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

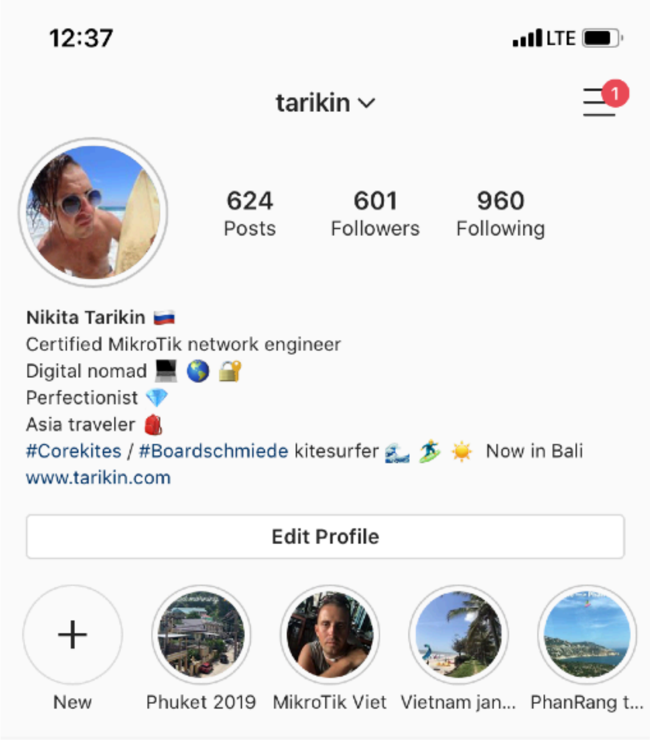
Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia

MTCNA	99%
MTCRE	95%
MTCTCE	96%
MTCWE	84%
MTCUME	90%
MTCSE	94%
MTCIPv6E	74%

BOARDSCHMIEDE
MikroTik
MALAYSIA
JUNE 2018
NEXUS

@tarikin



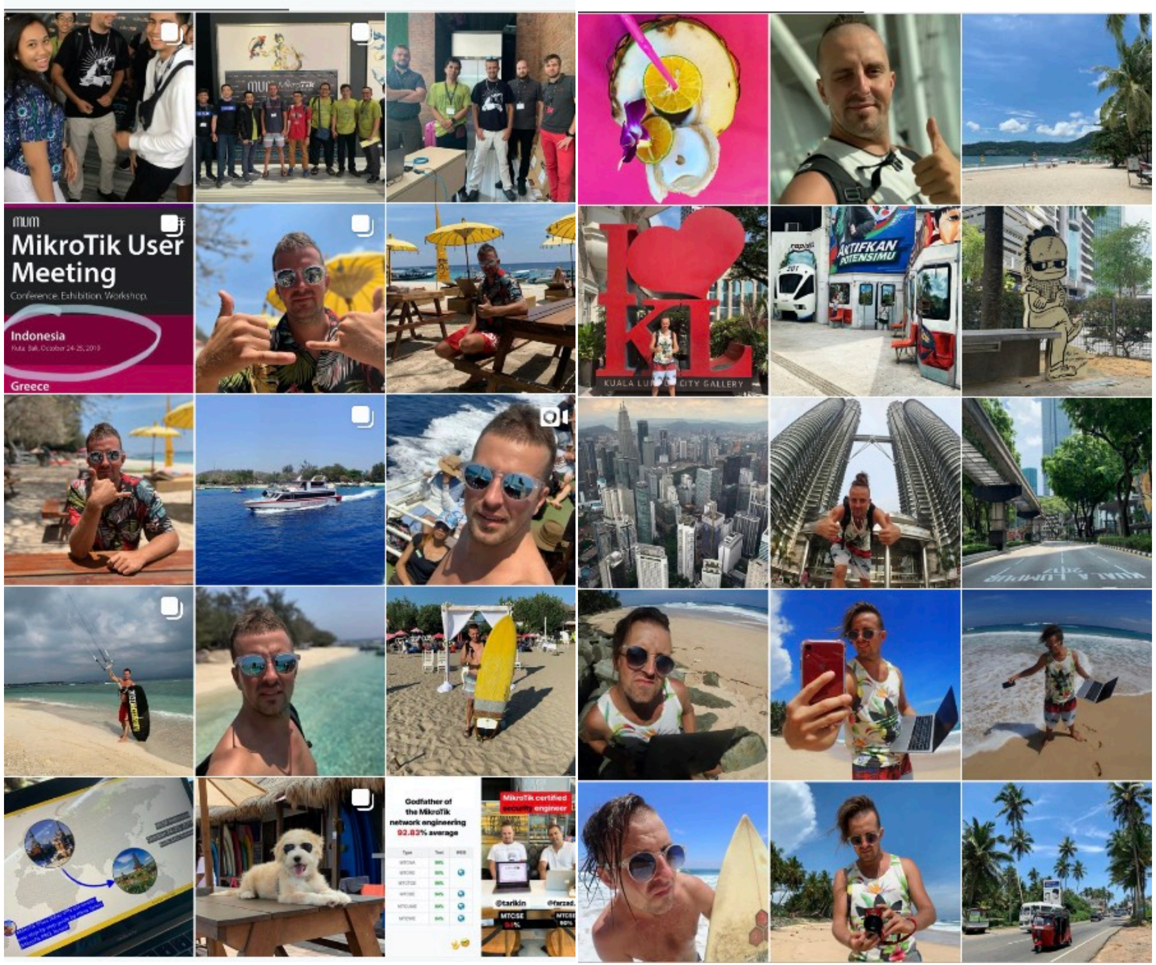
12:37 LTE

tarikin ⌄ 1

624 Posts 601 Followers 960 Following

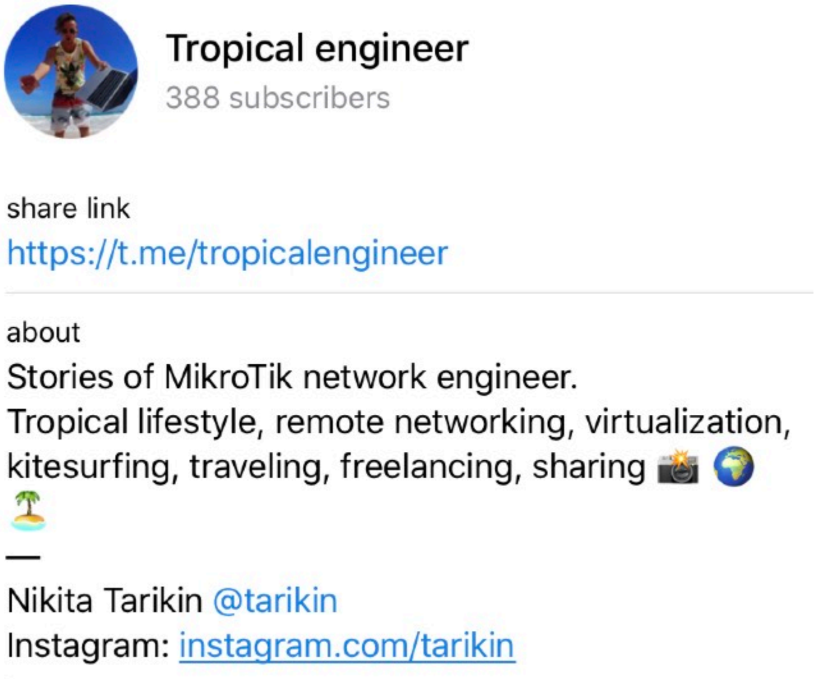
Nikita Tarikin 🇷🇺
Certified MikroTik network engineer
Digital nomad 💻 🌍 🔐
Perfectionist 💎
Asia traveler 🎒
#Corekites / #Boardschmiede kitesurfer 🌊 🏄 ☀️ Now in Bali
www.tarikin.com

Edit Profile



MUM
MikroTik User Meeting
Conference. Exhibition. Workshop.
Indonesia
Kuta, Bali, October 24-25, 2019
Greece
KUALA LUMPUR CITY GALLERY
AKTIFKAN POTENSIMU
Godfather of the MikroTik network engineering
92.83% average
MikroTik certified security engineer
@tarikin
@farzad
MTCSE

@tropicalengineer



Tropical engineer

388 subscribers

share link

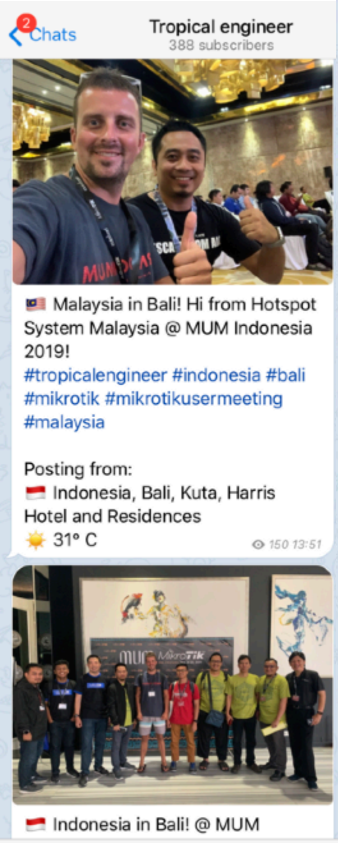
https://t.me/tropicalengineer

about

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

—

Nikita Tarikin @tarikin
Instagram: instagram.com/tarikin



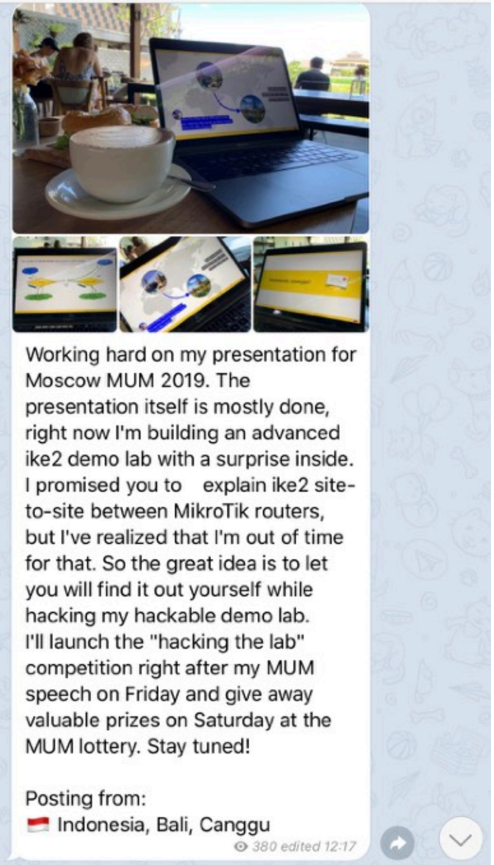
Tropical engineer
388 subscribers

🇲🇾 Malaysia in Bali! Hi from Hotspot System Malaysia @ MUM Indonesia 2019!
#tropicalengineer #indonesia #bali #mikrotik #mikrotikusermeeting #malaysia

Posting from:
🇮🇩 Indonesia, Bali, Kuta, Harris Hotel and Residences
☀️ 31° C

150 13:51

🇮🇩 Indonesia in Bali! @ MUM



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:

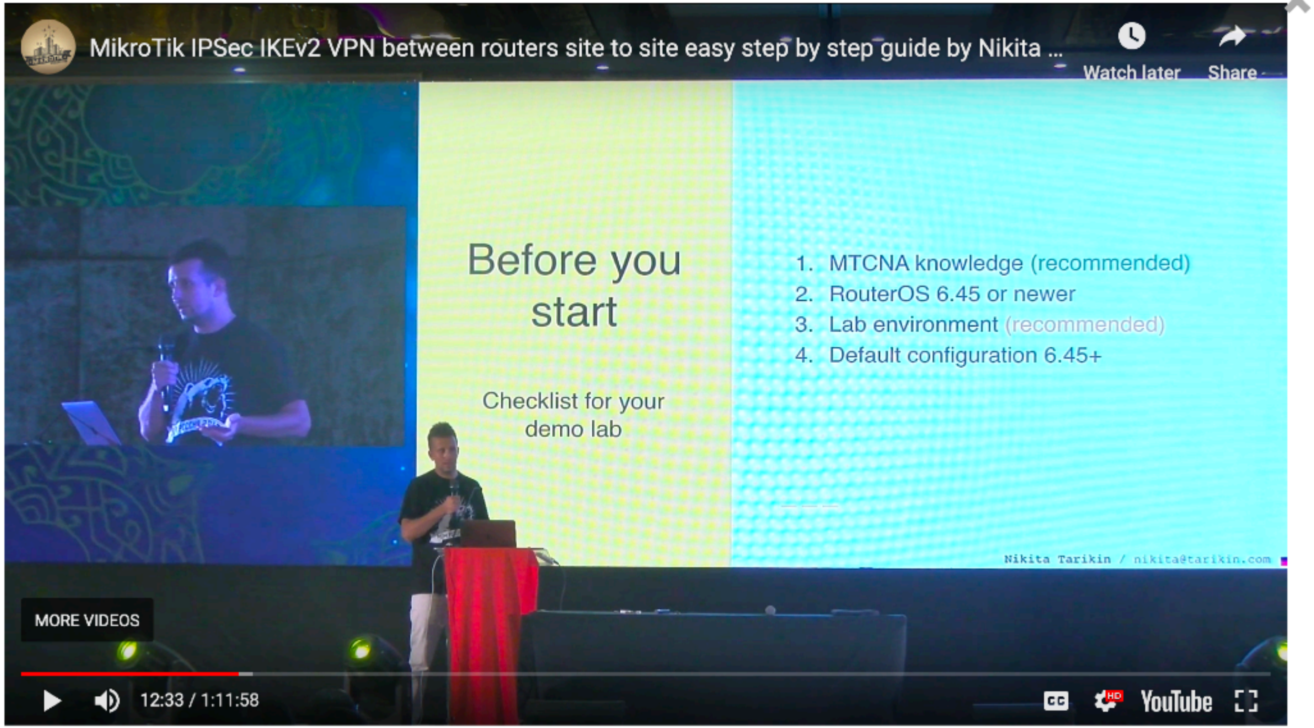
@tarikin

@tropicalengineer

Direct message me via:

Telegram t.me/tarikin

Messenger Nikita Tarikin



MikroTik IPSec IKEv2 VPN between routers site to site easy step by step guide by Nikita ...

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

Watch this presentation on YouTube

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

Why IPSec IKE2?

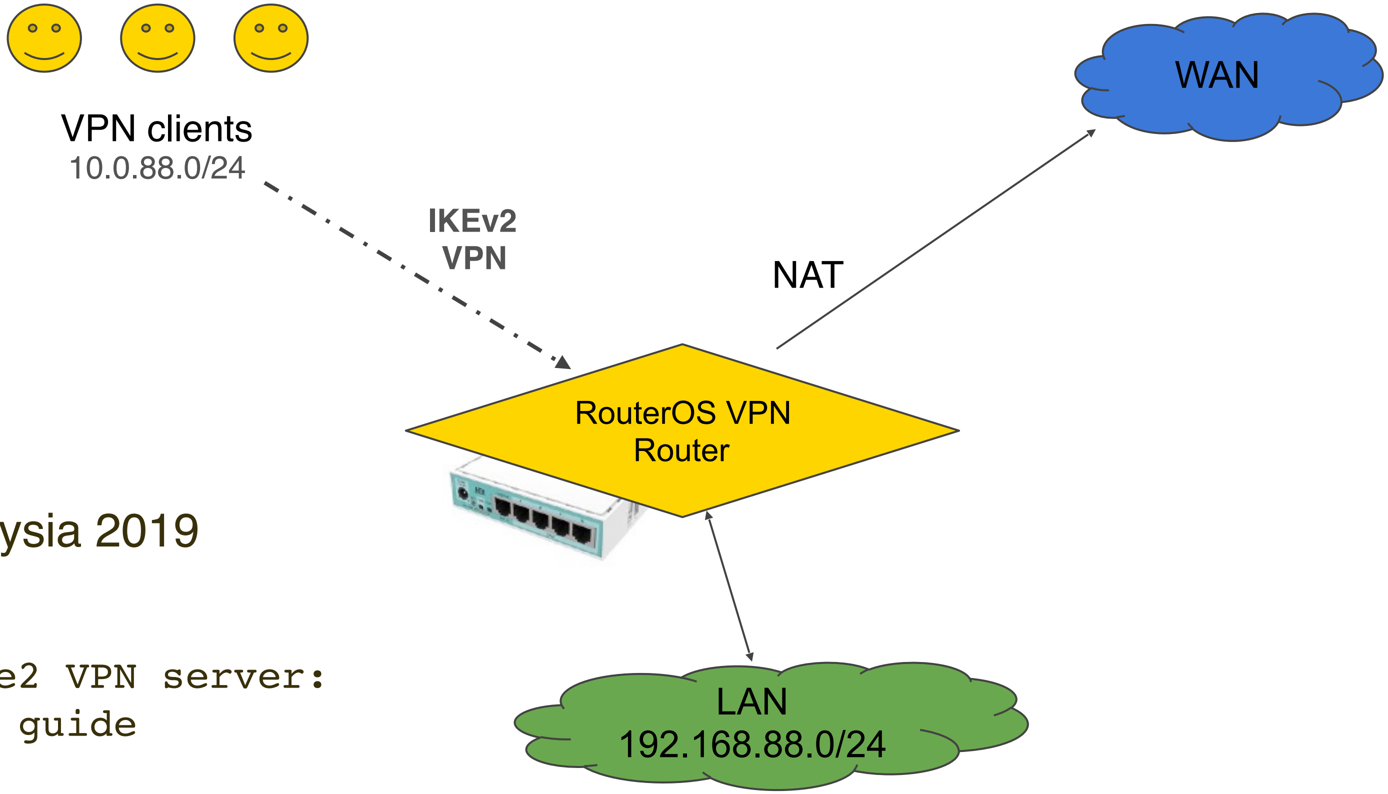
Compare VPN types (RouterOS)

	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



VPN clients
10.0.88.0/24

IKEv2
VPN

NAT

WAN

RouterOS VPN
Router

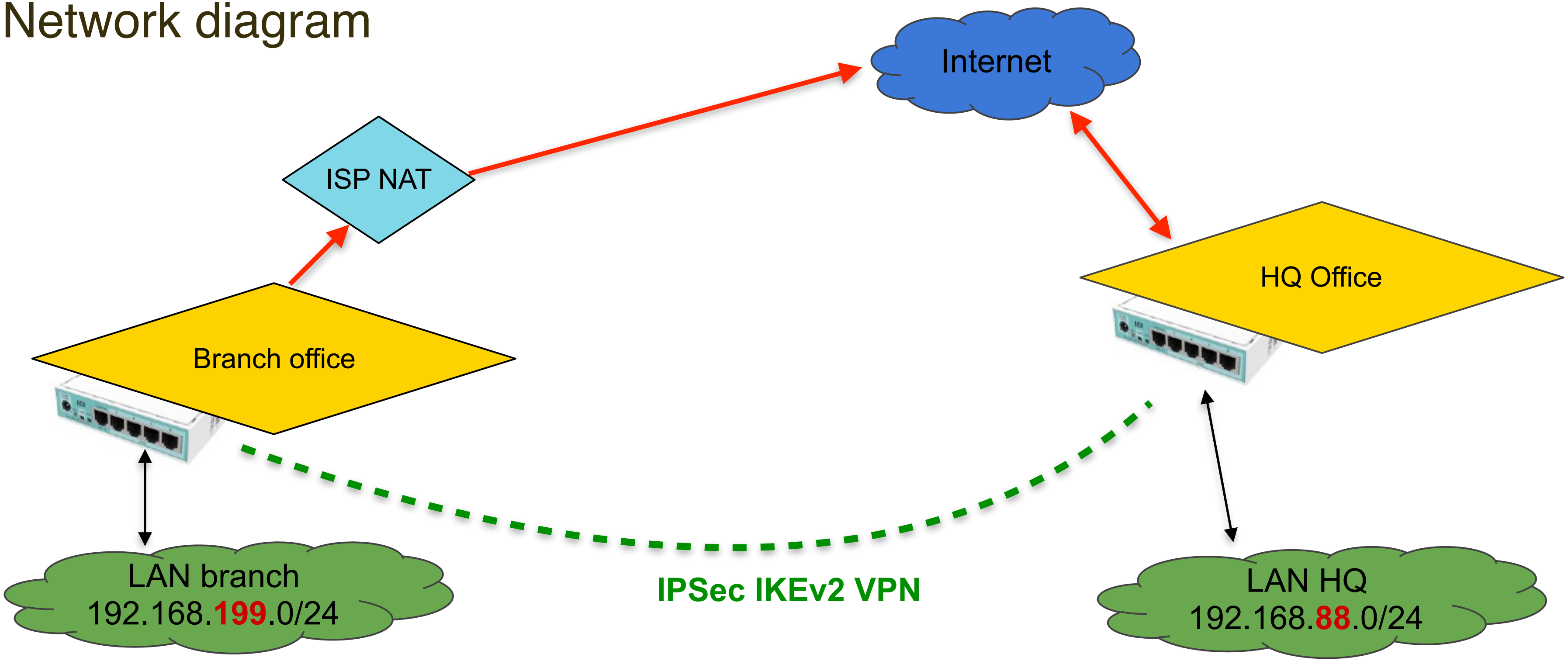
LAN
192.168.88.0/24

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

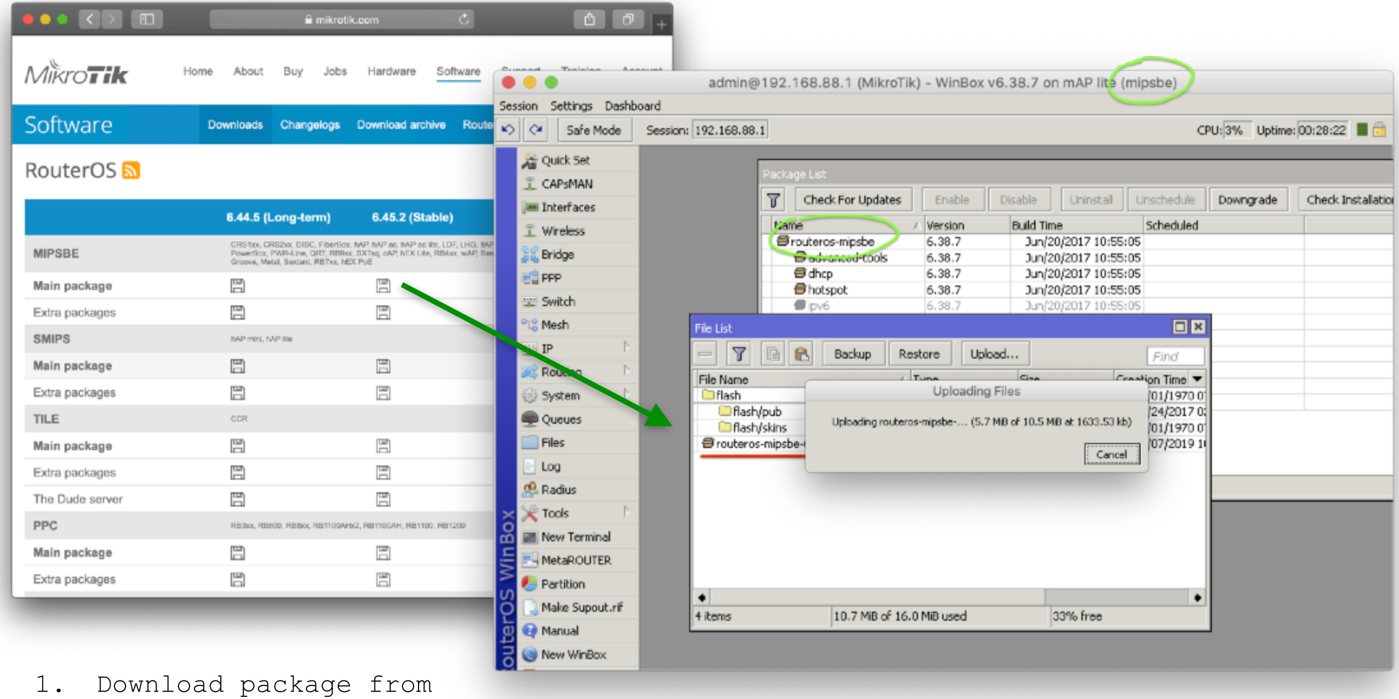
1. Before you start
2. Build SSL certificates
3. Setting up ipsec vpn server
4. Setting up ipsec vpn client
5. Site-to-site via **interface over ipsec**
6. Site-to-site via **ipsec policy**
7. ~~Setting up firewall~~ (see MUM Malaysia 2019)
8. Adjust TCP-MSS
9. Demo lab + hacking quiz

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+



RouterOS

	6.44.5 (Long-term)	6.45.2 (Stable)
MIPSBE	CRS1xx, CRS2xx, DISC, FiberBox, hAP, hAP ac, hAP ac lite, LDF, LHG, ... PowerBox, PWR-Line, QRT, RB9xx, SXTsq, cAP, hEX Lite, RB4xx, wAP, ... Groove, Metal, Sextant, RB7xx, hEX PoE	
Main package	💾	💾
Extra packages	💾	💾
SMIPS	hAP mini, hAP lite	
Main package	💾	💾
Extra packages	💾	💾
TILE	CCR	
Main package	💾	💾
Extra packages	💾	💾
The Dude server	💾	💾
PPC	RB3xx, RB600, RB8xx, RB1100AHx2, RB1100AH, RB1100, RB1200	
Main package	💾	💾
Extra packages	💾	💾

admin@192.168.88.1 (MikroTik) - WinBox v6.38.7 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU: 3% Uptime: 00:28:22

Package List

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	
ipv6	6.38.7	Jun/20/2017 10:55:05	

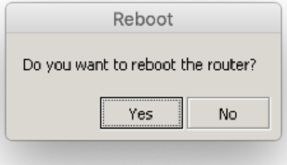
File List

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

4 items 10.7 MiB of 16.0 MiB used 33% free

Uploading Files

Uploading routeros-mipsbe-... (5.7 MiB of 10.5 MiB at 1633.53 kb)



Reboot

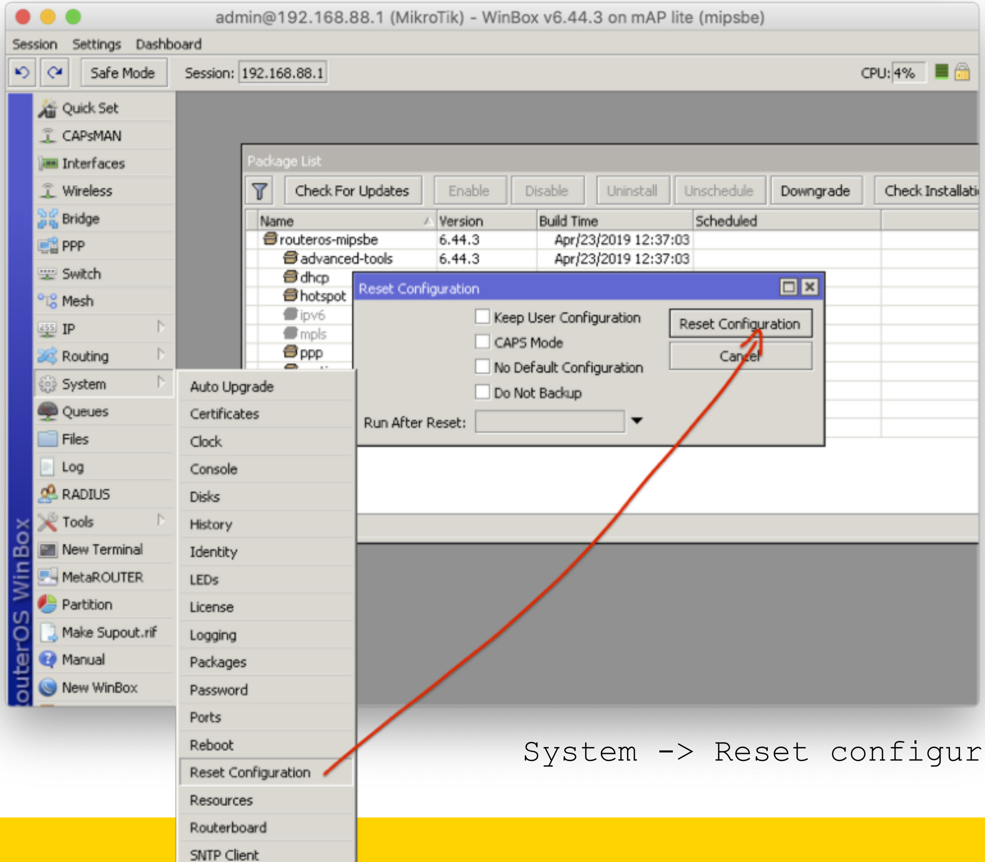
Do you want to reboot the router?

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

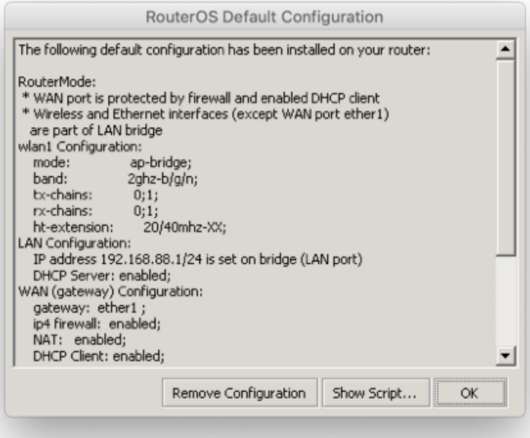


Name	Version	Build Time	Scheduled
routeros-mipsbe	6.44.3	Apr/23/2019 12:37:03	
advanced-tools	6.44.3	Apr/23/2019 12:37:03	
dhcp			
hotspot			
ipv6			
mpls			
ppp			

□ Keep User Configuration
□ CAPS Mode
□ No Default Configuration
□ Do Not Backup
Run After Reset:

System -> Reset configuration

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



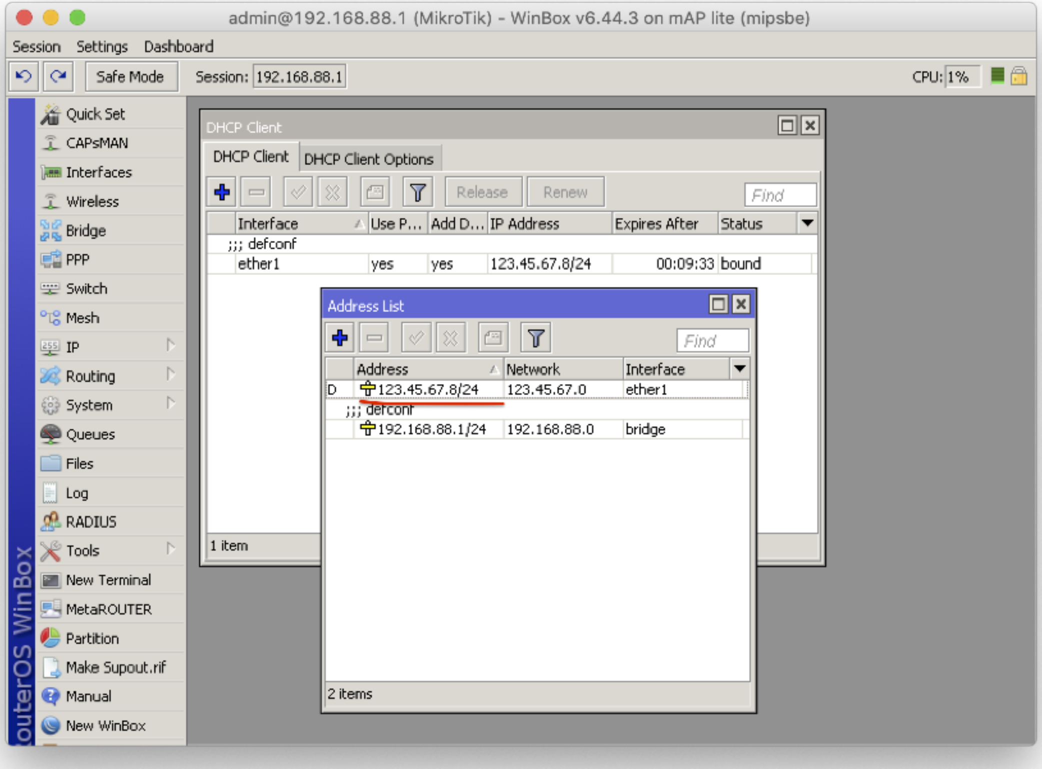
```
The following default configuration has been installed on your router:

RouterMode:
 * WAN port is protected by firewall and enabled DHCP client
 * Wireless and Ethernet interfaces (except WAN port ether1)
   are part of LAN bridge
wlan1 Configuration:
   mode:          ap-bridge;
   band:          2ghz-b/g/n;
   tx-chains:      0;1;
   rx-chains:      0;1;
   ht-extension:    20/40mhz-XX;
LAN Configuration:
   IP address 192.168.88.1/24 is set on bridge (LAN port)
   DHCP Server: enabled;
WAN (gateway) Configuration:
   gateway:  ether1 ;
   ip4 firewall:  enabled;
   NAT:   enabled;
   DHCP Client: enabled;
```

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



DHCP Client

Interface	Use P...	Add D...	IP Address	Expires After	Status
;;; defconf					
ether1	yes	yes	123.45.67.8/24	00:09:33	bound

1 item

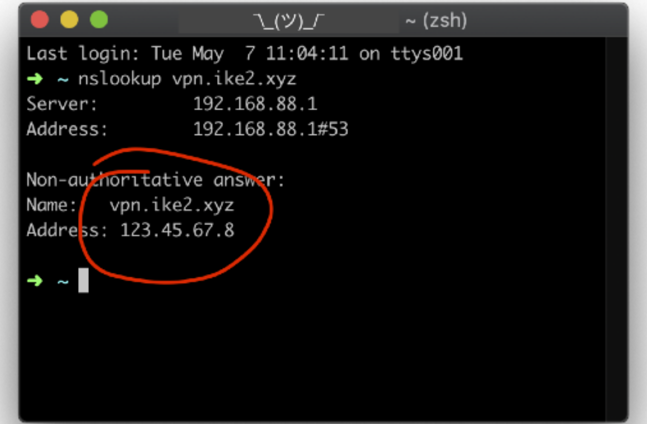
Address List

	Address	Network	Interface
D	123.45.67.8/24	123.45.67.0	ether1
	;;; defconf		
	192.168.88.1/24	192.168.88.0	bridge

2 items

123.45.67.8 is on WAN interface

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

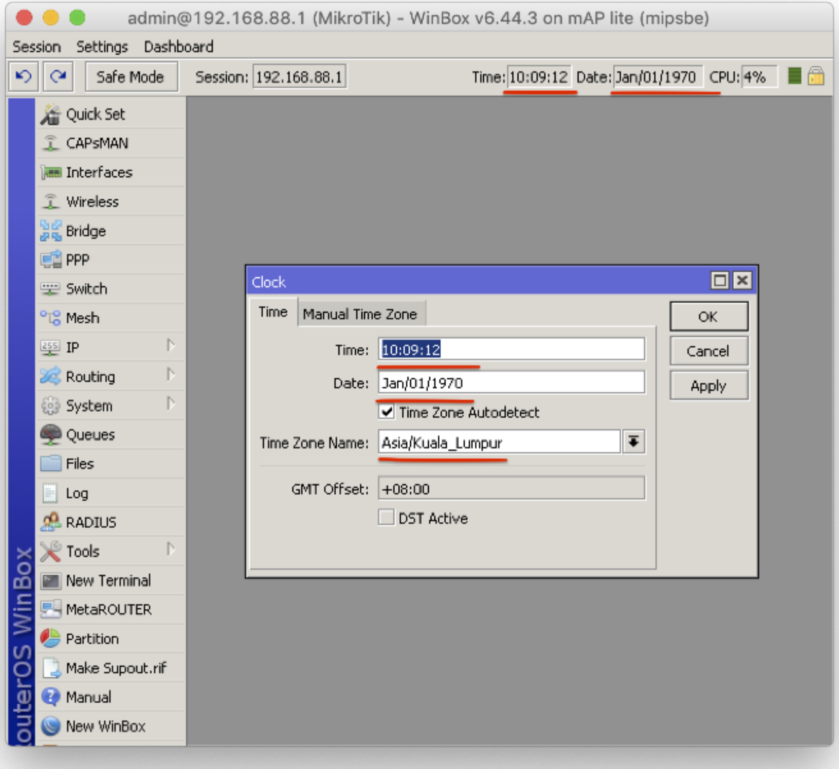


```
Last login: Tue May  7 11:04:11 on ttys001
➜ ~ nslookup vpn.ike2.xyz
Server:         192.168.88.1
Address:        192.168.88.1#53

Non-authoritative answer:
Name:   vpn.ike2.xyz
Address: 123.45.67.8

➜ ~
```

* Set DNS records with your domain name registrar control panel

Setup correct timezone

Important



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

Session: 192.168.88.1 Time: 10:09:12 Date: Jan/01/1970 CPU: 4%

Clock

Time: 10:09:12

Date: Jan/01/1970

☑ Time Zone Autodetect

Time Zone Name: Asia/Kuala_Lumpur

GMT Offset: +08:00

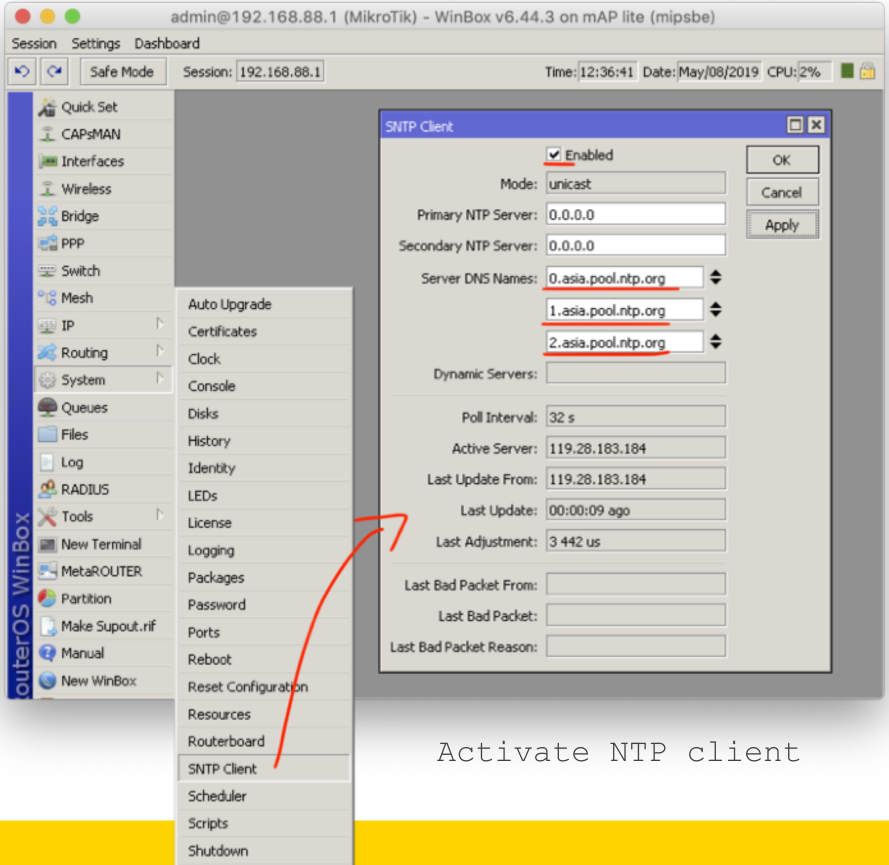
□ DST Active

System -> Clock

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

Setup auto date/time

Important



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

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

SNTP Client

☑ Enabled

Mode: unicast

Primary NTP Server: 0.0.0.0

Secondary NTP Server: 0.0.0.0

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

Dynamic Servers:

Poll Interval: 32 s

Active Server: 119.28.183.184

Last Update From: 119.28.183.184

Last Update: 00:00:09 ago

Last Adjustment: 3 442 us

Last Bad Packet From:

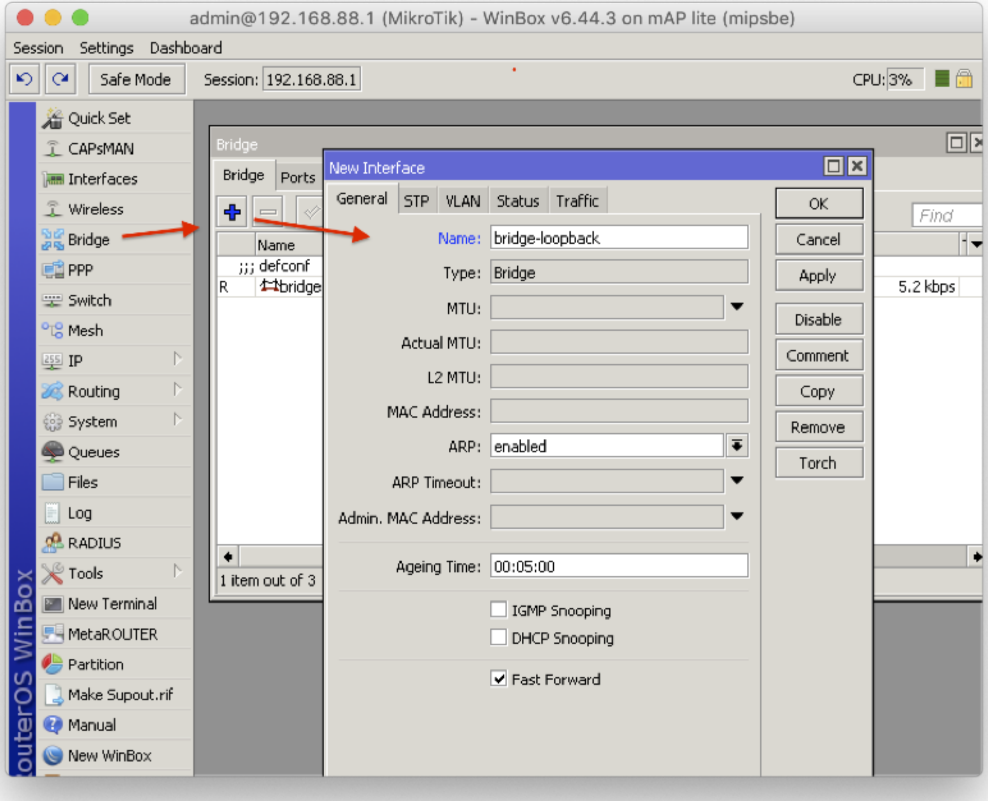
Last Bad Packet:

Last Bad Packet Reason:

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
```

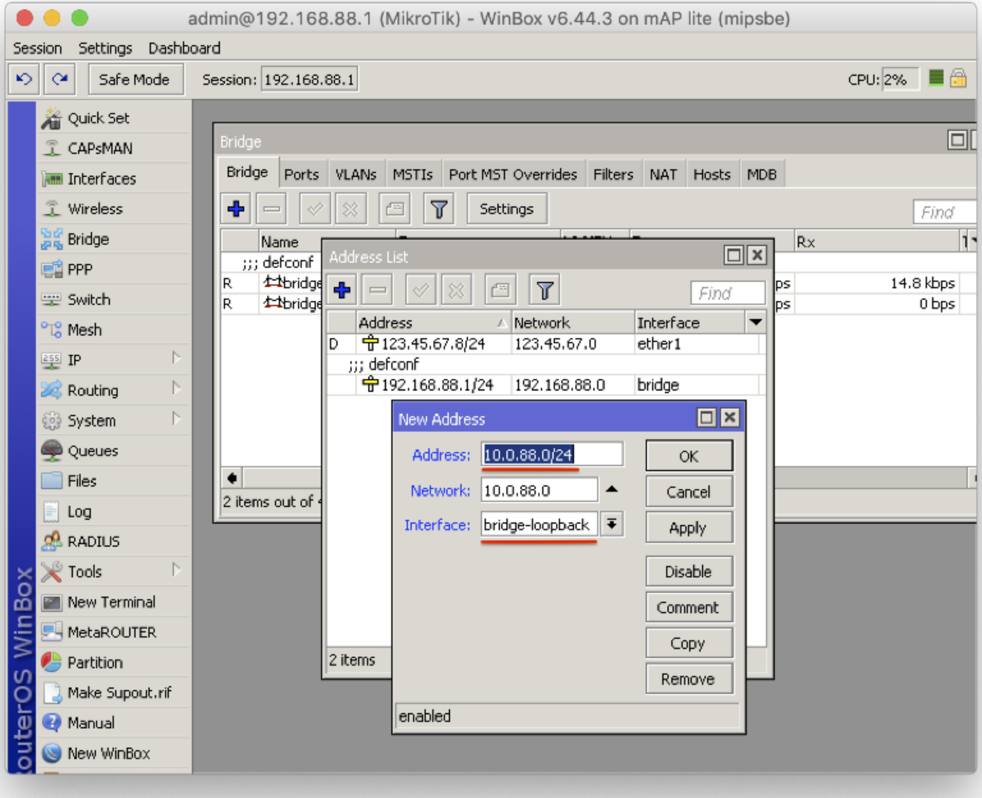
Add new loopback bridge



Name: bridge-loopback
Type: Bridge
MTU:
Actual MTU:
L2 MTU:
MAC Address:
ARP: enabled
ARP Timeout:
Admin. MAC Address:
Ageing Time: 00:05:00
☐ IGMP Snooping
☐ DHCP Snooping
☑ Fast Forward

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

Set loopback bridge IP address



	Name		Rx
	;;; defconf		
R	bridge	ps	14.8 kbps
R	bridge	ps	0 bps

	Address	Network	Interface
D	123.45.67.8/24	123.45.67.0	ether1
	;;; defconf		
	192.168.88.1/24	192.168.88.0	bridge

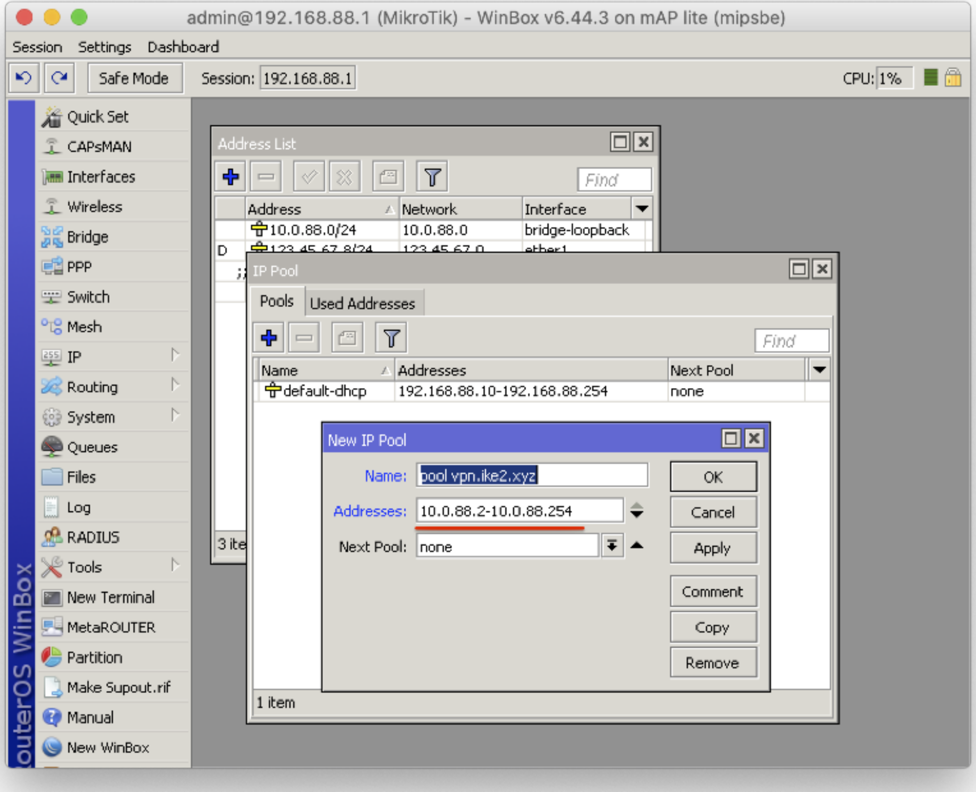
Address: 10.0.88.0/24

Network: 10.0.88.0

Interface: bridge-loopback

```
/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



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

Session: 192.168.88.1

Address List

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

3 ite

IP Pool

Name	Addresses	Next Pool
default-dhcp	192.168.88.10-192.168.88.254	none

1 item

New IP Pool

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

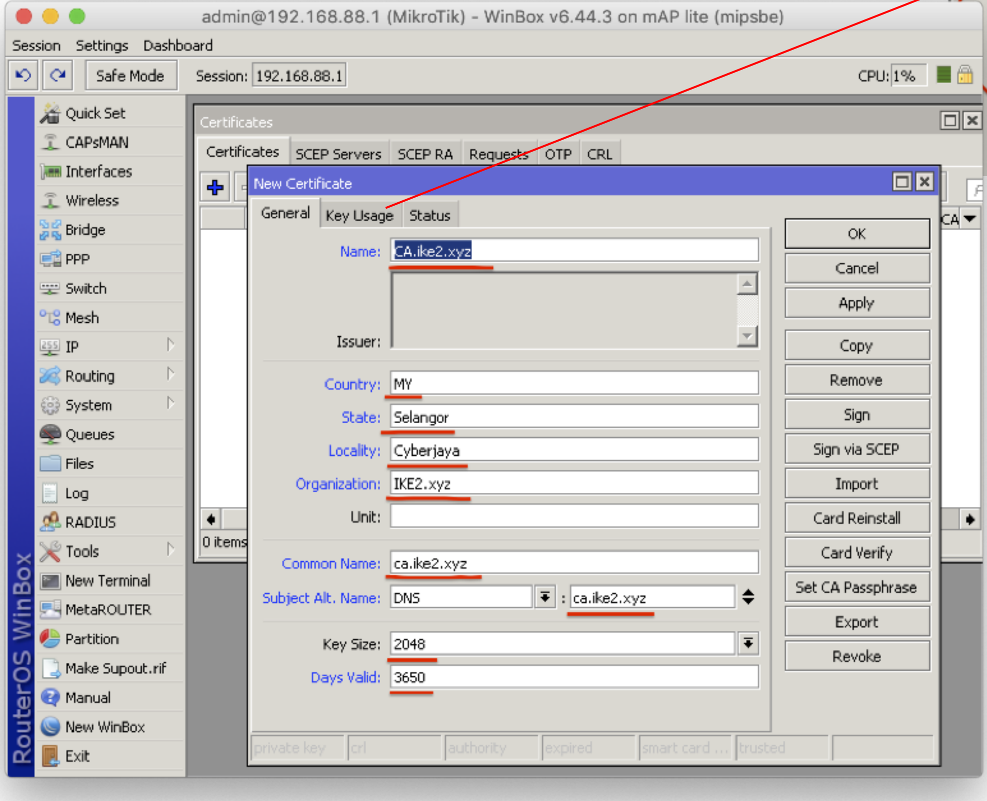
```
/ip pool add name="pool
vpn.ike2.xyz"
ranges=10.0.88.2-10.0.88.254
```

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



Name: CA.ike2.xyz

Issuer:

Country: MY

State: Selangor

Locality: Cyberjaya

Organization: IKE2.xyz

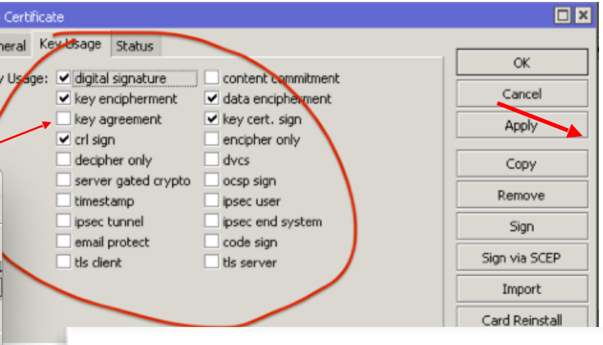
Unit:

Common Name: ca.ike2.xyz

Subject Alt. Name: DNS : ca.ike2.xyz

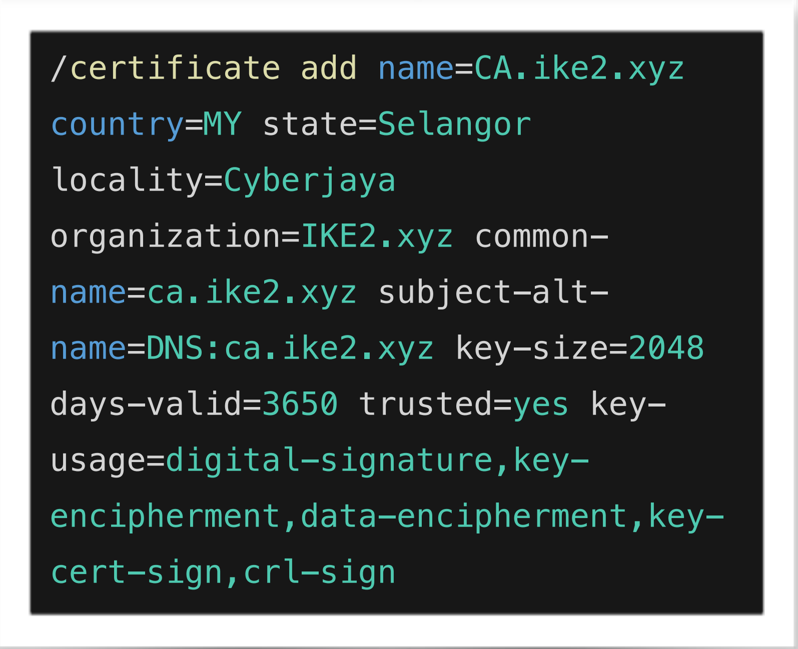
Key Size: 2048

Days Valid: 3650



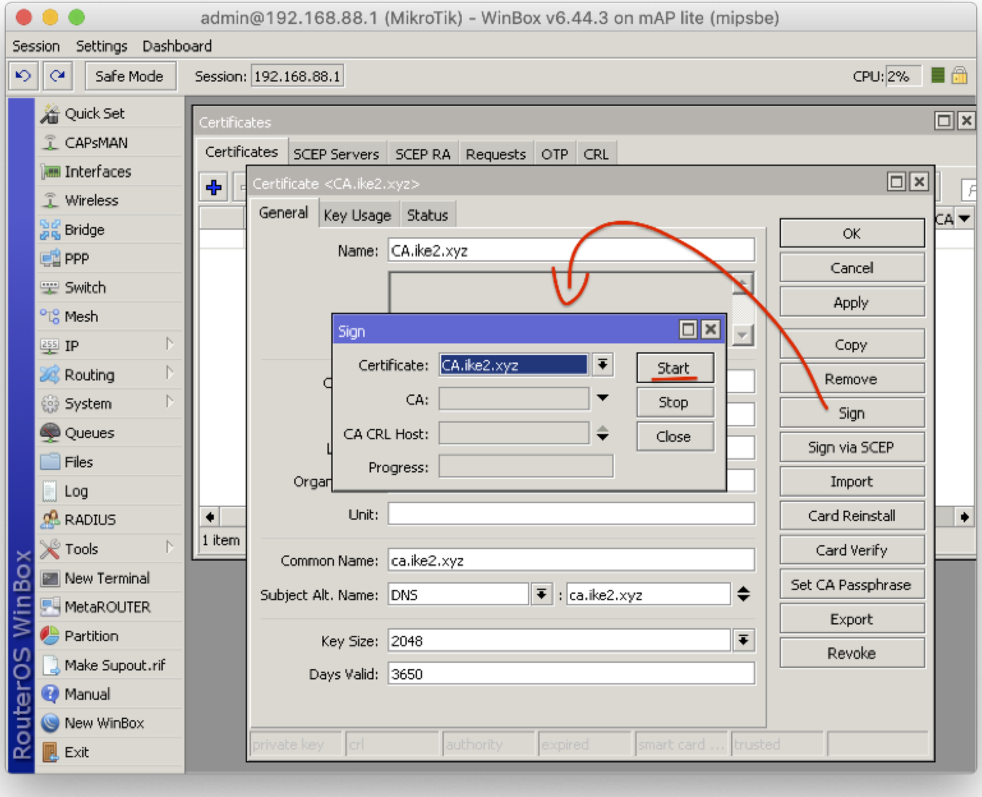
Key Usage:

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



```
/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)*


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

Session: 192.168.88.1

CPU: 2%

Certificate <CA.ike2.xyz>

Name: CA.ike2.xyz

Unit:

Common Name: ca.ike2.xyz

Subject Alt. Name: DNS : ca.ike2.xyz

Key Size: 2048

Days Valid: 3650

Sign

Certificate: CA.ike2.xyz

CA:

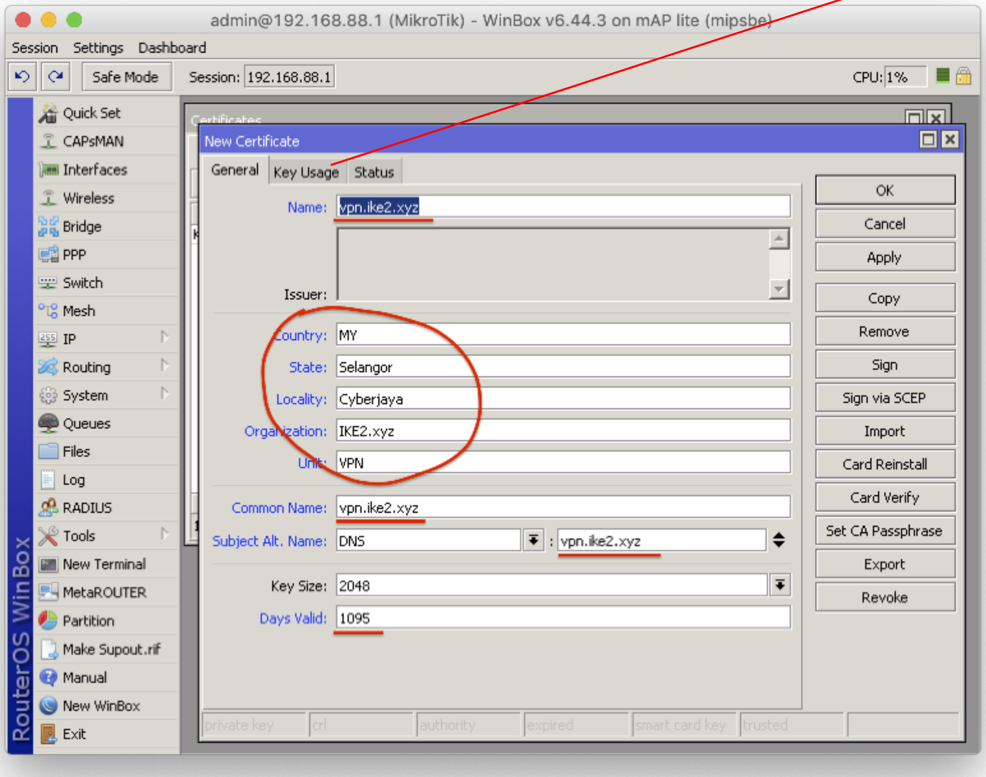
CA CRL Host:

Progress:

1 item

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

Generate server SSL certificate



Name: vpn.ike2.xyz

Issuer:

Country: MY

State: Selangor

Locality: Cyberjaya

Organization: IKE2.xyz

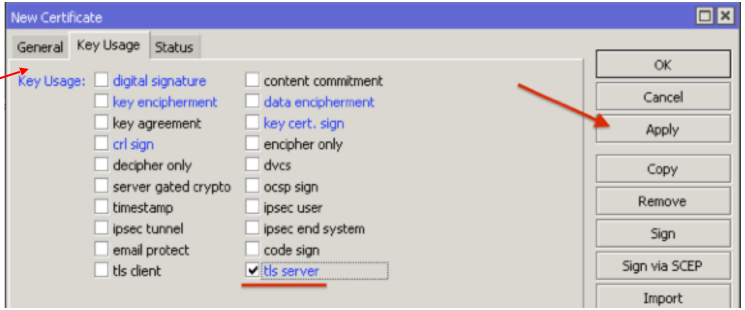
Unit: VPN

Common Name: vpn.ike2.xyz

Subject Alt. Name: DNS : vpn.ike2.xyz

Key Size: 2048

Days Valid: 1095

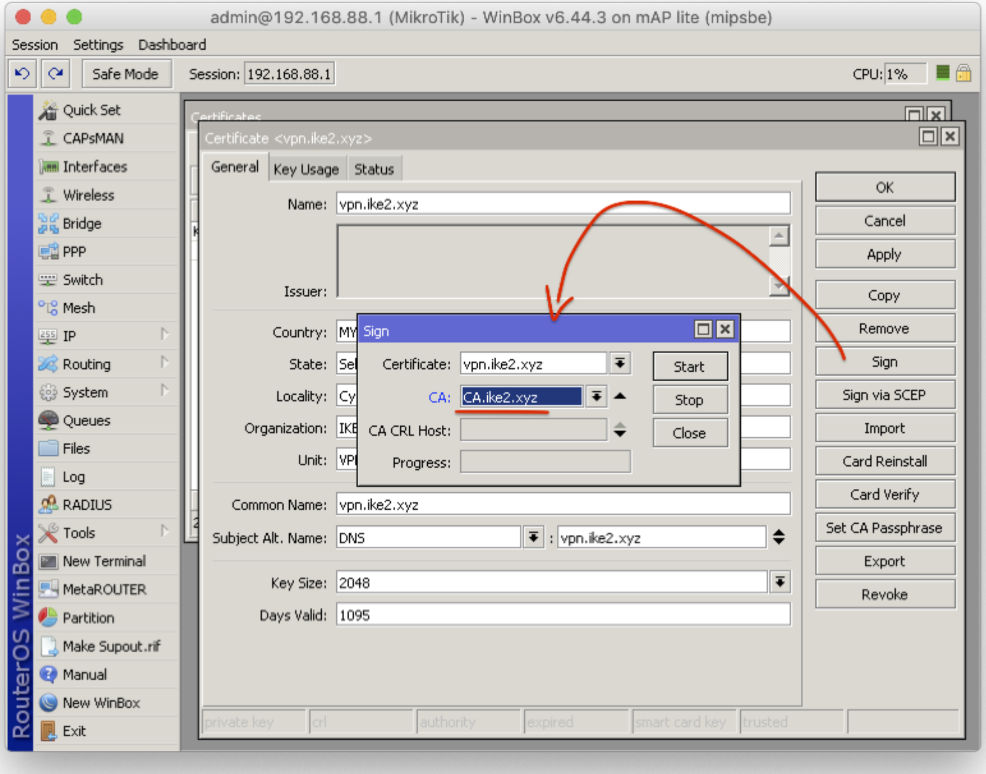


Key Usage:

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

```
/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



Session: 192.168.88.1

CPU: 1%

Certificate <vpn.ike2.xyz>

Name: vpn.ike2.xyz

Issuer:

Country: MY

State: Se

Locality: Cy

Organization: IKE

Unit: VPI

Certificate: vpn.ike2.xyz

CA: CA.ike2.xyz

CA CRL Host:

Progress:

Common Name: vpn.ike2.xyz

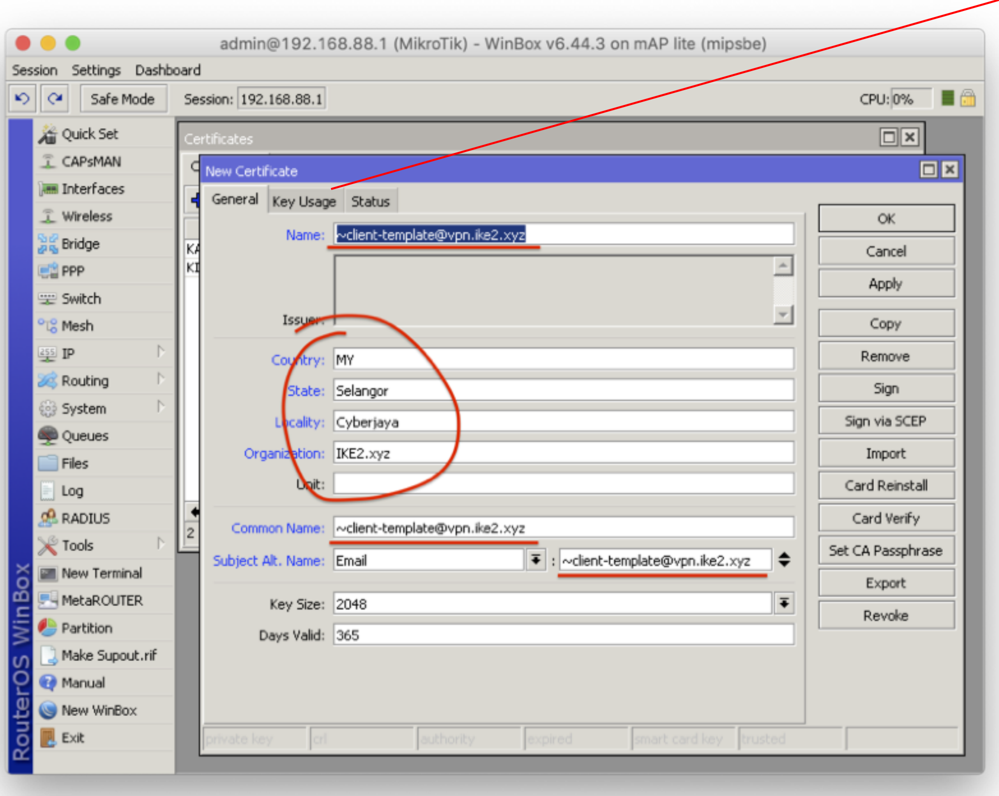
Subject Alt. Name: DNS : vpn.ike2.xyz

Key Size: 2048

Days Valid: 1095

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

Client certificate template



Name: ~client-template@vpn.ike2.xyz

Issuer:

Country: MY

State: Selangor

Locality: Cyberjaya

Organization: IKE2.xyz

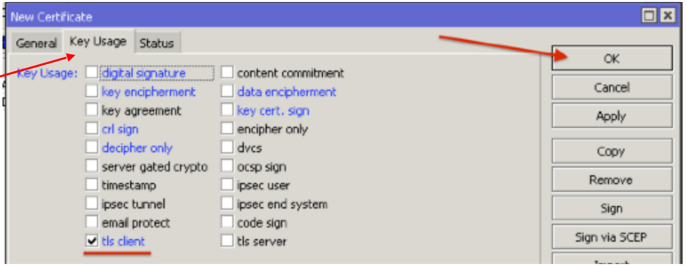
Unit:

Common Name: ~client-template@vpn.ike2.xyz

Subject Alt. Name: Email : ~client-template@vpn.ike2.xyz

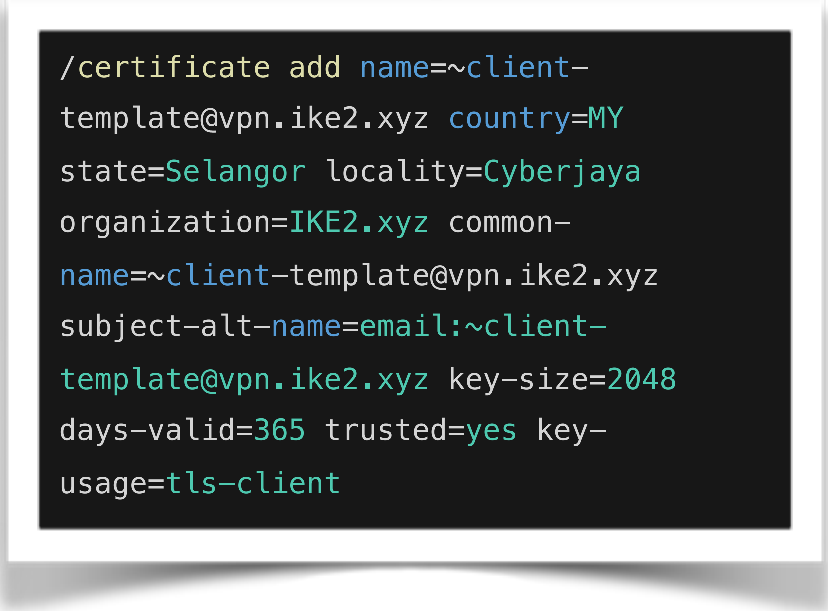
Key Size: 2048

Days Valid: 365



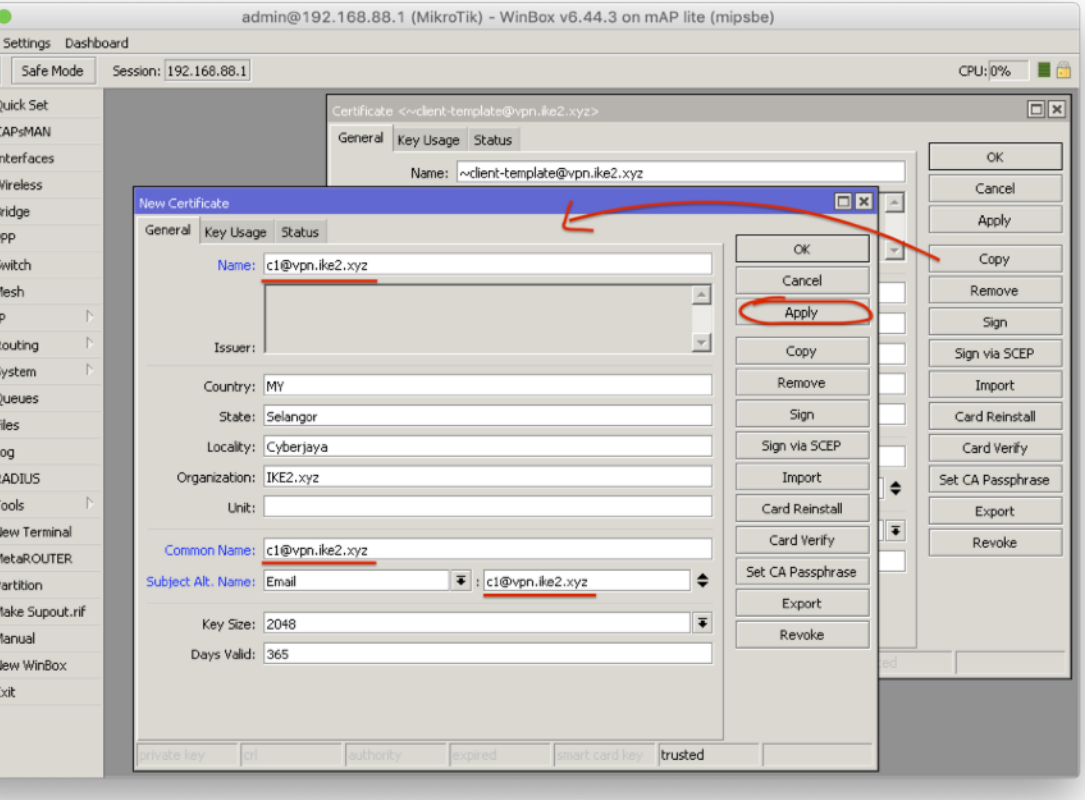
Key Usage:

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



```
/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



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

Session: 192.168.88.1

CPU: 0%

Certificate <~client-template@vpn.ike2.xyz>

Name: ~client-template@vpn.ike2.xyz

New Certificate

Name: c1@vpn.ike2.xyz

Issuer:

Country: MY

State: Selangor

Locality: Cyberjaya

Organization: IKE2.xyz

Unit:

Common Name: c1@vpn.ike2.xyz

Subject Alt. Name: Email : c1@vpn.ike2.xyz

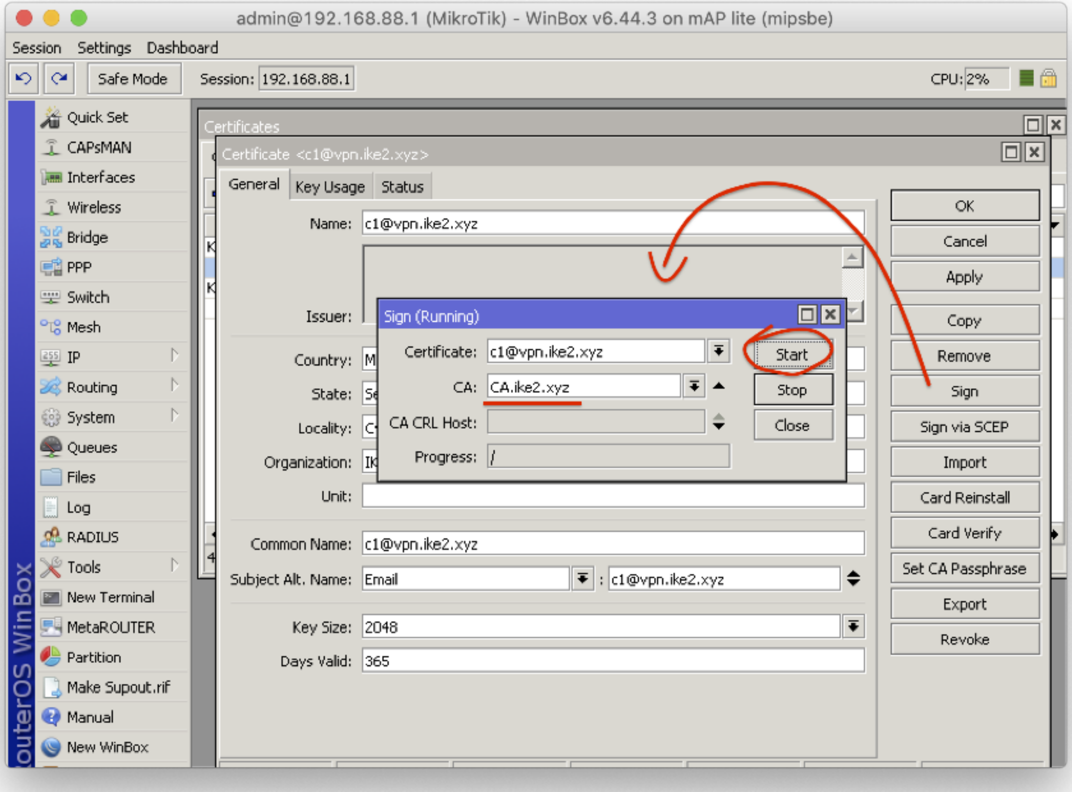
Key Size: 2048

Days Valid: 365

trusted

```
/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



Session: 192.168.88.1

CPU: 2%

Certificate <c1@vpn.ike2.xyz>

Name: c1@vpn.ike2.xyz

Issuer:

Country: M

State: Se

Locality: C

Organization: IK

Unit:

Common Name: c1@vpn.ike2.xyz

Subject Alt. Name: Email : c1@vpn.ike2.xyz

Key Size: 2048

Days Valid: 365

Sign (Running)

Certificate: c1@vpn.ike2.xyz

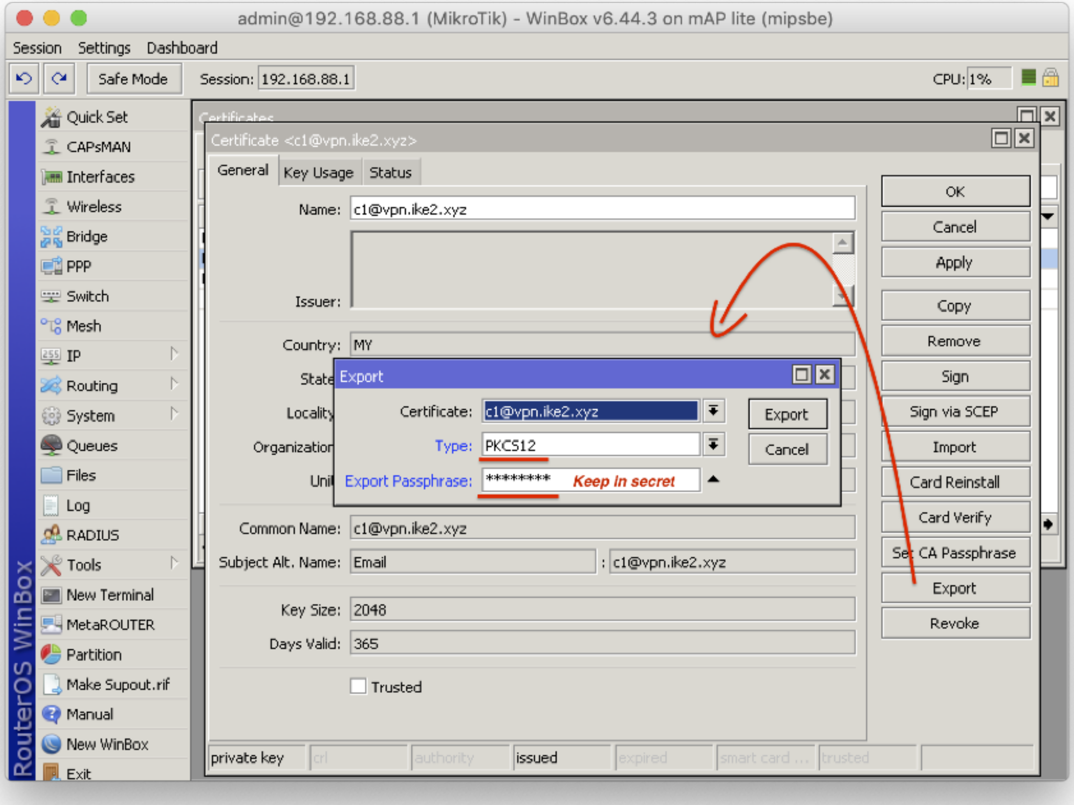
CA: CA.ike2.xyz

CA CRL Host:

Progress: /

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

Export client SSL certificate + private key to .p12 file



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

Session: 192.168.88.1

CPU: 1%

Certificate <c1@vpn.ike2.xyz>

Name: c1@vpn.ike2.xyz

Issuer:

Country: MY

Export

Certificate: c1@vpn.ike2.xyz

Type: PKCS12

Export Passphrase: ******** Keep in secret

Common Name: c1@vpn.ike2.xyz

Subject Alt. Name: Email : c1@vpn.ike2.xyz

Key Size: 2048

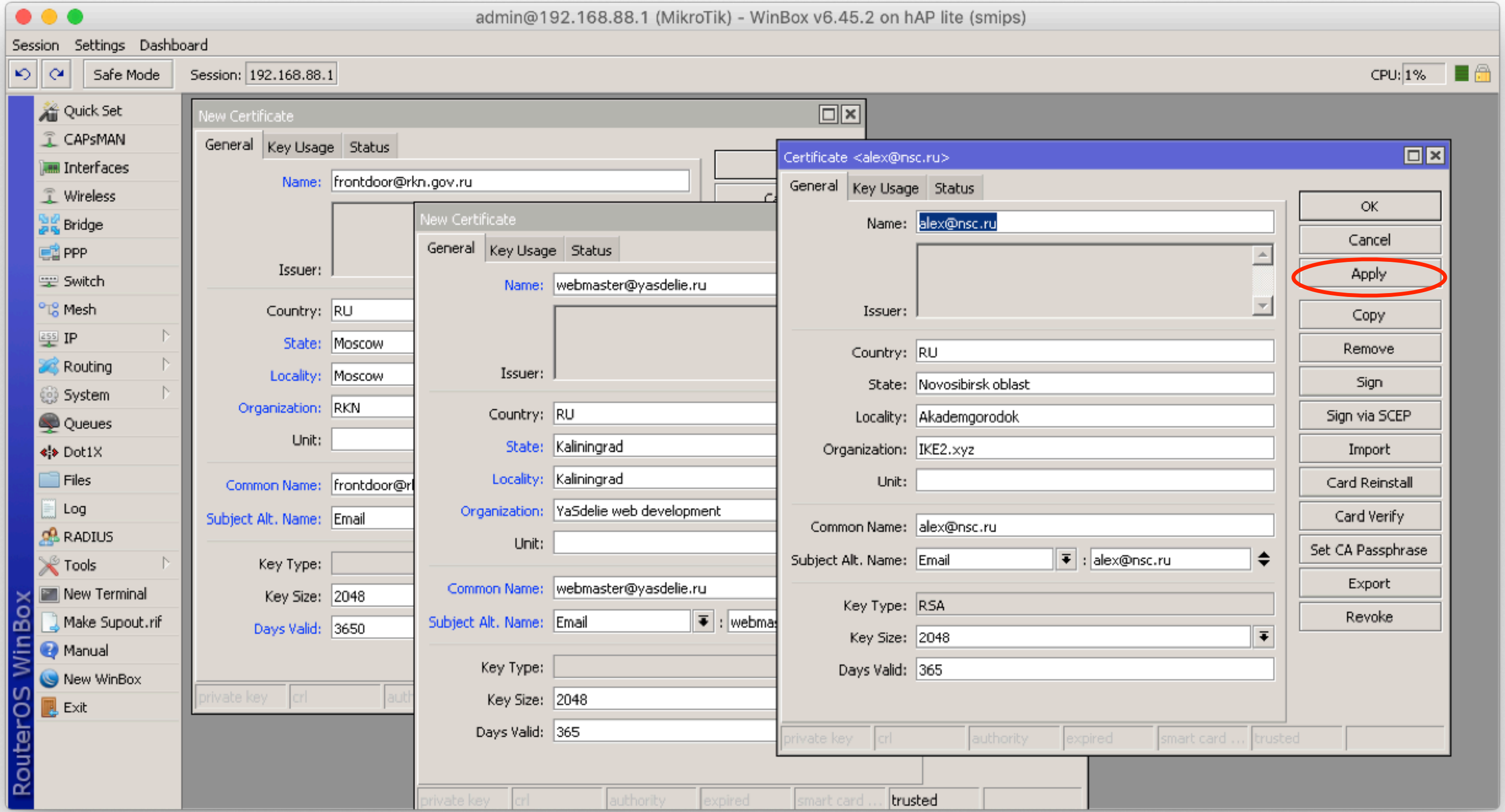
Days Valid: 365

□ Trusted

private key | crl | authority | issued | expired | smart card ... | trusted

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

Generate various client SSL certificates from template (example)



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

Session: 192.168.88.1

CPU: 1%

New Certificate

Name: frontdoor@rkn.gov.ru

Issuer:

Country: RU

State: Moscow

Locality: Moscow

Organization: RKN

Unit:

Common Name: frontdoor@r

Subject Alt. Name: Email

Key Type:

Key Size: 2048

Days Valid: 3650

New Certificate

Name: webmaster@yasdelie.ru

Issuer:

Country: RU

State: Kaliningrad

Locality: Kaliningrad

Organization: YaSdelie web development

Unit:

Common Name: webmaster@yasdelie.ru

Subject Alt. Name: Email : webmas

Key Type:

Key Size: 2048

Days Valid: 365

Certificate <alex@nsc.ru>

Name: alex@nsc.ru

Issuer:

Country: RU

State: Novosibirsk oblast

Locality: Akademgorodok

Organization: IKE2.xyz

Unit:

Common Name: alex@nsc.ru

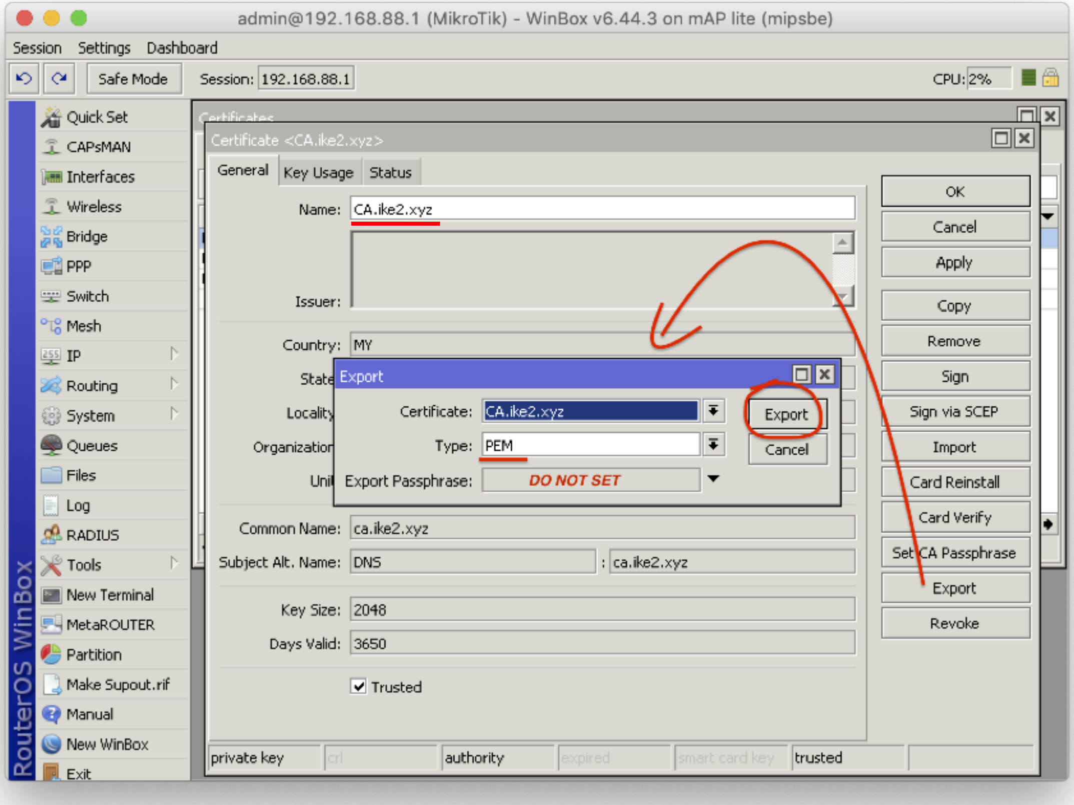
Subject Alt. Name: Email : alex@nsc.ru

Key Type: RSA

Key Size: 2048

Days Valid: 365

Export CA SSL certificate .crt file



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

Session: 192.168.88.1

CPU: 2%

Certificate <CA.ike2.xyz>

Name: CA.ike2.xyz

Issuer:

Country: MY

Common Name: ca.ike2.xyz

Subject Alt. Name: DNS : ca.ike2.xyz

Key Size: 2048

Days Valid: 3650

☑ Trusted

private key | crl | authority | expired | smart card key | trusted

Export

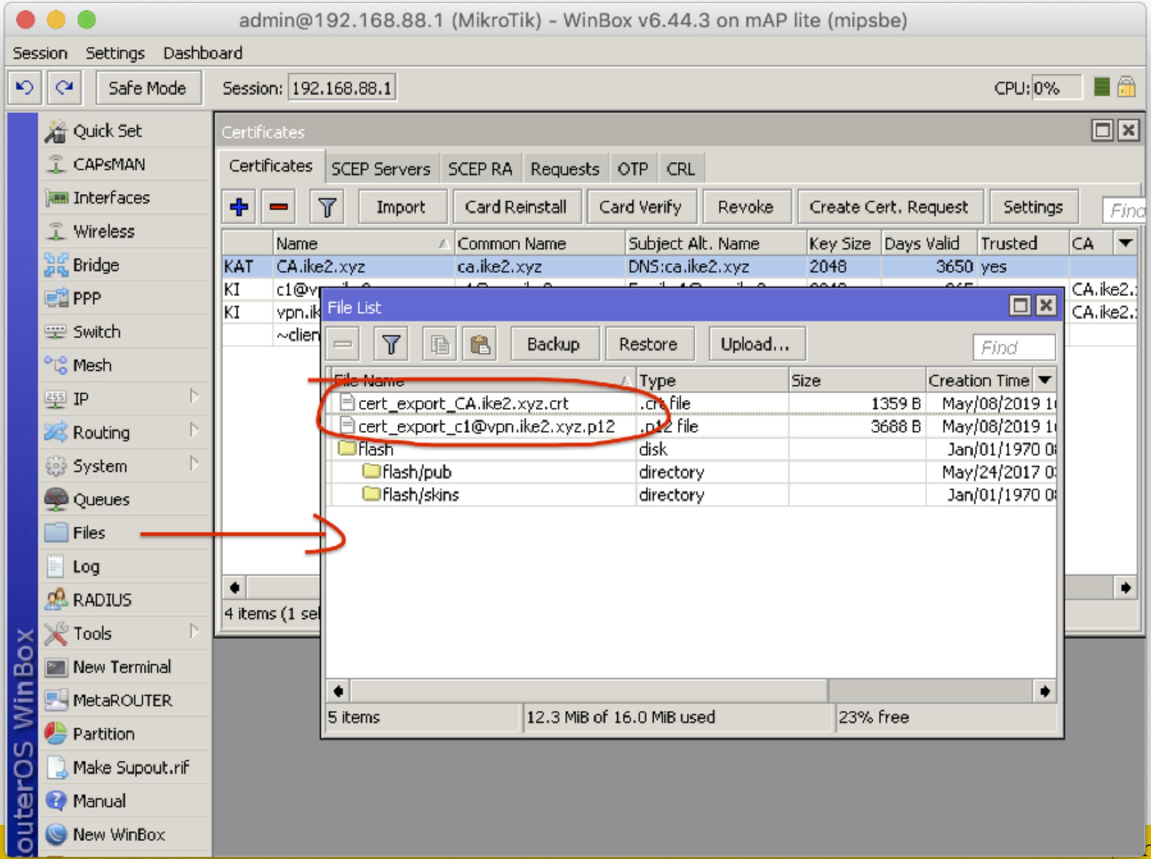
Certificate: CA.ike2.xyz

Type: PEM

Export Passphrase: *DO NOT SET*

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

Download exported SSL certificates

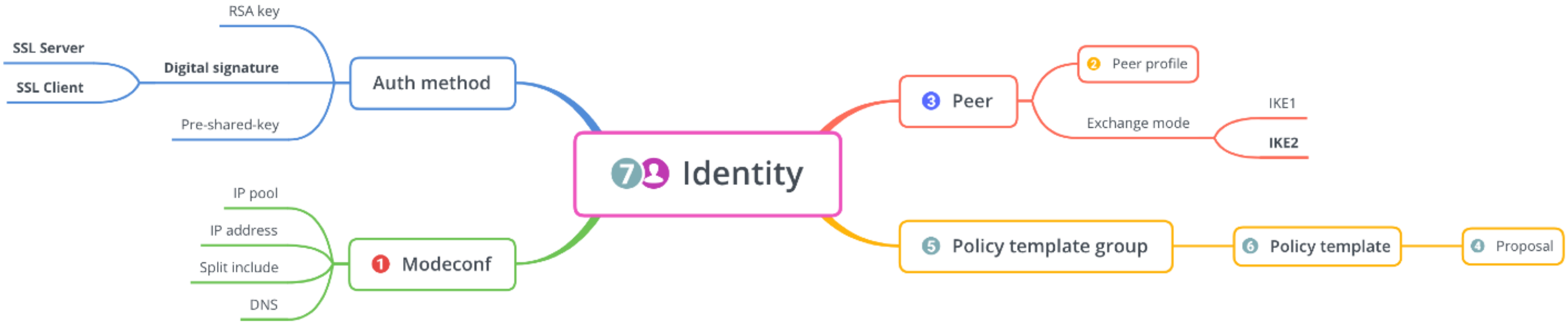


	Name	Common Name	Subject Alt. Name	Key Size	Days Valid	Trusted	CA
KAT	CA.ike2.xyz	ca.ike2.xyz	DNS:ca.ike2.xyz	2048	3650	yes	
KI	c1@v						CA.ike2.
KI	vpn.ik						CA.ike2.
	~clien						

4 items (1 sel

File Name	Type	Size	Creation Time
cert_export_CA.ike2.xyz.crt	.crt file	1359 B	May/08/2019 1
cert_export_c1@vpn.ike2.xyz.p12	.p12 file	3688 B	May/08/2019 1
flash	disk		Jan/01/1970 0
flash/pub	directory		May/24/2017 0
flash/skins	directory		Jan/01/1970 0

5 items | 12.3 MiB of 16.0 MiB used | 23% free



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;

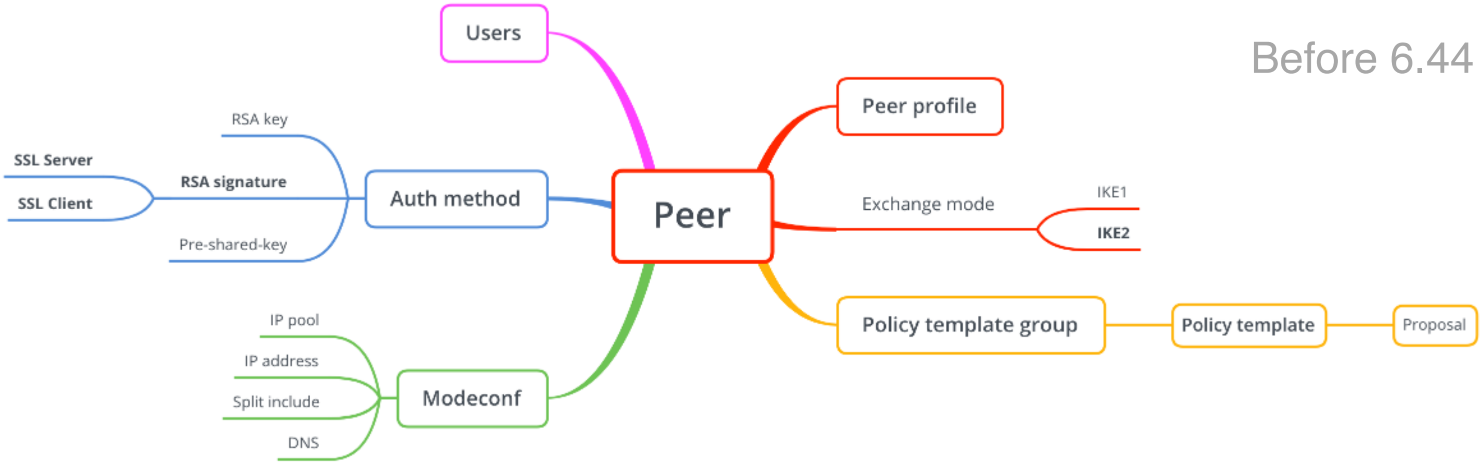
Key **ipsec** changes in RouterOS 6.44

*) 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;

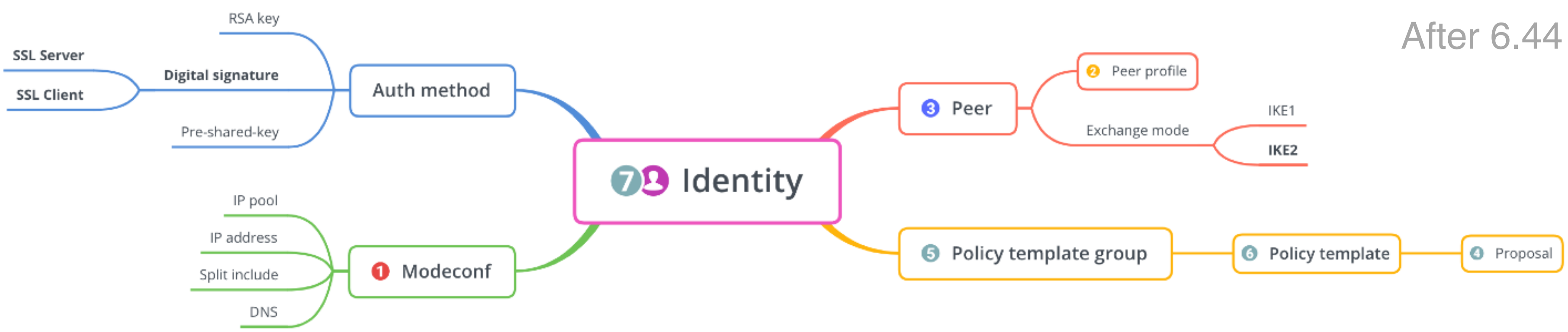
*) ike2 - added option to specify certificate chain;
*) ike2 - added peer identity validation for RSA auth (disabled after upgrade);
*) ike2 - allow to match responder peer by "my-id=fqdn" field;
*) ike2 - send split networks over DHCP (option 249) to Windows initiators if DHCP Inform is received;

IPSec structure

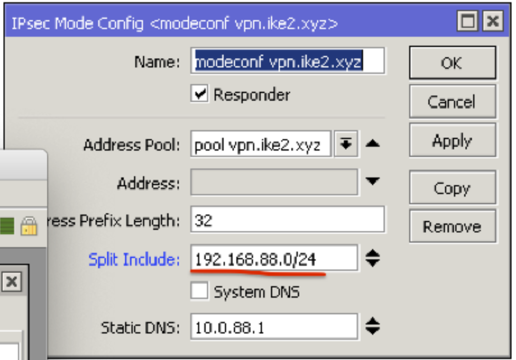
Before 6.44



After 6.44



1. Setting up new IPSec mode config



IPsec Mode Config <modeconf vpn.ike2.xyz>

Name: modeconf vpn.ike2.xyz

☑ Responder

Address Pool: pool vpn.ike2.xyz

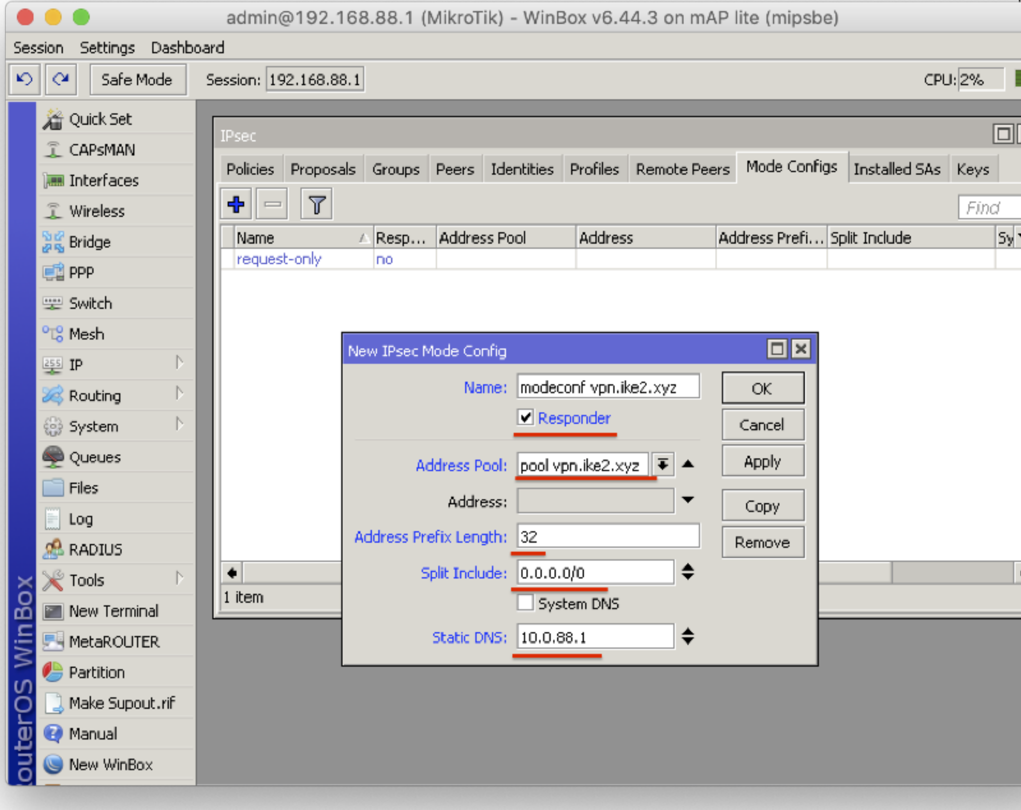
Address:

ress Prefix Length: 32

Split Include: 192.168.88.0/24

□ System DNS

Static DNS: 10.0.88.1



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

Session: 192.168.88.1 CPU: 2%

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

1 item

New IPsec Mode Config

Name: modeconf vpn.ike2.xyz

☑ Responder

Address Pool: pool vpn.ike2.xyz

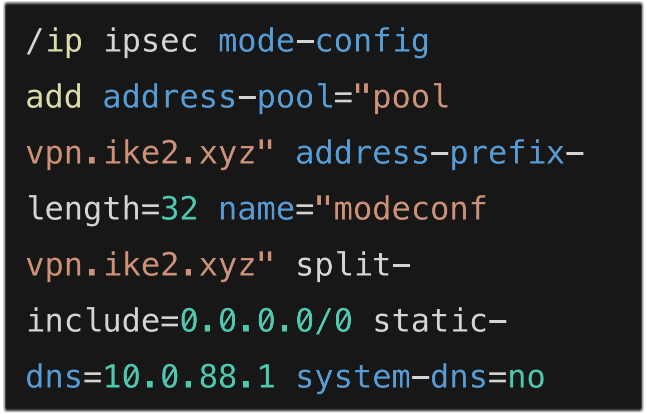
Address:

Address Prefix Length: 32

Split Include: 0.0.0.0/0

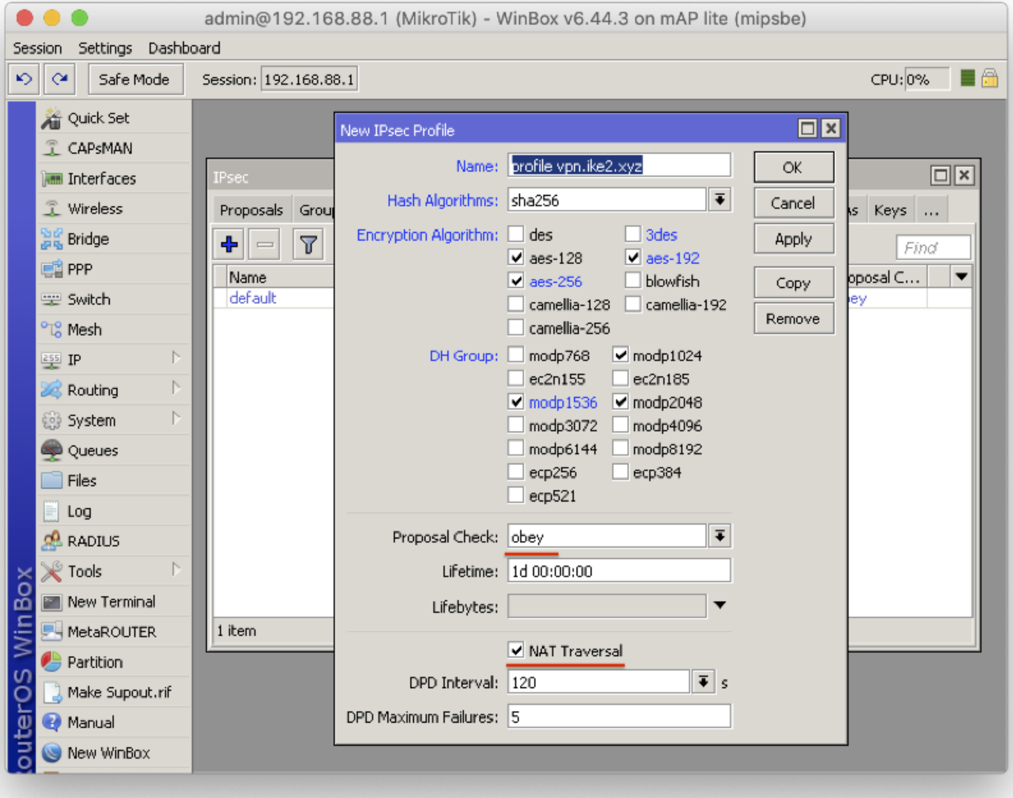
□ System DNS

Static DNS: 10.0.88.1



```
/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)*



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

Session: 192.168.88.1

CPU: 0%

New IPsec Profile

Name: profile vpn.ike2.xyz

Hash Algorithms: sha256

Encryption Algorithm: □ des □ 3des ☑ aes-128 ☑ aes-192 ☑ aes-256 □ blowfish □ camellia-128 □ camellia-192 □ camellia-256

DH Group: □ modp768 ☑ modp1024 □ ec2n155 □ ec2n185 ☑ modp1536 ☑ modp2048 □ modp3072 □ modp4096 □ modp6144 □ modp8192 □ ecp256 □ ecp384 □ ecp521

Proposal Check: obey

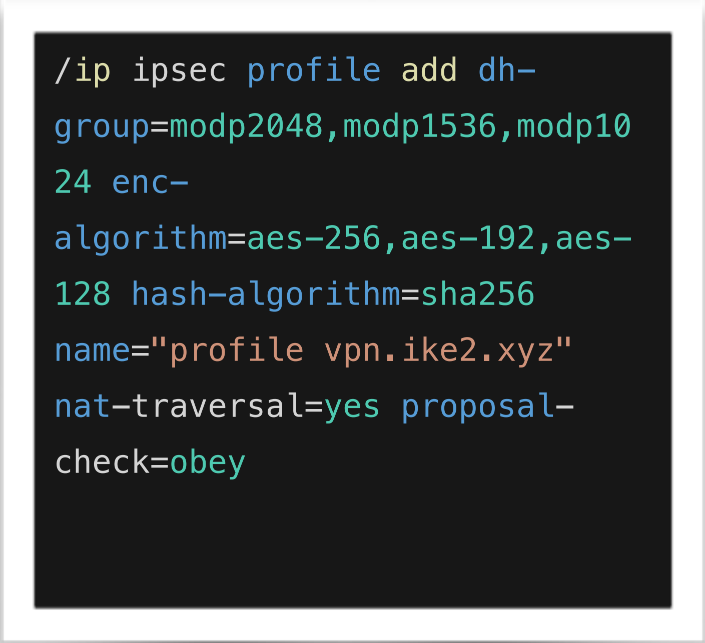
Lifetime: 1d 00:00:00

Lifebytes:

☑ NAT Traversal

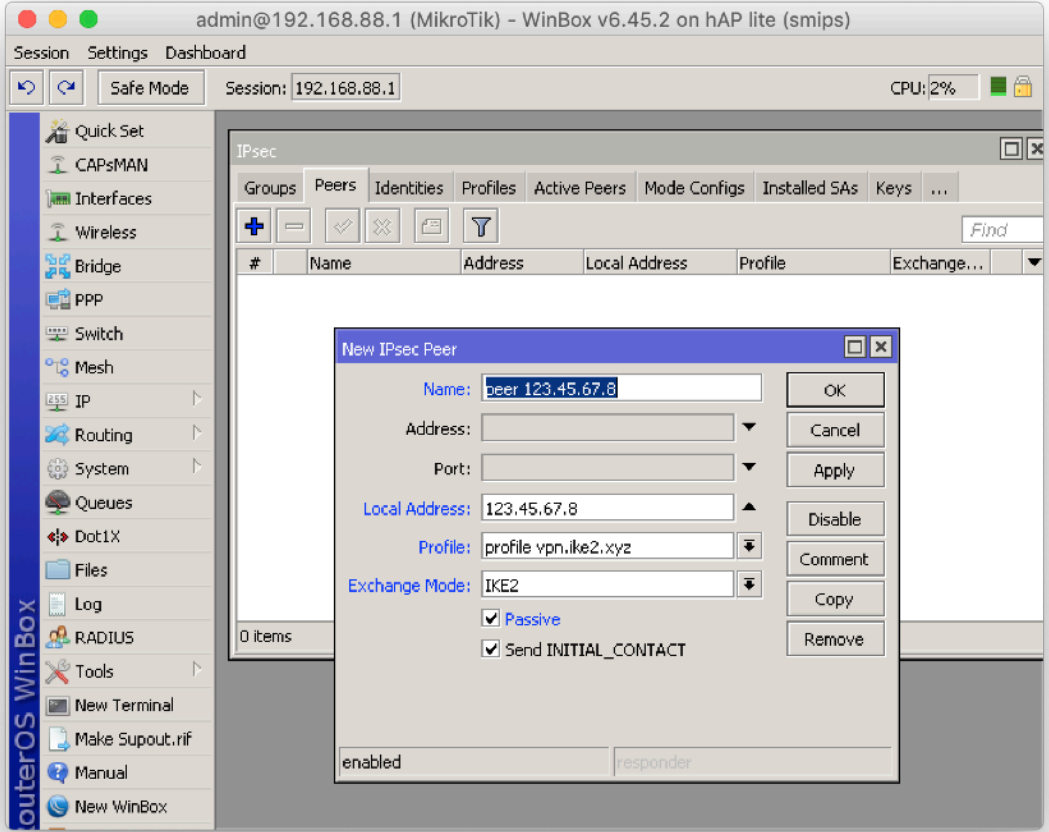
DPD Interval: 120 s

DPD Maximum Failures: 5



```
/ip ipsec profile add dh-group=modp2048,modp1536,modp1024 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)



Name: peer 123.45.67.8

Address:

Port:

Local Address: 123.45.67.8

Profile: profile vpn.ike2.xyz

Exchange Mode: IKE2

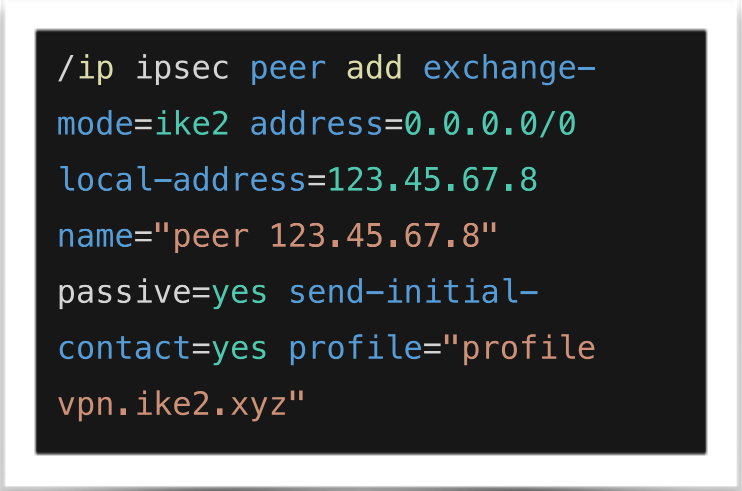
☑ Passive

☑ Send INITIAL_CONTACT

enabled | responder

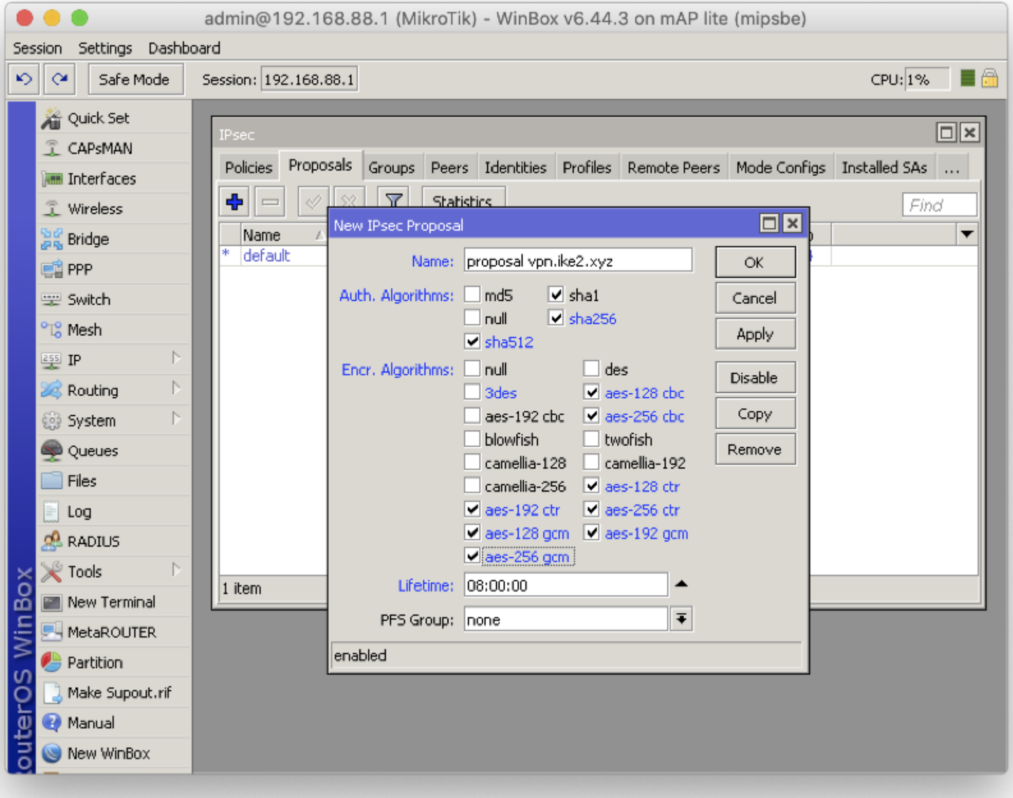
Accepting clients from all IP addresses **0.0.0.0/0**

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)*



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

New IPsec Proposal

Name: proposal vpn.ike2.xyz

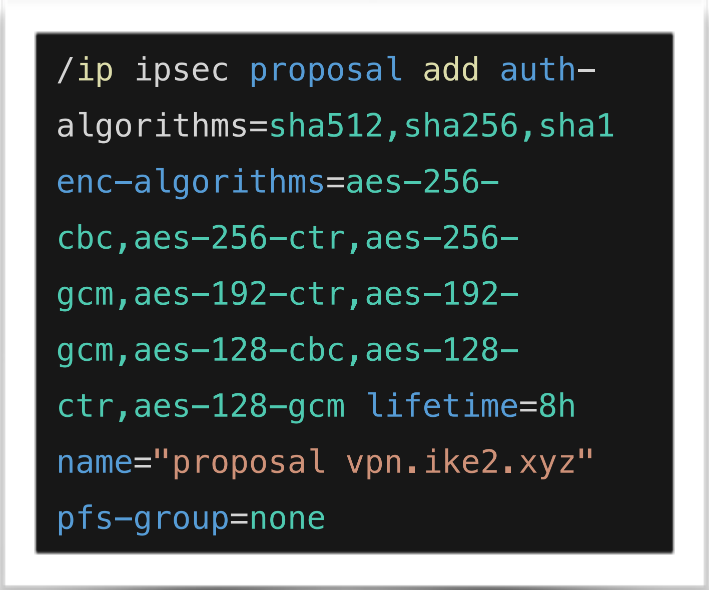
Auth. Algorithms: □ md5 ☑ sha1 □ null ☑ sha256 ☑ sha512

Encr. Algorithms: □ null □ des □ 3des ☑ aes-128 cbc □ aes-192 cbc ☑ aes-256 cbc □ blowfish □ twofish □ camellia-128 □ camellia-192 □ camellia-256 ☑ aes-128 ctr ☑ aes-192 ctr ☑ aes-256 ctr ☑ aes-128 gcm ☑ aes-192 gcm ☑ aes-256 gcm

Lifetime: 08:00:00

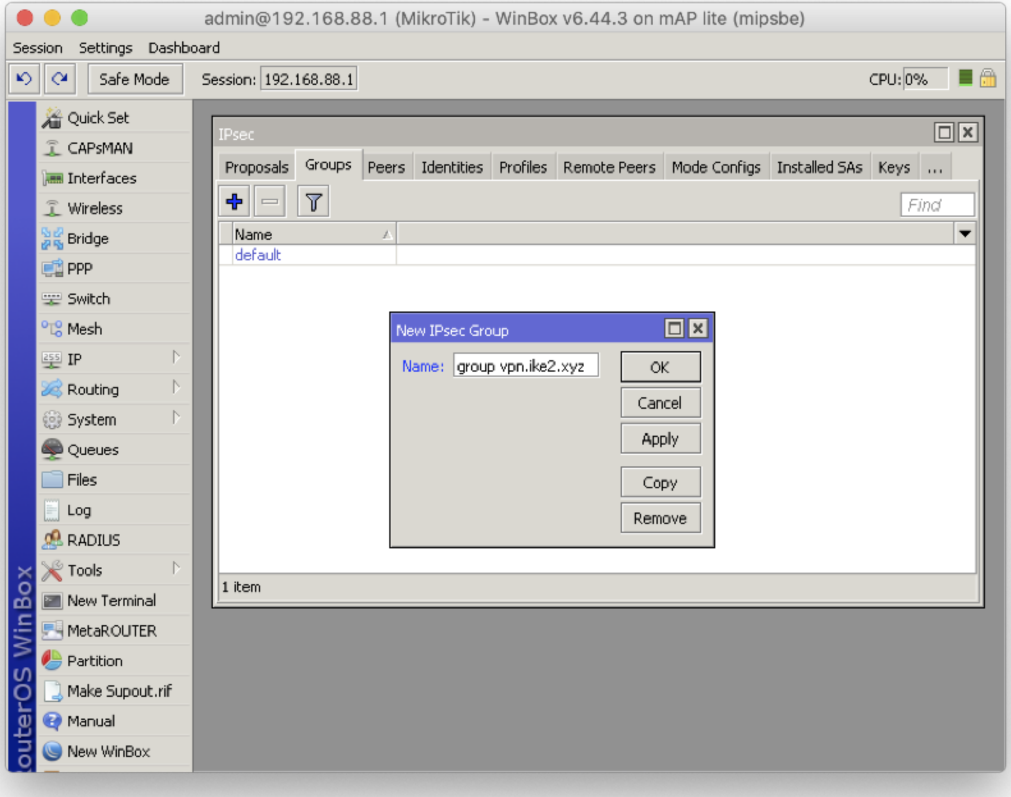
PFS Group: none

enabled



```
/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
```

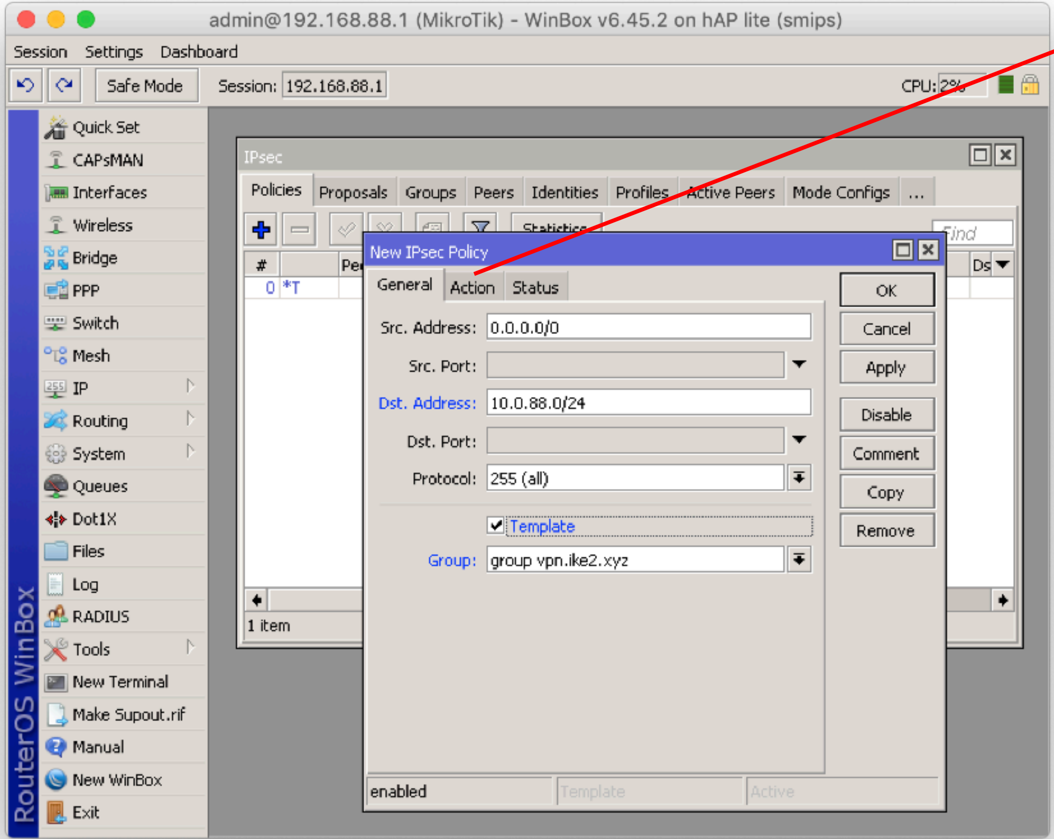
5. Setting up new IPSec policy group



Name: group vpn.ike2.xyz

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

6. Setting up new IPSec policy template



New IPsec Policy

General | Action | Status

Src. Address: 0.0.0.0/0

Src. Port:

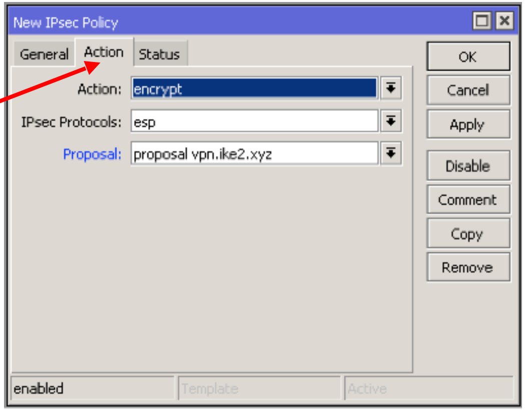
Dst. Address: 10.0.88.0/24

Dst. Port:

Protocol: 255 (all)

☑ Template

Group: group vpn.ike2.xyz



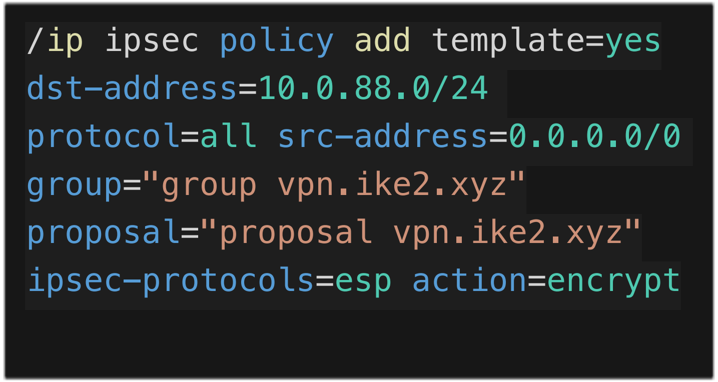
New IPsec Policy

General | Action | Status

Action: encrypt

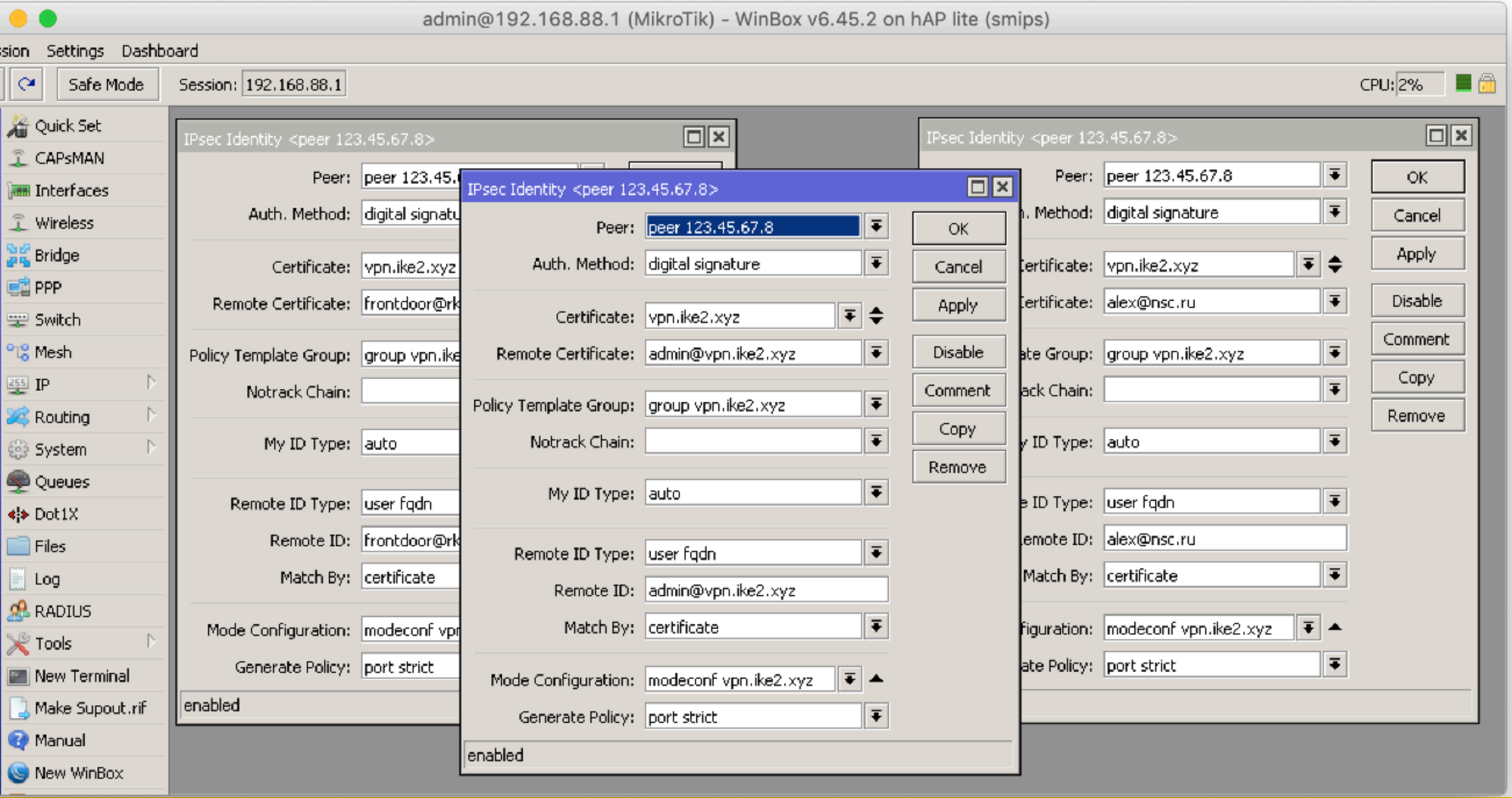
IPsec Protocols: esp

Proposal: proposal vpn.ike2.xyz



```
/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



IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.
Auth. Method: digital signatu
Certificate: vpn.ike2.xyz
Remote Certificate: frontdoor@rk
Policy Template Group: group vpn.ike
Notrack Chain:
My ID Type: auto
Remote ID Type: user fqdn
Remote ID: frontdoor@rk
Match By: certificate
Mode Configuration: modeconf vp
Generate Policy: port strict
enabled

IPsec Identity <peer 123.45.67.8>

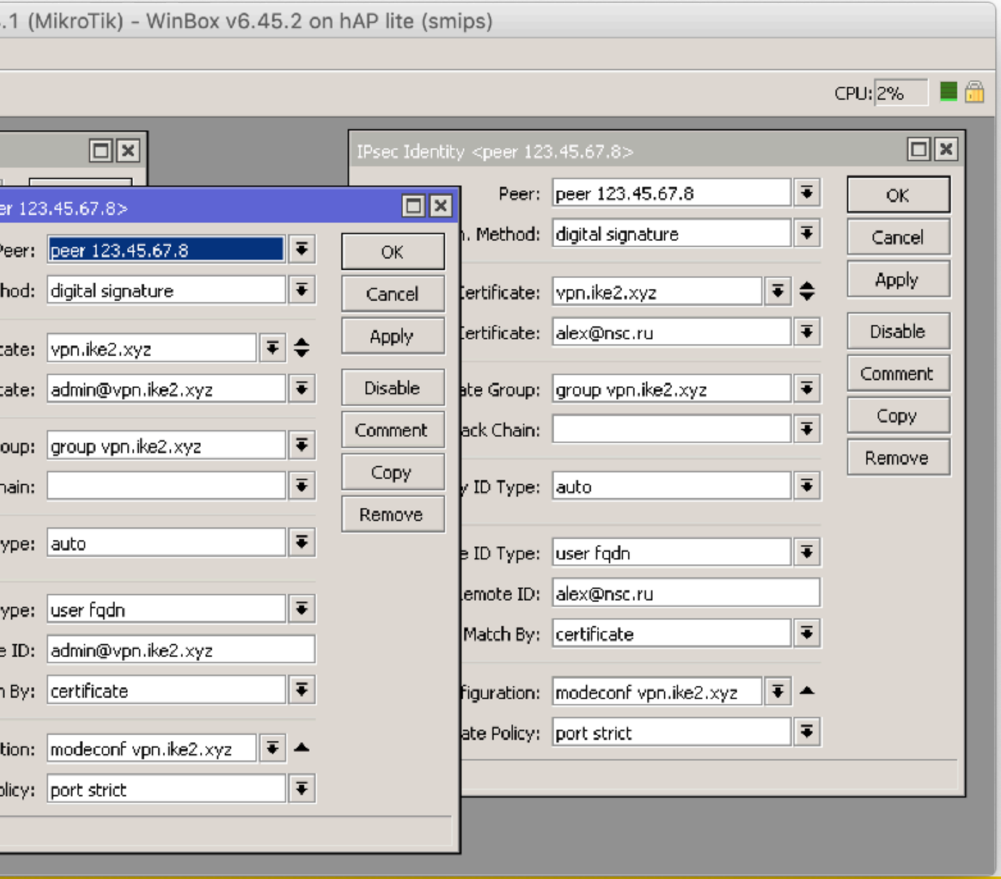
Peer: peer 123.45.67.8
Auth. Method: digital signature
Certificate: vpn.ike2.xyz
Remote Certificate: admin@vpn.ike2.xyz
Policy Template Group: group vpn.ike2.xyz
Notrack Chain:
My ID Type: auto
Remote ID Type: user fqdn
Remote ID: admin@vpn.ike2.xyz
Match By: certificate
Mode Configuration: modeconf vpn.ike2.xyz
Generate Policy: port strict
enabled

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8
. Method: digital signature
ertificate: vpn.ike2.xyz
ertificate: alex@nsc.ru
ate Group: group vpn.ike2.xyz
ack Chain:
y ID Type: auto
e ID Type: user fqdn
emote ID: alex@nsc.ru
Match By: certificate
figuration: modeconf vpn.ike2.xyz
ate Policy: port strict

```
/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

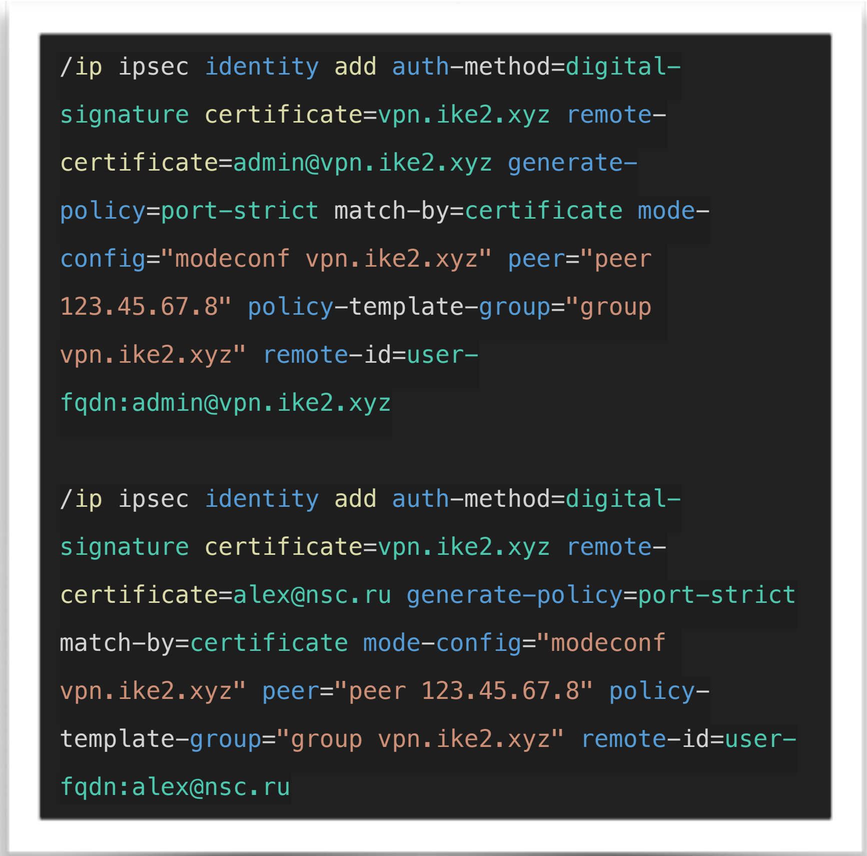


er 123.45.67.8>

Peer: peer 123.45.67.8
hod: digital signature
cate: vpn.ike2.xyz
cate: admin@vpn.ike2.xyz
oup: group vpn.ike2.xyz
hain:
ype: auto
ype: user fqdn
e ID: admin@vpn.ike2.xyz
n By: certificate
tion: modeconf vpn.ike2.xyz
licy: port strict

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8
. Method: digital signature
ertificate: vpn.ike2.xyz
ertificate: alex@nsc.ru
ate Group: group vpn.ike2.xyz
ack Chain:
y ID Type: auto
e ID Type: user fqdn
emote ID: alex@nsc.ru
Match By: certificate
figuration: modeconf vpn.ike2.xyz
ate Policy: port strict



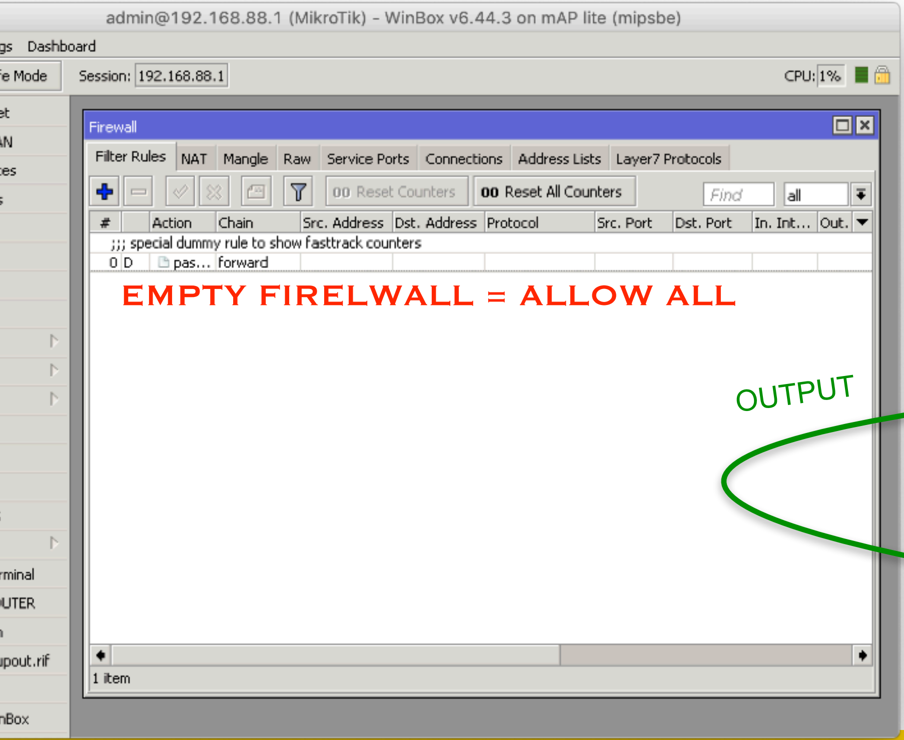
```
/ip ipsec identity add auth-method=digital-signature certificate=vpn.ike2.xyz remote-certificate=admin@vpn.ike2.xyz generate-policy=port-strict match-by=certificate mode-config="modeconf vpn.ike2.xyz" peer="peer 123.45.67.8" policy-template-group="group vpn.ike2.xyz" remote-id=user-fqdn:admin@vpn.ike2.xyz

/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



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

Session: 192.168.88.1 CPU: 1%

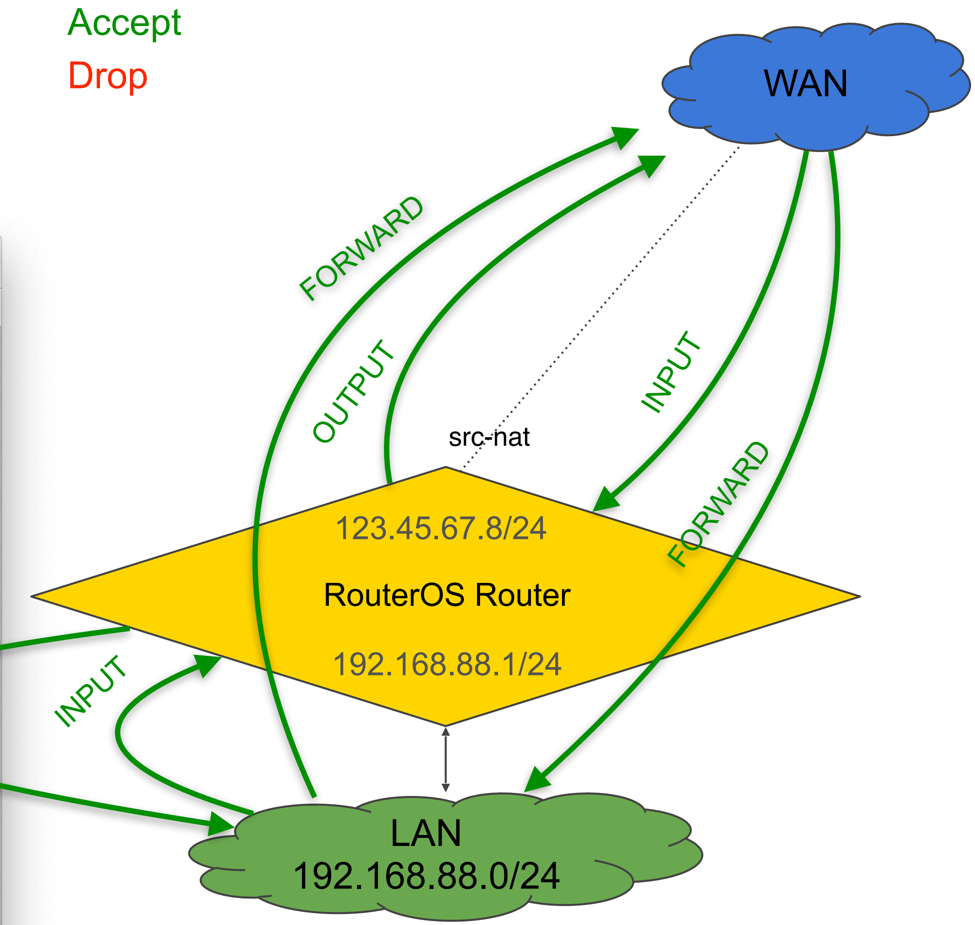
Firewall

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

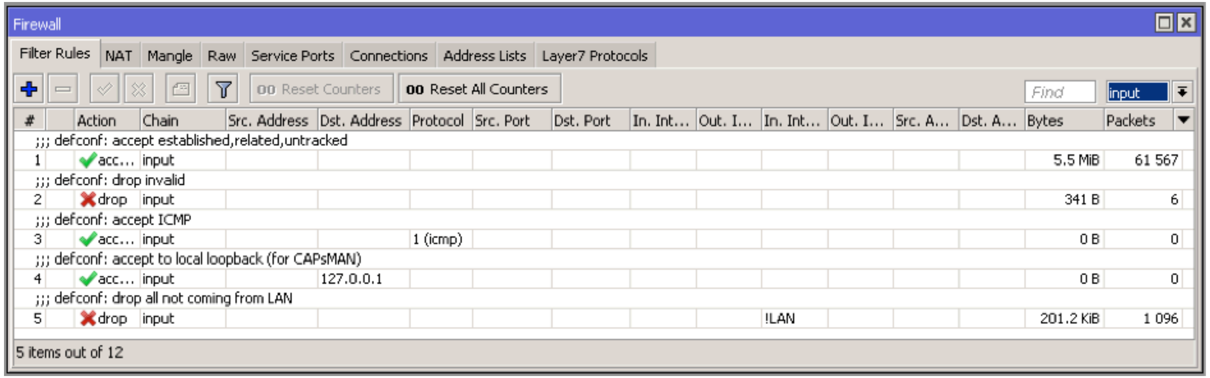
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out.
;;; special dummy rule to show fasttrack counters									
0 D	pas...	forward							

EMPTY FIRELWALL = ALLOW ALL

1 item



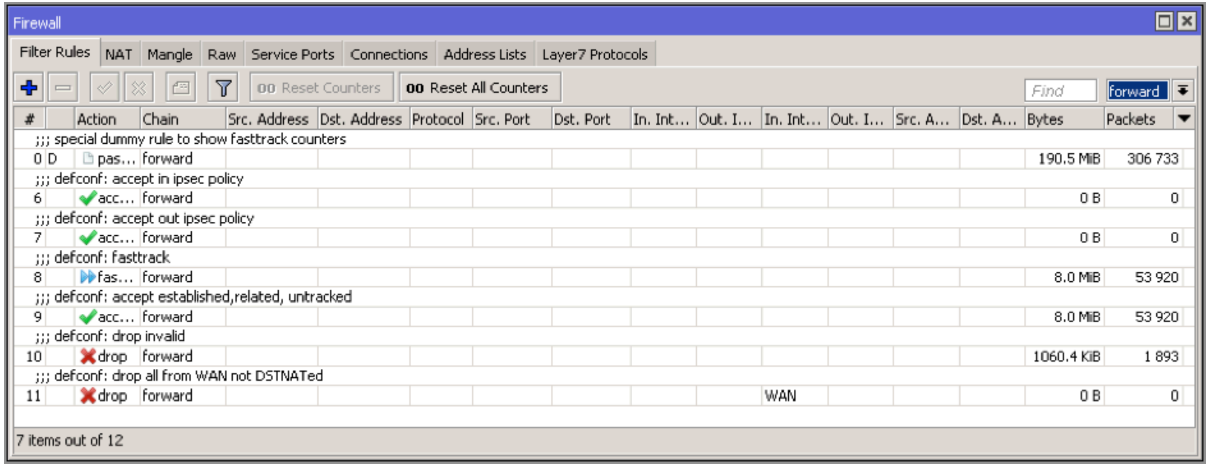
RouterOS 6.45+ default configuration firewall overview



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



forward

#	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
```

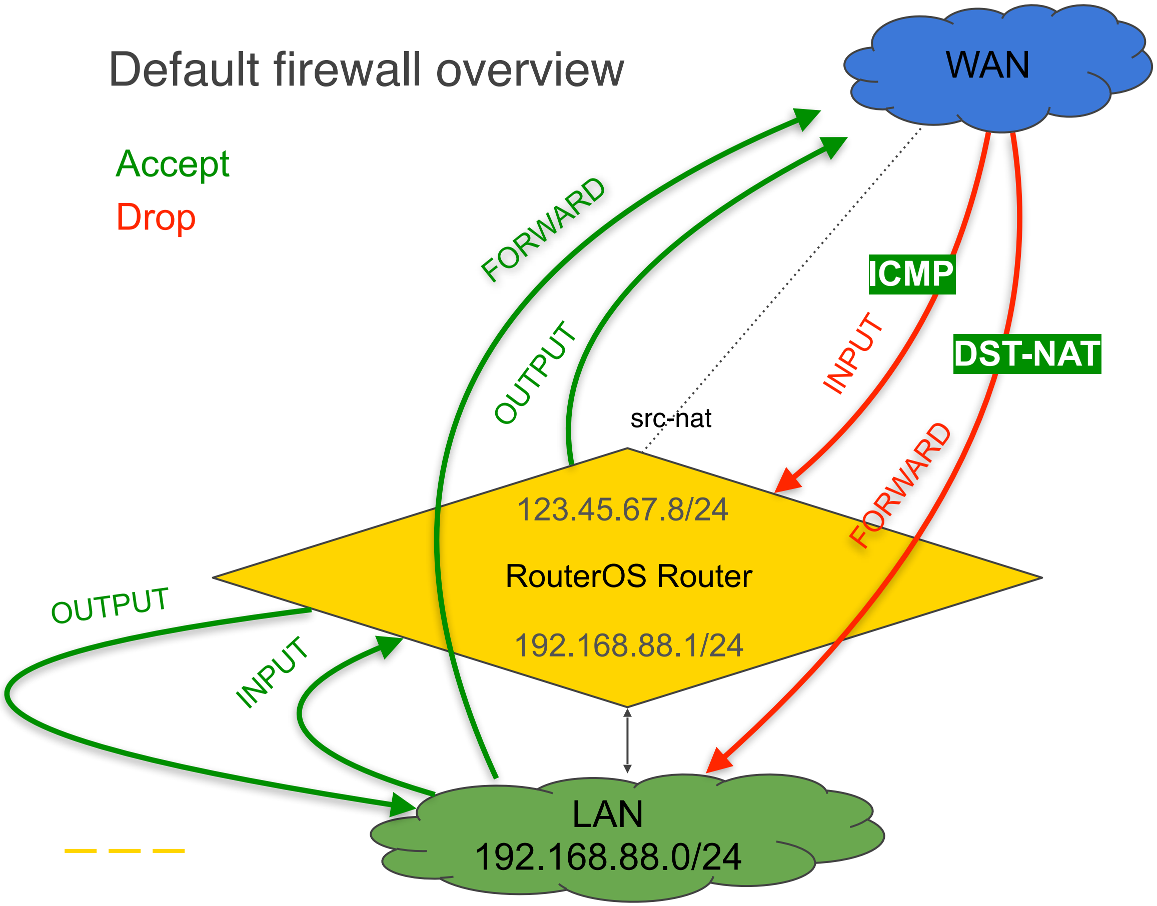
Setting up Firewall

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

Default firewall overview

Accept

Drop

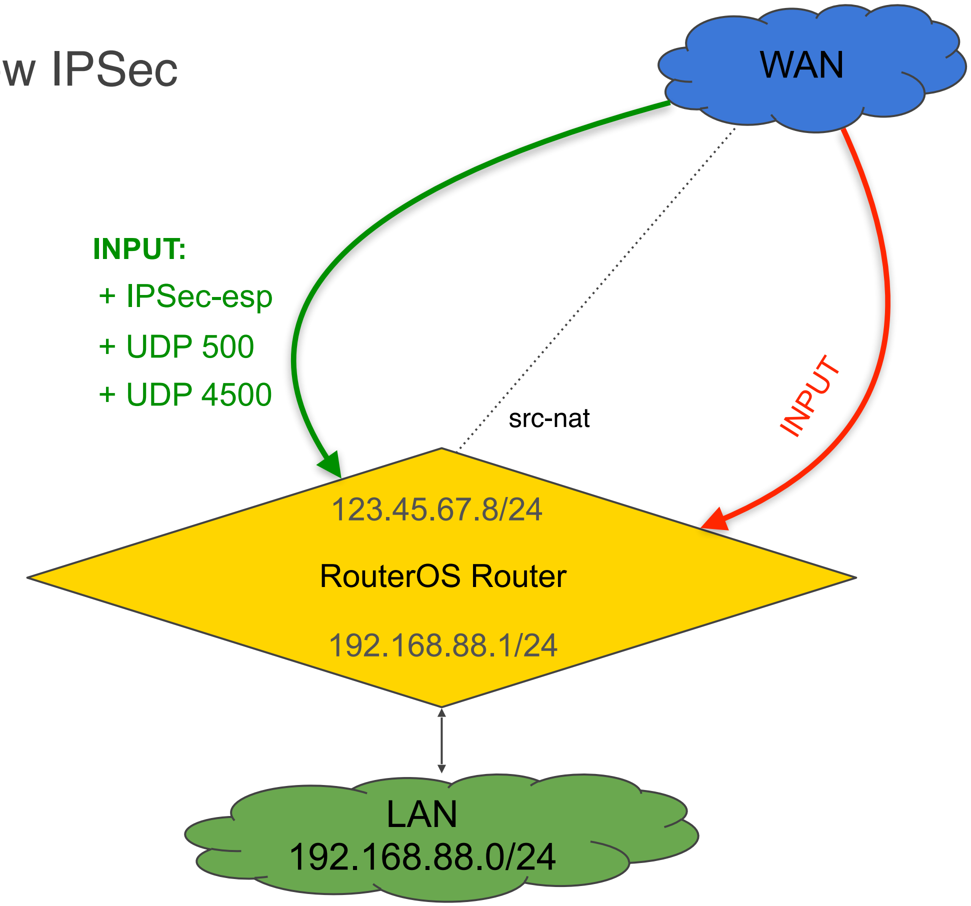


Nikita Tarikin / nikita@tarikin.com

Setting up Firewall

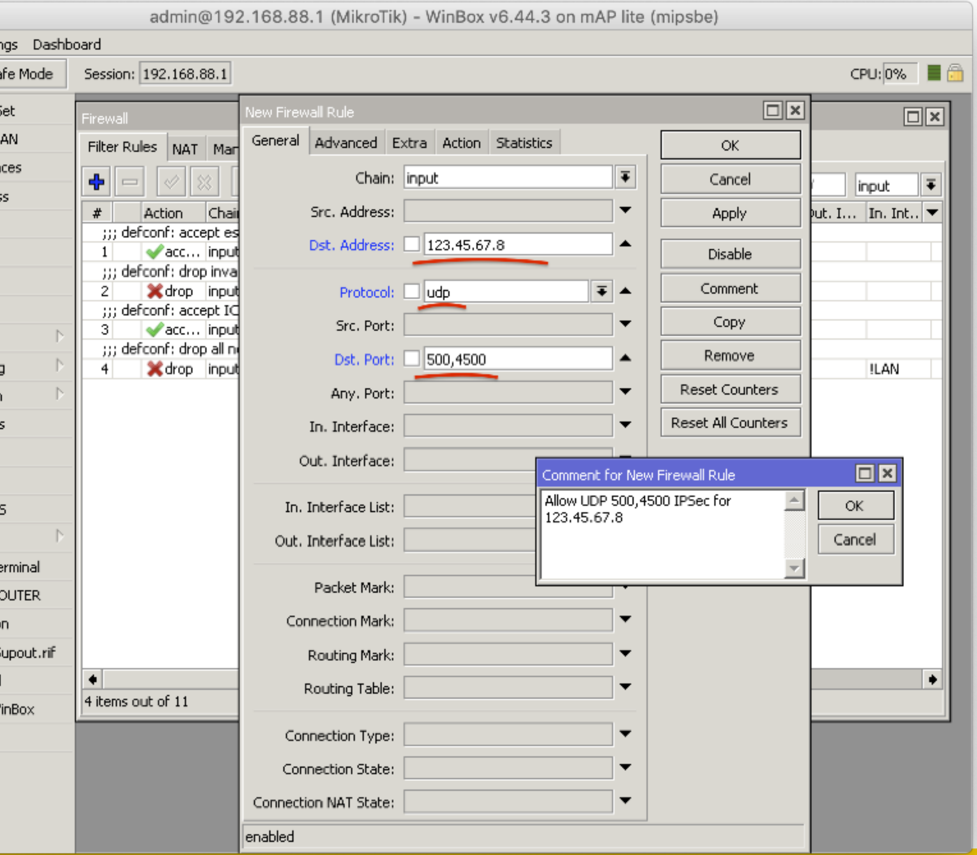
1. Default firewall overview
2. **Allow IPSec**

Allow IPSec



Firewall filter rules for IPSec packets (defconf)

INPUT chain



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

Session: 192.168.88.1

CPU: 0%

New Firewall Rule

Chain: input

Dst. Address: □ 123.45.67.8

Protocol: □ udp

Dst. Port: □ 500,4500

enabled

Comment for New Firewall Rule

Allow UDP 500,4500 IPSec for 123.45.67.8

#	Action	Chain
	;;; defconf: accept es	
1	✓ acc...	input
	;;; defconf: drop inva	
2	✗ drop	input
	;;; defconf: accept IC	
3	✓ acc...	input
	;;; defconf: drop all n	
4	✗ drop	input

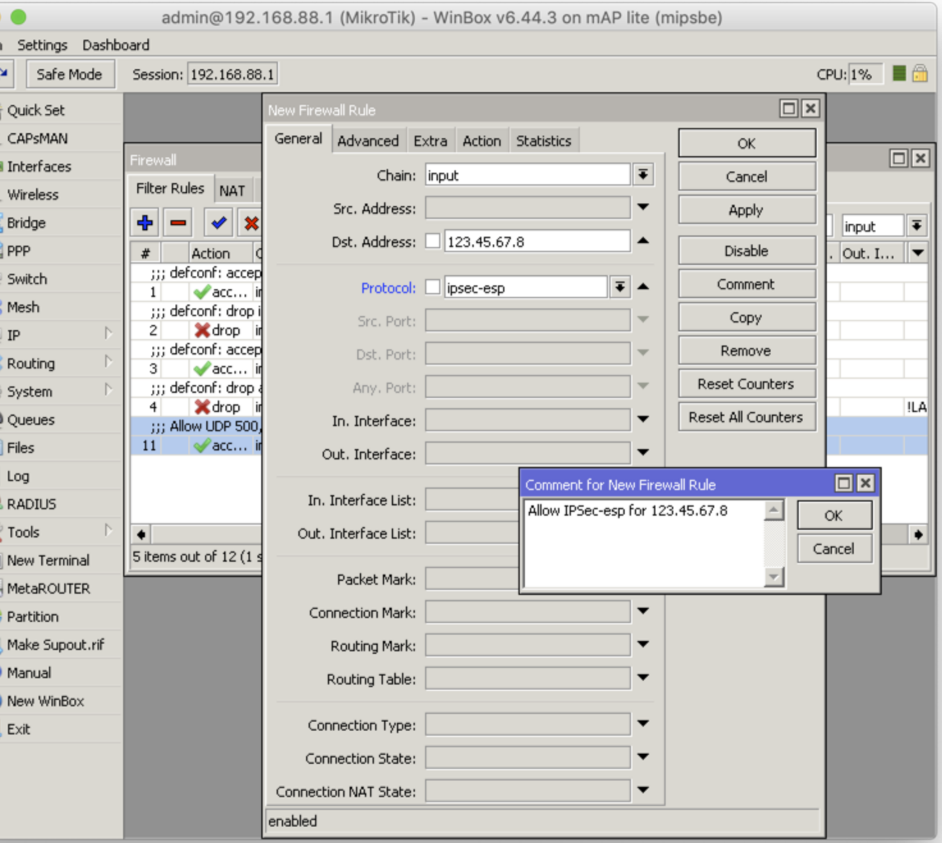
4 items out of 11

+ 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



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

Session: 192.168.88.1 CPU: 1%

Firewall — Filter Rules

#	Action
;;; defconf: accep	
1	acc...
;;; defconf: drop i	
2	drop
;;; defconf: accep	
3	acc...
;;; defconf: drop a	
4	drop
;;; Allow UDP 500,	
11	acc...

5 items out of 12 (1 s

New Firewall Rule — General

Chain: input

Dst. Address: 123.45.67.8

Protocol: ipsec-esp

enabled

Comment for New Firewall Rule

Allow IPSec-esp for 123.45.67.8

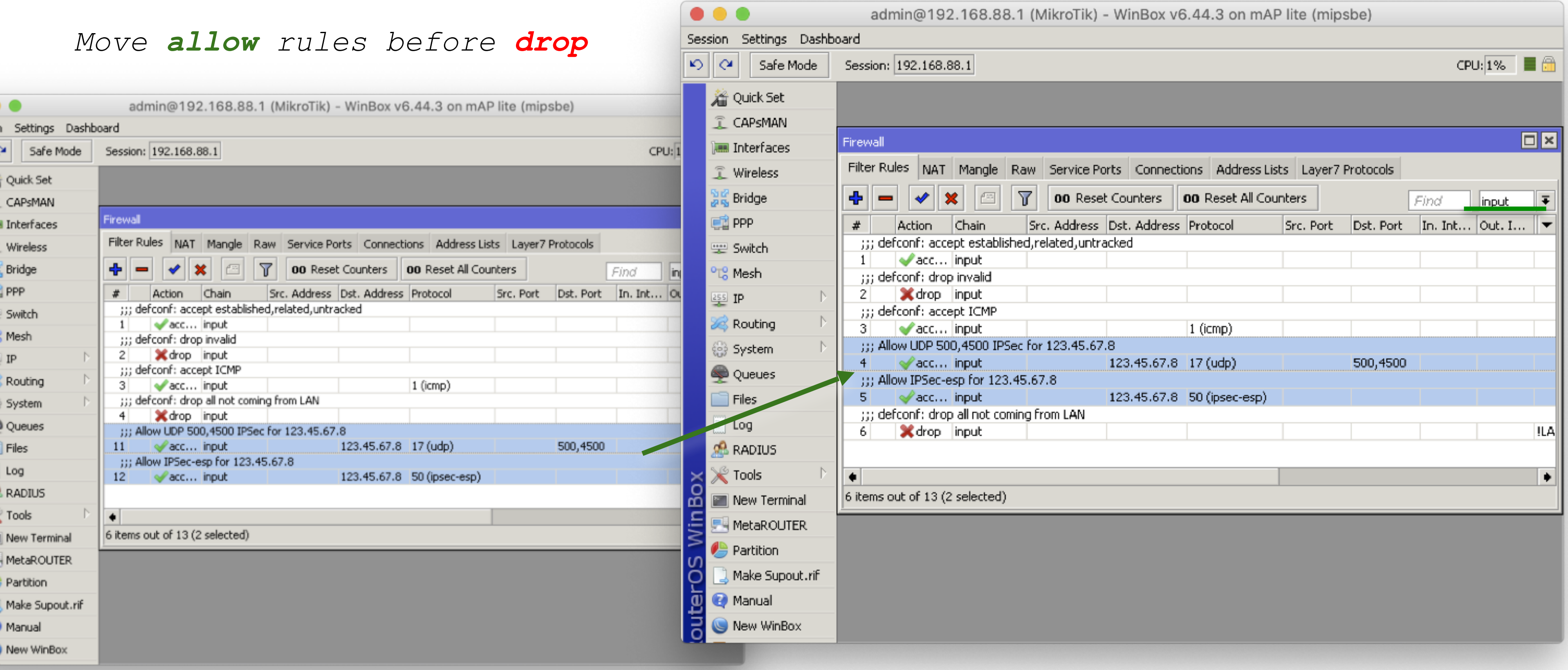
+ IPSec-esp (protocol 50)

```
/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***



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

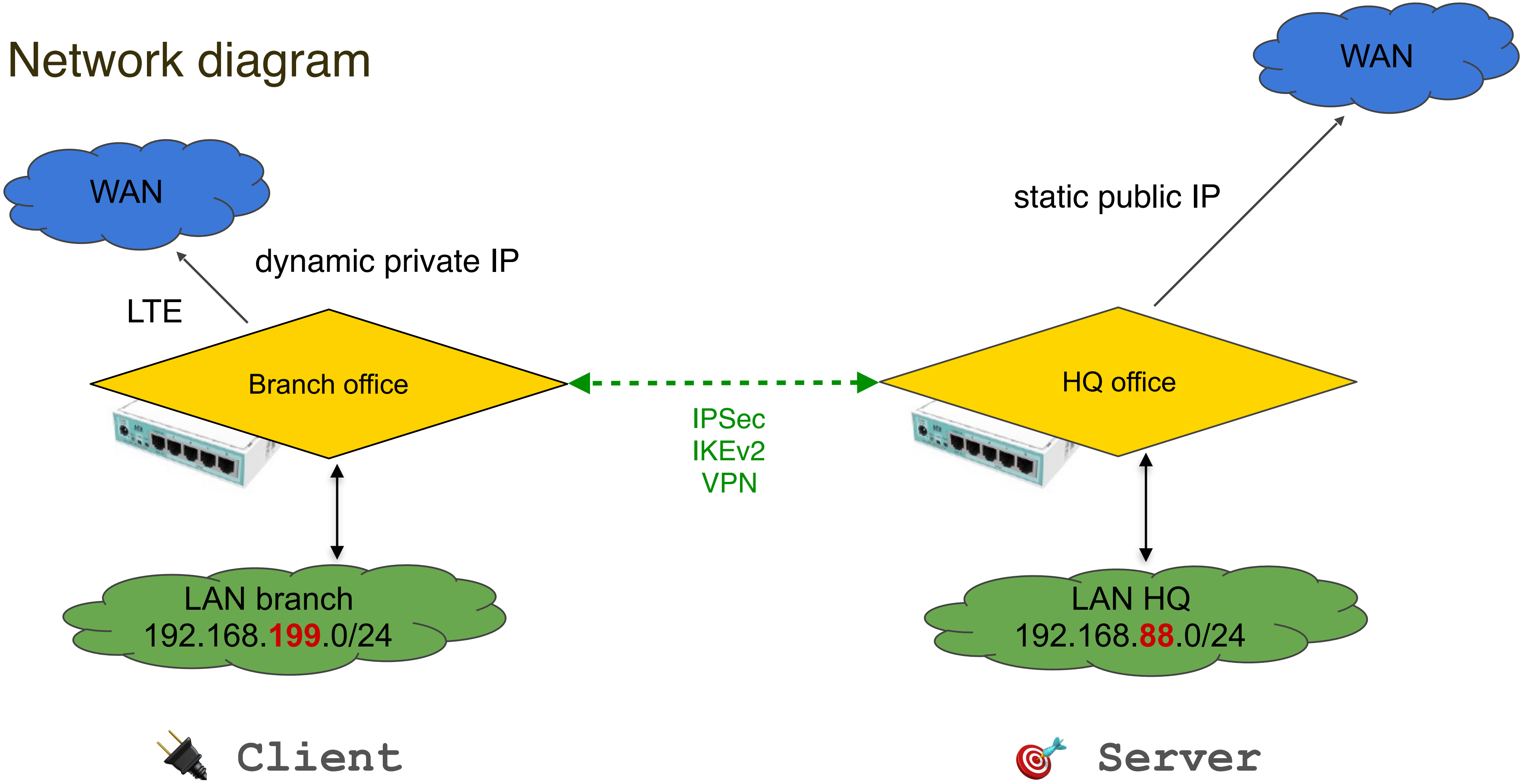
6 items out of 13 (2 selected)

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

6 items out of 13 (2 selected)

🎯 RouterOS IPSec IKEv2 server ready

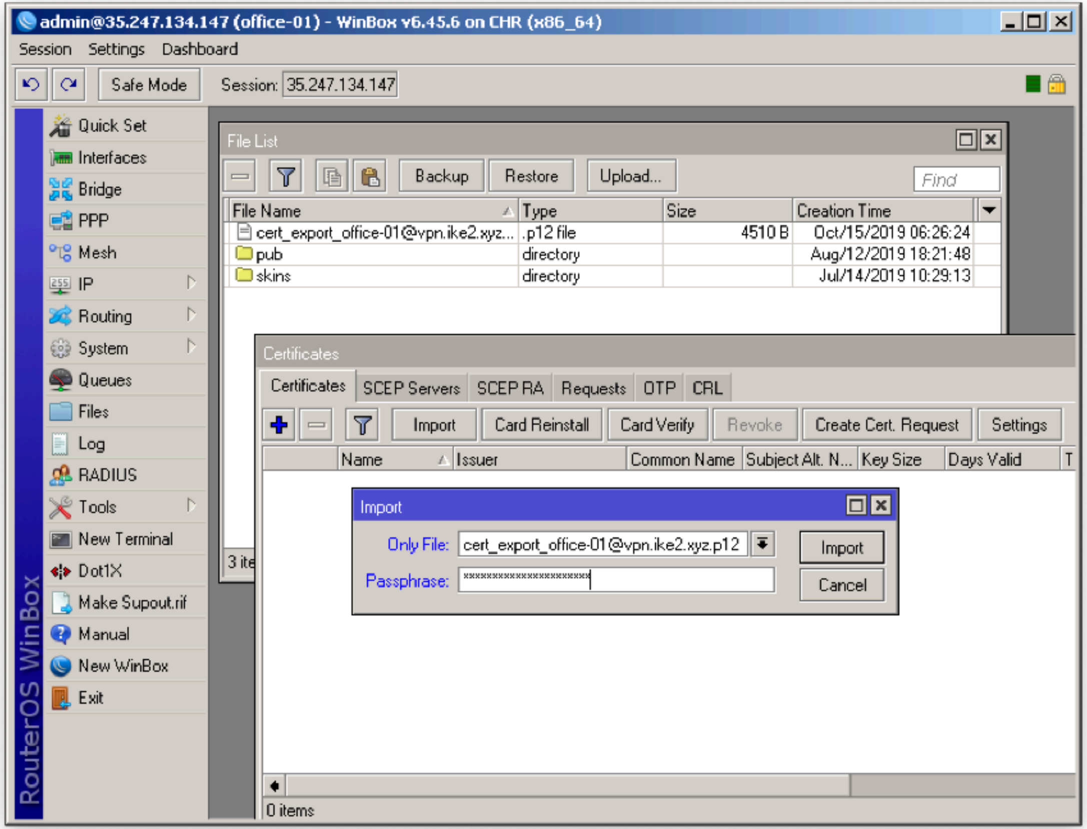
Network diagram



Setting up client RouterOS 🔌

Upload and install client SSL certificate

Client



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

Session: 35.247.134.147

File List

File Name	Type	Size	Creation Time
cert_export_office-01@vpn.ike2.xyz...	.p12 file	4510 B	Oct/15/2019 06:26:24
pub	directory		Aug/12/2019 18:21:48
skins	directory		Jul/14/2019 10:29:13

3 ite

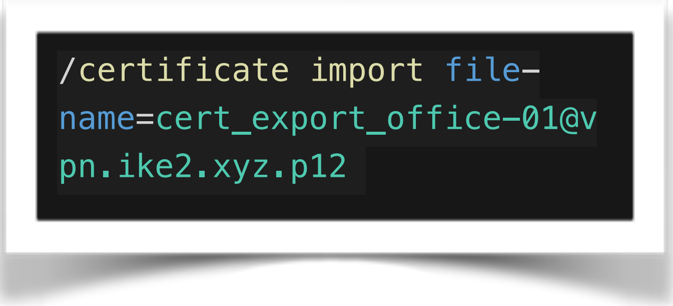
Certificates

Import

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

Passphrase: **********************

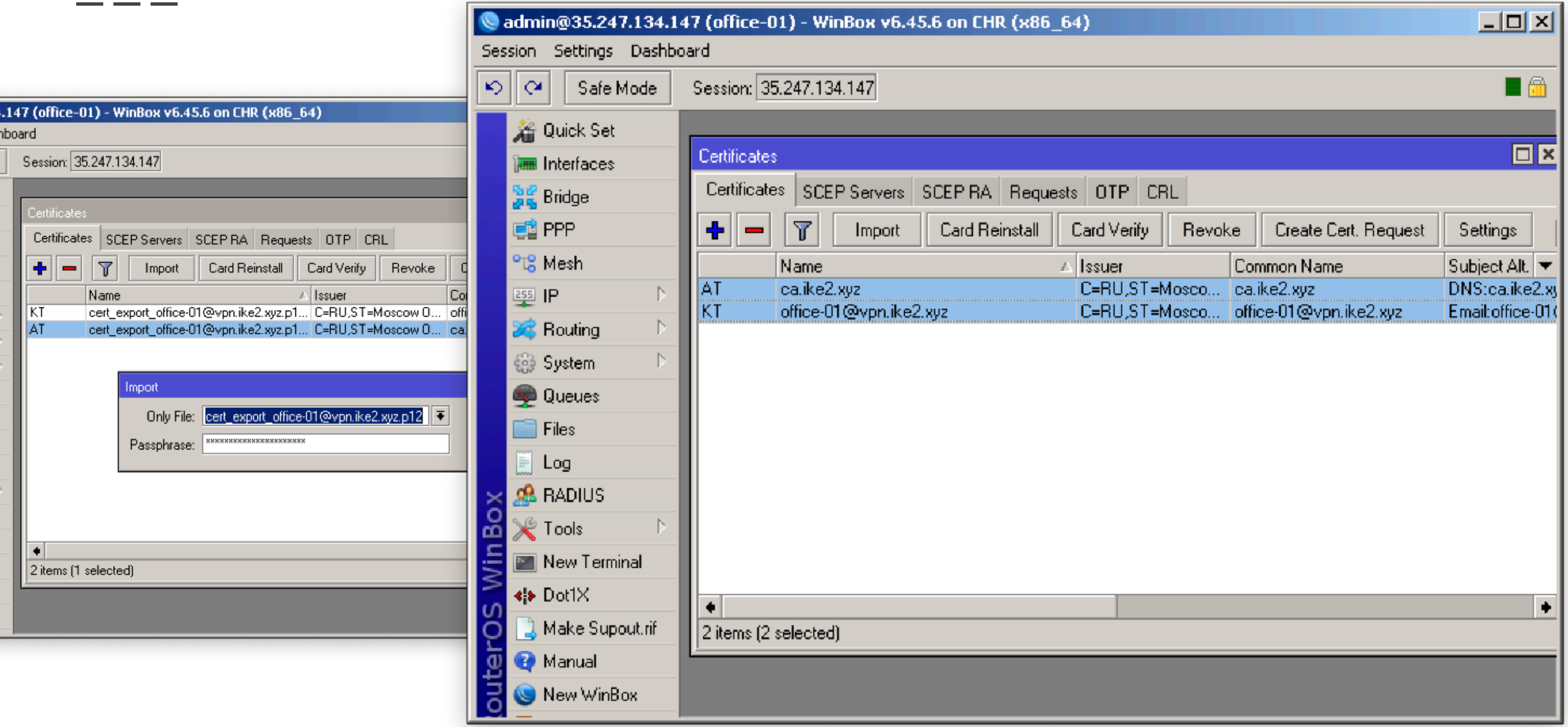
0 items



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

Rename installed SSL certificates: CA and client

Client



Session: 35.247.134.147

	Name	Issuer	Co
KT	cert_export_office-01@vpn.ike2.xyz.p1...	C=RU,ST=Moscow O...	offi
AT	cert_export_office-01@vpn.ike2.xyz.p1...	C=RU,ST=Moscow O...	ca.

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

Passphrase: ************************

2 items (1 selected)

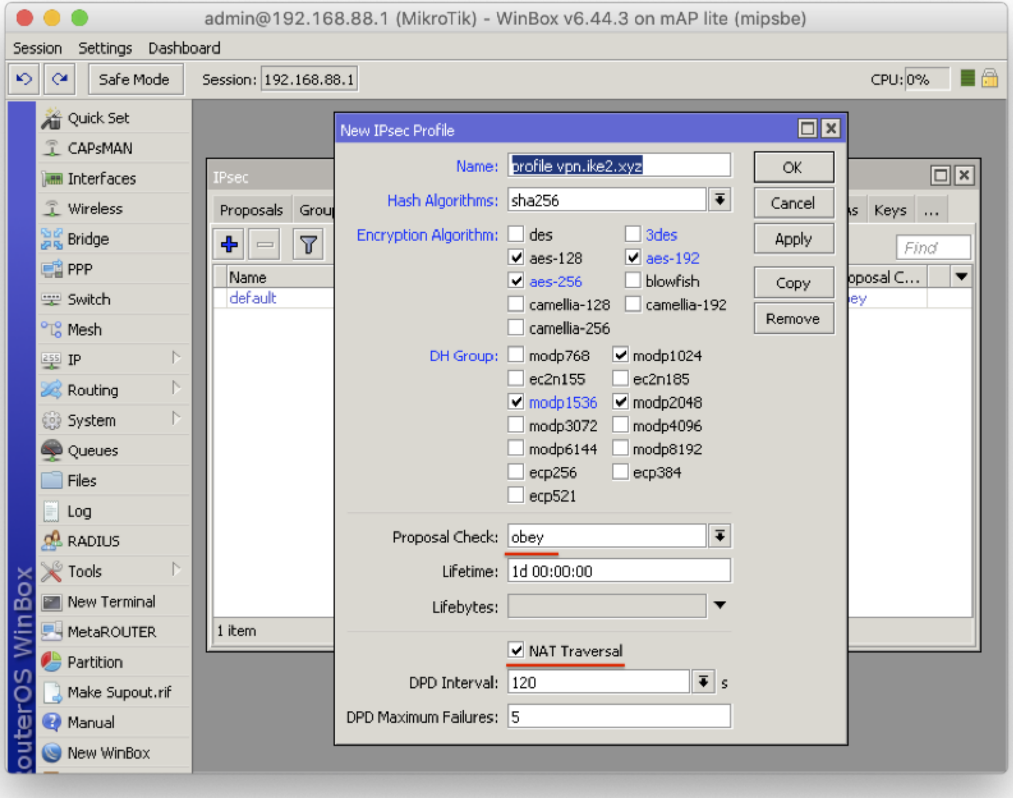
Session: 35.247.134.147

	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

2 items (2 selected)

Client

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



New IPsec Profile

Name: profile vpn.ike2.xyz

Hash Algorithms: sha256

Encryption Algorithm: ☐ des ☐ 3des ☑ aes-128 ☑ aes-192 ☑ aes-256 ☐ blowfish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256

DH Group: ☐ modp768 ☑ modp1024 ☐ ec2n155 ☐ ec2n185 ☑ modp1536 ☑ modp2048 ☐ modp3072 ☐ modp4096 ☐ modp6144 ☐ modp8192 ☐ ecp256 ☐ ecp384 ☐ ecp521

Proposal Check: obey

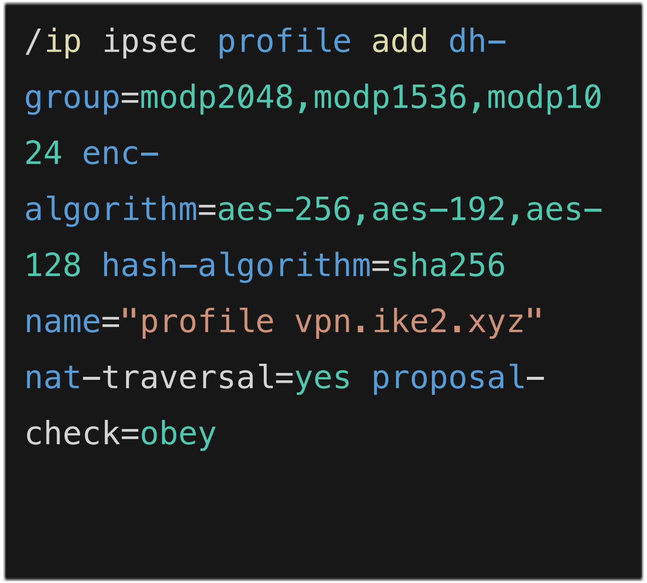
Lifetime: 1d 00:00:00

Lifebytes:

☑ NAT Traversal

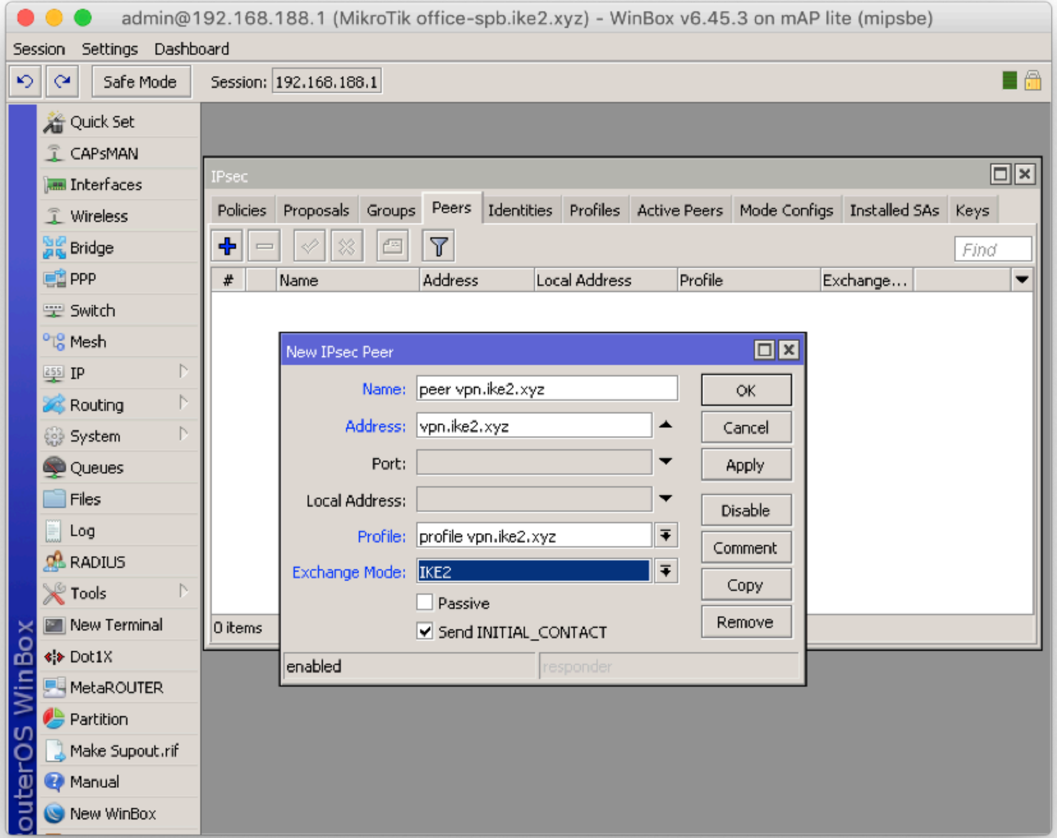
DPD Interval: 120 s

DPD Maximum Failures: 5



```
/ip ipsec profile add dh-group=modp2048,modp1536,modp1024 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)



admin@192.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on mAP lite (mipsbe)

Session: 192.168.188.1

New IPsec Peer

Name: peer vpn.ike2.xyz

Address: vpn.ike2.xyz

Port:

Local Address:

Profile: profile vpn.ike2.xyz

Exchange Mode: IKE2

□ Passive

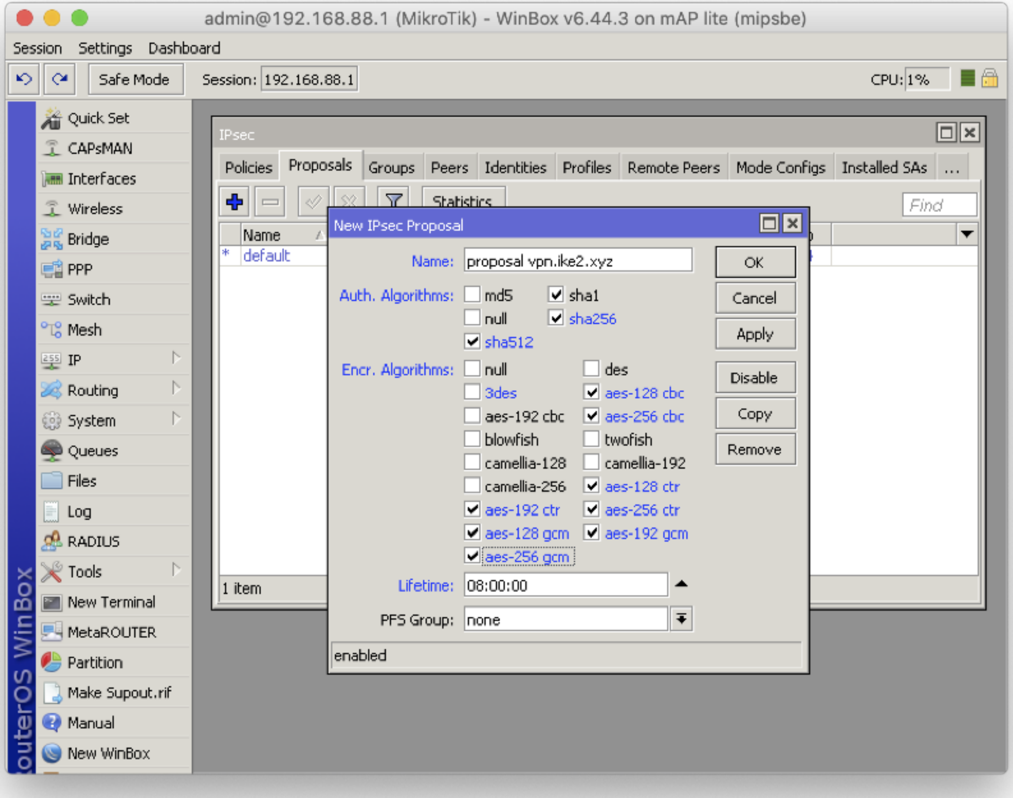
☑ Send INITIAL_CONTACT

enabled | responder

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

Client

Setting up new IPSec proposal *(phase 2)*



New IPsec Proposal

Name: proposal vpn.ike2.xyz

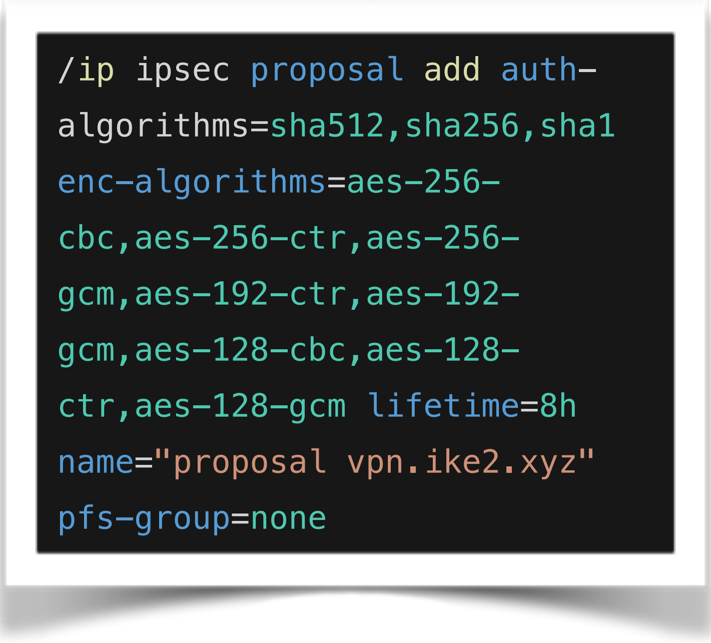
Auth. Algorithms: □ md5 ☑ sha1 □ null ☑ sha256 ☑ sha512

Encr. Algorithms: □ null □ des □ 3des ☑ aes-128 cbc □ aes-192 cbc ☑ aes-256 cbc □ blowfish □ twofish □ camellia-128 □ camellia-192 □ camellia-256 ☑ aes-128 ctr ☑ aes-192 ctr ☑ aes-256 ctr ☑ aes-128 gcm ☑ aes-192 gcm ☑ aes-256 gcm

Lifetime: 08:00:00

PFS Group: none

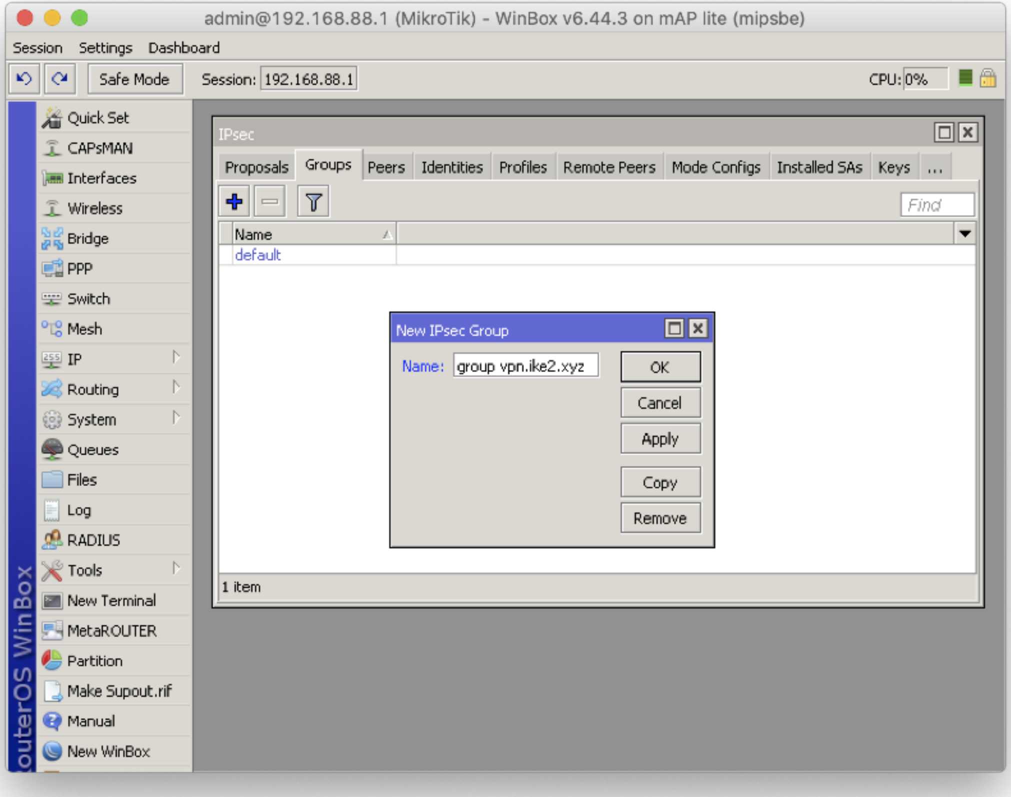
enabled



```
/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

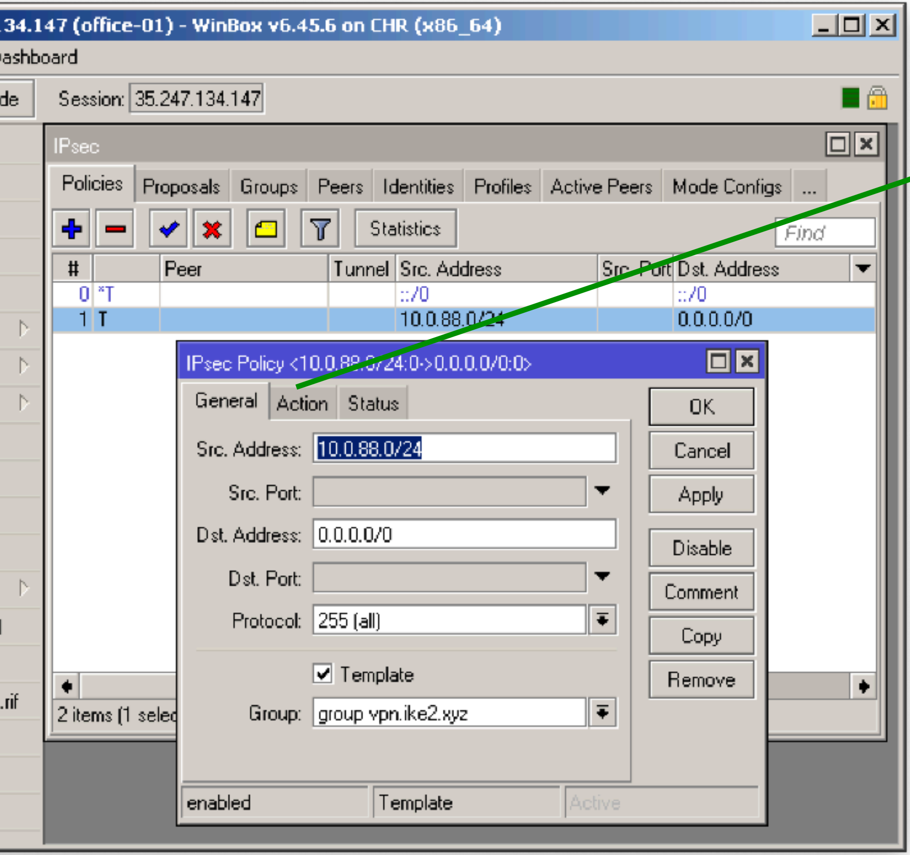
Client



Name: group vpn.ike2.xyz

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

Adding new IPSec policy template



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

Session: 35.247.134.147

IPsec

#		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 items (1 selec

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

Src. Address: 10.0.88.0/24

Src. Port:

Dst. Address: 0.0.0.0/0

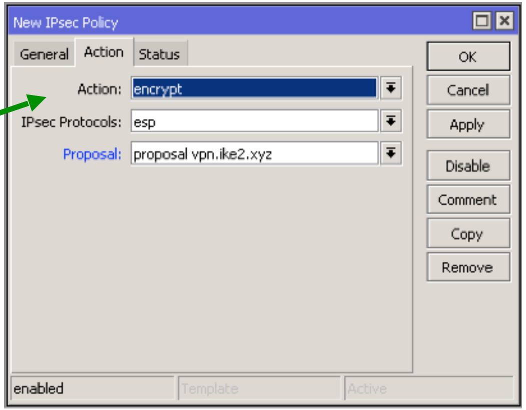
Dst. Port:

Protocol: 255 (all)

☑ Template

Group: group vpn.ike2.xyz

enabled | Template | Active



New IPsec Policy

Action: encrypt

IPsec Protocols: esp

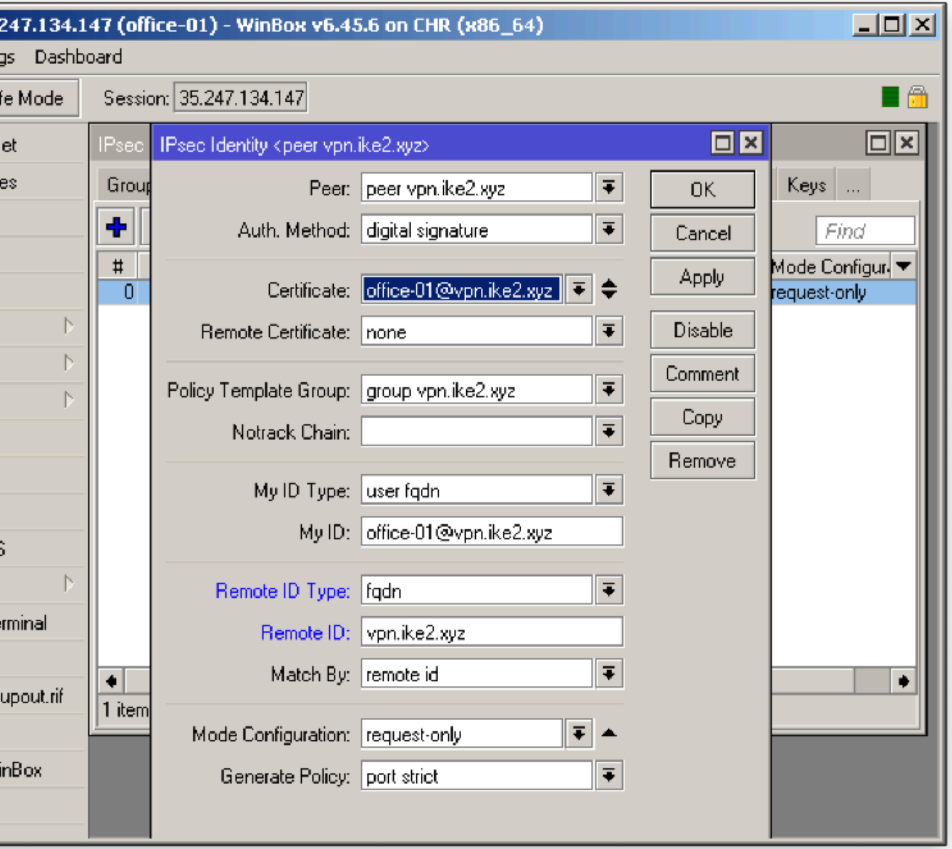
Proposal: proposal vpn.ike2.xyz

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

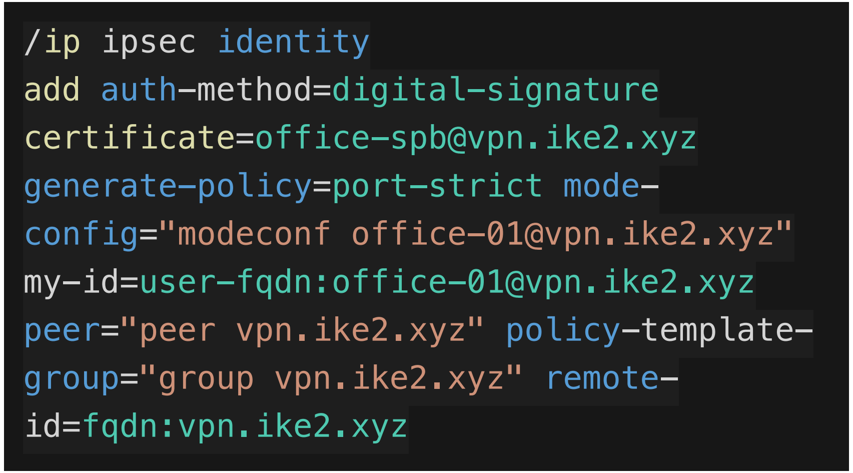
Client



Session: 35.247.134.147

IPsec Identity <peer vpn.ike2.xyz>

Peer: peer vpn.ike2.xyz
Auth. Method: digital signature
Certificate: office-01@vpn.ike2.xyz
Remote Certificate: none
Policy Template Group: group vpn.ike2.xyz
Notrack Chain:
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

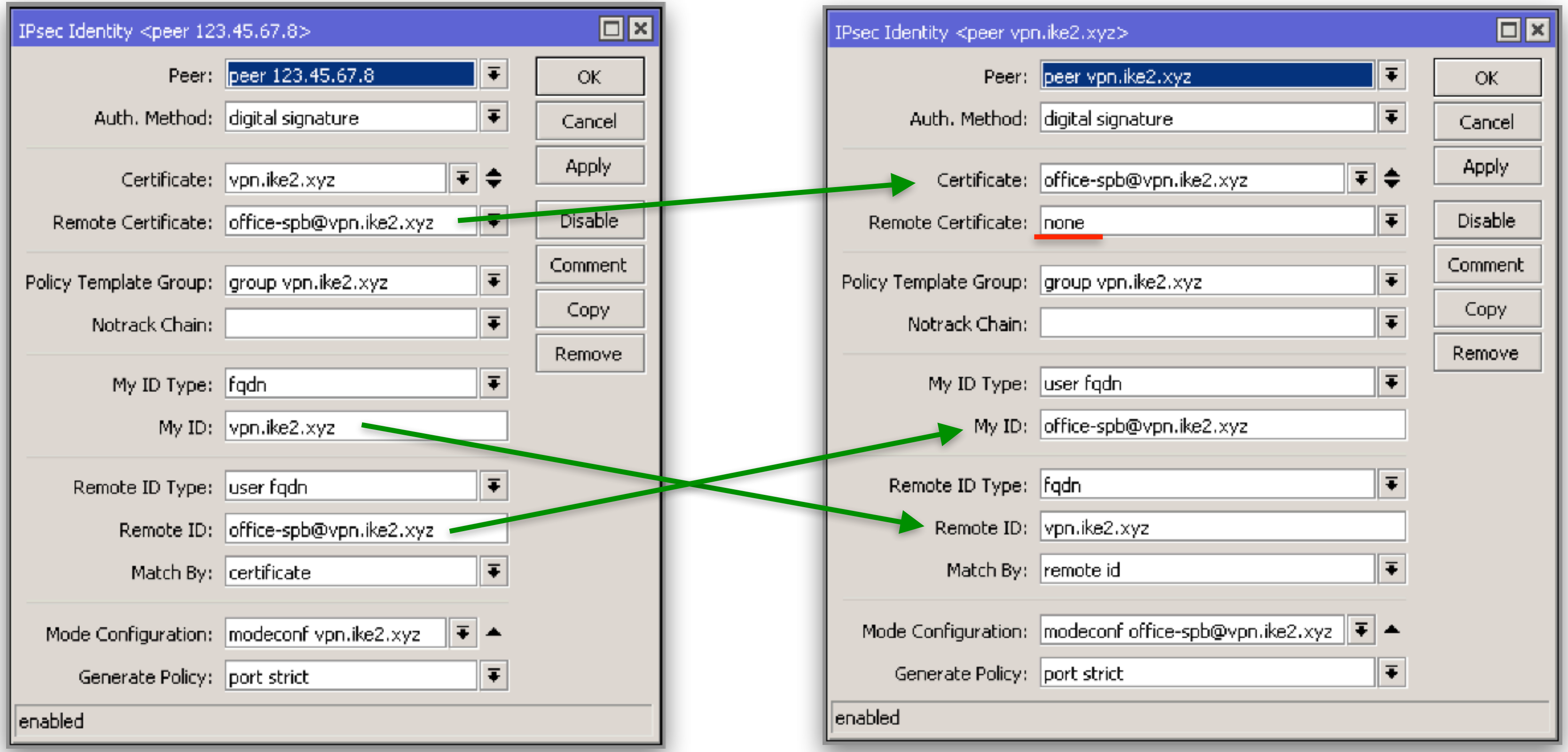


```
/ip ipsec identity
add auth-method=digital-signature
certificate=office-spb@vpn.ike2.xyz
generate-policy=port-strict mode-
config="modeconf office-01@vpn.ike2.xyz"
my-id=user-fqdn:office-01@vpn.ike2.xyz
peer="peer vpn.ike2.xyz" policy-template-
group="group vpn.ike2.xyz" remote-
id=fqdn:vpn.ike2.xyz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

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

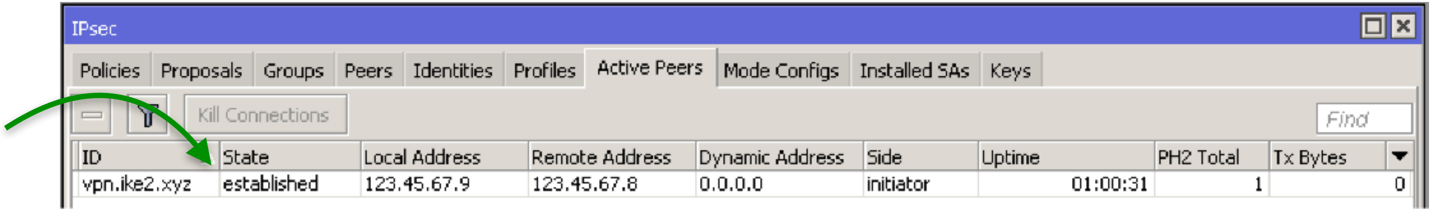
Generate Policy: port strict

enabled

Client

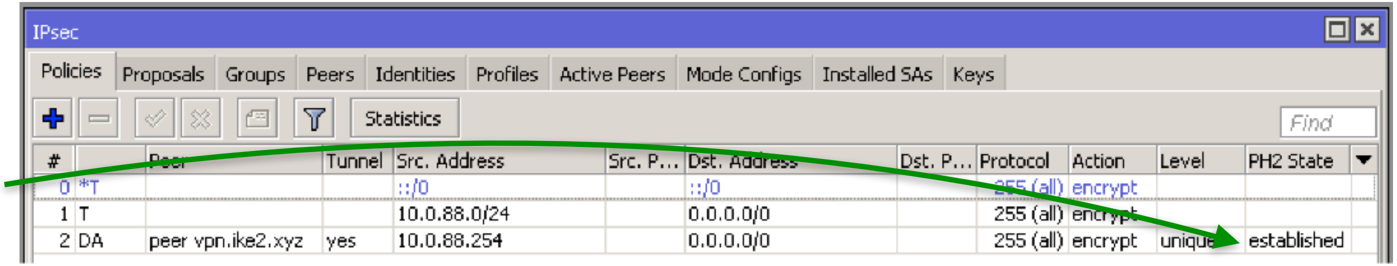
Testing the IKEv2 connectivity

Active peers
state: **established**



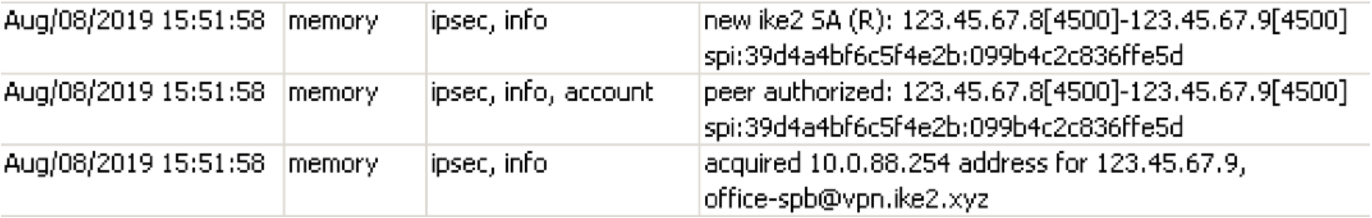
ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	PH2 Total	Tx Bytes
vpn.ike2.xyz	established	123.45.67.9	123.45.67.8	0.0.0.0	initiator	01:00:31	1	0

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



#		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

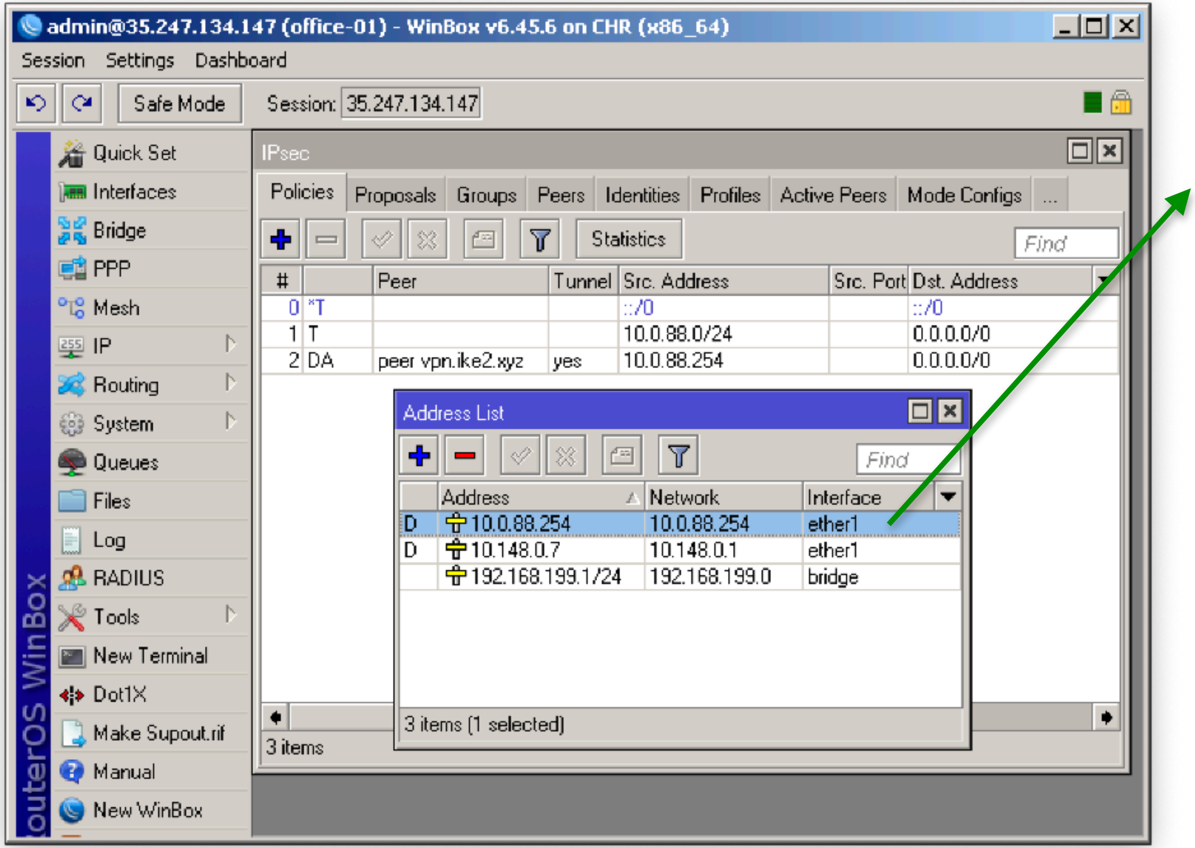
Peer: **authorized**
Address: **acquired**



```
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

Client



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

Session: 35.247.134.147

IPsec — Policies

#		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

3 items

Address List

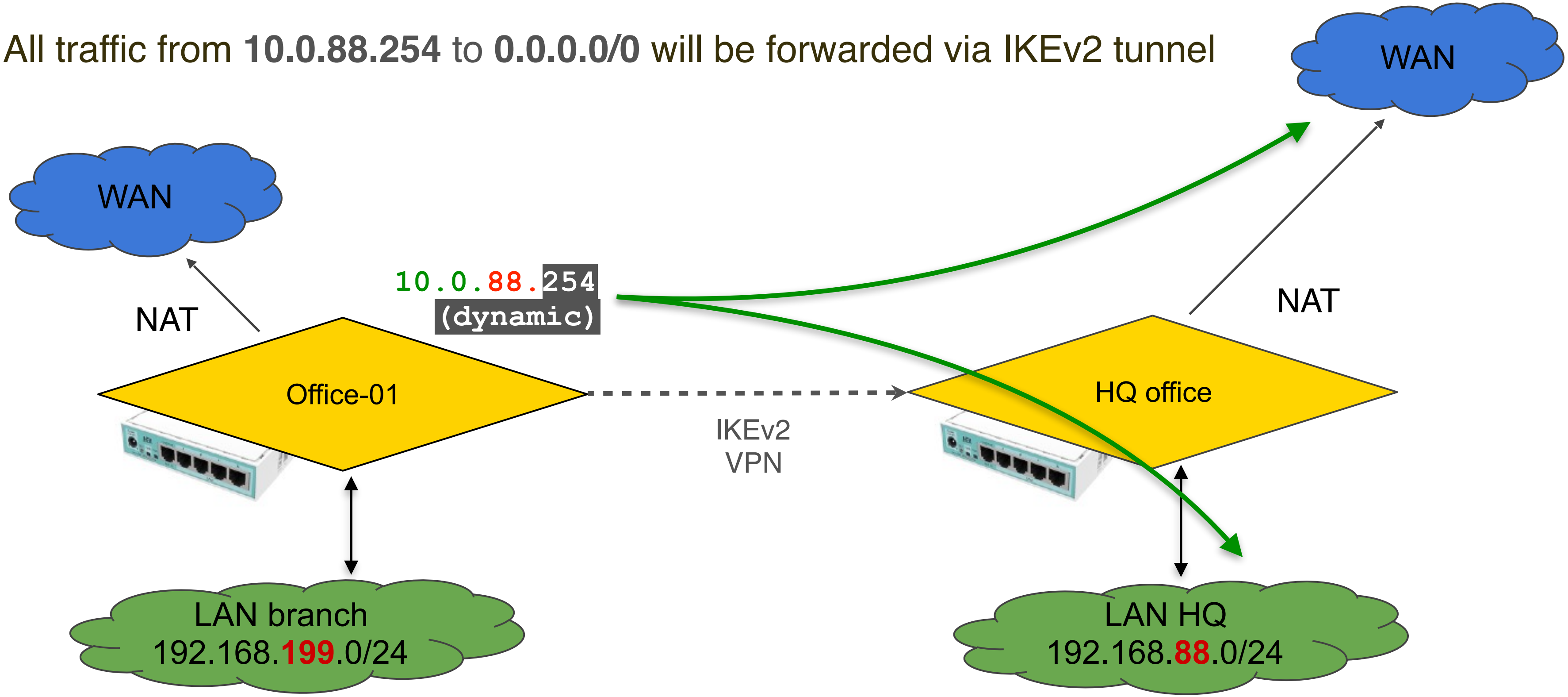
	Address	Network	Interface
D	10.0.88.254	10.0.88.254	ether1
D	10.148.0.7	10.148.0.1	ether1
	192.168.199.1/24	192.168.199.0	bridge

3 items (1 selected)

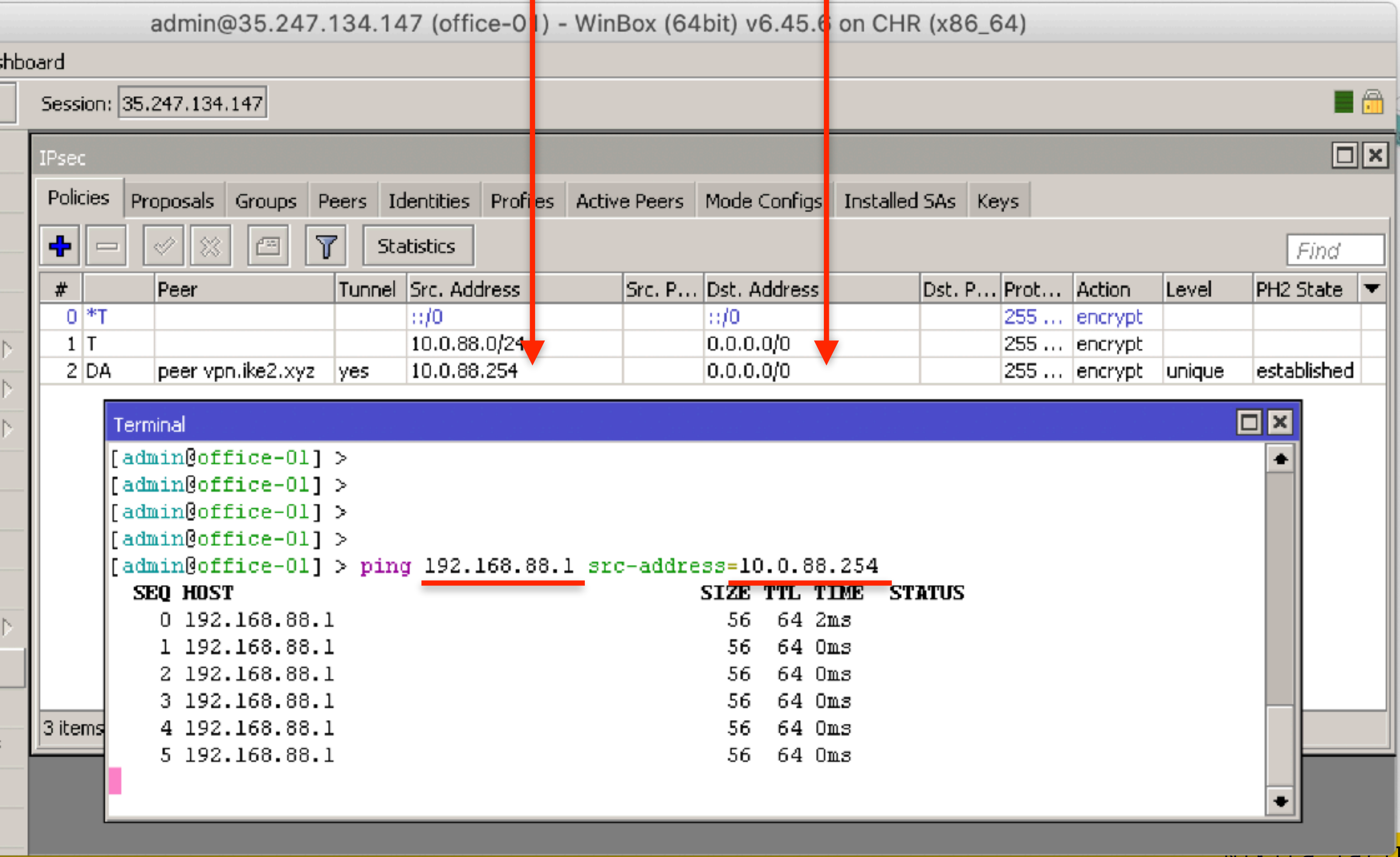
IP address 10.0.88.254

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



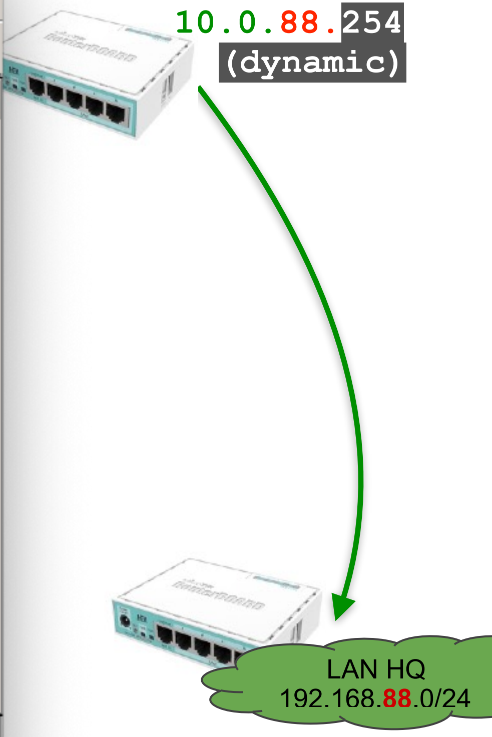
admin@35.247.134.147 (office-01) - WinBox (64bit) v6.45.6 on CHR (x86_64)

#		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

3 items

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

Routable

Has interface

No TCP MSS issues

Option 1 (easy)

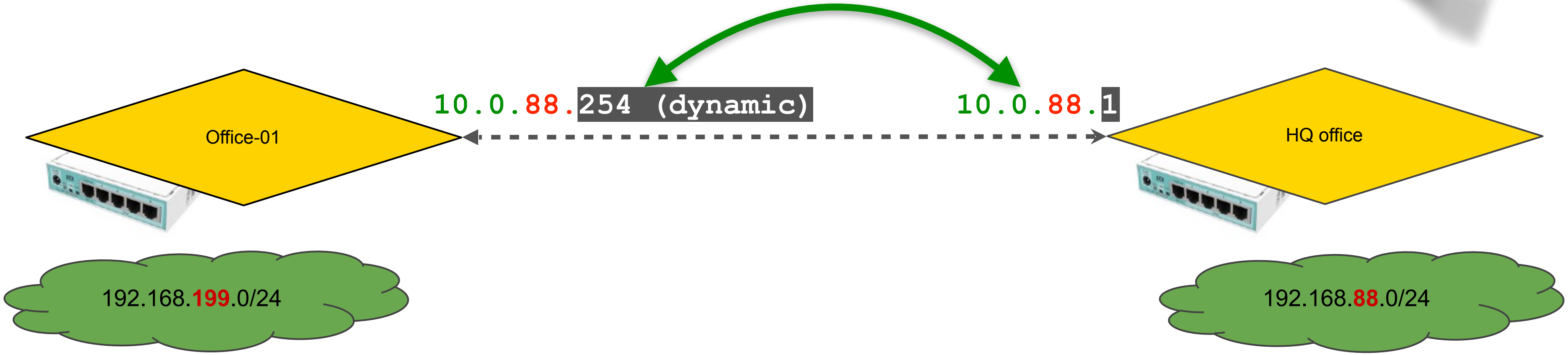
<interface> over ipsec ike2

Cons:

Decreased MTU due to extra encapsulation overhead

Takes longer to connect and reconnect

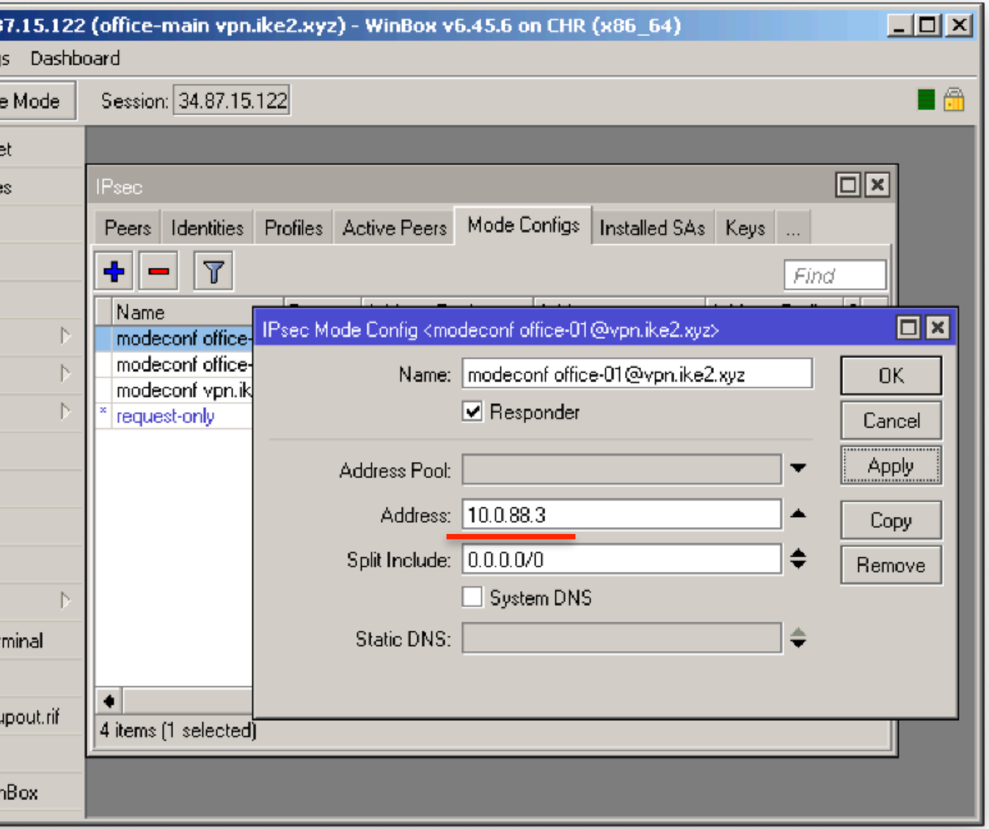
Option #1: **routable** using your favourite <interface> over IKEv2



Don't forget to **allow** this traffic on the firewall (both sides)

Create new ipsec modeconf with static IP address

Server



IPsec Mode Config <modeconf office-01@vpn.ike2.xyz>

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

☑ Responder

Address Pool:

Address: 10.0.88.3

Split Include: 0.0.0.0/0

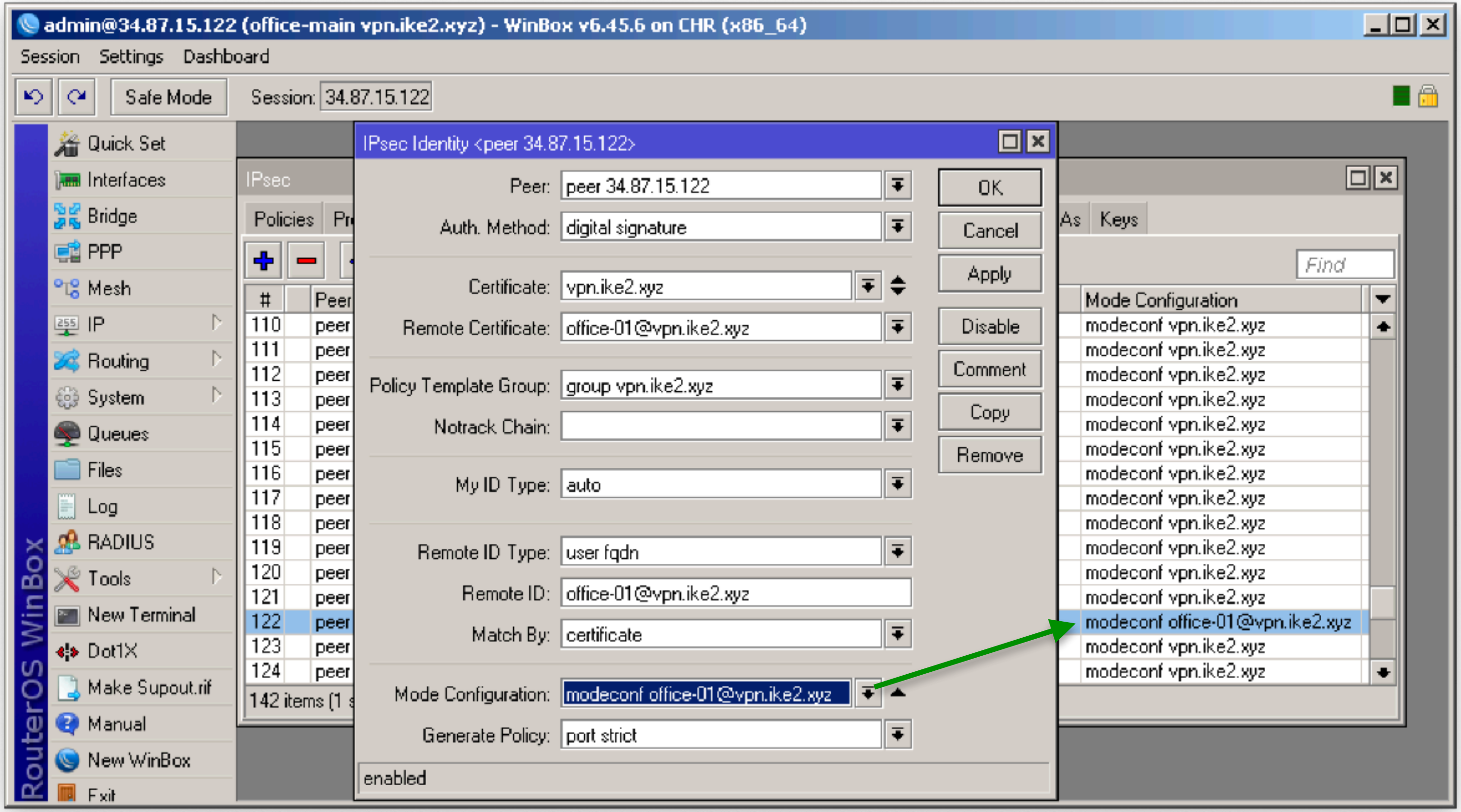
□ System DNS

Static DNS:

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



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

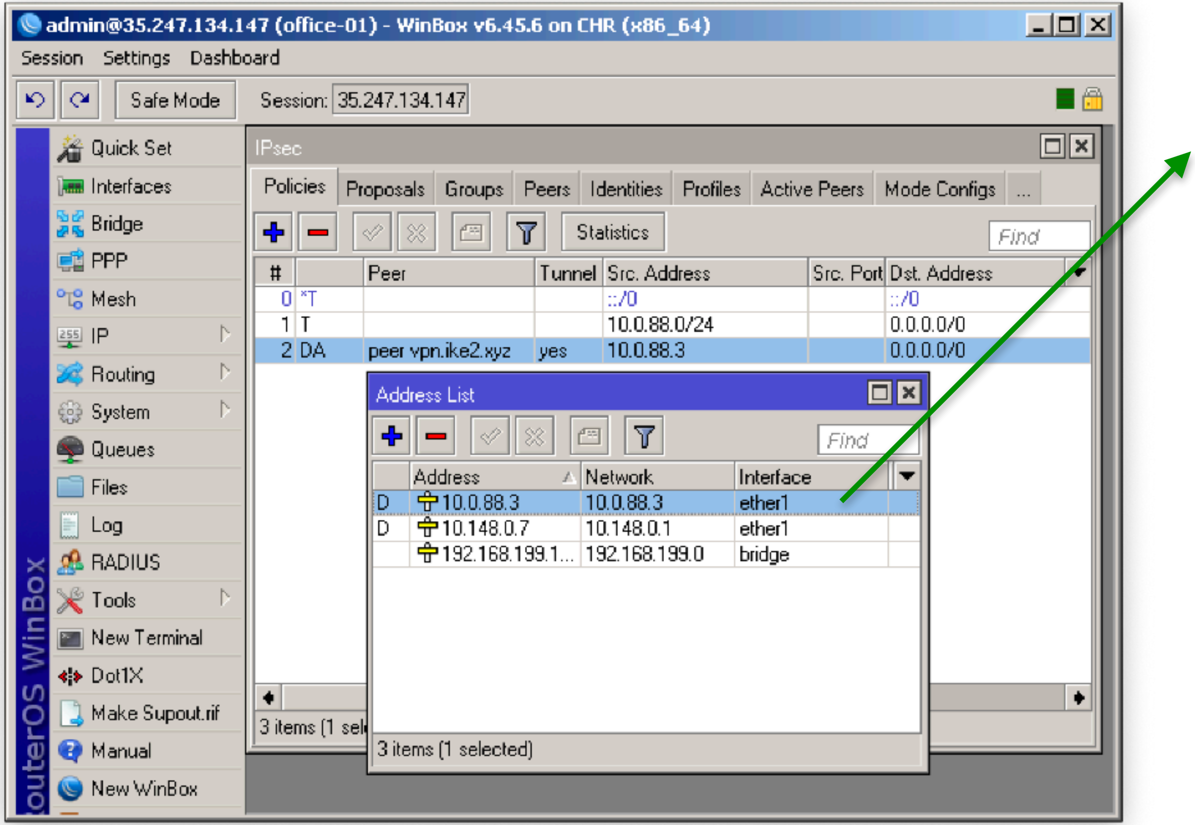
enabled

#	Peer	Mode Configuration
110	peer	modeconf vpn.ike2.xyz
111	peer	modeconf vpn.ike2.xyz
112	peer	modeconf vpn.ike2.xyz
113	peer	modeconf vpn.ike2.xyz
114	peer	modeconf vpn.ike2.xyz
115	peer	modeconf vpn.ike2.xyz
116	peer	modeconf vpn.ike2.xyz
117	peer	modeconf vpn.ike2.xyz
118	peer	modeconf vpn.ike2.xyz
119	peer	modeconf vpn.ike2.xyz
120	peer	modeconf vpn.ike2.xyz
121	peer	modeconf vpn.ike2.xyz
122	peer	modeconf office-01@vpn.ike2.xyz
123	peer	modeconf vpn.ike2.xyz
124	peer	modeconf vpn.ike2.xyz

142 items (1 s

Client

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: 35.247.134.147

#		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

3 items (1 sel

Address List

	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

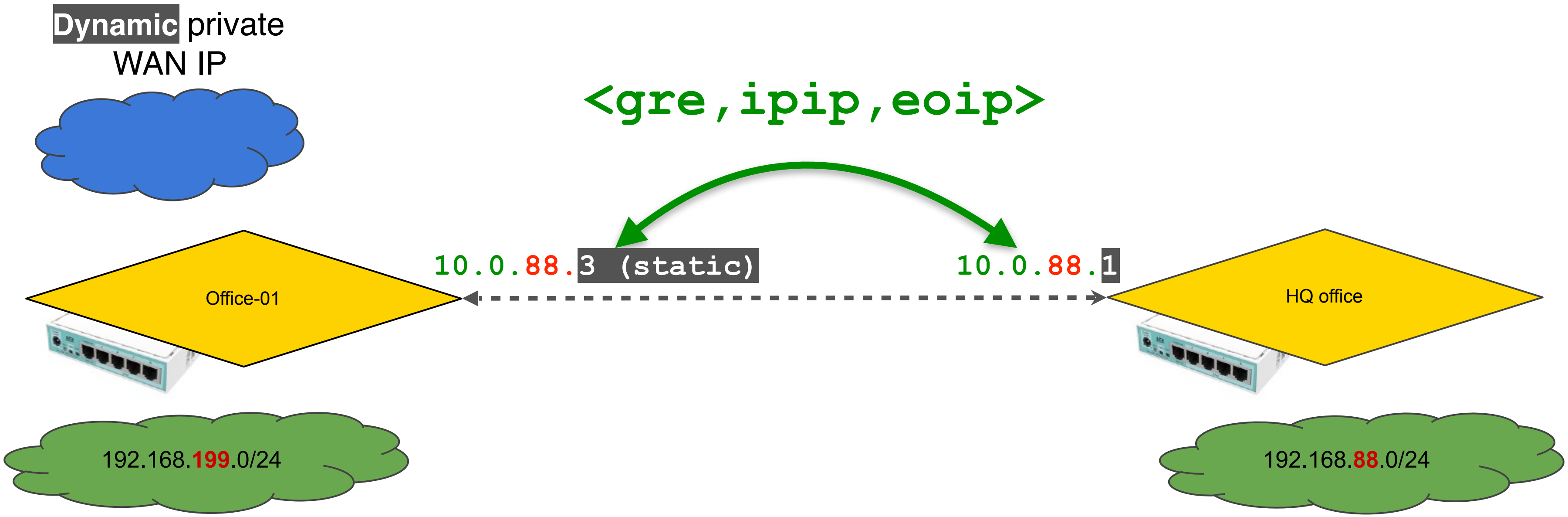
3 items (1 selected)

IP address	10.0.88.3
Interface	ether1

10.0.88.3

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

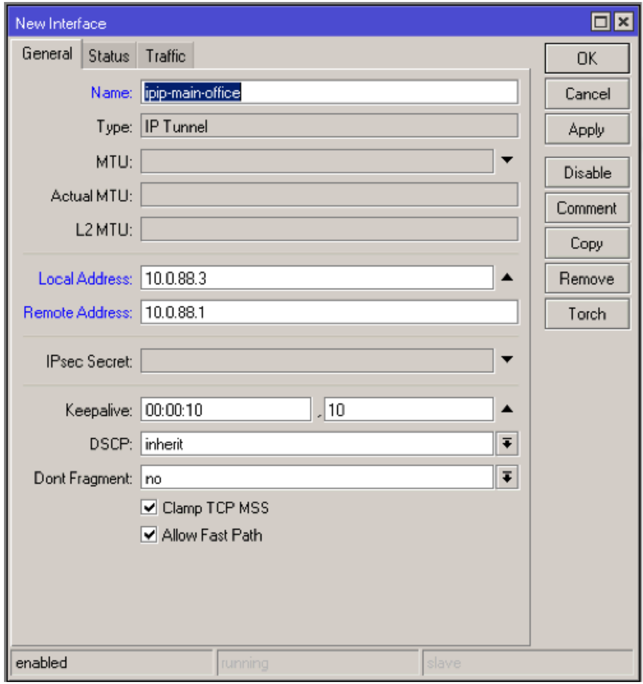
*Even if you have **dynamic** address on your ether1*



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

🔌 Client

🎯 Server

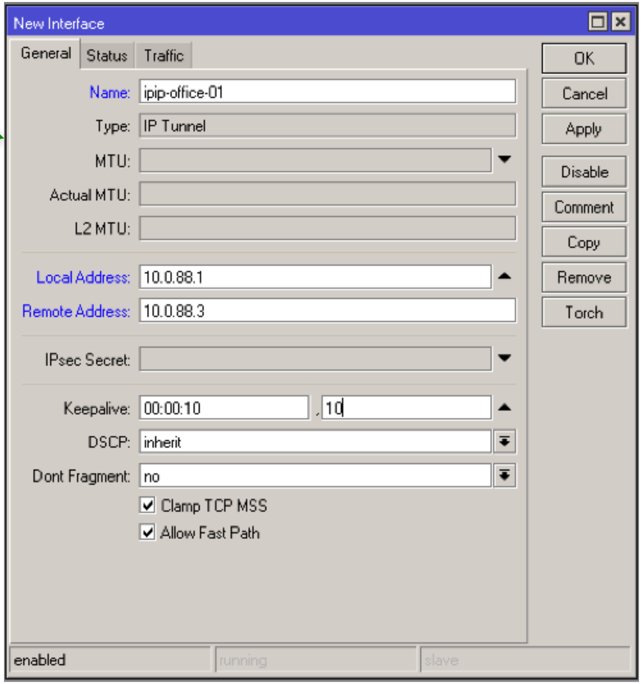


New Interface

General | Status | Traffic

- Name: ipip-main-office
- Type: IP Tunnel
- MTU:
- Actual MTU:
- L2 MTU:
- Local Address: 10.0.88.3
- Remote Address: 10.0.88.1
- IPsec Secret:
- Keepalive: 00:00:10 , 10
- DSCP: inherit
- Dont Fragment: no
- ☑ Clamp TCP MSS
- ☑ Allow Fast Path

<ipip>



New Interface

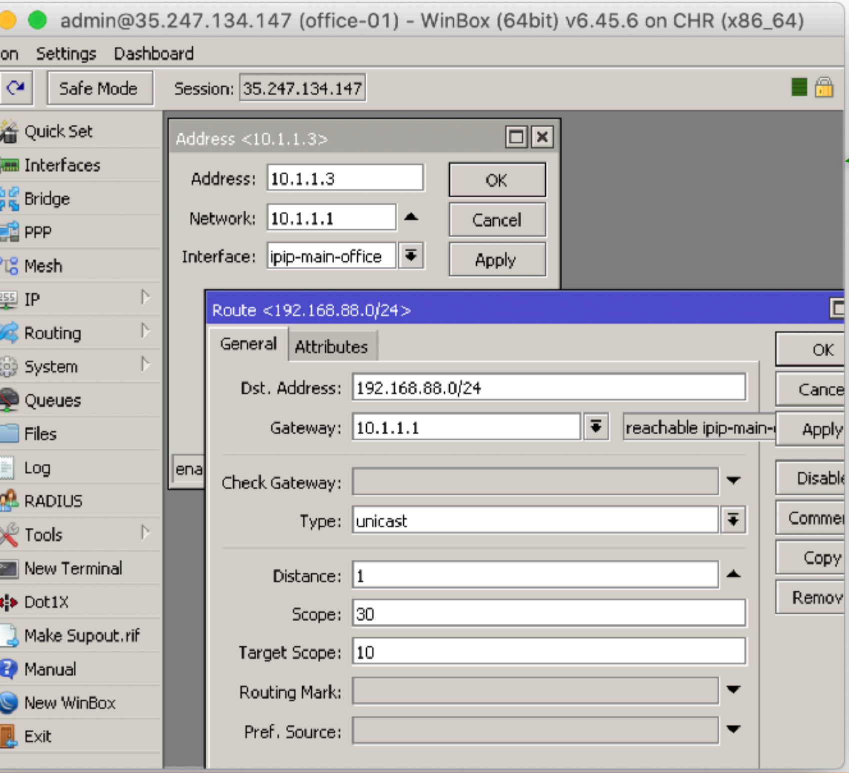
General | Status | Traffic

- Name: ipip-office-01
- Type: IP Tunnel
- MTU:
- Actual MTU:
- L2 MTU:
- Local Address: 10.0.88.1
- Remote Address: 10.0.88.3
- IPsec Secret:
- Keepalive: 00:00:10 , 10
- DSCP: inherit
- Dont Fragment: no
- ☑ Clamp TCP MSS
- ☑ Allow Fast Path

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

Client

Server



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

Network: 10.1.1.1

Interface: ipip-main-office

Route <192.168.88.0/24>

Dst. Address: 192.168.88.0/24

Gateway: 10.1.1.1 reachable ipip-main-

Check Gateway:

Type: unicast

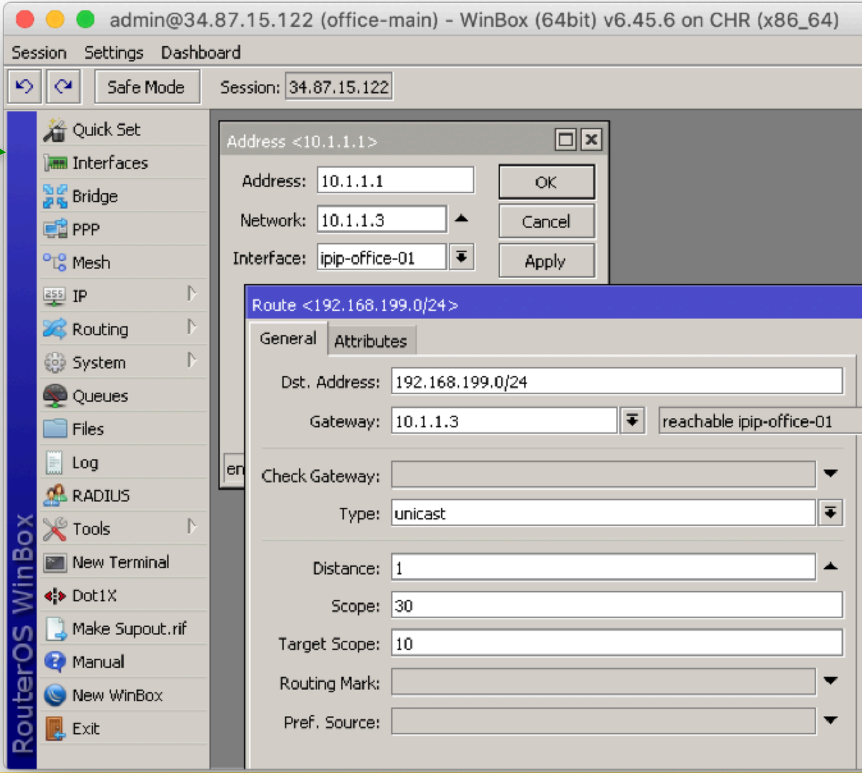
Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:



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

Network: 10.1.1.3

Interface: ipip-office-01

Route <192.168.199.0/24>

Dst. Address: 192.168.199.0/24

Gateway: 10.1.1.3 reachable ipip-office-01

Check Gateway:

Type: unicast

Distance: 1

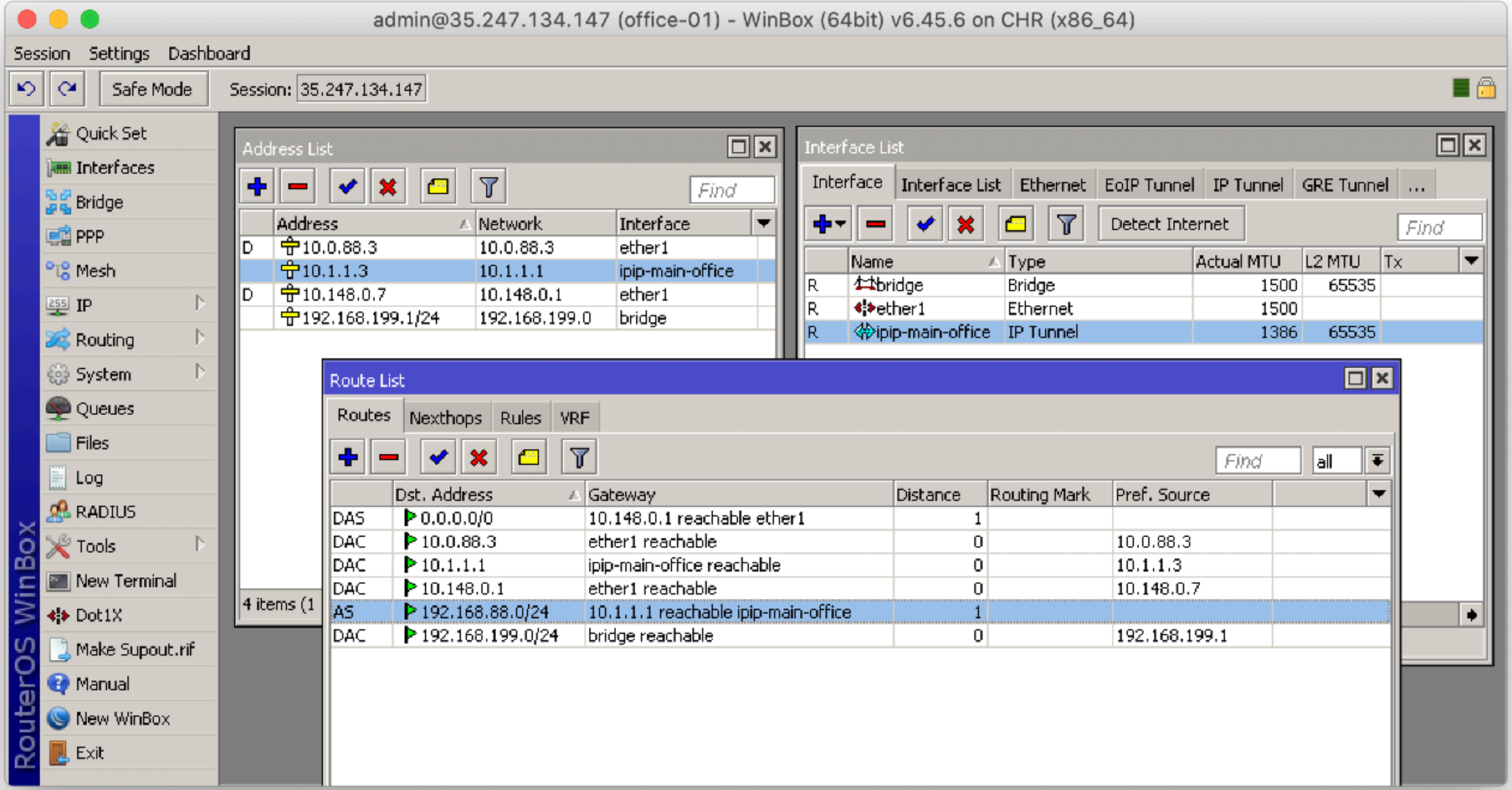
Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

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



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

4 items (1

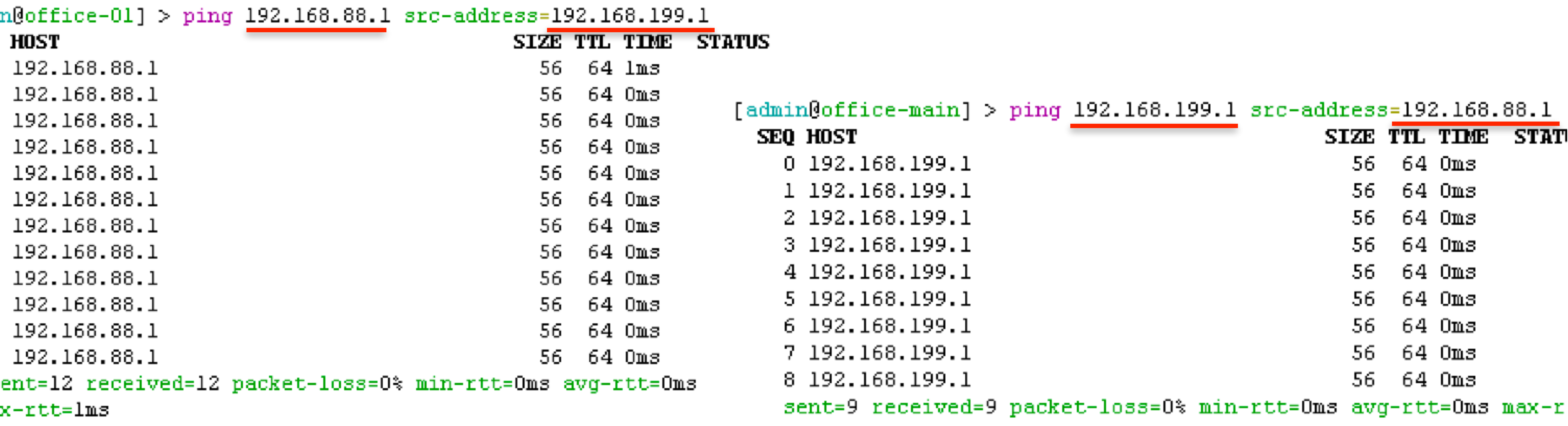
Interface List

	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

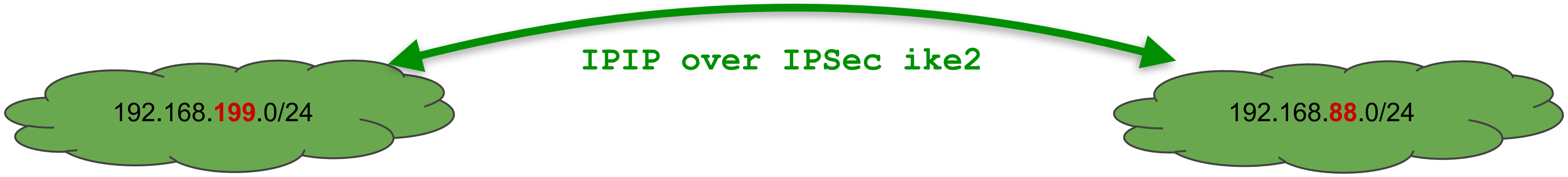
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	10.148.0.1 reachable ether1	1		
DAC	10.0.88.3	ether1 reachable	0		10.0.88.3
DAC	10.1.1.1	ipip-main-office reachable	0		10.1.1.3
DAC	10.148.0.1	ether1 reachable	0		10.148.0.7
AS	192.168.88.0/24	10.1.1.1 reachable ipip-main-office	1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

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

OSPF ~~works~~

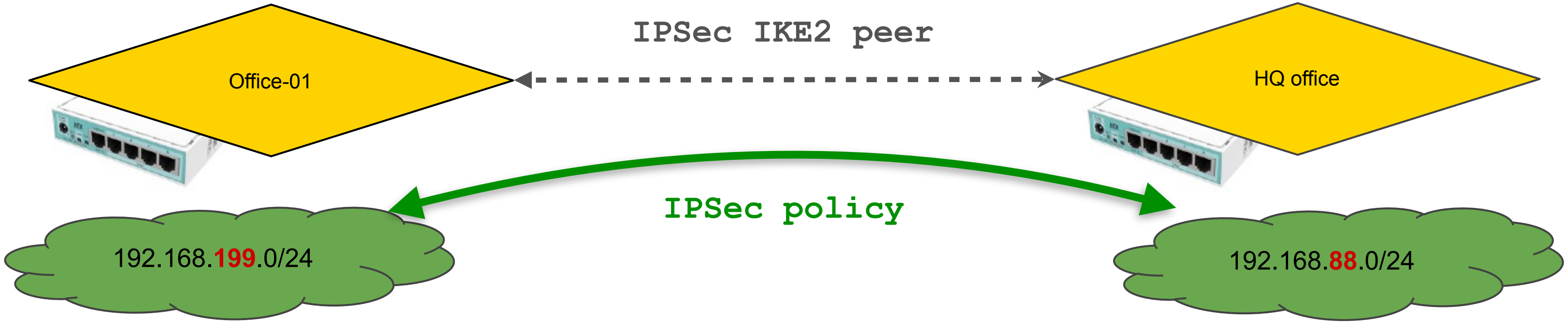
Harder to configure and understand

Has no routable interface

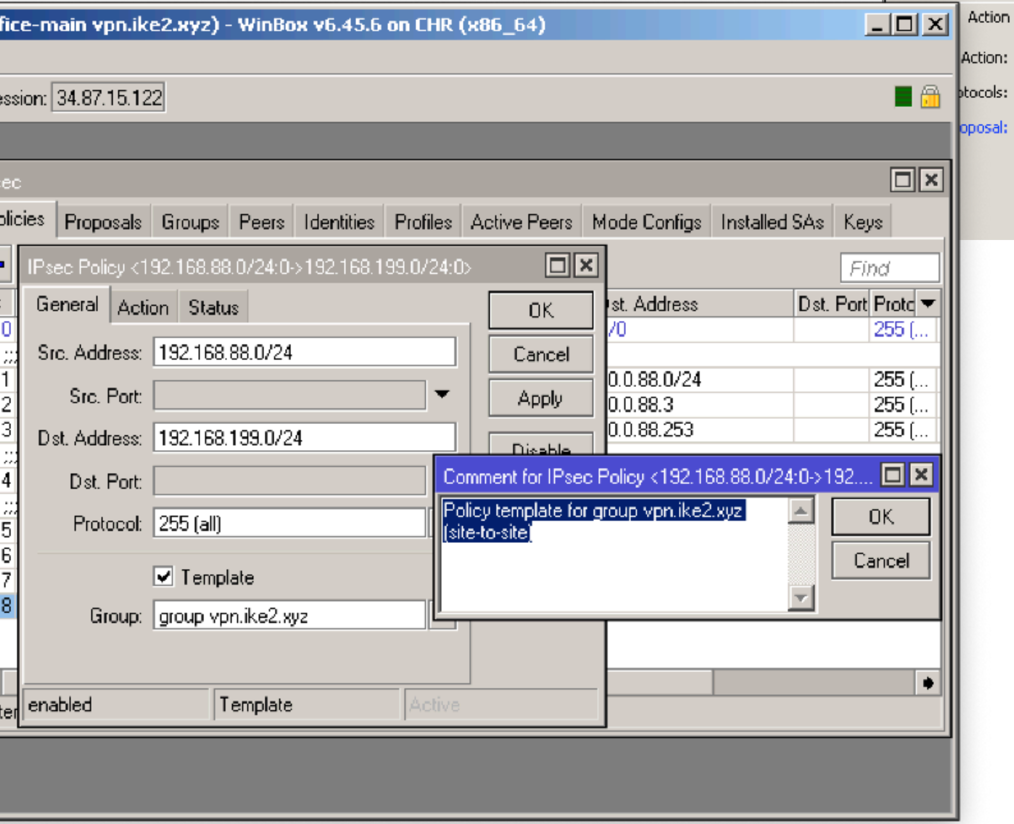
Need to adjust TCP MSS manually

Cons:

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



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


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

ession: 34.87.15.122

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

Src. Address: 192.168.88.0/24

Src. Port:

Dst. Address: 192.168.199.0/24

Dst. Port:

Protocol: 255 (all)

☑ Template

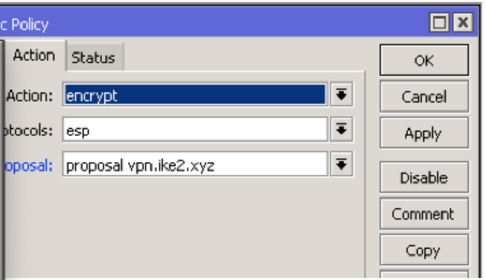
Group: group vpn.ike2.xyz

enabled | Template | Active

```
st. Address    Dst. Port  Proto
/0                        255 (...
0.0.88.0/24               255 (...
0.0.88.3                  255 (...
0.0.88.253                255 (...
```

Comment for IPsec Policy <192.168.88.0/24:0->192....

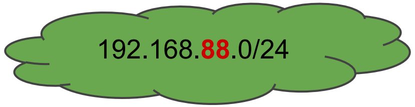
Policy template for group vpn.ike2.xyz (site-to-site)

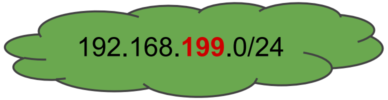

New IPsec Policy

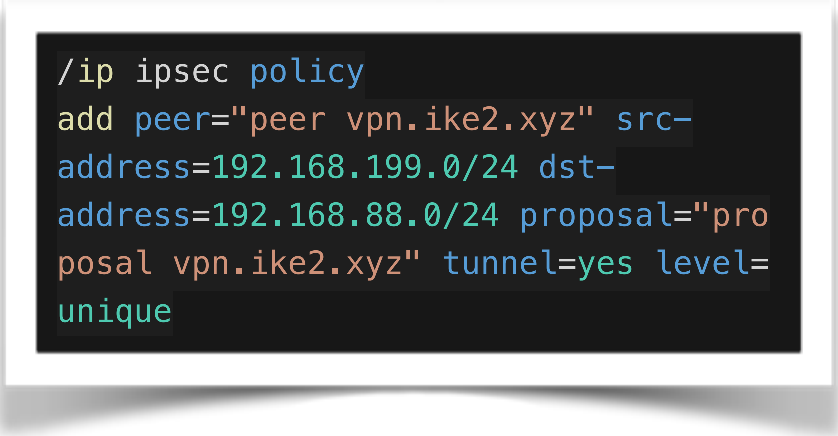
Action: encrypt

otocols: esp

oposal: proposal vpn.ike2.xyz

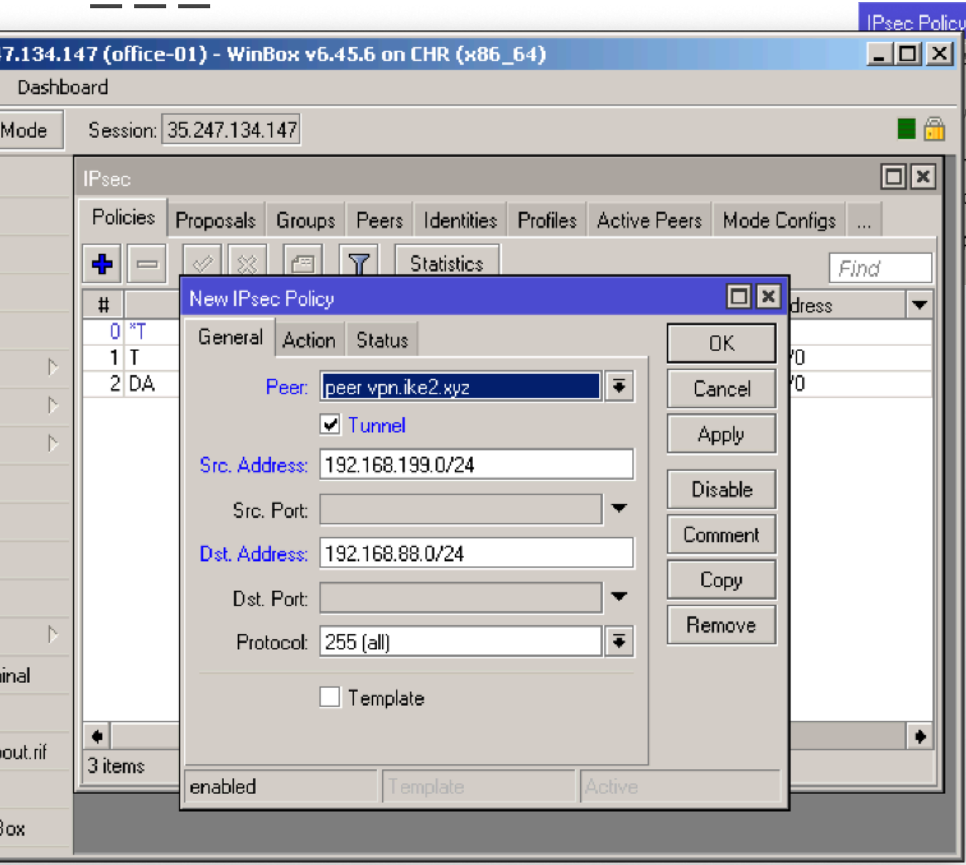





```
/ip ipsec policy
add peer="peer vpn.ike2.xyz" src-address=192.168.199.0/24 dst-address=192.168.88.0/24 proposal="proposal vpn.ike2.xyz" tunnel=yes level=unique
```

Client

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



Session: 35.247.134.147

#	
0	*T
1	T
2	DA

3 items

New IPsec Policy

General | Action | Status

Peer: peer vpn.ike2.xyz

☑ Tunnel

Src. Address: 192.168.199.0/24

Src. Port:

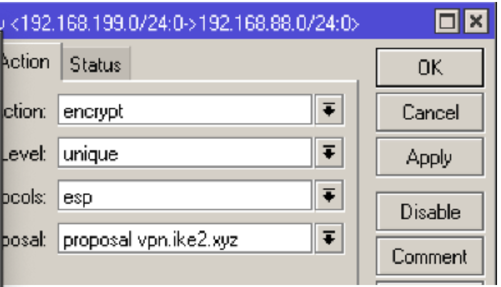
Dst. Address: 192.168.88.0/24

Dst. Port:

Protocol: 255 (all)

□ Template

enabled | Template | Active



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

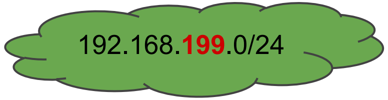
Action | Status

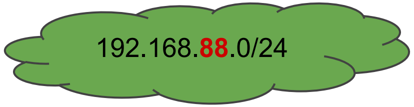
ction: encrypt

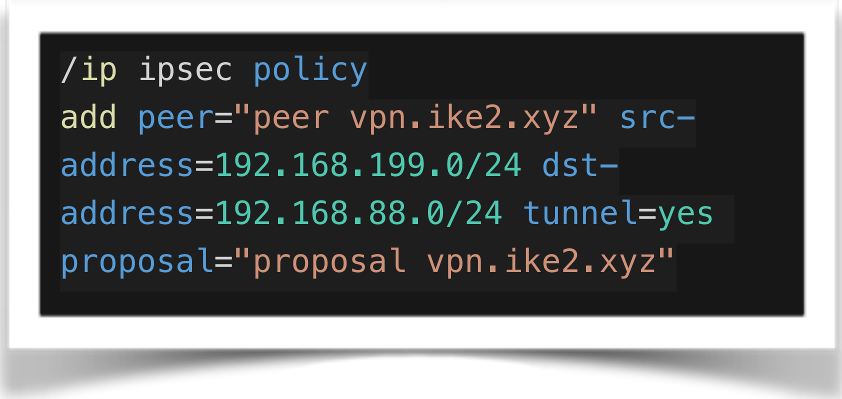
evel: unique

ocols: esp

osal: proposal vpn.ike2.xyz





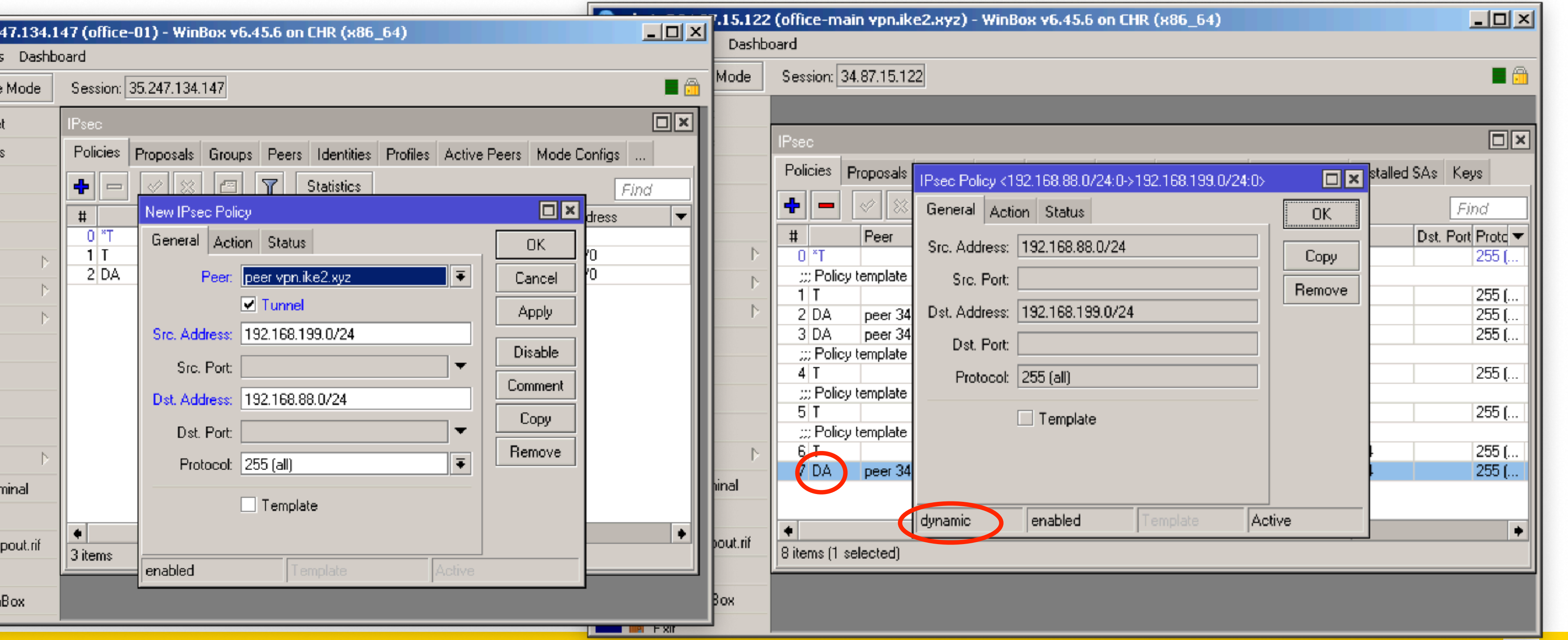


```
/ip ipsec policy
add peer="peer vpn.ike2.xyz" src-
address=192.168.199.0/24 dst-
address=192.168.88.0/24 tunnel=yes
proposal="proposal vpn.ike2.xyz"
```

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

Client

Server



Client: 47.134.147 (office-01) - WinBox v6.45.6 on CHR (x86_64)

Session: 35.247.134.147

IPsec — Policies

#	
0	*T
1	T
2	DA

3 items

New IPsec Policy — General

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

enabled | Template | Active

Server: .15.122 (office-main vpn.ike2.xyz) - WinBox v6.45.6 on CHR (x86_64)

Session: 34.87.15.122

IPsec — Policies

#		Peer
0	*T	
;;; Policy template		
1	T	
2	DA	peer 34
3	DA	peer 34
;;; Policy template		
4	T	
;;; Policy template		
5	T	
;;; Policy template		
6	T	
7	DA	peer 34

8 items (1 selected)

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

Src. Address: 192.168.88.0/24

Src. Port:

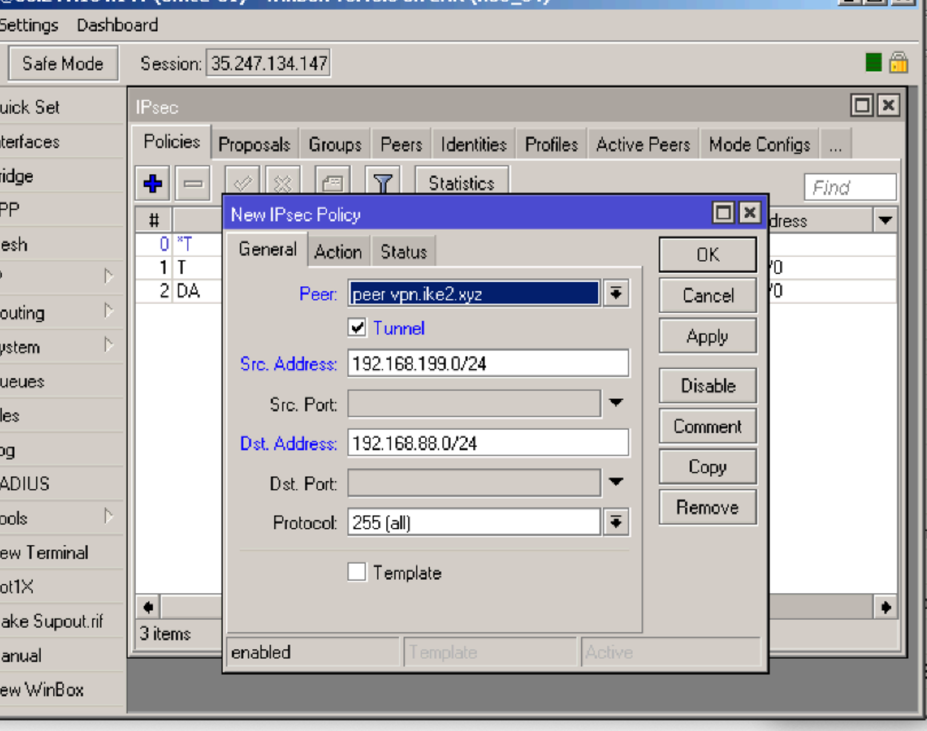
Dst. Address: 192.168.199.0/24

Dst. Port:

Protocol: 255 (all)

□ Template

dynamic | enabled | Template | Active



Session: 35.247.134.147

#	
0	*T
1	T
2	DA

3 items

New IPsec Policy

Peer: peer vpn.ike2.xyz

☑ Tunnel

Src. Address: 192.168.199.0/24

Src. Port:

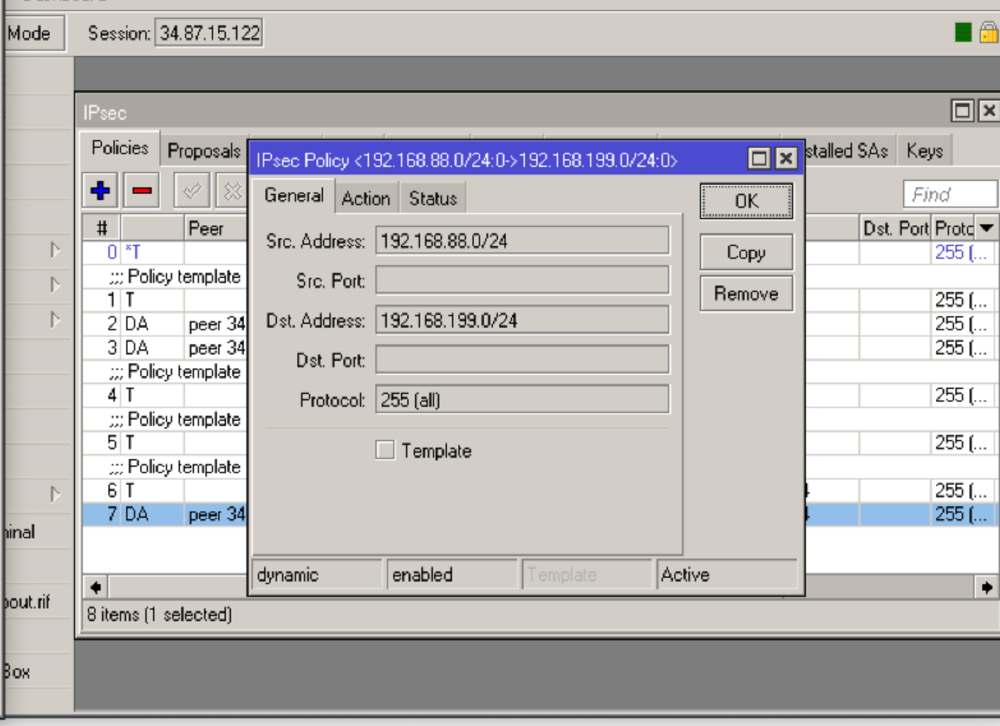
Dst. Address: 192.168.88.0/24

Dst. Port:

Protocol: 255 (all)

□ Template

enabled | Template | Active



Session: 34.87.15.122

#		Peer	Dst. Port	Protc
0	*T			255 (...
;;; Policy template				
1	T			255 (...
2	DA	peer 34		255 (...
3	DA	peer 34		255 (...
;;; Policy template				
4	T			255 (...
;;; Policy template				
5	T			255 (...
;;; Policy template				
6	T			255 (...
7	DA	peer 34		255 (...

8 items (1 selected)

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

Src. Address: 192.168.88.0/24

Src. Port:

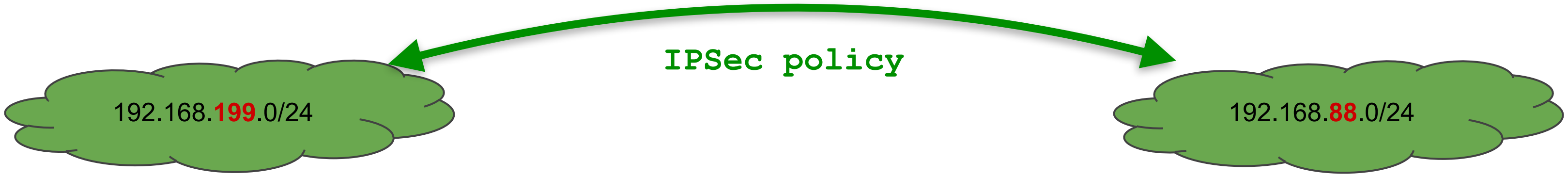
Dst. Address: 192.168.199.0/24

Dst. Port:

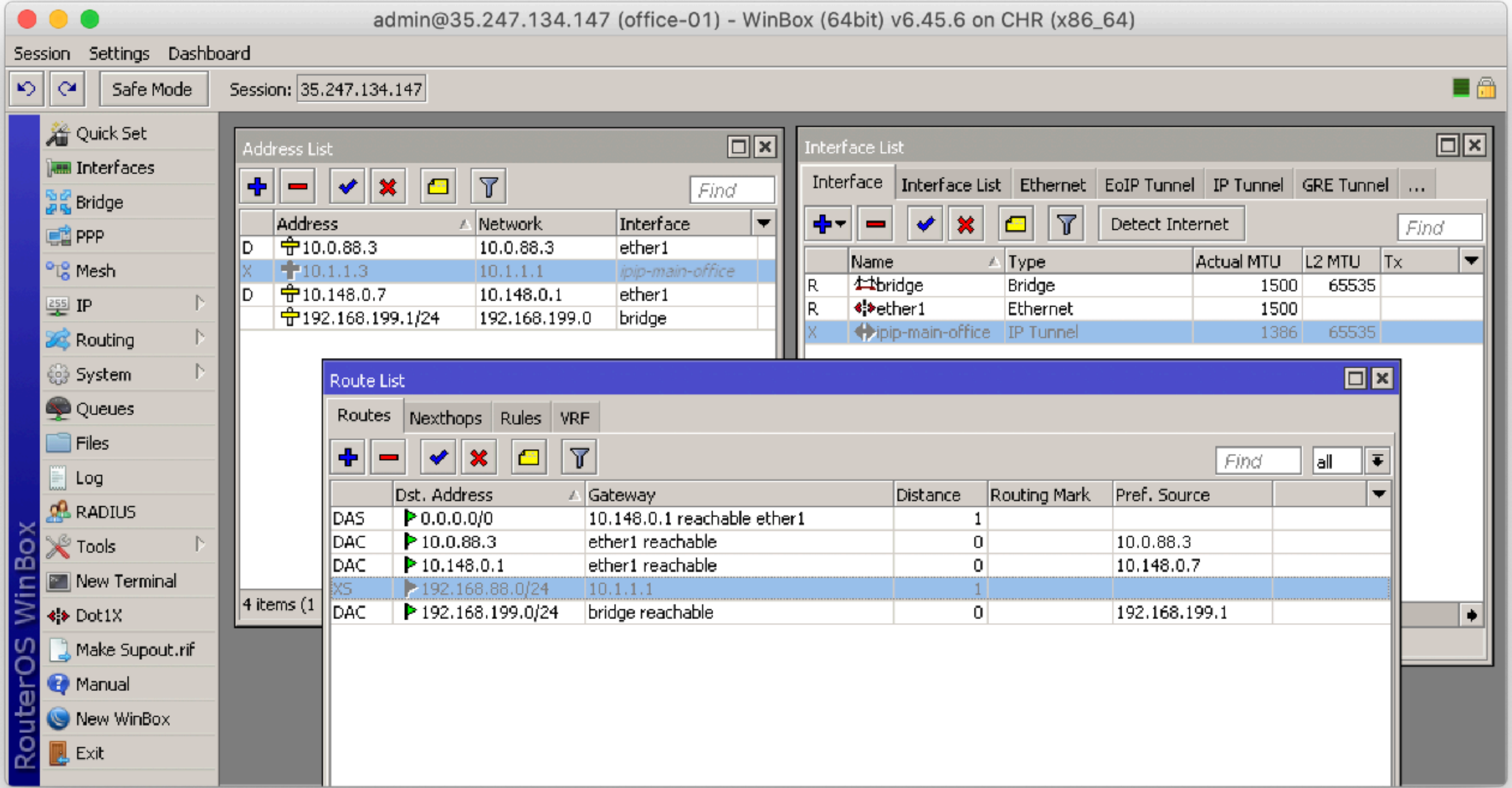
Protocol: 255 (all)

□ Template

dynamic | enabled | Template | Active



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



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

4 items (1

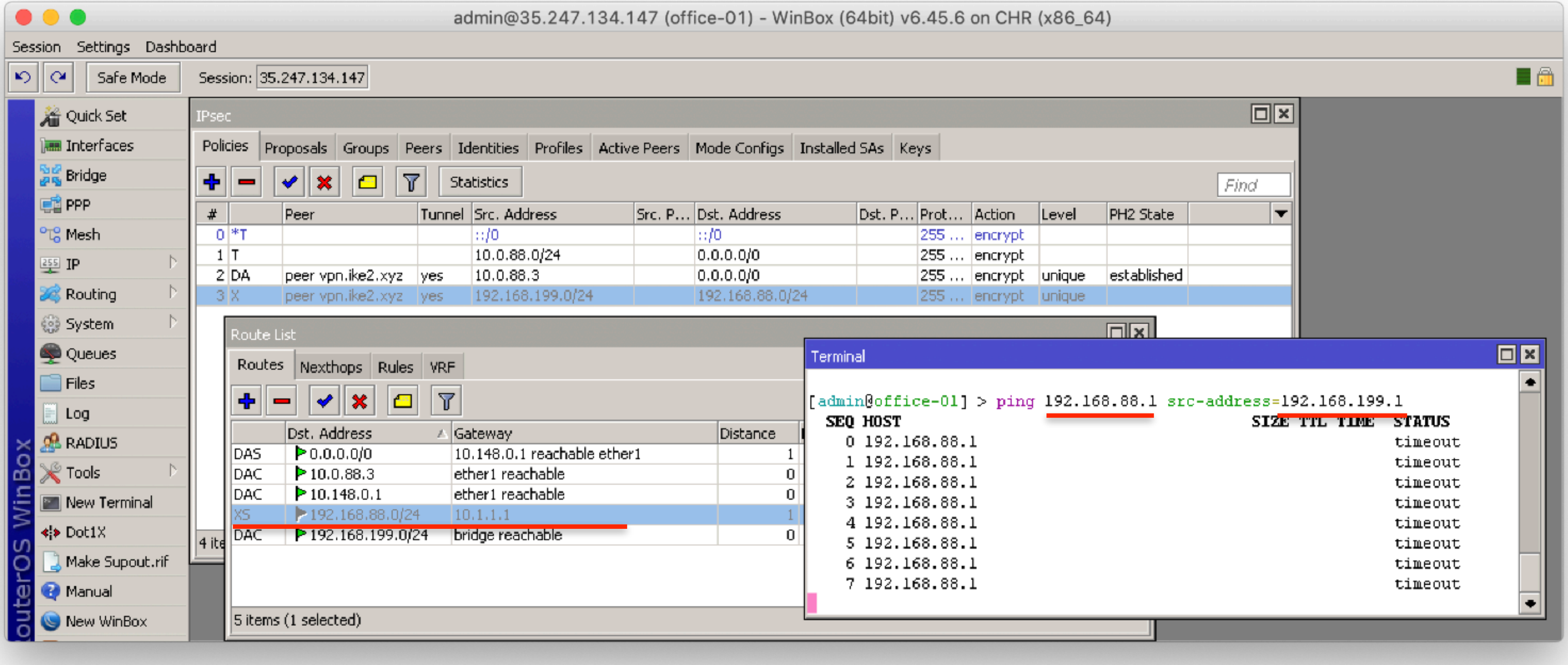
Interface List

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

Route List

	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	10.148.0.1	ether1 reachable	0		10.148.0.7
XS	192.168.88.0/24	10.1.1.1	1		
DAC	192.168.199.0/24	bridge reachable	0		192.168.199.1

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



Session: 35.247.134.147

#		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	X	peer vpn.ike2.xyz	yes	192.168.199.0/24		192.168.88.0/24		255 ...	encrypt	unique	

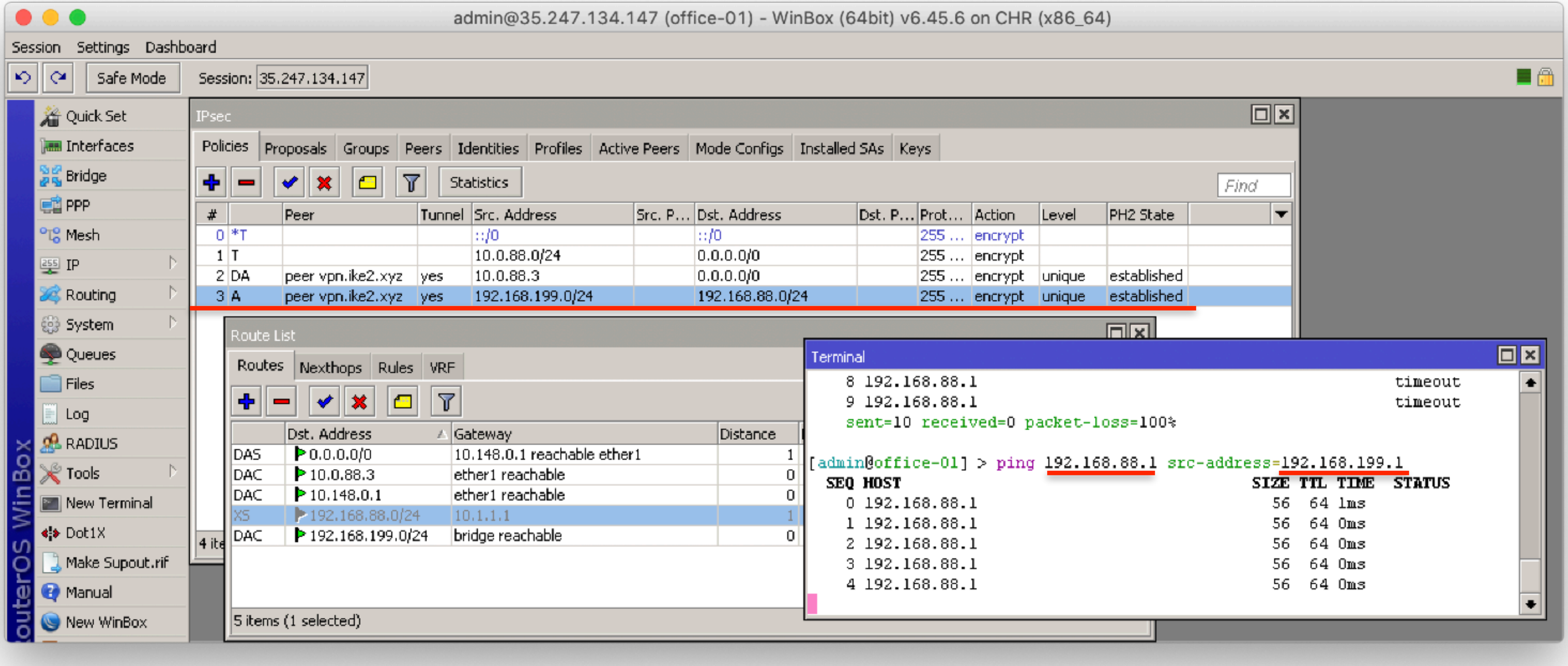
4 ite

	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

5 items (1 selected)

```
[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



#		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

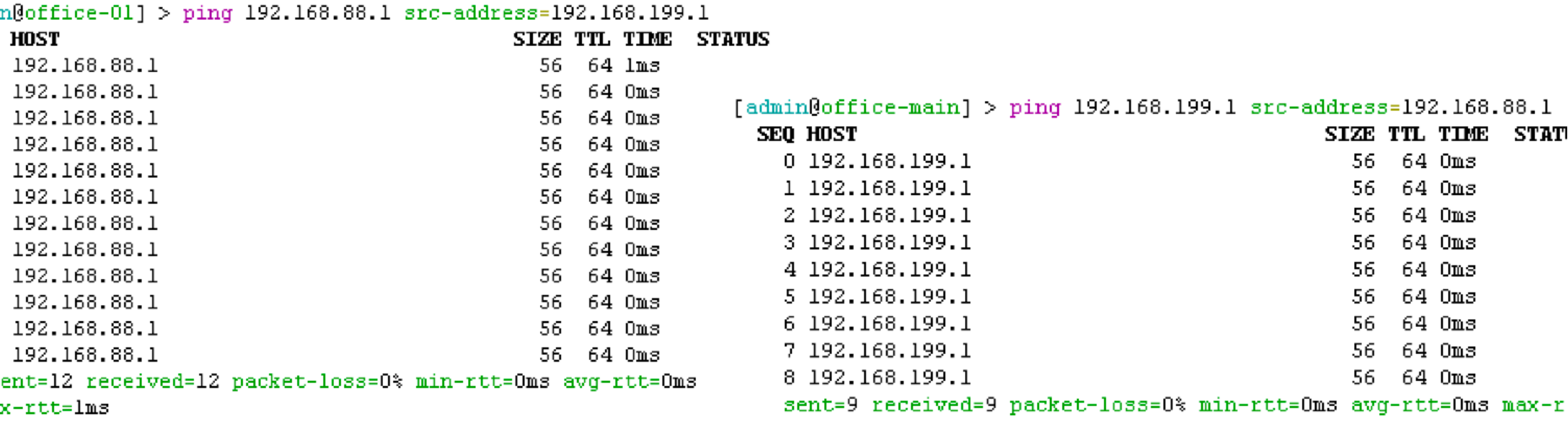
4 ite

	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

5 items (1 selected)

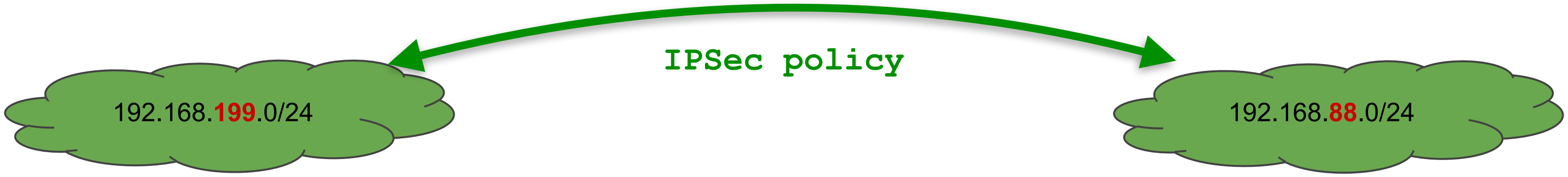
```
    8 192.168.88.1                                              timeout
    9 192.168.88.1                                              timeout
    sent=10 received=0 packet-loss=100%

[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



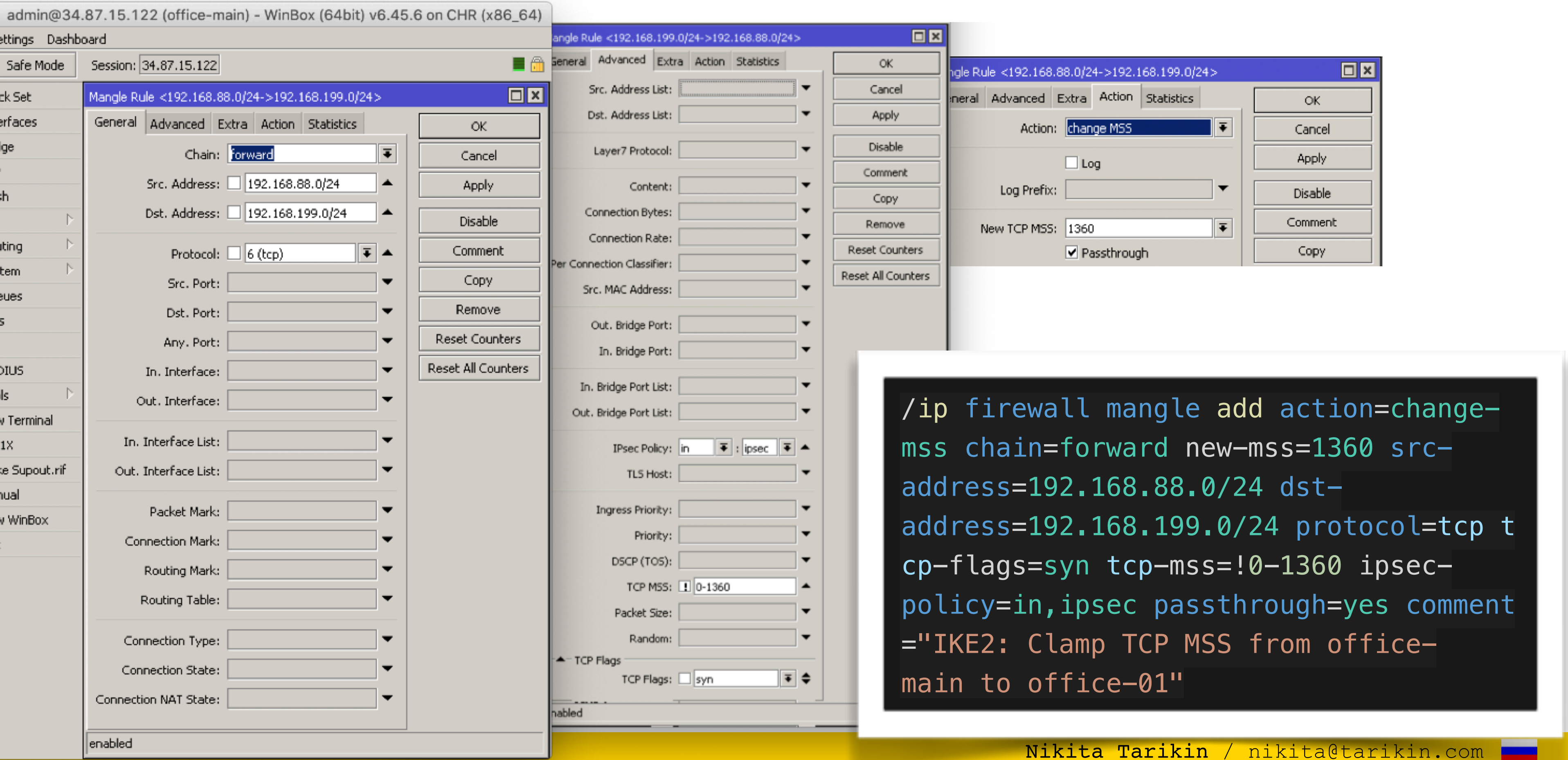
```
n@office-01] > ping 192.168.88.1 src-address=192.168.199.1
 HOST                                     SIZE TTL TIME  STATUS
 192.168.88.1                               56  64 1ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               56  64 0ms
 192.168.88.1                               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  STATU
    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



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

Session: 34.87.15.122

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

General tab:

- 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

Advanced tab:

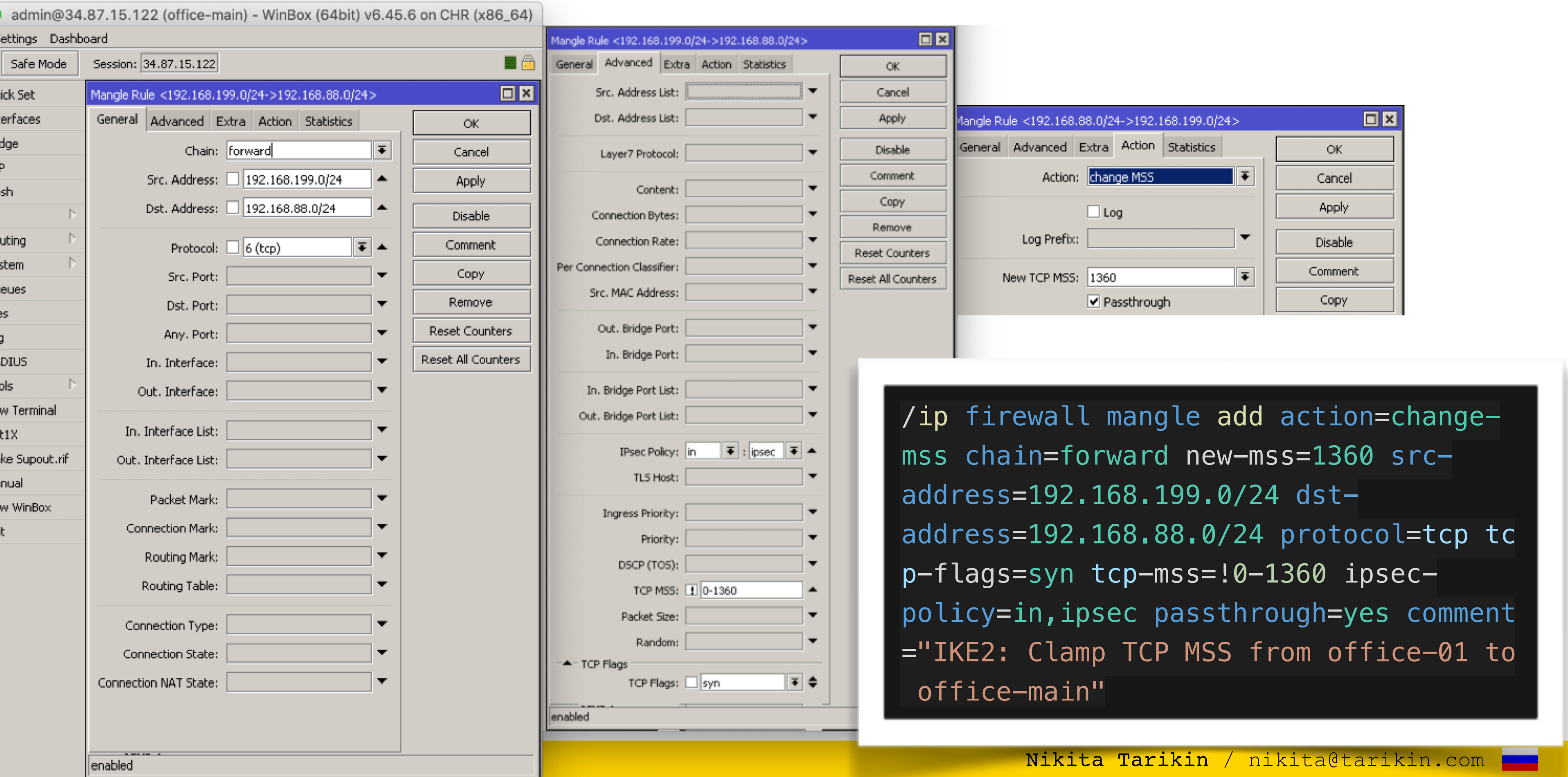
- Src. Address List:
- Dst. Address List:
- Layer7 Protocol:
- Content:
- Connection Bytes:
- Connection Rate:
- Per Connection Classifier:
- Src. MAC Address:
- Out. Bridge Port:
- In. Bridge Port:
- In. Bridge Port List:
- Out. Bridge Port List:
- IPsec Policy: in : ipsec
- TLS Host:
- Ingress Priority: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

Action tab:

- 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)

Session: 34.87.15.122

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

General:

- 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:

enabled

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

Advanced:

- 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

enabled

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

Action:

- 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=192.168.199.0/24 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

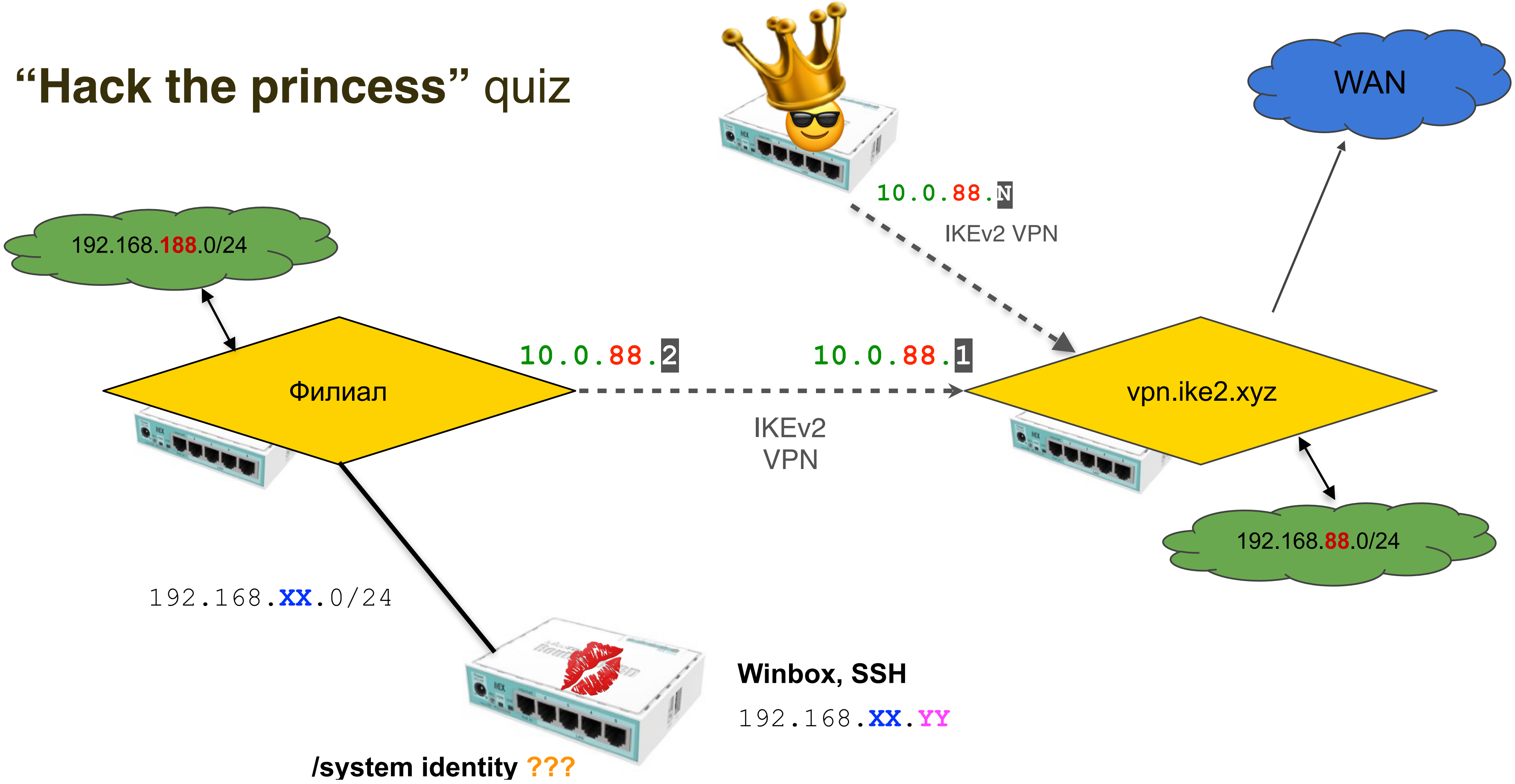
Login lab
Password lab

IPSec quiz time!

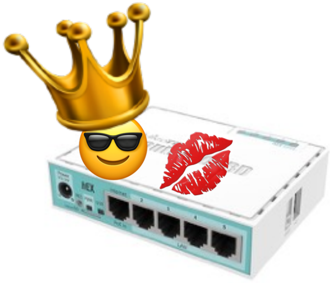
“ Hack the princess ”

Will be open until 31 December 2019

“Hack the princess” quiz

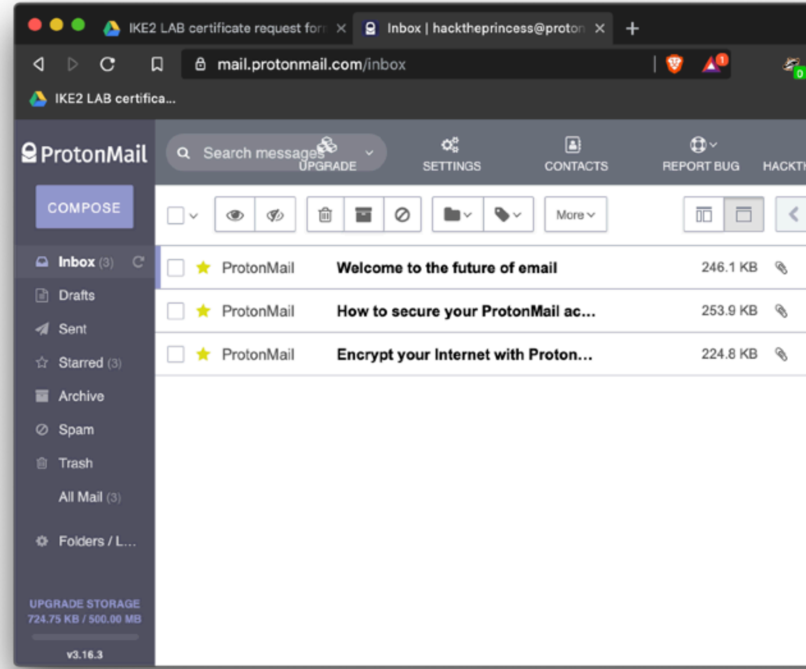


hacktheprincess@protonmail.com



```
192.168.XX.0/24

192.168.XX.YY

/system identity ???
```

Send results to e-mail



☆ ProtonMail	Welcome to the future of email	246.1 KB	
☆ ProtonMail	How to secure your ProtonMail ac...	253.9 KB	
☆ ProtonMail	Encrypt your Internet with Proton...	224.8 KB	

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