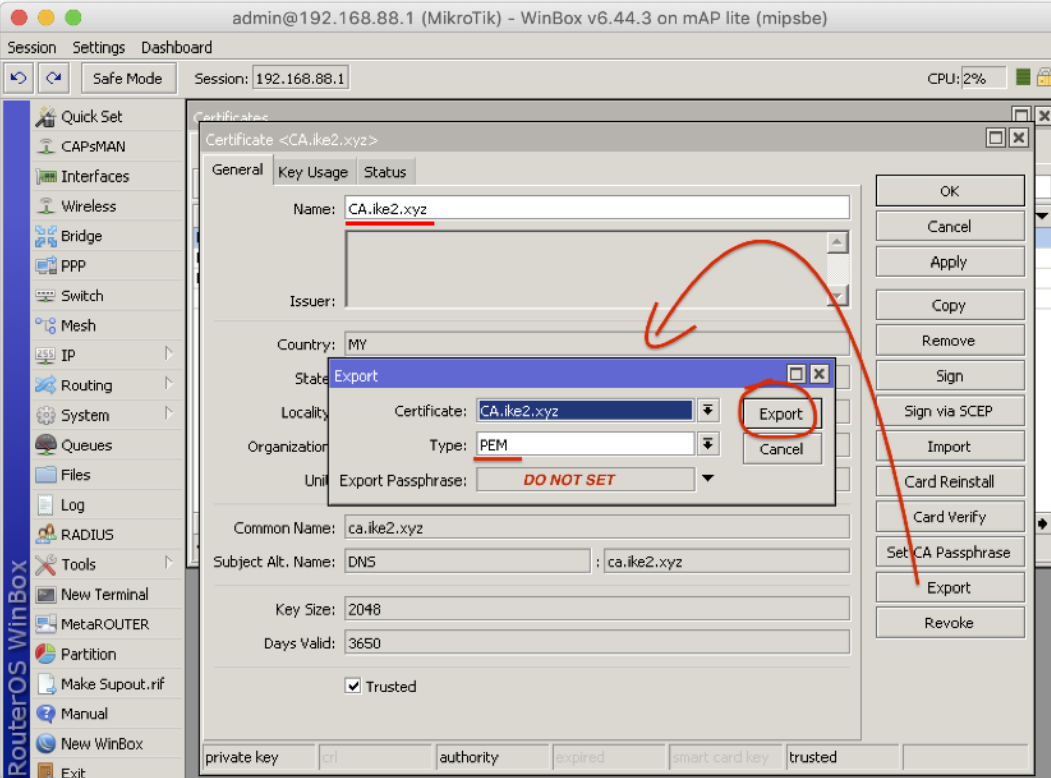
```
/certificate export-certificate  
c1@vpn.ike2.xyz type=pkcs12  
export-passphrase=keepinsecret
```

```
export-passphrase=keepinsecret
```

Generate various client SSL certificates from template (example)



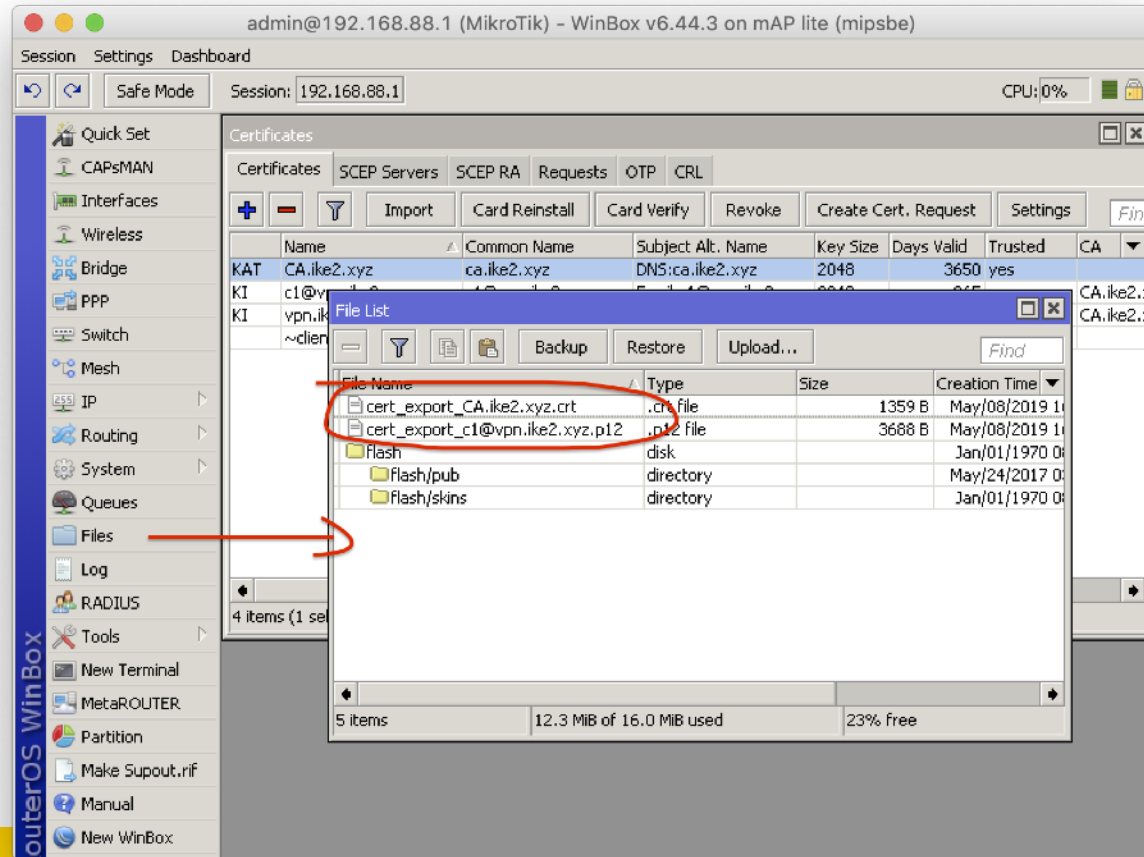
Export CA SSL certificate .crt file

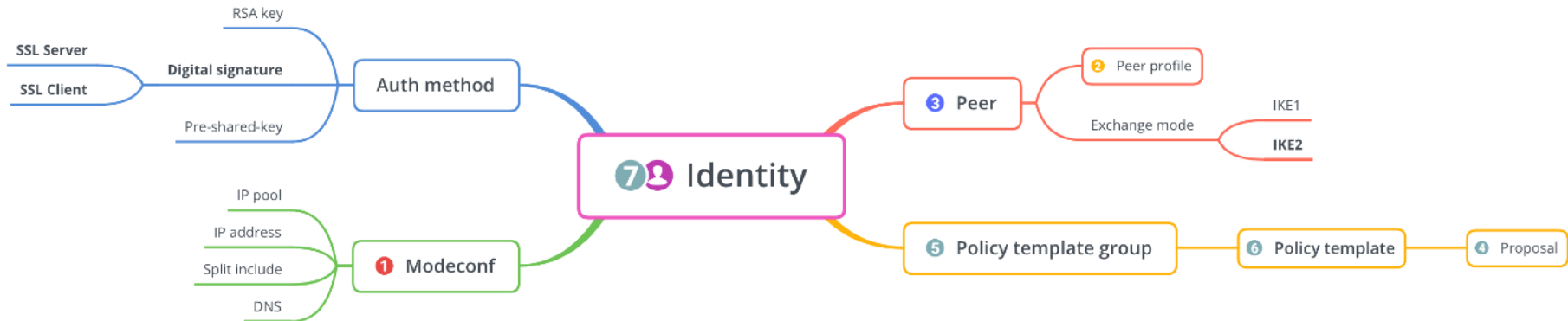


```
/certificate  
export-certificate CA.ike2.xyz  
type=pem  
fλbε=εσω
```

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

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;

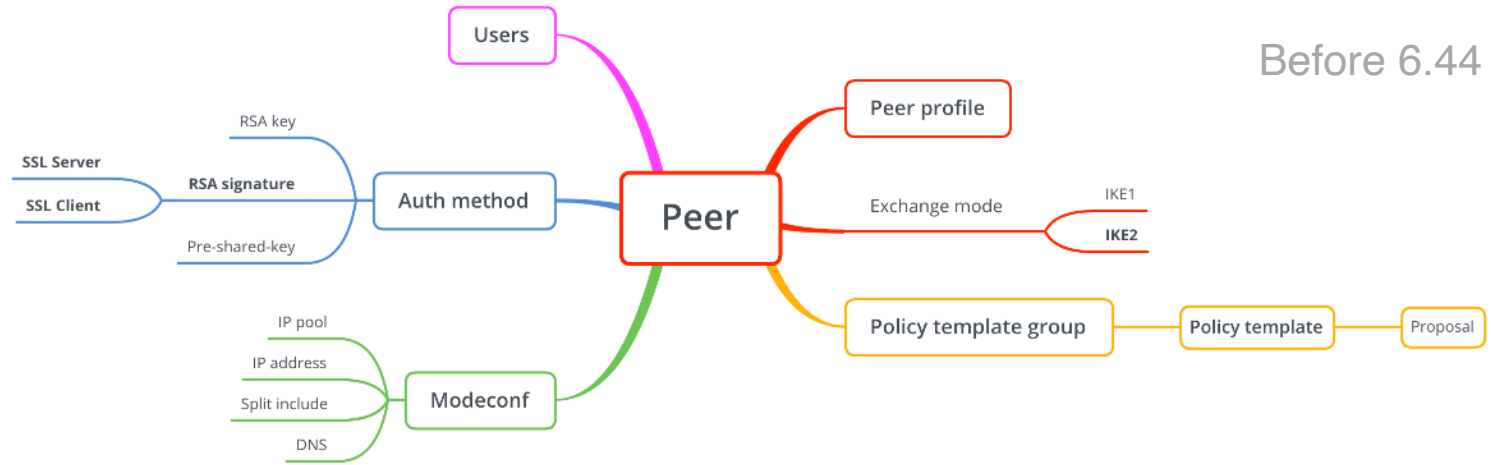
Key **ipsec** changes in RouterOS 6.44

- *) 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;

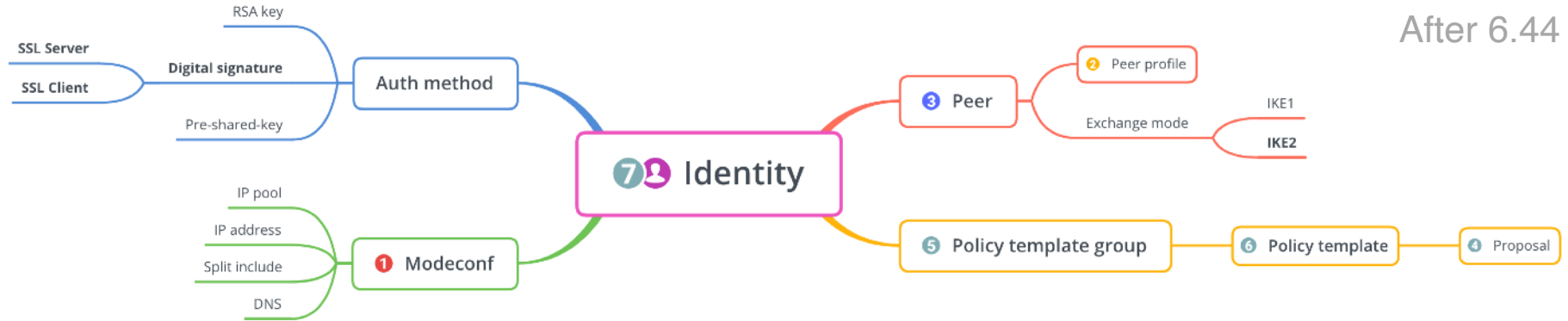
- *) ike2 - added option to specify certificate chain;
- *) ike2 - added peer identity validation for RSA auth (disabled after upgrade);
- *) ike2 - allow to match responder peer by "my-id=fqdn" field;
- *) ike2 - send split networks over DHCP (option 249) to Windows initiators if DHCP Inform is received;

IPSec structure

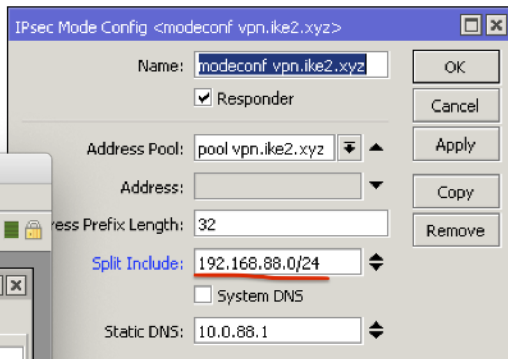
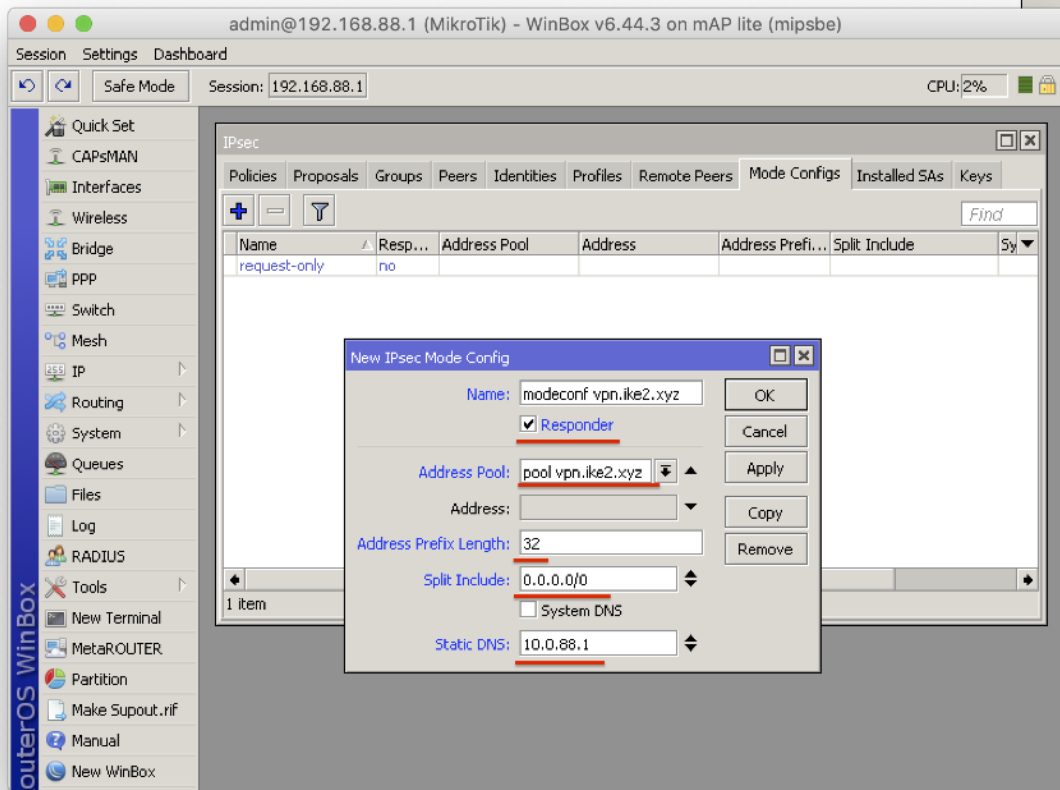
Before 6.44



After 6.44

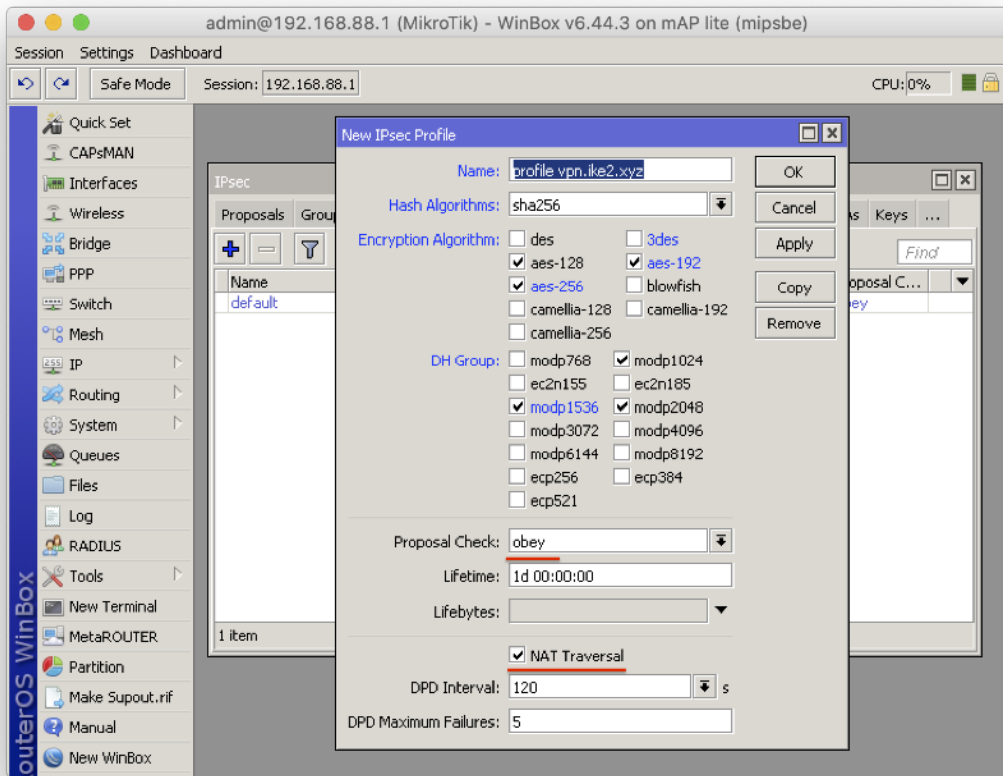


1. Setting up new IPsec mode config



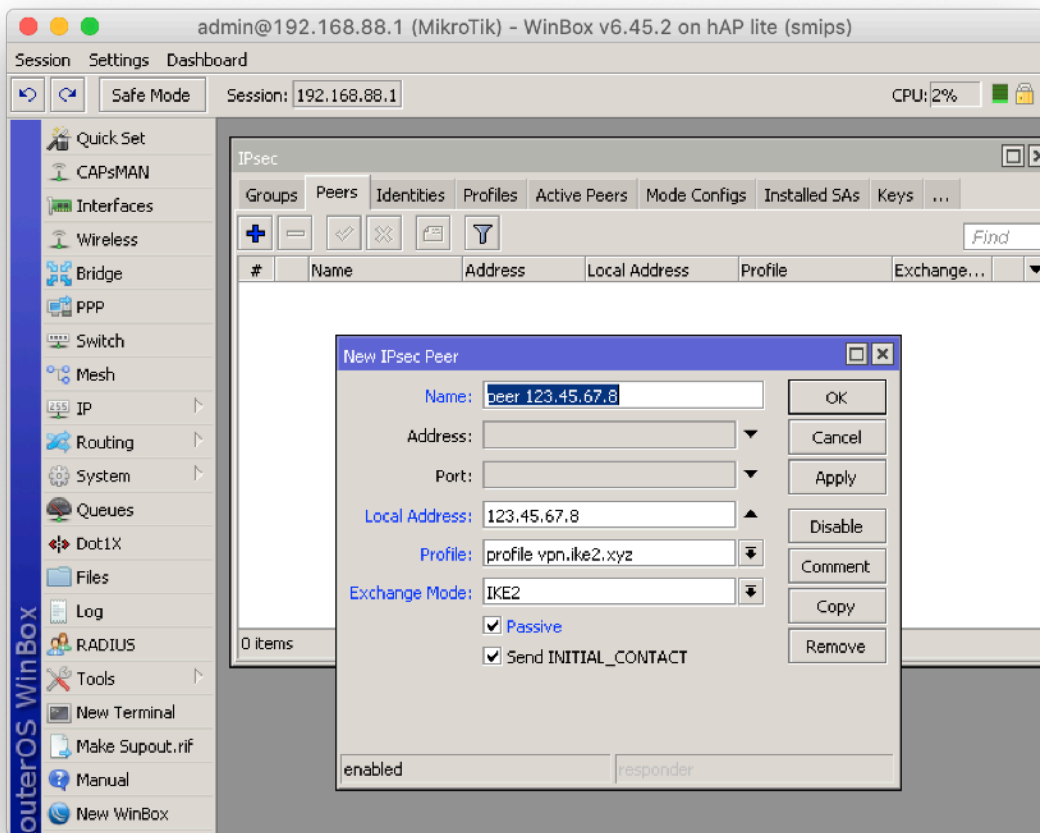
```
/ip ipsec mode-config
add address-pool="pool
vpn.ike2.xyz" address-prefix-
length=32 name="modeconf
vpn.ike2.xyz" split-
include=0.0.0.0/0 static-
dns=10.0.88.1 system-dns=no
```

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)

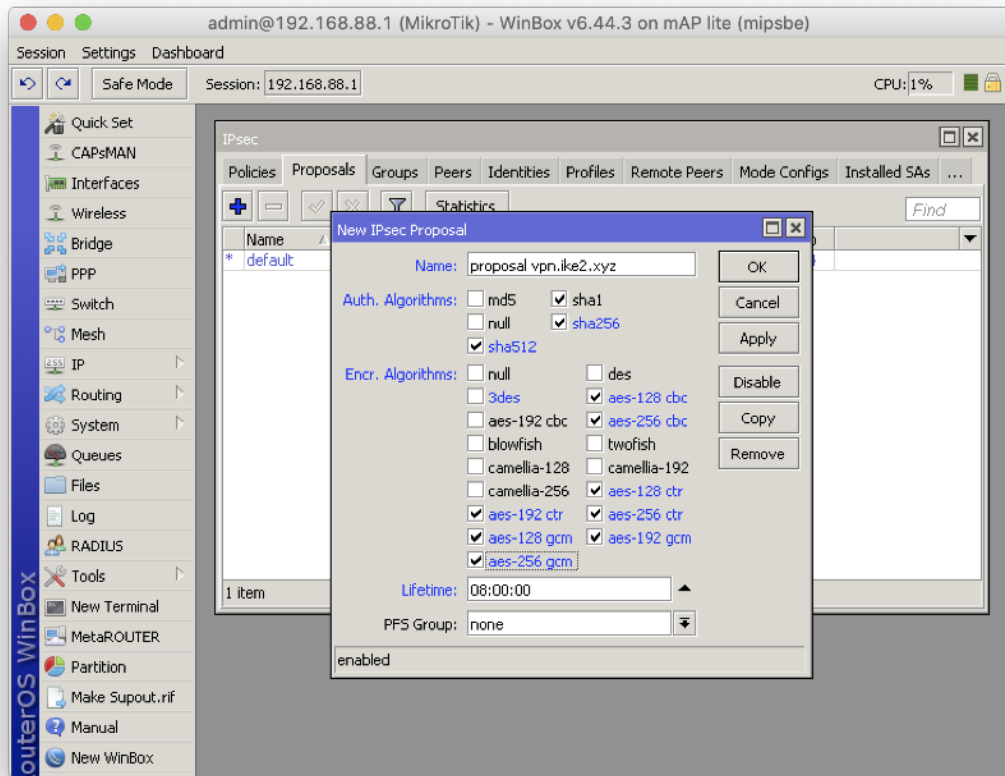


Accepting clients from all IP addresses **0.0.0.0/0**

Accepting clients on public IP address **123.45.67.8**

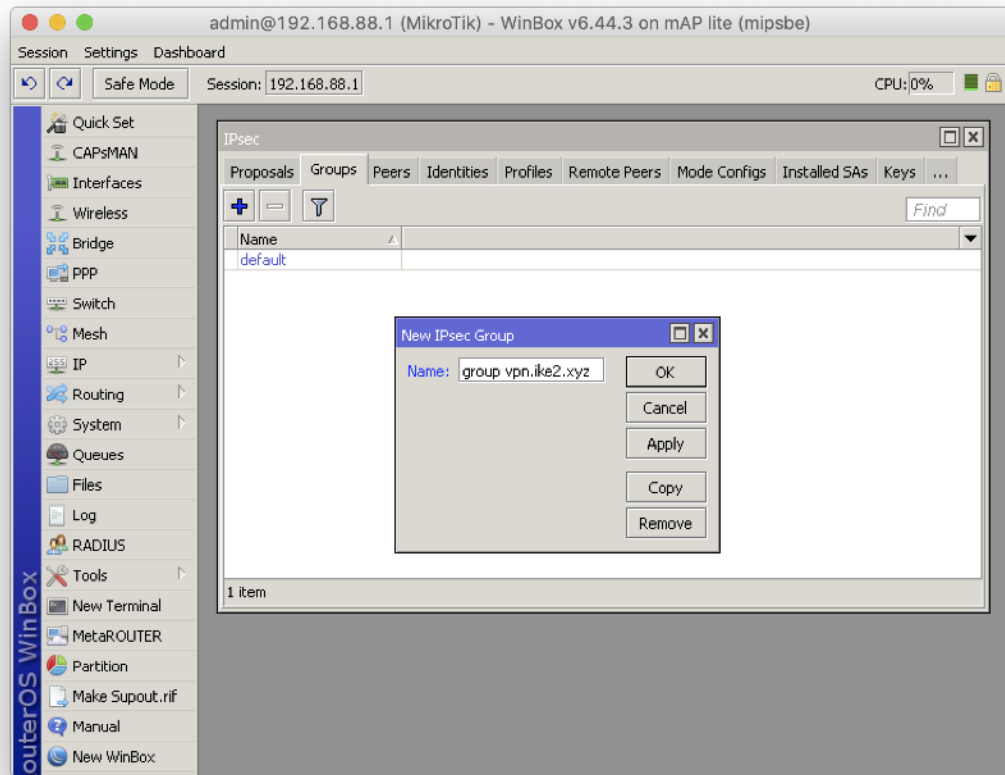
```
/ip ipsec peer add exchange-  
mode=ike2 address=0.0.0.0/0  
local-address=123.45.67.8  
name="peer 123.45.67.8"  
passive=yes send-initial-  
contact=yes profile="profile  
vpn.ike2.xyz"
```

4. Setting up new IPsec proposal (phase 2)



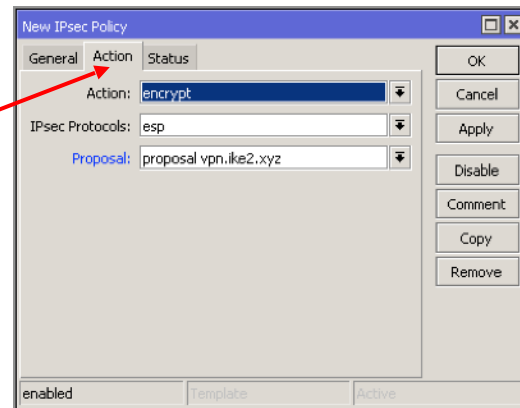
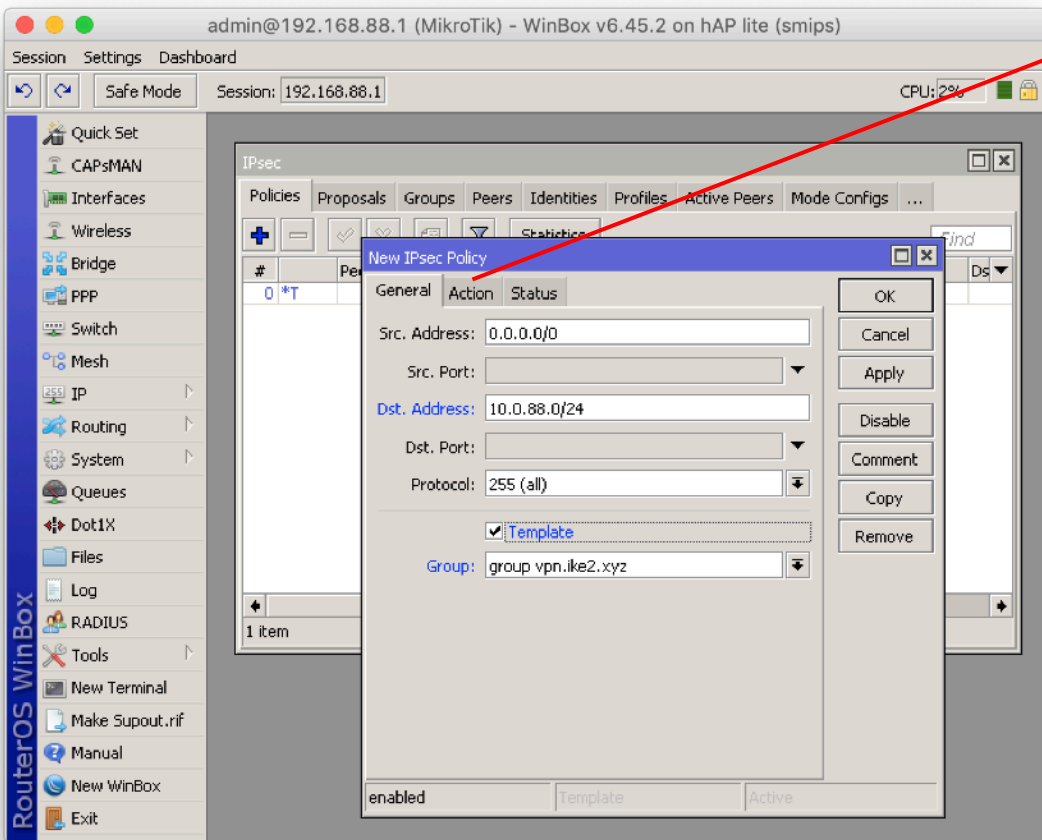
```
/ip ipsec proposal add auth-  
algorithms=sha512,sha256,sha1  
enc-algorithms=aes-256-  
cbc,aes-256-ctr,aes-256-  
gcm,aes-192-ctr,aes-192-  
gcm,aes-128-cbc,aes-128-  
ctr,aes-128-gcm lifetime=8h  
name="proposal vpn.ike2.xyz"  
pfs-group=none
```

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

admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)

Session: 192.168.88.1 CPU: 2%

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP Routing System Queues Dot1X Files Log RADIUS Tools New Terminal Make Supout.rif Manual New WinBox

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: frontdoor@rk

Policy Template Group: group vpn.ike2

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: frontdoor@rk

Match By: certificate

Mode Configuration: modeconf vpn.ike2

Generate Policy: port strict

enabled

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: admin@vpn.ike2.xyz

Policy Template Group: group vpn.ike2

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: admin@vpn.ike2.xyz

Match By: certificate

Mode Configuration: modeconf vpn.ike2

Generate Policy: port strict

enabled

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: alex@nsc.ru

Policy Template Group: group vpn.ike2

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: alex@nsc.ru

Match By: certificate

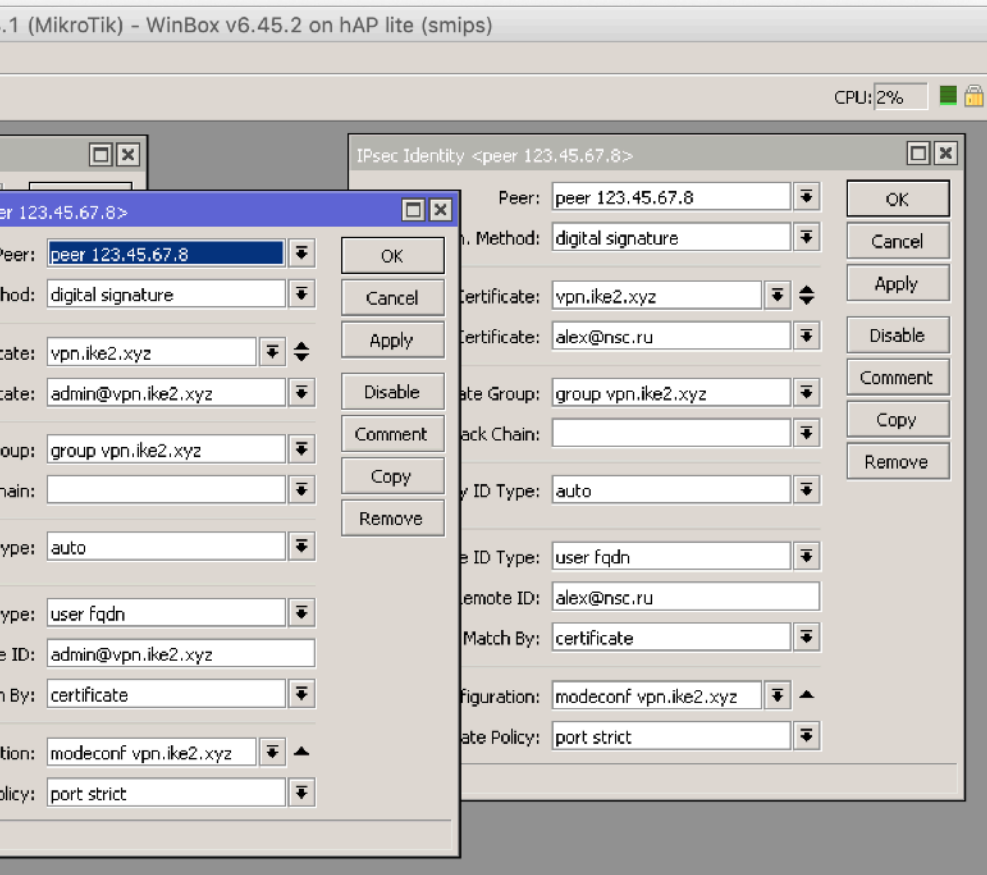
Mode Configuration: modeconf vpn.ike2

Generate Policy: port strict

OK Cancel Apply Disable Comment Copy Remove

```
/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
```

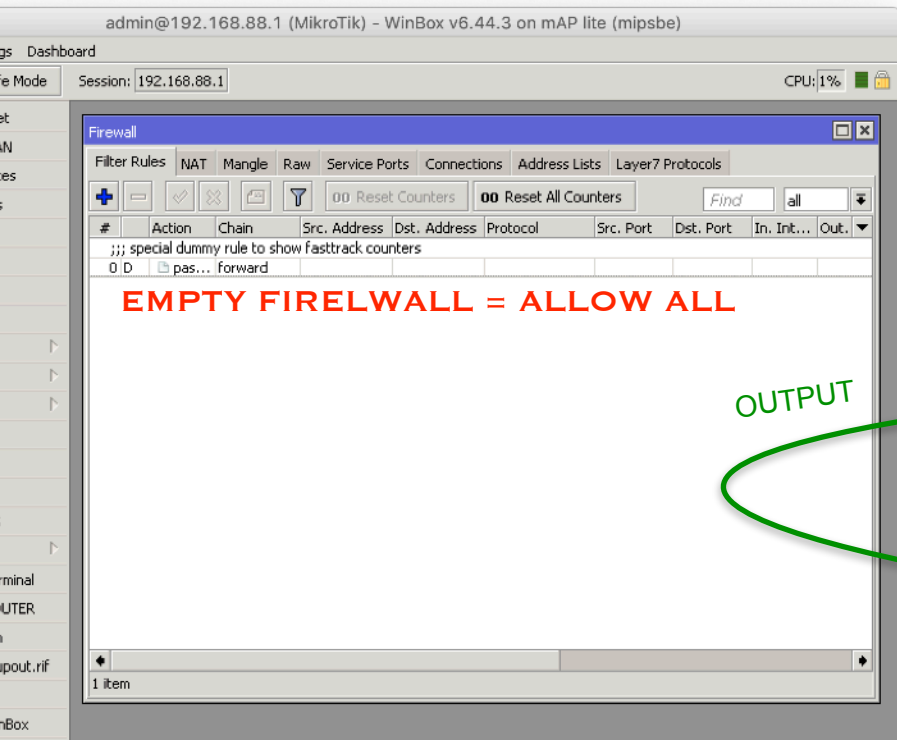
```
/ip ipsec identity add auth-method=digital-  
signature certificate=vpn.ike2.xyz remote-  
certificate=alex@nsc.ru generate-policy=port-strict  
match-by=certificate mode-config="modeconf  
vpn.ike2.xyz" peer="peer 123.45.67.8" policy-  
template-group="group vpn.ike2.xyz" remote-id=user-  
fqdn:alex@nsc.ru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

Setting up Firewall

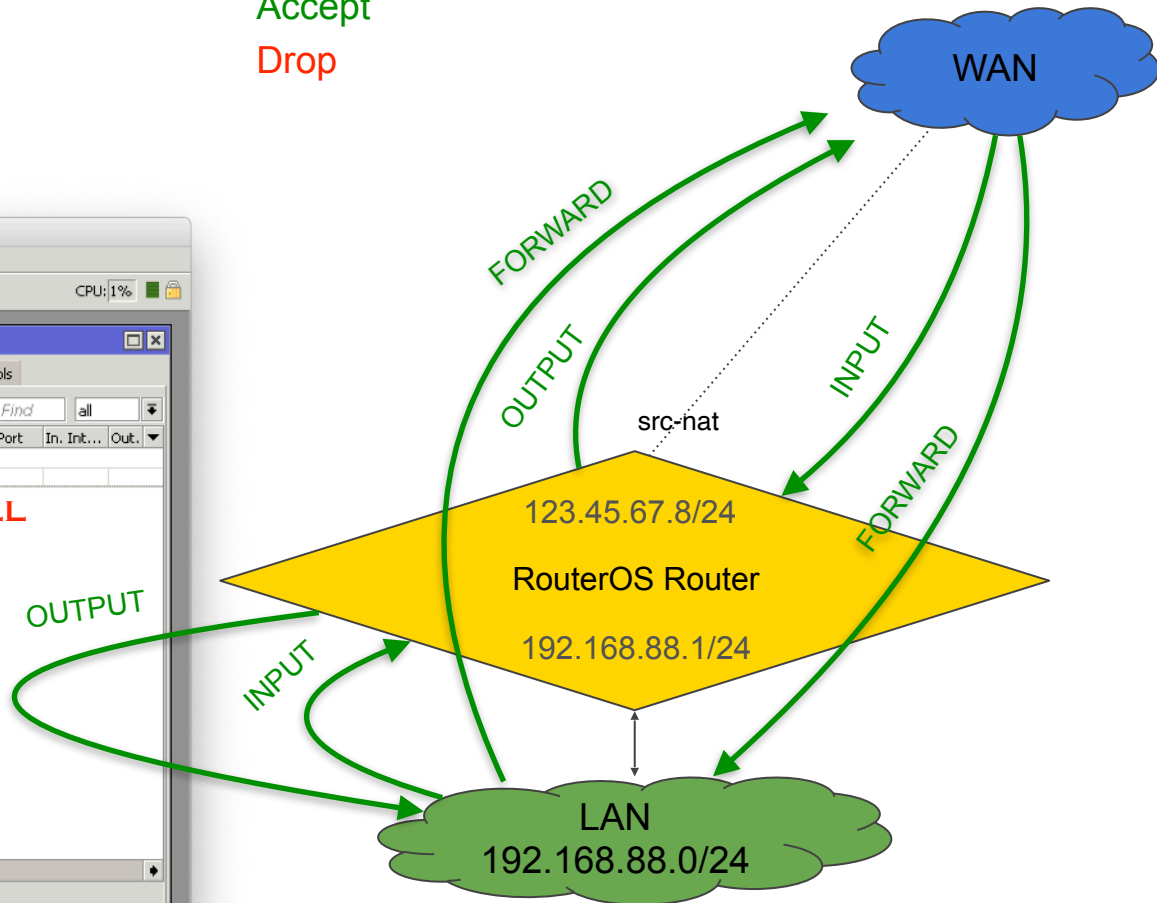
Understanding the default firewall filter

Important

Empty FIREWALL filter



Accept
Drop



RouterOS 6.45+ default configuration firewall overview

Firewall															
Filter Rules		NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols							
		00 Reset Counters		00 Reset All Counters		Find input									
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
;;; defconf: accept established,related,untracked															
1	acc...	input												5.5 MiB	61 567
;;; defconf: drop invalid															
2	drop	input												341 B	6
;;; defconf: accept ICMP															
3	acc...	input			1 (icmp)									0 B	0
;;; defconf: accept to local loopback (for CAPsMAN)															
4	acc...	input		127.0.0.1										0 B	0
;;; defconf: drop all not coming from LAN															
5	drop	input								!LAN				201.2 KiB	1 096
5 items out of 12															

Firewall															
Filter Rules		NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols							
     		 Reset Counters		 Reset All Counters		Find 									
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
;;; special dummy rule to show fasttrack counters															
0	D	pas...	forward											190.5 MiB	306 733
;;; defconf: accept in ipsec policy															
6		acc...	forward											0 B	0
;;; defconf: accept out ipsec policy															
7		acc...	forward											0 B	0
;;; defconf: fasttrack															
8		fas...	forward											8.0 MiB	53 920
;;; defconf: accept established,related, untracked															
9		acc...	forward											8.0 MiB	53 920
;;; defconf: drop invalid															
10		drop	forward											1060.4 KiB	1 893
;;; defconf: drop all from WAN not DSTNATed															
11		drop	forward								WAN			0 B	0
7 items out of 12															

#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
```

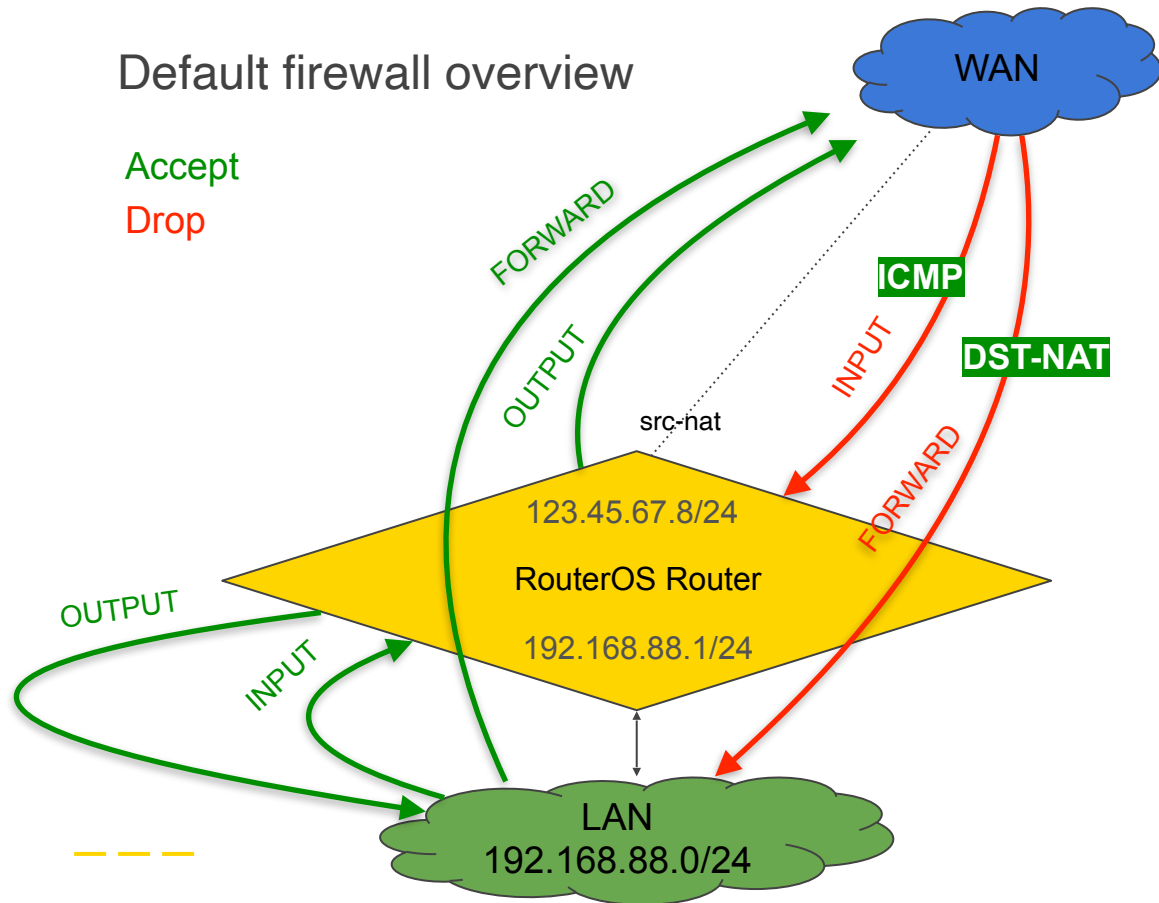
```
add action=accept chain=forward comment="defconf: accept established,related, untracked" connection-  
state=established,related,untracked
```

```
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

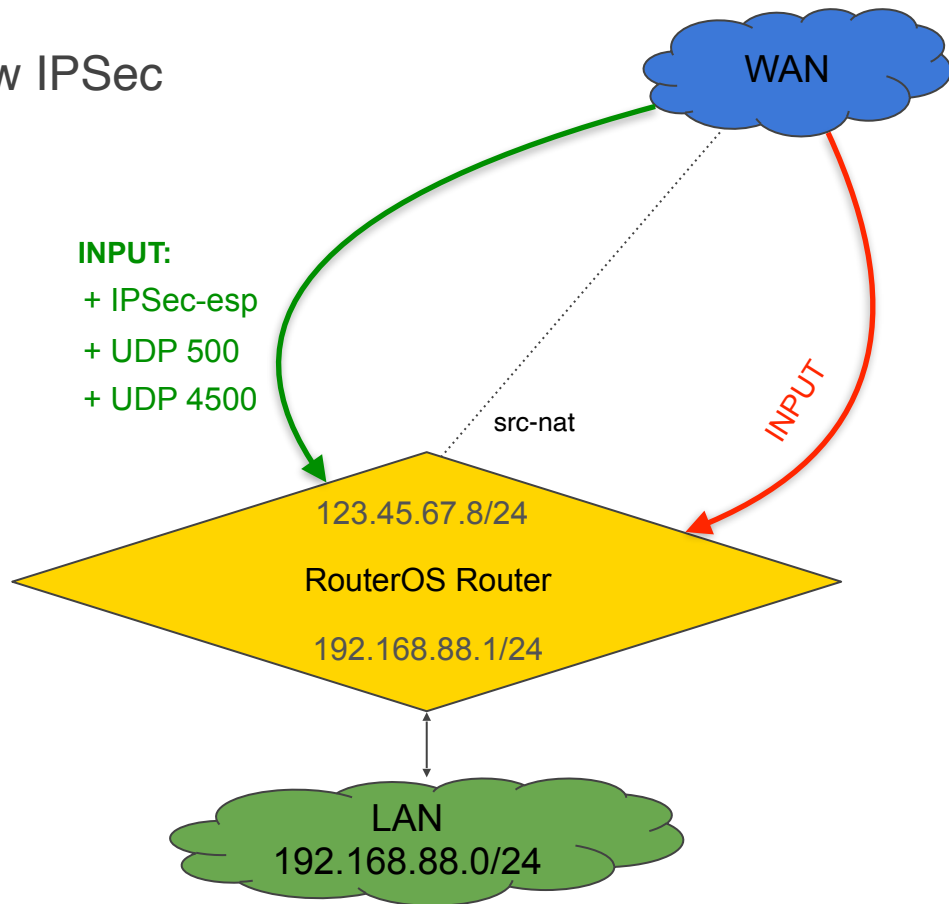
1. Default firewall overview
2. Allow IPsec



Setting up Firewall

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

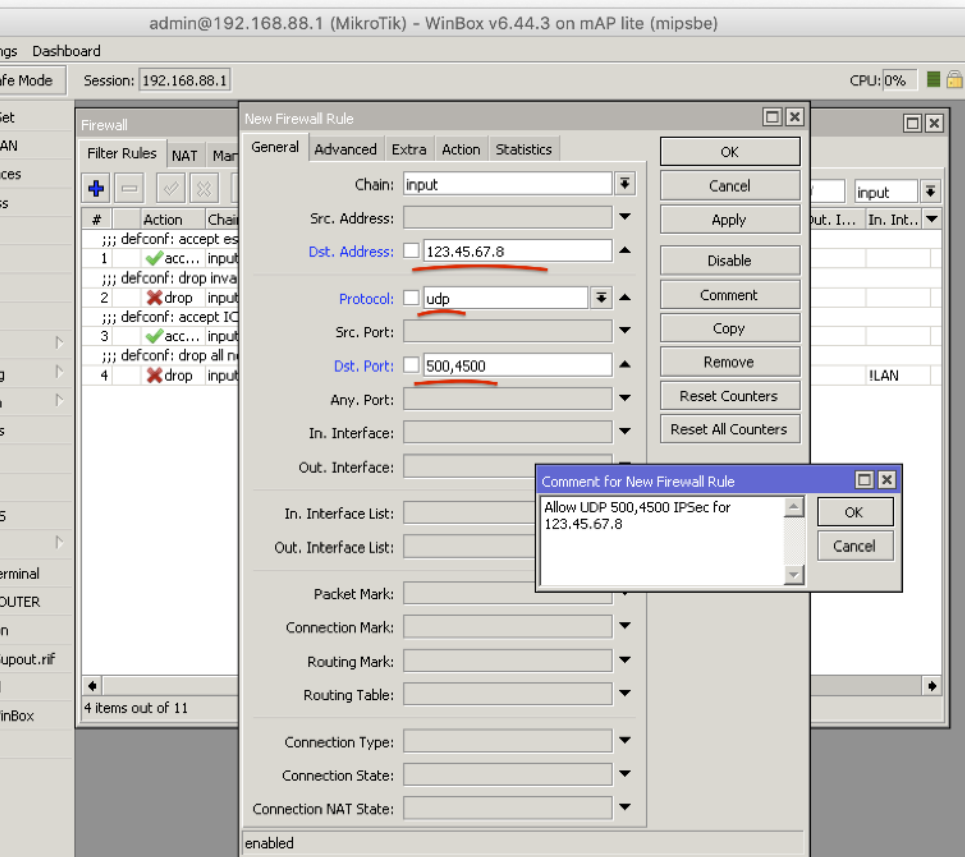
Allow IPSec



Firewall filter rules for IPSec packets (defconf)

INPUT chain

+ UDP 500
+ UDP 4500

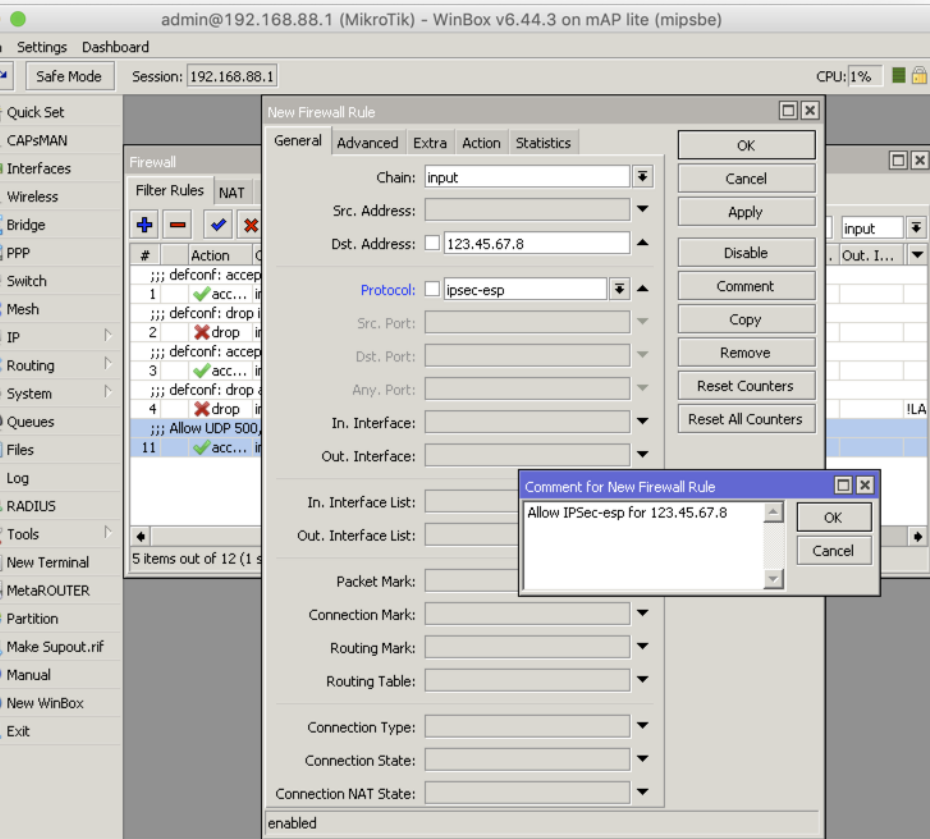


```
/ip firewall filter add place-  
before=[ find where  
comment~"defconf: drop all not  
coming from LAN" ] protocol=udp dst-  
port=500,4500 dst-  
address=123.45.67.8 action=accept  
chain=input comment="Allow UDP  
500,4500 IPSec for 123.45.67.8"
```

Firewall filter rules for IPSec packets (defconf)

INPUT chain

+ IPSec-esp (protocol 50)

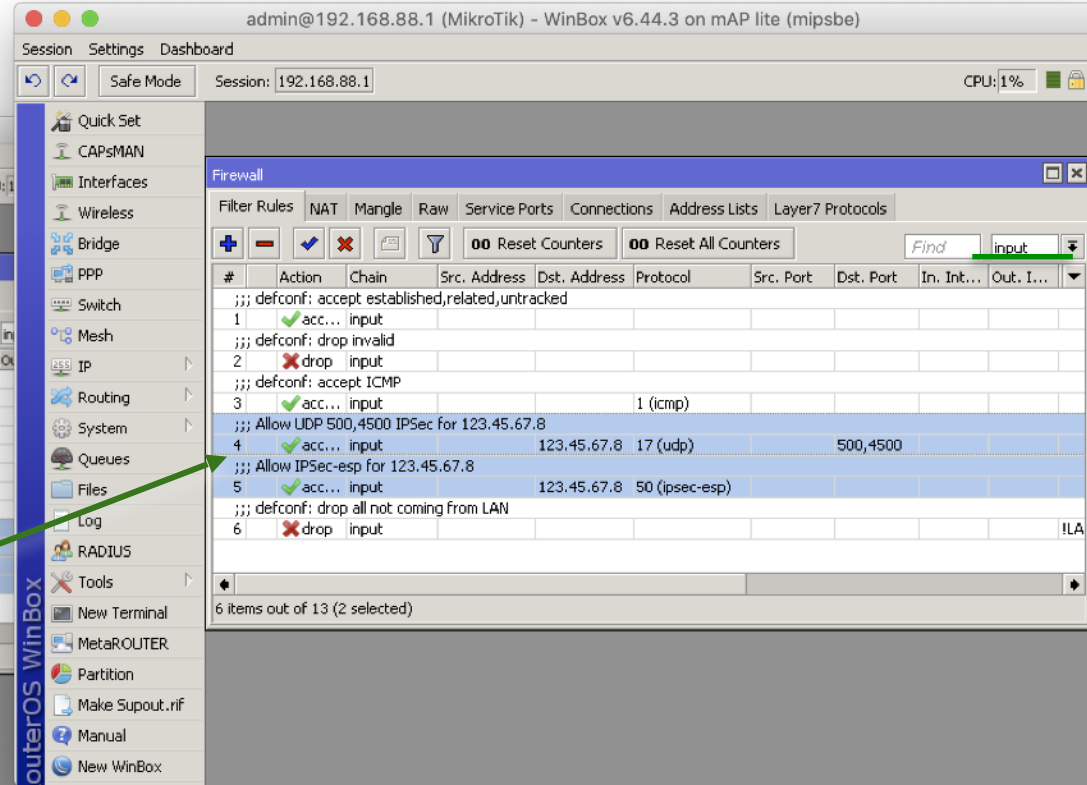
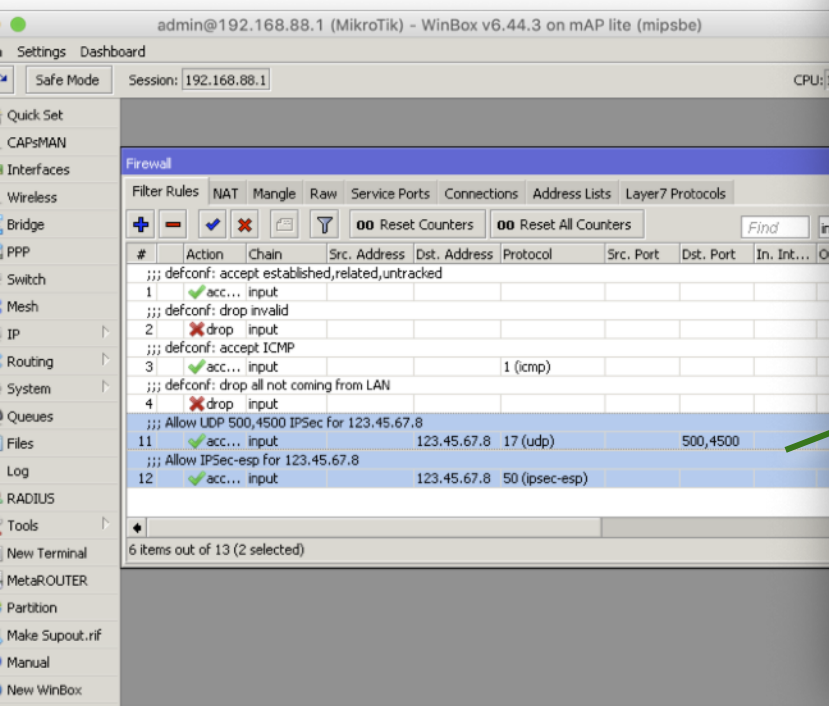


```
/ip firewall filter add place-  
before=[ find where  
comment~"defconf: drop all not  
coming from LAN" ] protocol=ipsec-  
esp dst-address=123.45.67.8  
action=accept chain=input  
comment="Allow IPSec-esp for  
123.45.67.8"
```

REorder firewall filter rules for IPSec packets (defconf)

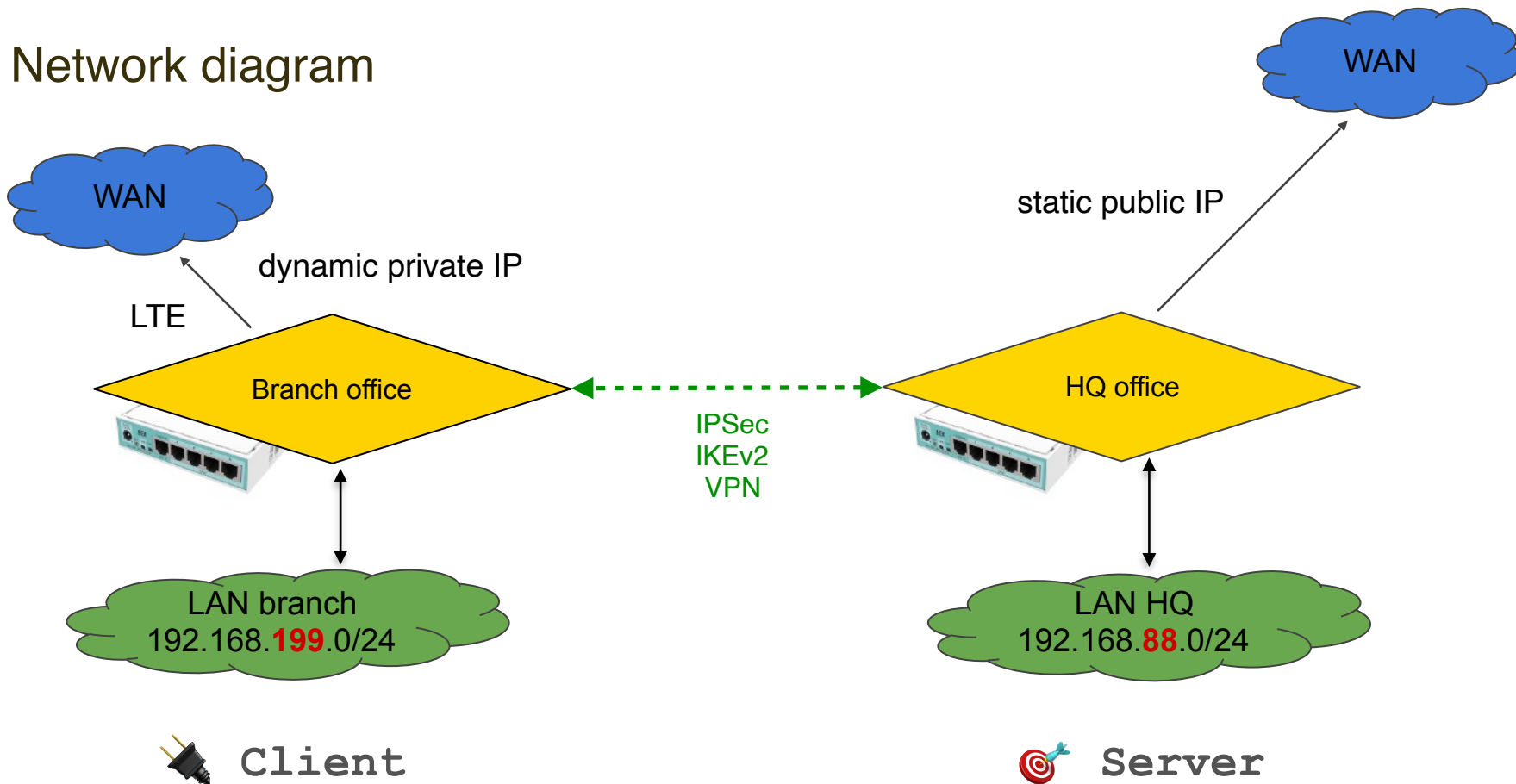
INPUT chain

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



RouterOS IPSec IKEv2 server ready

Network diagram

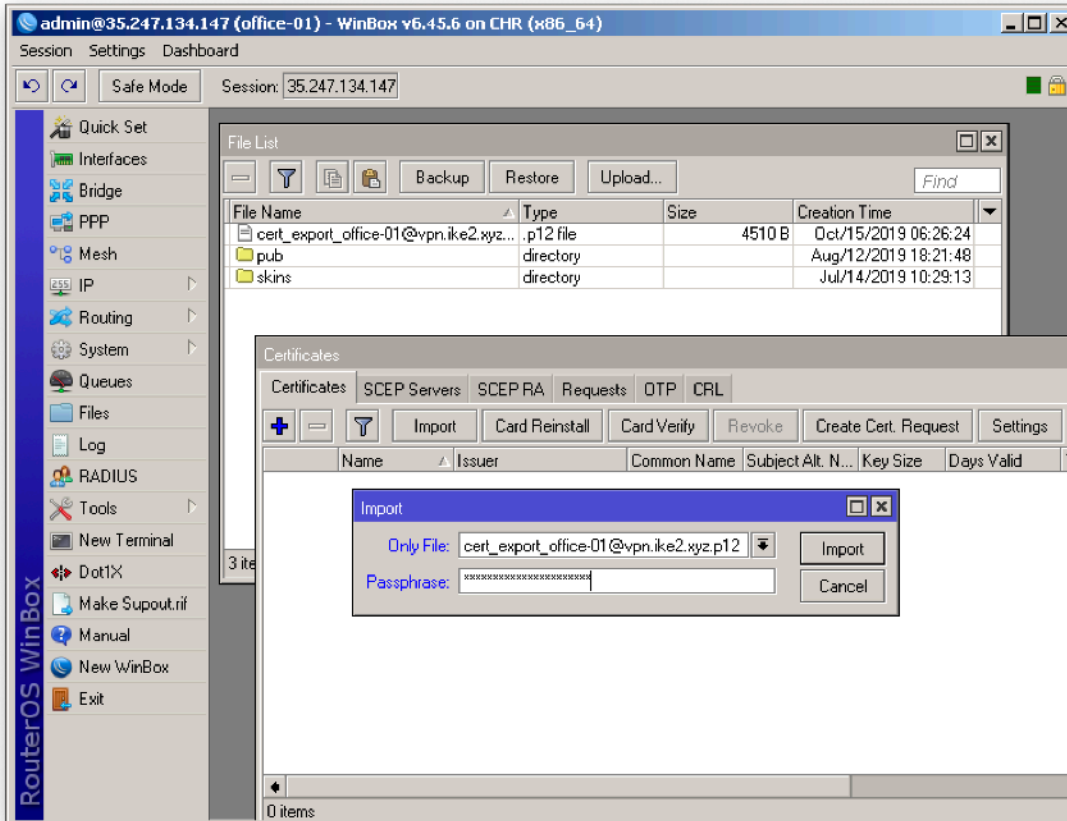


Setting up client RouterOS

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



admin@35.247.134.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 35.247.134.147

Certificates

Certificates SCEP Servers SCEP RA Requests OTP CRL

+ - Import Card Reinstall Card Verify Revoke Create Cert. Request Settings

	Name	Issuer	Common Name	Subject Alt.
AT	ca.ike2.xyz	C=RU,ST=Mosco...	ca.ike2.xyz	DNS:ca.ike2.x...
KT	office-01@vpn.ike2.xyz	C=RU,ST=Mosco...	office-01@vpn.ike2.xyz	Email:office-01...

Import

Only File: cert_export_office-01@vpn.ike2.xyz.p12

Passphrase: *****

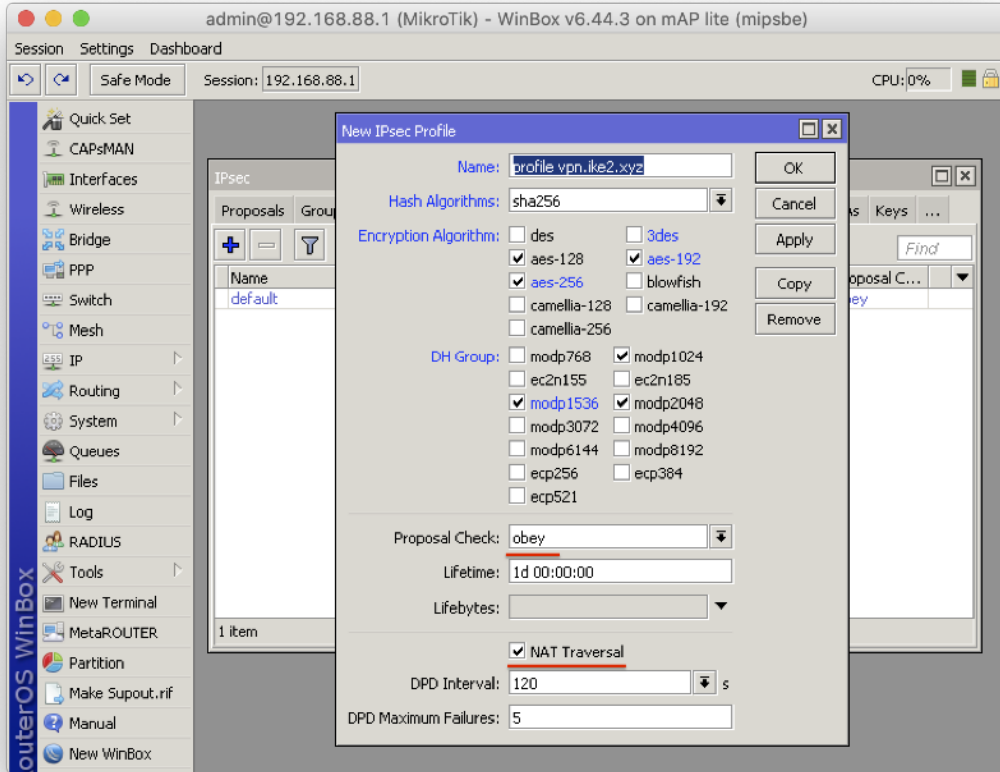
2 items (1 selected)

2 items (2 selected)

routerOS WinBox

- Quick Set
- Interfaces
- Bridge
- PPP
- Mesh
- IP
- Routing
- System
- Queues
- Files
- Log
- RADIUS
- Tools
- New Terminal
- DotIX
- Make Supout.tif
- Manual
- New WinBox

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

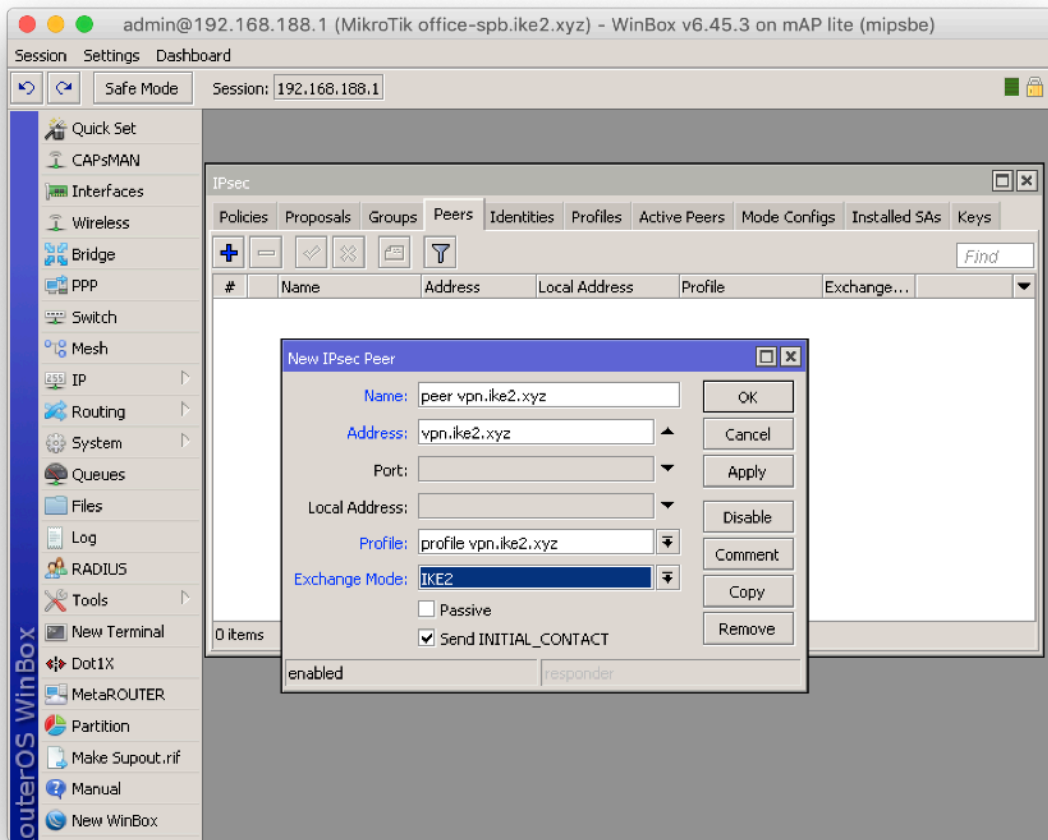


```
/ip ipsec profile add dh-  
group=modp2048,modp1536,modp10  
24 enc-  
algorithm=aes-256,aes-192,aes-  
128 hash-algorithm=sha256  
name="profile.vpn.ike2.xyz"  
nat-traversal=yes proposal-  
check=obey
```

Adding new client IPsec peer (initiator)



Client

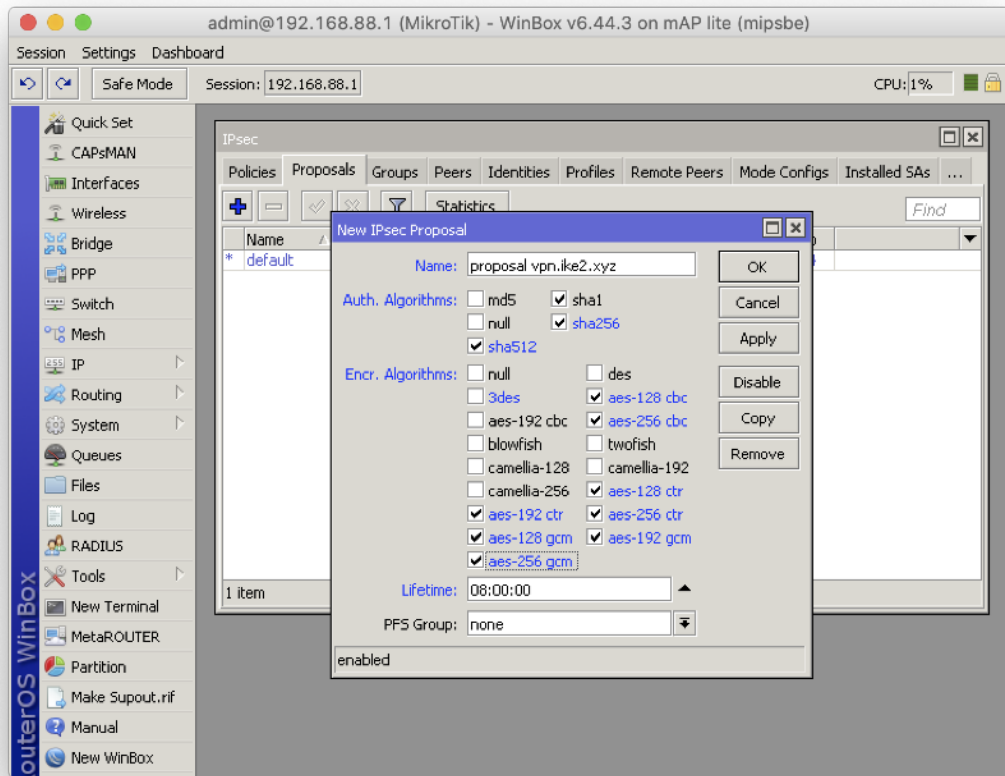


```
/ip ipsec peer  
add address=vpn.ike2.xyz exchange-  
mode=ike2 name="peer vpn.ike2.xyz"  
profile="profile vpn.ike2.xyz"
```

```
blotifg=„blotifg Abu*Jk65*xλs,,
```



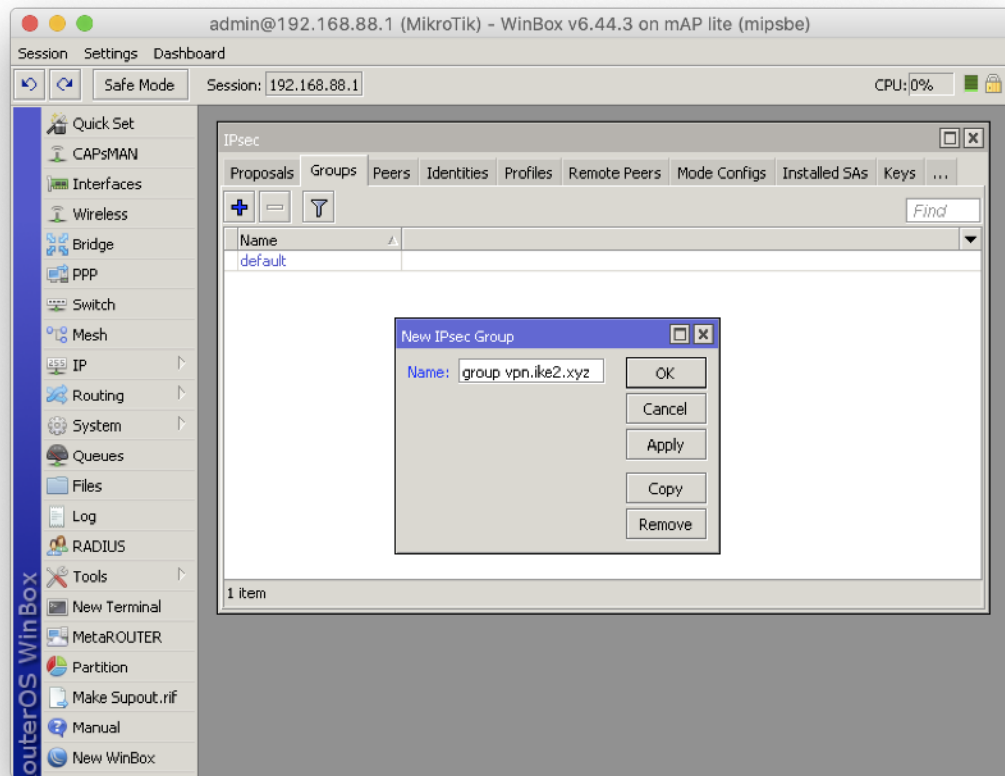
Setting up new IPsec proposal (phase 2)



```
/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
```



Adding new IPsec policy group



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



Adding new IPsec policy template



Client

34.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Session: 35.247.134.147

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs ...

Find

#	Peer	Tunnel	Src. Address	Src. Port	Dst. Address
0	T		::/0		::/0
1	T		10.0.88.0/24		0.0.0.0/0

IPsec Policy <10.0.88.0/24:0>0.0.0.0/0:0>

General Action Status

Src. Address: 10.0.88.0/24

Src. Port:

Dst. Address: 0.0.0.0/0

Dst. Port:

Protocol: 255 (all)

☒ Template

Group: group vpn.ike2.xyz

enabled Template Active

New IPsec Policy

General Action Status

Action: encrypt

IPsec Protocols: esp

Proposal: proposal vpn.ike2.xyz

OK Cancel Apply Disable Comment Copy Remove

enabled Template Active

```
/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

247.134.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Dashboard

Session: 35.247.134.147

IPsec Identity <peer vpn.ike2.xyz>

Group: [peer vpn.ike2.xyz] OK Cancel

Auth. Method: digital signature Apply

Certificate: office-01@vpn.ike2.xyz Disable

Remote Certificate: none Comment

Policy Template Group: group vpn.ike2.xyz Copy

Notrack Chain: Remove

My ID Type: user fqdn

My ID: office-01@vpn.ike2.xyz

Remote ID Type: fqdn

Remote ID: vpn.ike2.xyz

Match By: remote id

Mode Configuration: request-only

Generate Policy: port strict

```
/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
```

Имя клиента: vpn.ike2.xyz

Имя клиента: vpn.ike2.xyz

Nikita Tarikin / nikita@tarikin.com



Cross-check IPSec identity (example)



Server



Client

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: office-spb@vpn.ike2.xyz

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: fqdn

My ID: vpn.ike2.xyz

Remote ID Type: user fqdn

Remote ID: office-spb@vpn.ike2.xyz

Match By: certificate

Mode Configuration: modeconf vpn.ike2.xyz

Generate Policy: port strict

enabled

IPsec Identity <peer vpn.ike2.xyz>

Peer: peer vpn.ike2.xyz

Auth. Method: digital signature

Certificate: office-spb@vpn.ike2.xyz

Remote Certificate: none

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: user fqdn

My ID: office-spb@vpn.ike2.xyz

Remote ID Type: fqdn

Remote ID: vpn.ike2.xyz

Match By: remote id

Mode Configuration: modeconf office-spb@vpn.ike2.xyz

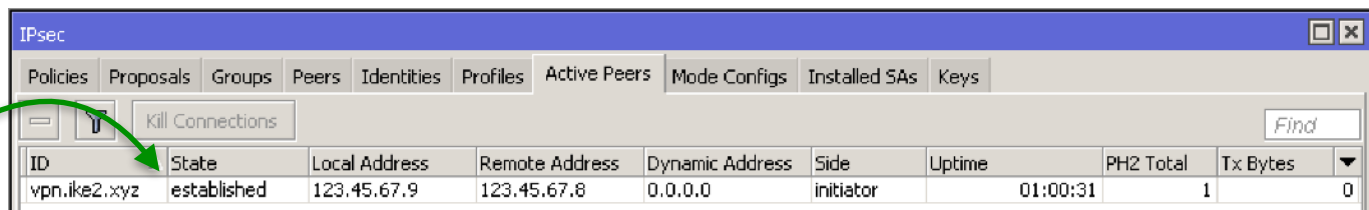
Generate Policy: port strict

enabled

Testing the IKEv2 connectivity



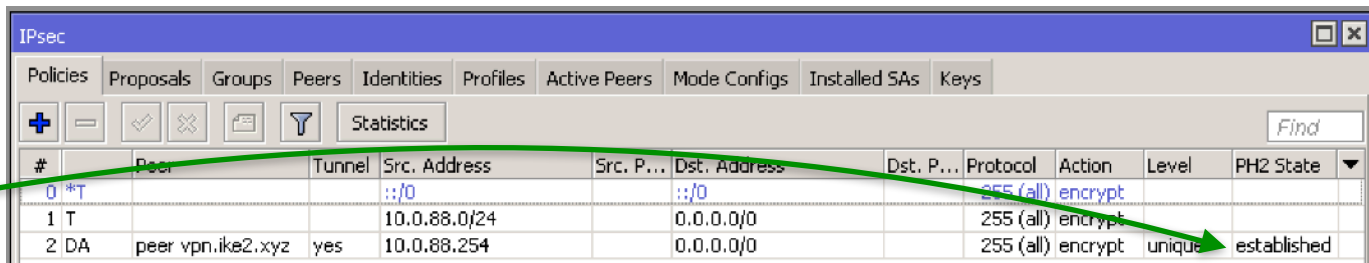
Active peers
state: **established**

A screenshot of the IPsec configuration window, specifically the "Active Peers" tab. A green arrow points from the text "state: established" to the "State" column of the table.

ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	PH2 Total	Tx Bytes
vpn.ike2.xyz	established	123.45.67.9	123.45.67.8	0.0.0.0	initiator	01:00:31	1	0

Dynamic Active (DA)
IPSec policy
generated from
Template (T)

PH2 state:
established

A screenshot of the IPsec configuration window, specifically the "Policies" tab. A green arrow points from the text "PH2 state: established" to the "PH2 State" column of the table.

#	Peer	Tunnel	Src. Address	Src. P...	Dst. Address	Dst. P...	Protocol	Action	Level	PH2 State
0	*T		::/0		::/0		255 (all)	encrypt		
1	T		10.0.88.0/24		0.0.0.0/0		255 (all)	encrypt		
2	DA	peer vpn.ike2.xyz	yes	10.0.88.254		0.0.0.0/0	255 (all)	encrypt	unique	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

admin@35.247.134.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 35.247.134.147

Quick Set
Interfaces
Bridge
PPP
Mesh
IP
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Make Supout.tif
Manual
New WinBox

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs ...

+ - [check] [x] [info] [filter] Statistics Find

#	Peer	Tunnel	Src. Address	Src. Port	Dst. Address
0	T		:::0		:::0
1	T		10.0.88.0/24		0.0.0.0/0
2	DA peer vpn.ike2.xyz	yes	10.0.88.254		0.0.0.0/0

Address List

+ - [check] [x] [info] [filter] Find

	Address	Network	Interface
D	10.0.88.254	10.0.88.254	ether1
D	10.148.0.7	10.148.0.1	ether1
	192.168.199.1/24	192.168.199.0	bridge

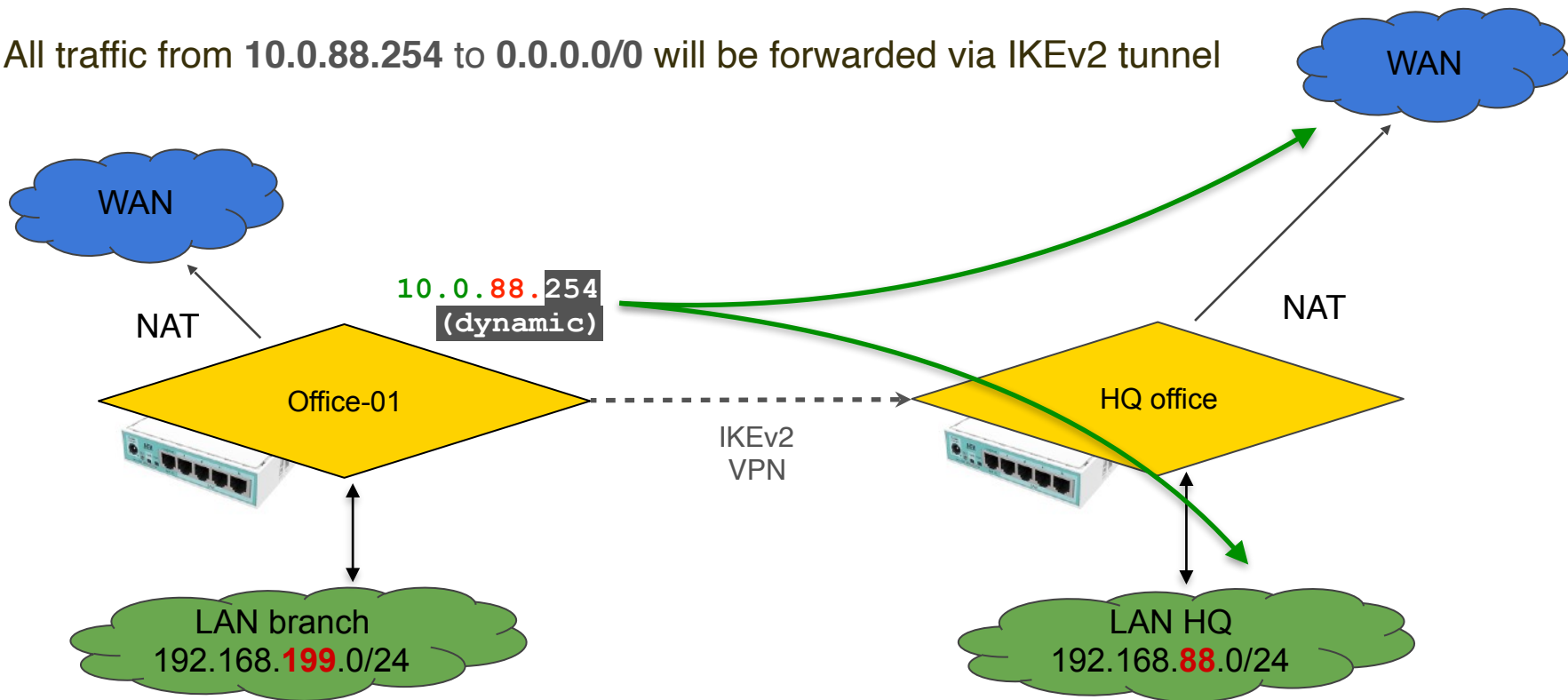
3 items (1 selected)

3 items

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

admin@35.247.134.147 (office-01) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Session: 35.247.134.147

IPsec

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

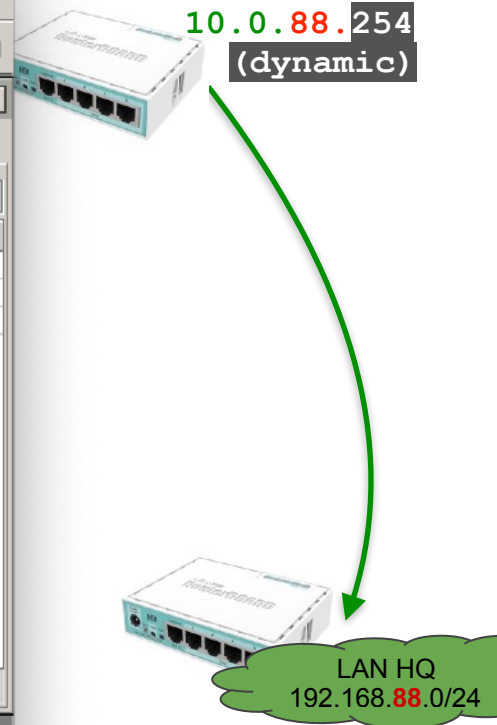
Statistics Find

#	Peer	Tunnel	Src. Address	Src. P...	Dst. Address	Dst. P...	Prot...	Action	Level	PH2 State
0	*T		::/0		::/0		255 ...	encrypt		
1	T		10.0.88.0/24		0.0.0.0/0		255 ...	encrypt		
2	DA peer vpn.ike2.xyz	yes	10.0.88.254		0.0.0.0/0		255 ...	encrypt	unique	established

Terminal

```
[admin@office-01] >
[admin@office-01] >
[admin@office-01] >
[admin@office-01] >
[admin@office-01] > ping 192.168.88.1 src-address=10.0.88.254
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	192.168.88.1	56	64	2ms	
1	192.168.88.1	56	64	0ms	
2	192.168.88.1	56	64	0ms	
3	192.168.88.1	56	64	0ms	
4	192.168.88.1	56	64	0ms	
5	192.168.88.1	56	64	0ms	



Pros:

Easy to configure
and understand

OSPF works

No TCP MSS
issues

Routable

Has
interface

Option 1 (easy)

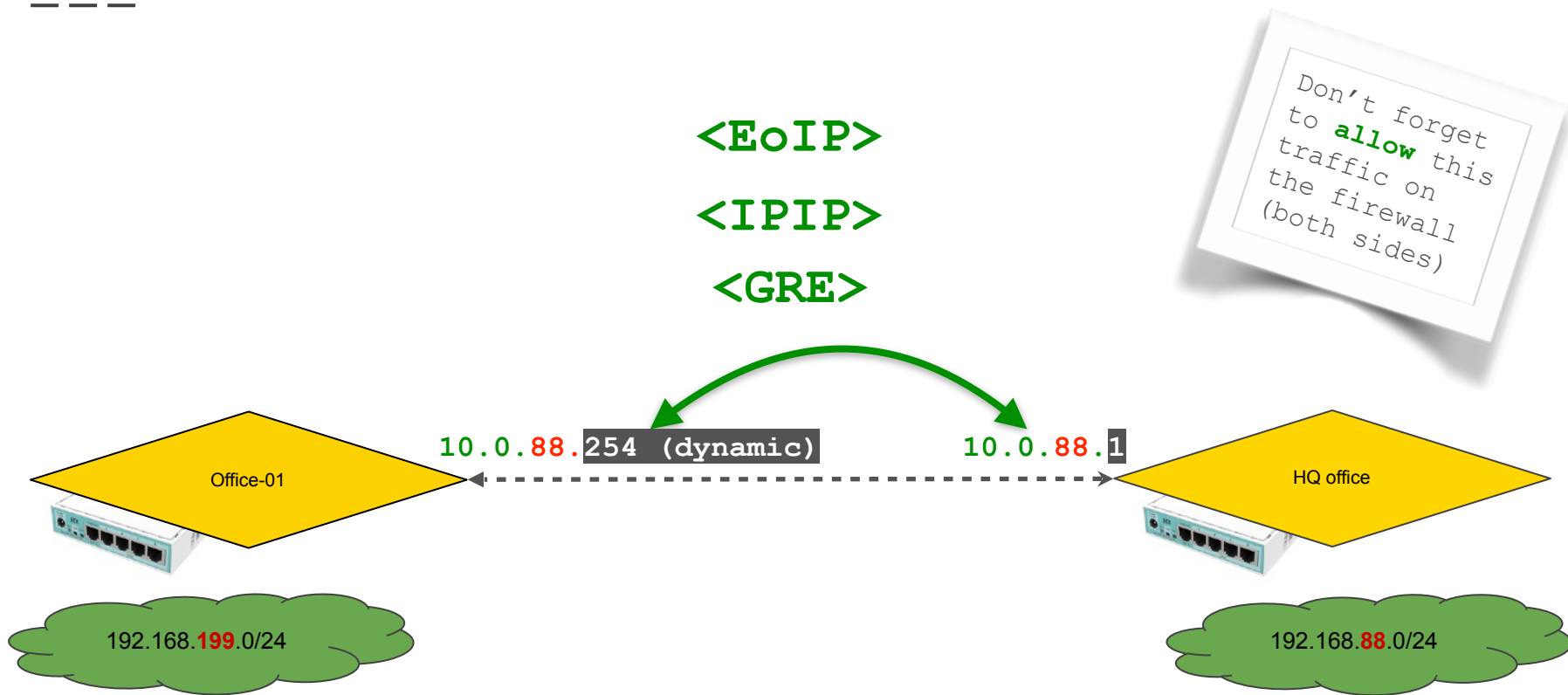
<interface> over ipsec ike2

Decreased MTU due to extra
encapsulation overhead

Takes longer
to connect and
reconnect

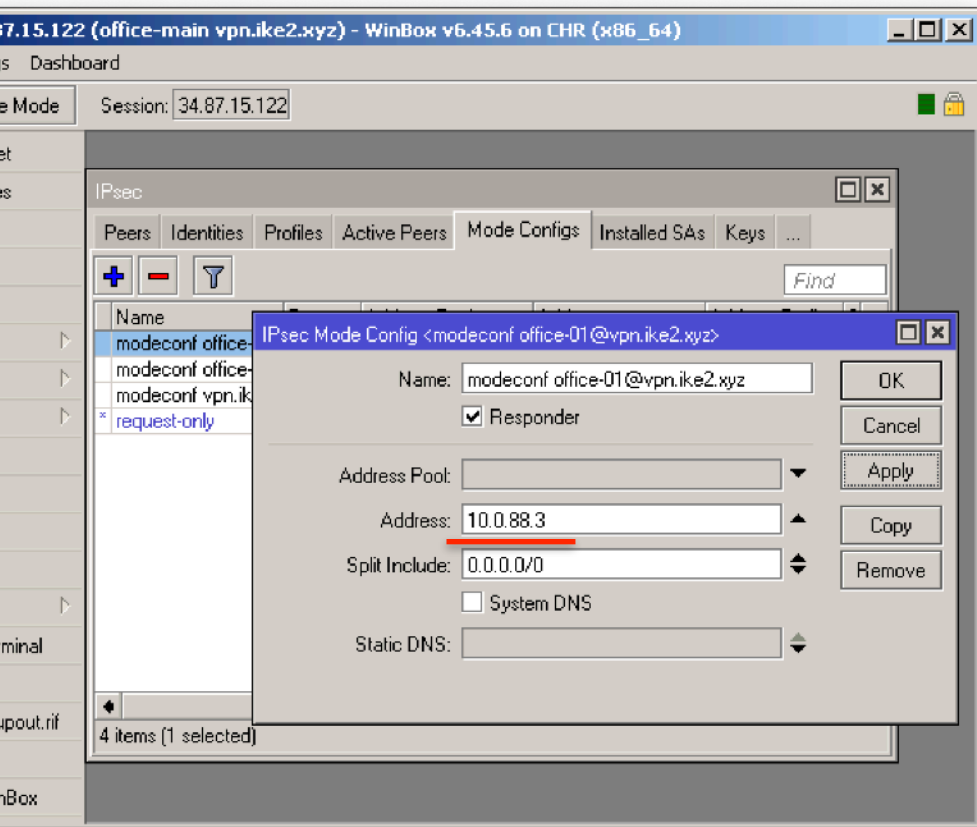
Cons:

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





Create new ipsec modeconf with **static** IP address



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

admin@34.87.15.122 (office-main vpn.ike2.xyz) - WinBox v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 34.87.15.122

RouterOS WinBox

Quick Set
Interfaces
Bridge
PPP
Mesh
IP
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Make Supout.tif
Manual
New WinBox
Exit

IPsec

#	Peer
110	peer
111	peer
112	peer
113	peer
114	peer
115	peer
116	peer
117	peer
118	peer
119	peer
120	peer
121	peer
122	peer
123	peer
124	peer
142 items (1 s)	

IPsec Identity <peer 34.87.15.122>

Peer: peer 34.87.15.122

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: office-01@vpn.ike2.xyz

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: office-01@vpn.ike2.xyz

Match By: certificate

Mode Configuration: modeconf office-01@vpn.ike2.xyz

Generate Policy: port strict

enabled

As Keys

Find

Mode Configuration

- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf office-01@vpn.ike2.xyz
- modeconf vpn.ike2.xyz
- modeconf vpn.ike2.xyz

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



admin@35.247.134.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 35.247.134.147

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs ...

+ - [Icons] Find

#	Peer	Tunnel	Src. Address	Src. Port	Dst. Address
0	T		::/0		::/0
1	T		10.0.88.0/24		0.0.0.0/0
2	DA peer vpn.ike2.xyz	yes	10.0.88.3		0.0.0.0/0

Address List

+ - [Icons] Find

	Address	Network	Interface
D	10.0.88.3	10.0.88.3	ether1
D	10.148.0.7	10.148.0.1	ether1
	192.168.199.1...	192.168.199.0	bridge

3 items (1 selected)

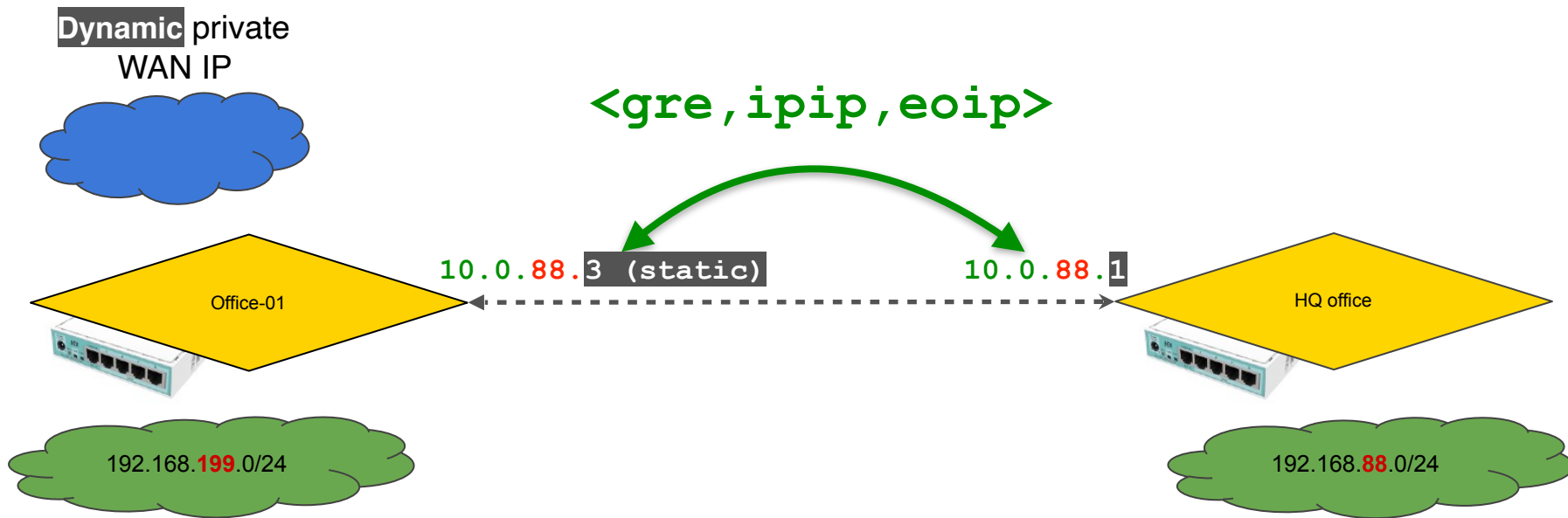
IP address 10.0.88.3

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

New Interface

General Status Traffic

Name:

Type: IP Tunnel

MTU:

Actual MTU:

L2 MTU:

Local Address:

Remote Address:

IPsec Secret:

Keepalive:

DSCP:

Dont Fragment:

☒ Clamp TCP MSS

☒ Allow Fast Path

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

<ipip>

New Interface

General Status Traffic

Name:

Type: IP Tunnel

MTU:

Actual MTU:

L2 MTU:

Local Address:

Remote Address:

IPsec Secret:

Keepalive:

DSCP:

Dont Fragment:

☒ Clamp TCP MSS

☒ Allow Fast Path

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

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



Client

admin@35.247.134.147 (office-01) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Session: 35.247.134.147

Address <10.1.1.3>

Address: 10.1.1.3 OK

Network: 10.1.1.1 Cancel

Interface: ipip-main-office Apply

Route <192.168.88.0/24>

General Attributes

Dst. Address: 192.168.88.0/24

Gateway: 10.1.1.1 reachable ipip-main-office Apply

Check Gateway: Disable

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:



Server

admin@34.87.15.122 (office-main) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Session: 34.87.15.122

Address <10.1.1.1>

Address: 10.1.1.1 OK

Network: 10.1.1.3 Cancel

Interface: ipip-office-01 Apply

Route <192.168.199.0/24>

General Attributes

Dst. Address: 192.168.199.0/24

Gateway: 10.1.1.3 reachable ipip-office-01

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:



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

admin@35.247.134.147 (office-01) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 35.247.134.147

RouterOS WinBox

Quick Set

Interfaces

Bridge

PPP

Mesh

IP

Routing

System

Queues

Files

Log

RADIUS

Tools

New Terminal

Dot1X

Make Supout.rif

Manual

New WinBox

Exit

Address List

	Address	Network	Interface
D	10.0.88.3	10.0.88.3	ether1
	10.1.1.3	10.1.1.1	ipip-main-office
D	10.148.0.7	10.148.0.1	ether1
	192.168.199.1/24	192.168.199.0	bridge

Interface List

Interface	Name	Type	Actual MTU	L2 MTU	Tx
R	bridge	Bridge	1500	65535	
R	ether1	Ethernet	1500		
R	ipip-main-office	IP Tunnel	1386	65535	

Route List

Routes	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	10.148.0.1 reachable ether1	1		
DAC	10.0.88.3	ether1 reachable	0		10.0.88.3
DAC	10.1.1.1	ipip-main-office reachable	0		10.1.1.3
DAC	10.148.0.1	ether1 reachable	0		10.148.0.7
AS	192.168.88.0/24	10.1.1.1 reachable ipip-main-office	1		
DAC	192.168.199.0/24	bridge reachable	0		192.168.199.1

4 items (1)

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
```

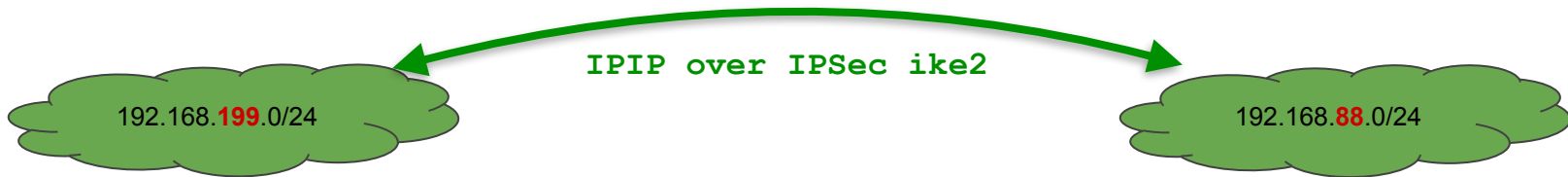
HOST	SIZE	TTL	TIME	STATUS
192.168.88.1	56	64	1ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	

```
sent=12 received=12 packet-loss=0% min-rtt=0ms avg-rtt=0ms  
max-rtt=1ms
```

```
[admin@office-main] > ping 192.168.199.1 src-address=192.168.88.1
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
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-rtt=0ms
```



Pros:

No MTU overhead ->
performs faster

Connects and
reconnects much
faster

Much more **stable**,
less reconnects

Option 2 (advanced)

100% policy based ipsec ike2

Harder to
configure and
understand

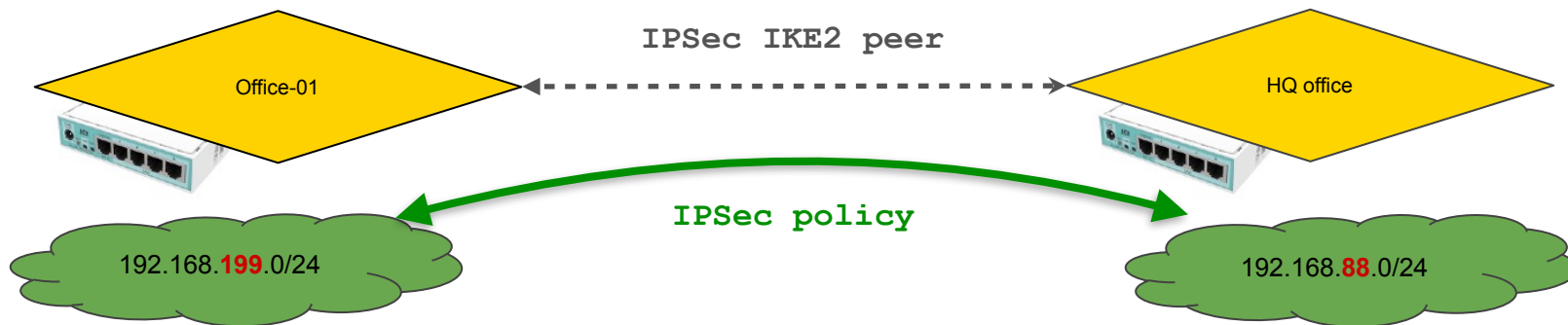
OSPF ~~works~~

Has no routable
interface

Need to adjust
TCP MSS manually

Cons:

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





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

WinBox v6.45.6 on CHR (x86_64)

Session: 34.87.15.122

IPsec Policy <192.168.88.0/24>192.168.199.0/24>

General Action Status

Src. Address: 192.168.88.0/24

Src. Port: [dropdown]

Dst. Address: 192.168.199.0/24

Dst. Port: [dropdown]

Protocol: 255 (all)

☒ Template

Group: group vpn.ike2.xyz

OK Cancel Apply Disable

Src. Address	Dst. Address	Dst. Port	Prot
0.0.0.0/0	0.0.0.0/0	255	...
0.0.88.0/24		255	...
0.0.88.3		255	...
0.0.88.253		255	...

Comment for IPsec Policy <192.168.88.0/24>192.168.199.0/24>

Policy template for group vpn.ike2.xyz (site-to-site)

OK Cancel

New IPsec Policy

Action Status

Action: encrypt

Protocols: esp

Proposal: proposal vpn.ike2.xyz

OK Cancel Apply Disable Comment Copy

192.168.88.0/24

192.168.199.0/24

```
/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
```




Client

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

7.134.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Dashboard

Mode Session: 35.247.134.147

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs ...

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

IPsec Policy <192.168.199.0/24:0->192.168.88.0/24:0>

Action Status

Action: encrypt

Level: unique

Protocols: esp

Proposal: proposal vpn.ike2.xyz

OK Cancel Apply Disable Comment

192.168.199.0/24

192.168.88.0/24

```
/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

192.168.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Dashboard

Mode Session: 35.247.134.147

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs ...

Find

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

192.15.122 (office-main vpn.ike2.xyz) - WinBox v6.45.6 on CHR (x86_64)

Dashboard

Mode Session: 34.87.15.122

IPsec

Policies Proposals

Find

IPsec Policy <192.168.88.0/24>192.168.199.0/24:0>

General Action Status

OK Copy Remove

Src. Address: 192.168.88.0/24

Src. Port:

Dst. Address: 192.168.199.0/24

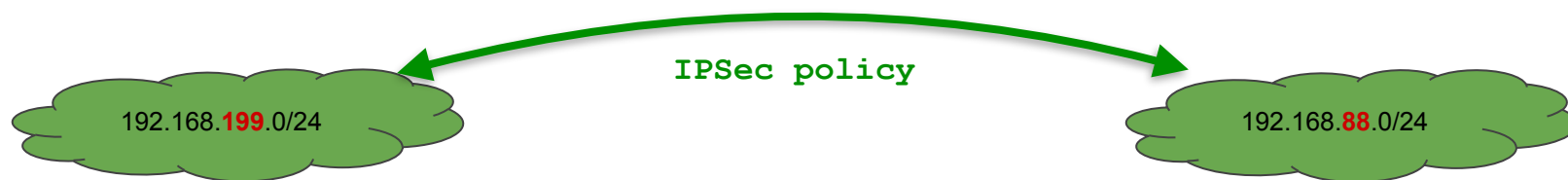
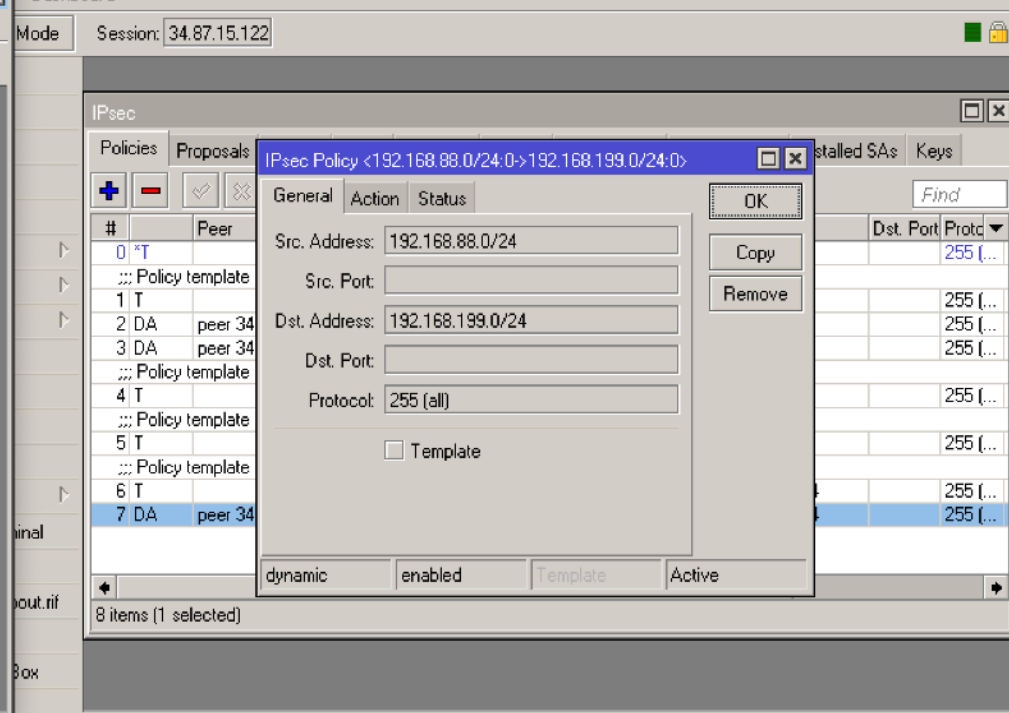
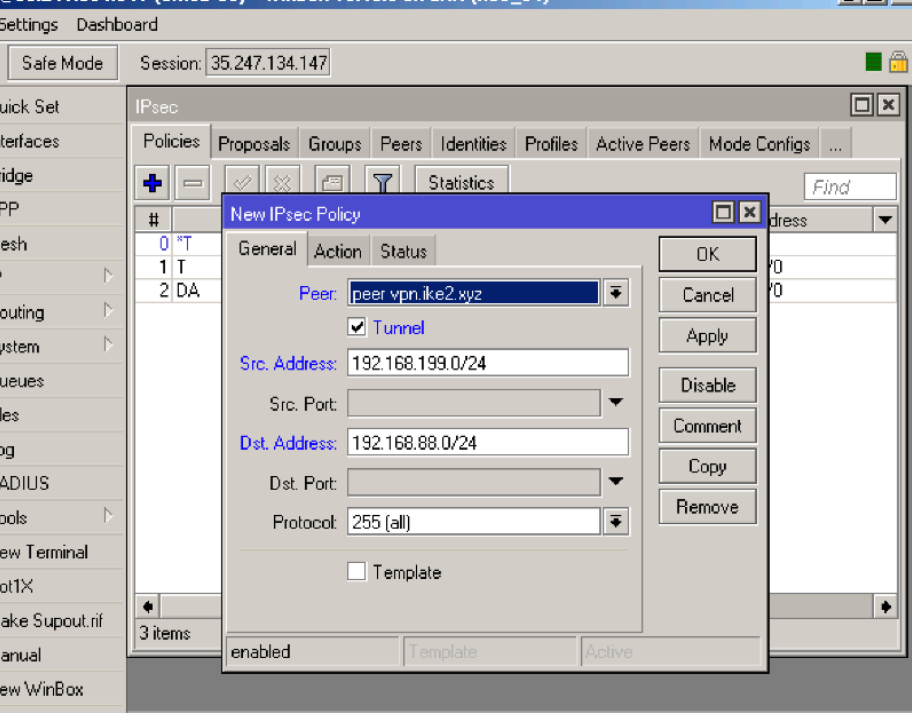
Dst. Port:

Protocol: 255 (all)

☐ Template

dynamic enabled Template Active

8 items (1 selected)



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

admin@35.247.134.147 (office-01) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 35.247.134.147

RouterOS WinBox

Quick Set

Interfaces

Bridge

PPP

Mesh

IP

Routing

System

Queues

Files

Log

RADIUS

Tools

New Terminal

Dot1X

Make Supout.rif

Manual

New WinBox

Exit

Address List

	Address	Network	Interface
D	10.0.88.3	10.0.88.3	ether1
X	10.1.1.3	10.1.1.1	ipip-main-office
D	10.148.0.7	10.148.0.1	ether1
	192.168.199.1/24	192.168.199.0	bridge

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	...
R	bridge	Bridge				
R	ether1	Ethernet				
X	ipip-main-office	IP Tunnel				

Route List

Routes	Next hops	Rules	VRF
DAS	0.0.0.0/0	10.148.0.1 reachable ether1	1
DAC	10.0.88.3	ether1 reachable	0
DAC	10.148.0.1	ether1 reachable	0
X	192.168.88.0/24	10.1.1.1	1
DAC	192.168.199.0/24	bridge reachable	0

4 items (1)

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

admin@35.247.134.147 (office-01) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 35.247.134.147

Quick Set

Interfaces

Bridge

PPP

Mesh

IP

Routing

System

Queues

Files

Log

RADIUS

Tools

New Terminal

Dot1X

Make Supout.rif

Manual

New WinBox

IPsec

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

Find

#	Peer	Tunnel	Src. Address	Src. P...	Dst. Address	Dst. P...	Prot...	Action	Level	PH2 State
0	*T		::/0		::/0		255 ...	encrypt		
1	T		10.0.88.0/24		0.0.0.0/0		255 ...	encrypt		
2	DA	peer vpn.ike2.xyz	10.0.88.3		0.0.0.0/0		255 ...	encrypt	unique	established
3	X	peer vpn.ike2.xyz	192.168.199.0/24		192.168.88.0/24		255 ...	encrypt	unique	

Route List

Routes Nexthops Rules VRF

	Dst. Address	Gateway	Distance
DAS	0.0.0.0/0	10.148.0.1 reachable ether1	1
DAC	10.0.88.3	ether1 reachable	0
DAC	10.148.0.1	ether1 reachable	0
XS	192.168.88.0/24	10.1.1.1	1
DAC	192.168.199.0/24	bridge reachable	0

4 items

5 items (1 selected)

Terminal

```
[admin@office-01] > ping 192.168.88.1 src-address=192.168.199.1
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	192.168.88.1				timeout
1	192.168.88.1				timeout
2	192.168.88.1				timeout
3	192.168.88.1				timeout
4	192.168.88.1				timeout
5	192.168.88.1				timeout
6	192.168.88.1				timeout
7	192.168.88.1				timeout

Let's enable ipsec policy and keep ip route disabled

admin@35.247.134.147 (office-01) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 35.247.134.147

Quick Set

Interfaces

Bridge

PPP

Mesh

IP

Routing

System

Queues

Files

Log

RADIUS

Tools

New Terminal

Dot1X

Make Supout.rif

Manual

New WinBox

IPsec

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

Find

#	Peer	Tunnel	Src. Address	Src. P...	Dst. Address	Dst. P...	Prot...	Action	Level	PH2 State
0	*T		::/0		::/0		255 ...	encrypt		
1	T		10.0.88.0/24		0.0.0.0/0		255 ...	encrypt		
2	DA peer vpn.ike2.xyz	yes	10.0.88.3		0.0.0.0/0		255 ...	encrypt	unique	established
3	A peer vpn.ike2.xyz	yes	192.168.199.0/24		192.168.88.0/24		255 ...	encrypt	unique	established

Route List

Routes Nexthops Rules VRF

	Dst. Address	Gateway	Distance
DAS	0.0.0.0/0	10.148.0.1 reachable ether1	1
DAC	10.0.88.3	ether1 reachable	0
DAC	10.148.0.1	ether1 reachable	0
XS	192.168.88.0/24	10.1.1.1	1
DAC	192.168.199.0/24	bridge reachable	0

4 items

5 items (1 selected)

Terminal

```

8 192.168.88.1 timeout
9 192.168.88.1 timeout
sent=10 received=0 packet-loss=100%
[admin@office-01] > ping 192.168.88.1 src-address=192.168.199.1
SEQ HOST SIZE TTL TIME STATUS
0 192.168.88.1 56 64 1ms
1 192.168.88.1 56 64 0ms
2 192.168.88.1 56 64 0ms
3 192.168.88.1 56 64 0ms
4 192.168.88.1 56 64 0ms

```

Testing site-to-site ipsec policy based connectivity

```
m@office-01] > ping 192.168.88.1 src-address=192.168.199.1
```

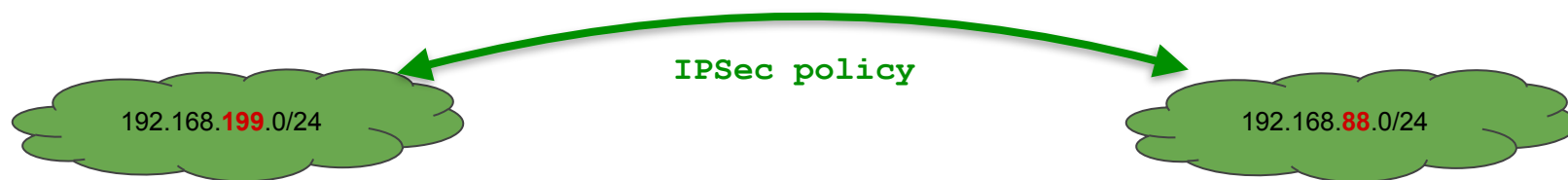
HOST	SIZE	TTL	TIME	STATUS
192.168.88.1	56	64	1ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	
192.168.88.1	56	64	0ms	

```
sent=12 received=12 packet-loss=0% min-rtt=0ms avg-rtt=0ms  
max-rtt=1ms
```

```
[admin@office-main] > ping 192.168.199.1 src-address=192.168.88.1
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
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-rtt=0ms
```



Setting up TCP MSS 🎯

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

admin@34.87.15.122 (office-main) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Settings Dashboard

Safe Mode

Session: 34.87.15.122

Check Set

Interfaces

Sh

h

nting

tem

ues

s

DIUS

ls

y Terminal

1X

se Supout.rif

ual

y WinBox

Mangle Rule <192.168.88.0/24->192.168.199.0/24>

General Advanced Extra Action Statistics

Chain: forward

Src. Address: 192.168.88.0/24

Dst. Address: 192.168.199.0/24

Protocol: 6 (tcp)

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

Mangle Rule <192.168.199.0/24->192.168.88.0/24>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

IPsec Policy: in : ipsec

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

TCP MSS: 0-1360

Packet Size:

Random:

TCP Flags

TCP Flags: syn

Mangle Rule <192.168.88.0/24->192.168.199.0/24>

General Advanced Extra Action Statistics

Action: change MSS

Log

Log Prefix:

New TCP MSS: 1360

Passthrough

```
/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 tcp-flags=syn tcp-mss=!0-1360 ipsec-policy=in,ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from office-main to office-01"
```

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

admin@34.87.15.122 (office-main) - WinBox (64bit) v6.45.6 on CHR (x86_64)

Settings Dashboard

Safe Mode Session: 34.87.15.122

Mangle Rule <192.168.199.0/24->192.168.88.0/24>

General Advanced Extra Action Statistics

Chain: forward

Src. Address: 192.168.199.0/24

Dst. Address: 192.168.88.0/24

Protocol: 6 (tcp)

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

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

Mangle Rule <192.168.199.0/24->192.168.88.0/24>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

IPsec Policy: in : ipsec

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

TCP MSS: 10-1360

Packet Size:

Random:

TCP Flags

TCP Flags: syn

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

Mangle Rule <192.168.88.0/24->192.168.199.0/24>

General Advanced Extra Action Statistics

Action: change MSS

Log

Log Prefix:

New TCP MSS: 1360

Passthrough

OK Cancel Apply Disable Comment Copy

```
/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 tcp-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

— — —

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>



Demo lab

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

Wait for your certificate

Manual processing for this LAB, sorry :)

— — —

Demo lab

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

IKE2 VPN Server address

`vpn.ike2.xyz`

— — —

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

— — —

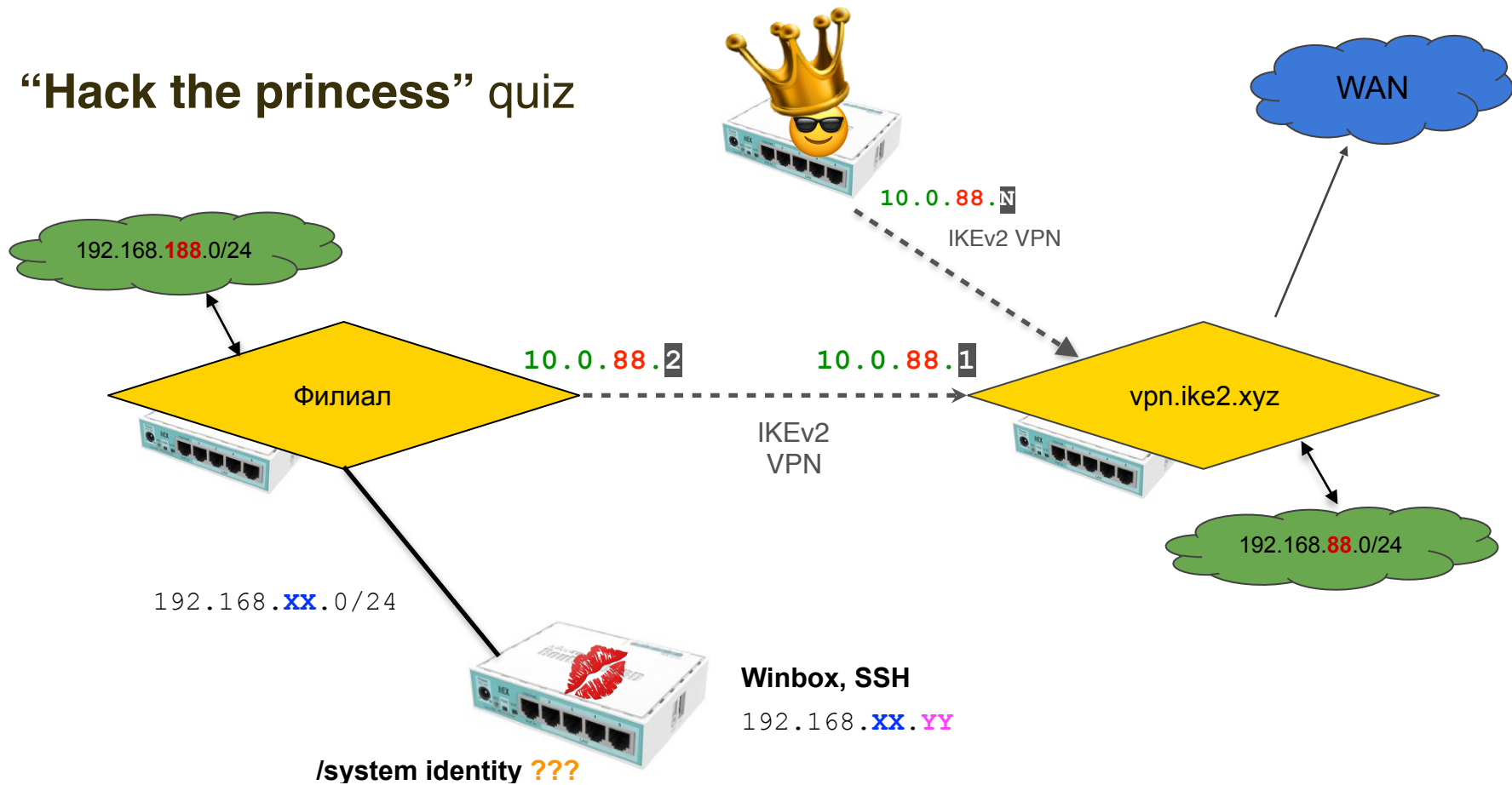
IPSec quiz time!

“ Hack the princess ”

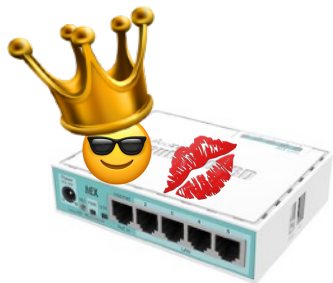


Will be open until 31 December 2019

“Hack the princess” quiz



hacktheprincess@protonmail.com

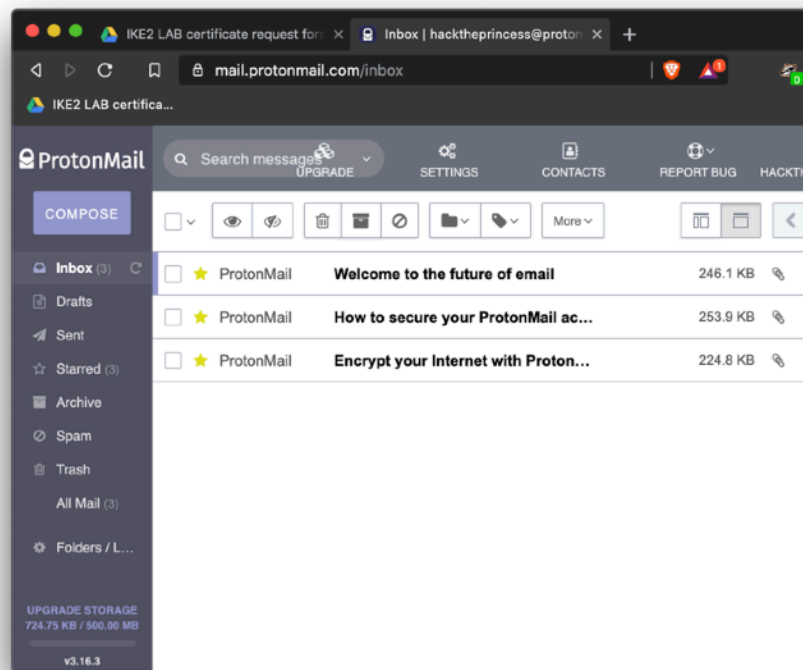


192.168.**XX**.0/24

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

— — —