

## Nikita Tarikin

Certified network engineer MikroTik PRO, Russia



## Nikita Tarikin

Certified network engineer MikroTik PRO, Russia







### @tarikin



Edit Profile



New

Phuket 2019 MikroTik Viet Vietnam jan... 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 Tropical engineer

Chats



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



O 150 13:51





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 siteto-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

🛃 Indonesia in Bali! @ MUM

# Let's keep in touch

Send me e-mail: nikita@tarikin.com





0

@tropicalengineer

Direct message me via:





#### Watch this presentation on YouTube

https://www.youtube.com/watch?v=n5\_Af2vIIOA

## Why IPSec IKE2?

Nikita Tarikin / nikita@tarikin.com

#### 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

Nikita Tarikin / nikita@tarikin.com 🚃

## 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**

Nikita Tarikin / nikita@tarikin.com



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



## 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+



. Download package from www.mikrotik.com/download

 Upload package to / of your RouterBoard

#### Reset RouterBoard to default v6.45+ configuration

	admin@192.168.8	8.1 (MikroTik) - Wir	nBox v6.44.3 on mAP	lite (mipsbe)	
Session Settings Dashbo	Session: 192.168.88.1				CPU: 4%
	Auto Upgrade Certificates Clock Console Disks History Identity LEDs License Logging Packages Password	Updates Enable v Version sbe 6.44.3 -tools 6.44.3 Reset Configuration Ke CA No Run After Reset:	Disable Uninstall Build Time Apr/23/2019 12:37 Apr/23/2019 12:37 Rep User Configuration APS Mode to Default Configuration to Not Backup	Unschedule Scheduled 103 103 Reset Configuration Cance	Check Installati
	Reboot Reset Configuration Resources		System -	-> Reset c	onfiguratio
	Routerboard SNTP Client				

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

The following default co	nfiguration has been ins	talled on your router:	<b></b>
RouterMode:			
* WAN port is protecte	d by firewall and enable	d DHCP dient	
* Wireless and Etherne	t interfaces (except WA	N port ether1)	
are part of LAN bridge	9		
wlan1 Configuration:			
mode: ap-b	ridge;		
band: 2ghz	·b/g/n;		
tx-chains: 0;1;			
rx-chains: U;1;	40mba VV		
AN Configuration: 20	/+011112-775j		
IP address 192,168,6	38.1/24 is set on bridge	(LAN port)	
DHCP Server: enable	d:	(	
WAN (gateway) Config	uration:		
gateway: ether1;			
ip4 firewall: enabled			
NAT: enabled;			
DHCP Client: enabled	l;		•
	Remove Configuration	Show Script	OK

Nikita Tarikin / nikita@tarikin.com

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

Sefe Mode       Section: 192.166.88.1         CAPSHAN       Interfaces         CAPSHAN       Interface         Wreless       Find         Strike       Offor         S	sion Settings Dashbo	ard	Check DNS records:
Quark Set       Interface       Image: Set of the	😋 🛛 Safe Mode	Session: 192.168.88.1	<sup>(PU:1%</sup> ■a Name: <b>vpn.ike2.xvz</b>
Partition           Make Supput.rif           Manual           2 Items   * Set DNS records with your domain n	Quick Set  CAPSMAN  CAPSMAN  Im Interfaces  Wireless  Bridge  PPP  Switch  Switch  CapsMesh  PR  CapsMesh  PR  CapsMesh  Cap	DHCP Client DHCP Client Options	Address: 123.45.67.
Manual     A Set DNS records with your domain n	Partition           Make Supout.rif		
	😯 Manual	2 items	* Set DNS records with your doma

123.45.67.8 is on WAN interface

registrar

#### Setup correct timezone

Session Settings Dashb	editional admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)           Session         Settings         Dashboard					
Safe Mode	Session: 192.168.88.1 Time: 10:09:12 Date: Jan	/01/1970 CPU: 4% 🔳 🛅				
CAPSMAN						
Standard Bridge						
PPP						
📟 Switch	Clock					
°ा8 Mesh	Time Manual Time Zone	ОК				
255 IP 🗅	Time: 10:09:12	Cancel				
😹 Routing 🛛 🗈	Date: Jan/01/1970	Apply				
💮 System 🛛 🗅	Time Zone Autodetect					
🙊 Queues	Time Zone Name: Asia/Kuala_Lumpur 🖛	1				
Files						
Log	GMT Offset: +08:00					
A RADIUS	DST Active					
🗙 🔀 Tools 🔹 🗅						
🞽 🔚 New Terminal						
MetaROUTER						
n Partition						
Q 🔔 Make Supout.rif						
🔮 🔮 Manual						
🗟 🔘 New WinBox						

System -> Clock



/system clock set time-zone-name=Asia/ Kuala\_Lumpur

kua.a\_\_umpui

Nikita Tarikin / nikita@tarikin.com 🚃

#### Setup auto date/time

Section Settingt Dathb	admin@192.168.88.1 (N	/likroTik) - WinBox v6.44	.3 on mAP lite (mipsbe)	
Safe Mode	Session: 192.168.88.1		Time: 12:36:41 Date: May/08/	2019 CPU: 2% 📕 🛅
A Quick Set		SNTP Client		
Interfaces		Mode:	unicast	OK Cancel
Bridge		Primary NTP Server: Secondary NTP Server:	0.0.0.0	Apply
Switch	Outo Liborade	Server DNS Names:	0.asia.pool.ntp.org	
IP ► Routing ► System ►	Certificates Clock	Dynamic Servers:	1.asia.pool.ntp.org     ♥       2.asia.pool.ntp.org     ♥	
Queues Files Log	Console Disks History Identity	Poll Interval: Active Server:	32 s 119.28.183.184	
RADIUS     Tools     New Terminal	LEDs License Logging	Last Update: Last Adjustment:	00:00:09 ago 3 442 us	
Partition Make Supout.rif Manual	Packages Password Ports Rebort	Last Bad Packet From: Last Bad Packet: Last Bad Packet Reason:		
New WinBox	Reset Configuration Resources Routerboard SNTP Client Scheduler Scripts	Activa	ate NTP cl.	ient
	Shutdown			

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

tp.org,2.asia.pool.ntp.org

Nikita Tarikin / nikita@tarikin.com



#### Add new loopback bridge

e e e	idmin@192.168.88	.1 (MikroTik) - \	WinBox v6.44.3 on mAP lite (mips	sbe)	
Session Settings Dashbo	pard				
Safe Mode	Session: 192.168.88.1		•	CPU;	3% 📕 🛅
Image: Safe Mode         Image: Quick Set         Image: CAPsMAN         Image: Interfaces         Image: Wireless         Image: Bridge         Image: PPP         Image: Switch         Image: PP         Image: Switch         Image: Routing         Image: Rou	Session: 192.168.88.1	Interface Interface Name: Type: MTU: Actual MTU: L2 MTU: L2 MTU: MAC Address: ARP: ARP Timeout: nin. MAC Address: Ageing Time:	Status Traffic bridge-loopback Bridge enabled Control of the second	CPU: OK Cancel Disable Comment Copy Remove Torch	3%

/interface bridge add
name=bridge-loopback

Nikita Tarikin / nikita@tarikin.com 🚃

#### Set loopback bridge IP address

•	<b>•</b> •	dmin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	
Ses	sion Settings Dashb	bard	
ю	😋 🛛 Safe Mode	Session: 192.168.88.1	CPU: 2% 📕 🛅
ß	Safe Mode         Quick Set         CAPsMAN         Interfaces         Wireless         Bridge         PP         Switch         Mesh         IP         Routing         Piles         Queues         Files         Log         ADDUS	Session: 192.168.88.1	CPU; 2%
outerOS WinBox	KADOS     Tools     New Terminal     MetaROUTER     Partition     Make Supout.rif     Manual     New WinBox	2 items enabled	

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

network=10.0.88.0

#### Add new IP Pool for ike2 VPN clients



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

ranges=10.0.88.2-10.0.88.254

Nikita Tarikin / nikita@tarikin.com

## Generate SSL certificates

Agenda for next slides

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



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



#### /certificate sign CA.ike2.xyz

(	Generate server SSL certificate								
-									
•	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)								
Ses	sion Settings Dashb	ooar	d						
ю	Cafe Mode	s	ession: 192.168.8	8.1					CPU: 1% 📕 🔒
	🔏 Quick Set	Г	ertificates		/				
	I CAPSMAN	Ľ	New Certificate						
	Interfaces	l	General Key U	sage Status					
	🤶 Wireless		Nar	vnn.ike2.x	WZ				ОК
	👷 🖁 Bridge	5	- Non						Cancel
	📑 PPP	ľ							Apply
	🛫 Switch		Iccu					-	
	°t <mark>8</mark> Mesh		1330						
	255 IP 🗅		Lounti	r <b>y:</b> MY					Remove
	🎉 Routing 💦 🖹		Stal	e: Selangor					Sign
	🛞 System 🛛 ▷		Locali	y: Cyberjaya					Sign via SCEP
	룢 Queues		Organizatio	n: IKE2.xyz					Import
	📄 Files			VPN					Card Reinstall
	📄 Log			~					Cand Haville
	🧟 RADIUS		Common Nam	e: vpn.ike2.x	yz				
×	🎇 Tools 🛛 🗅	Ľ	Subject Alt, Nam	e: DNS		₹ : vpn.ike2.	хуг	<b>\$</b>	Set CA Passphrase
B	📰 New Terminal								Export
/in	RetaROUTER		Key Sia	:e: 2048					Revoke
>	Nertition		Days Va	id: 1095					
Ö	🔒 Make Supout.rif								
Ter	🤁 Manual								
out	New WinBox				and the section			The sector of	
Ř	🛃 Exit		private key	cri	authority	expired	Ismart card key	ftrusted	

New Certificate		
General Key Usage Status Key Usage: digital signature key encipherment	content commitment	OK Cancel
key agreement crl sign decipher only	key cert. sign encipher only dvcs	Apply
server gated crypto timestamp ipsec tunnel	ocsp sign ipsec user ipsec end system	Remove Sign
tls dient	v tis server	Sign via SCEP Import

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

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

🔴 😑 🛑 admin@	9192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	
Session Settings Dashboard		
Safe Mode Session: 192	2.168.88.1	CPU: 1% 📕 🛅
Quick Set		
I CAPSMAN Certificate		
🛲 Interfaces 🚽 🚽 General	Key Usage Status	
🌊 Wireless	Name: vpn.ike2.xvz	ОК
월쑳 Bridge		Cancel
E PPP		Apply
🙄 Switch	Issuer:	Copy
°t8 Mesh		Demous
255 IP	Country: MY Sign	Remove
🔀 Routing 🗈	State: Sel Certificate: vpn.ike2.xyz 🔻 Start	Sign
💮 System 🗈	Locality: Cy CA: CA.ike2.xyz 🖛 Stop	Sign via SCEP
See Queues Org	anization: IKE CA CRL Host:	Import
Files	Unit: VP Progress:	Card Reinstall
		Card Verify
2 Comm	non Name: vpn.ike2.xyz	Set CA Basebrase
Subject 4	Alt. Name: DNS 🗧 : vpn.ike2.xyz	Set CA Passpirase
Mew Terminal	Key Sizer 2049	Export
		Revoke
Partition L	Jays Valid: 1095	
Make Supout.rif		
🗿 🥶 Manual		
New WinBox	v cri authority evpired smart card key trusted	
	y Jen Jacenoney Jexpired Jeniari cara kay ferasea	1

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

са=са.ткег.хуг

Nikita Tarikin / nikita@tarikin.com 🚃

#### Client certificate template

•	• •	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	
Ses	sion Settings Dashb	oard	
ø	Cafe Mode	Session: 192.168.88.1	CPU: 0% 📕 🧯
	🔏 Quick Set	Certificates	
	CAPsMAN	New Certificate	
	Interfaces	General Key Usage Status	
	🚊 Wireless		OK
	😹 Bridge		Cancel
	e PPP	KI L	Apply
	🛫 Switch		
	°18 Mesh	Issuer	Сору
	∰ IP ►	Country: MY	Remove
	😹 Routing 🗈	State: Selangor	Sign
	😳 System 🗅	Lycality: Cyberjaya	Sign via SCEP
	👳 Queues	Organization: TKE2.xvz	Import
	Files		Card Deinstall
	Log		
	S RADIUS	2 Common Name: ~client-template@vpn.ike2.xyz	Card Verity
_	X Tools	Subject Alt. Name: Email  F: ~client-template@vpn.ike2.xyz	♦ Set CA Passphrase
ĝ	New Terminal		Export
Ē		Key Size: 2048	▼ Revoke
≥	Make Superturin	Days Valid: 365	
SC	Magual		
er			
ut		Entertaine Entertaine Entertaine Entertaine Entertaine Entertaine	
8	EXIC	private key on jauthonity expired smart card key trusted	

levi Certif	icate		
General Key Usag	Key Usage Status e: digital signature key anicpherment key agreement cri sign decipher only server gated crypto timestamp jopse tunnel email protect v tis client	content commitment data encipherment key cert, sign encipher only dvcs ocsp sign ipsec user ipsec end system code sign tls server	CK Cancel Apply Copy Remove Sign Sign Sign SCEP
			in the second

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

#### Generate client SSL certificate from template

Safe Mode	Session: 192.168.88.1									CPU: 0%
Set		c	ertificate	<~client-te	emplate@vpn	.ike2.xyz>				
MAN			General	Key Usage	e Status					
faces				Name	orlient-templ	ate@vnn.ike2.v	1/72		_	OK
ess	New Certificate			Nume:	- cione compi	acoerprincers	.72			Cancel
e	General Key Licas	e Statur				6				Apply
	noy cody	o status						ОК	2	Copy
h	Name:	c1@vpn.ike2	.xyz					Cancel		Сору
l							<u>^</u>	Apply		Remove
P								Арру		Sign
ng D	Issuer:	1					<u> </u>	Сору		Sign via SCEP
m 🗈	Country:	MY						Remove		Import
es	State:	Selangor						Sign		Card Reinstall
	Locality:	Cyberjaya						Sign via SCEP		Card Verify
US	Organization:	IKE2.xyz						Import		Set CA Passphrase
۲.	Unit:							Card Reinstall	-	Export
Terminal								Card Verify	₹	Revoke
ROUTER	Common Name:	c1@vpn.ike2	.xyz					Cab CA Daarahaaaa		Refere
ion	Subject Alt, Name:	Email				ike2.xyz	<b>+</b>	Det CA Passpirrase		
Supout.rif	Key Ster	2049					I	Export		
al	Ney Jize.	2010						Revoke		
WinBox	Days Valid:	365							red	

/certificate add copy-from=~clienttemplate@vpn.ike2.xyz name=c1@vpn.ike2.xyz commonname=c1@vpn.ike2.xyz subject-altname=email:c1@vpn.ike2.xyz

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

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)									
Safe Mode	Session: 192.168.88.1	CPU: 2%							
🔏 Quick Set	Certificates								
I CAPSMAN	Certificate <c1@vpn.ike2.xyz></c1@vpn.ike2.xyz>								
🖬 Interfaces	General Key Usage Status								
🤶 Wireless	Name: c1@unp.ike2.vuz	ОК							
😹 Bridge		Cancel							
📑 PPP		Apply							
🙄 Switch									
°ĩ¦8 Mesh		Сору							
IP D	Country: M Certificate: c1@vpn.ike2.xyz 🔹 Start	Remove							
🌌 Routing 🗈 🗎	State: Se CA: CA.ike2.xyz ∓ ▲ Stop	Sign							
System ▷	Locality: C CA CRL Host:	Sign via SCEP							
🙊 Queues	Organization: IN Progress: /	Import							
Files		Card Beinstall							
Log	OTRA								
A RADIUS	Common Name: c1@vpn.ike2.xyz	Card Verify							
🗙 💥 Tools 🔹 🗅	└┘ Subject Alt. Name: Email 〒: c1@vpn.ike2.xyz ◆	Set CA Passphrase							
🞽 🔳 New Terminal		Export							
MetaROUTER	Key Size: 2048	Revoke							
n 🖉 Partition	Days Valid: 365								
on 🗋 Make Supout.rif									
🔮 📢 Manual									
o New WinBox									

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

ci@vpn.ikeZ.xyz ca=LA.ikeZ.xyz

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

	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	
Safe Mode	Session: 192.168.88.1	CPU: 1% 📕 🛅
A Quick Set	Certificates Certificate <c1@vpn.ike2.xyz></c1@vpn.ike2.xyz>	
Wireless	Name: c1@vpn.ike2.xyz	OK Cancel
PPP Switch	Tssuer	Apply
°tô Mesh ≝ IP ▷	Country: MY	Remove
Routing     Note:	State Export Locality Certificate: c1@vpn.ike2.xyz Export Export	Sign Sign via SCEP
E Queues	Organization Type: PKCS12 Cancel Unit Export Passphrase: ****** Keep In secret	Import Card Reinstall
RADIUS	Common Name: c1@vpn.ike2.xyz Subject Alt. Name: Email : c1@vpn.ike2.xyz	Card Verify Set CA Passphrase
MetaROUTER	Key Size: 2048	Export Revoke
Partition           Make Supout.rif	Days Valid: 365	
💜 Manual 🍥 New WinBox	private key of authority issued expired event event	

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

export-passphrase=keepinsecret

#### Generate various client SSL certificates from template (example)

		admin@1	92.168.88.1 (MikroTik) - Wir	1Box v6.45.2 on h	nAP lite (smips)				
ssion Settings Dasht	Session: 192.168.88.1					CPU: 1%			
A Quick Set	New Certificate								
I CAPSMAN	General Key Licage Statu	c .							
🚛 Interfaces	Key Usage Diato			Certificate <alex@n< td=""><td colspan="2"></td></alex@n<>					
I Wireless	Name:  rrontdo	or@rkn.gov.ru		General Key Usag	Or				
😹 Bridge		New Certificate		Name:	alex@nsc.ru				
📑 PPP		General Key Usag	e Status		<u> </u>	Cancel			
🙄 Switch	Issuer:	Name:	webmaster@yasdelie.ru			Apply			
°T¦8 Mesh	Country: RU			Issuer:		Сору			
255 IP 🗅	State: Moscow			Couptrus	PU	Remove			
🌌 Routing 👘 🗅	Locality: Moscow	Issuer:		Codinary.	No.	Sign			
💮 System 🛛 🗅	Organization: RKN	Caustan	DU	State:					
💭 Queues	Lipity	Country:	RU	Locality:	Akademgorodok	Sign via SCEP			
<b>«¦&gt;</b> Dot1X		State:	Kaliningrad	Organization:	IKE2.xyz	Import			
Files	Common Name: frontdo	or@rl Locality:	Kaliningrad	Unit:		Card Reinstall			
Log	Subject Alt. Name: Email	Organization:	YaSdelie web development	Common Name:	alex@psc ru	Card Verify			
A RADIUS		Unit:		Cubicat Alt Name		Set CA Passphrase			
🔀 Tools 🔹 🗈	Кеу Туре:	Common Namou	webmaster@uasdelie ru	Subject Alc. Name:	Email • : alex@nsc.ru •	Export			
New Terminal	Key Size: 2048	Common Warne.	webiliaster@yasdelle.rd	Key Type:	RSA	Devoke			
Make Supout.rif	Days Valid: 3650	Subject Alt, Name:	Email • : webma	Key Size:	2048	Keyoke			
Manual		Кеу Туре:		Days Valid:	365				
New WINBOX	private key crl	auth Key Size:	2048						
EXIL		Days Valid:	365		Frankrike Frankrike Frankrike Frankrike				
5		5 Sy 5 Yallar		private key [crl	authority expired smart card trus	sted			
2									
		private key crl	authority expired	smart card tru	isted				

#### Nikita Tarikin / nikita@tarikin.com

#### Export CA SSL certificate .crt file

•	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)								
Session Settings Dashboard									
ю	📯 🛛 Safe Mode	Session: 192.168.88.1	CPU: 2% 📕 🔂						
	🔏 Quick Set	Cartificatos							
	I CAPSMAN	Certificate <ca.ike2.xyz></ca.ike2.xyz>							
	🔚 Interfaces	General Key Usage Status							
	🧘 Wireless	Name: CA.ike2.xyz							
	🕌 🖁 Bridge		Cancel						
	📑 PPP		Apply						
	📰 Switch	Issuer:	Сору						
	°T¦8 Mesh		Remove						
	별 IP 🔹 🕨								
	😹 Routing 💦 🖹	State Export	Sign						
	🛞 System 🛛 🗅	Locality Certificate: CA.ike2.xyz	Sign via SCEP						
	룢 Queues	Organization Type: PEM T Cancel	Import						
	Files	Unil Export Passphrase: DO NOT SET	Card Reinstall						
	Log	Common Mamou i ca ika2 vua	Card Verify						
	S RADIUS		Set CA Passphrase						
Xo	💥 Tools 🔹 🖻	Subject Alt. Name: DNS : ca.ike2.xyz							
ğ	📰 New Terminal	Key Size: 2048	- Export						
Vir	NetaROUTER	Dave Uslide 2000	Revoke						
~ 0	🅗 Partition	Days Valid: 3050							
ò	Make Supout.rif Trusted								
Ę	Manual								
tou	New WinBox	private key cri authority expired smart card key trusted							
DY_	Evit								

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

type=pem
## Download exported SSL certificates



hikita@tarikin.com



# 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 Mode Config <modeconf vpn.ike2.xyz=""></modeconf>
1. Setting up new IPSec mode config	Name: modeconf vpn.ike2.xyz OK
5 1 5	Responder Cancel
	Address Pool: pool vpn.ike2.xyz 🔻 🔺 Apply
admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	Address:
Session Settings Dashboard	ress Prefix Length: 32
	Solit Include: 192.168.88.0/24
Quick Set	System DNS
Policies Proposals Groups Peers Identities Profiles Remote Peers Mode Configs Installed SAs Keys	Static DNS: 10.0.88.1
i Wireless Find	
Bridge Name 🛆 Resp Address Pool Address Address Prefi Split Include St	iy 🕶
PPP no no	
💬 Switch	
New These Made Config	
Routing Name: modeconi vpn.ike2.xyz OK	/ip ipsec mode-config
Cancel	
Address Pool: pool vpn.ike2.xyz T A Apply	add address-pool="pool
Address: Copy	vpp iko2 vvz" addrocc profiv
Address Prefix Length: 32 Remove	vpniitkezixyz aduress-prerix-
Split Include: 0.0.0.0/0 ♦	<pre>length=32 name="modeconf</pre>
New Terminal	
E MetaROUTER Static DNS: 10.0.88.1	vpn.ike2.xyz" split-
Partition	include-0 0 0 0/0 static
👸 🗋 Make Supout.rif	
📴 😢 Manual	dns=10.0.88.1 system-dns=no
Rew WinBox	

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

e e admin@192.16 Session Settings Dashboard	8.88.1 (MikroTik) - V	VinBox v6.44.3 on mAP lite (	mipsbe)	
Safe Mode Session: 192.168.8	8.1			CPU: 0% 📕 🛅
Auguick Set   CAPSMAN   Im Interfaces   Wireless   Proposals Group   Bridge   Proposals Group   Proposals Group <	New IPsec Profile Name: Hash Algorithms: Encryption Algorithm: DH Group: Proposal Check: Lifebytes: Lifebytes: DPD Interval: DPD Maximum Failures:	grofile vpn.ike2.xyz         sha256       ▼         des       3des         v aes-128       aes-192         > aes-256       blowfish         camellia-128       camellia-192         camellia-126       camellia-192         camellia-126       modp1024         ec2n155       ec2n185         modp1536       modp2048         modp1536       ecp384         ecp521       ecp521         obey       ▼         1d 00:00:00       ▼         I20       ▼ s         5       5	Cancel Apply Copy Remove	s Keys Find oposal C V ey

/ip ipsec profile add dhgroup=modp2048,modp1536,modp10
24 encalgorithm=aes-256,aes-192,aes128 hash-algorithm=sha256
name="profile vpn.ike2.xyz"
nat-traversal=yes proposalcheck=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 exchangemode=ike2 address=0.0.0.0/0 local-address=123.45.67.8 name="peer 123.45.67.8" passive=yes send-initialcontact=yes profile="profile vpn.ike2.xyz"

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

Session Settings Dashb	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	
Safe Mode	Session: 192.168.88.1	CPU: 1% 📕 着
Image: CAPSMAN         Image:	IPsec         Policies       Proposals       Groups       Peers       Identities       Profiles       Remote Peers       Mode Configs         Image: I	Installed SAs Find

/ip ipsec proposal add authalgorithms=sha512,sha256,sha1 enc-algorithms=aes-256cbc,aes-256-ctr,aes-256gcm,aes-192-ctr,aes-192gcm,aes-128-cbc,aes-128ctr,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"

<b>6</b> . Sell	ing up new IPSec polic	cy template
• • • a	dmin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on h&	AP lite (smips)
ession Settings Dashboa	rd	
Safe Mode 🔅	Session: 192.168.88.1	CPU: 2%
🖄 Quick Set		
î CAPSMAN	IPsec	
Interfaces	Policies Proposals Groups Peers Identities Profiles Activ	ve Peers Mode Configs
1 Wireless		Find
32 Bridge	New IPsec Policy	
PPP	0 *T General Action Status	OK
🙄 Switch	Src. Address: 0.0.0.0/0	Cancel
°t\$ Mesh	See Death	
255 IP	Src. Porc:	Арруу
🔀 Routing 🔰	Dst. Address: 10.0.88.0/24	Disable
💮 System 🗈	Dst. Port:	Comment
Queues	Protocol: 255 (all)	T Copy
<b>«¦&gt;</b> Dot1X	V. Template	
Files		
Log	Group: Group vpn.ikez.xyz	
📌 RADIUS	1 item	+
🄀 Tools 🛛 🖻		
🔤 New Terminal		
C 🛄 Make Supout.rif		
😧 Manual		
🕒 New WinBox		Asticus
📃 Exit		Active

 $O_{a}$ 

0



/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

•		adm	in@192.168.88.1 (N	MikroTik) – WinBox v	6.45.2 on	hAP lite (sm	nips)			
sion Settings Dashbo	bard									
Cafe Mode	Session: 192.168.88.1									CPU: 2% 📕 🛅
A Quick Set	IPsec Identity <peer 123<="" th=""><th>3.45.67.8&gt;</th><th></th><th></th><th></th><th>IPsec Identi</th><th>ty <peer 120<="" th=""><th>3.45.67.8&gt;</th><th></th><th></th></peer></th></peer>	3.45.67.8>				IPsec Identi	ty <peer 120<="" th=""><th>3.45.67.8&gt;</th><th></th><th></th></peer>	3.45.67.8>		
Interfaces	Peer:	peer 123.45.	IPsec Identity <peer 12:<="" th=""><th>3.45.67.8&gt;</th><th></th><th></th><th>Peer:</th><th>peer 123.45.67.8</th><th>₹</th><th>ок</th></peer>	3.45.67.8>			Peer:	peer 123.45.67.8	₹	ок
📜 Wireless	Auth. Method:	digital signatu	Peer:	peer 123.45.67.8	Ŧ	ОК	h. Method:	digital signature	₹	Cancel
<b>알综 Bridge</b>	Certificate:	von.ike2.xvz	Auth. Method:	digital signature	Ŧ	Cancel	ertificate:	vpn.ike2.xyz	∓ ≑	Apply
📑 PPP	Domoto Cortificator	Front door @rk					artificato	alex@pcc.ru		Disable
🛫 Switch	Remote Certificate:	roncoorers	Certificate:	vpn.ike2.xyz	∓ \$	Арріу	ler un cace.	alex@risc.ru	•	
ିଅଟି Mesh	Policy Template Group:	group vpn.ike	Remote Certificate:	admin@vpn.ike2.xyz	₹	Disable	ate Group:	group vpn.ike2.xyz	₹	Comment
255 IP 🗅	Notrack Chain:					Comment	ack Chain:		∓	Сору
🎉 Routing 🛛 🖒			Policy Template Group:	group vpn.ike2.xyz	•	Copy	-			Remove
🌐 System 🗈 🕑	My ID Type:	auto	Notrack Chain:		₹	Сору	V ID Type:	auto	₹	
👰 Queues			My ID Type:	auto	Ŧ	Remove	-			
<b>«¦&gt;</b> Dot1X	Remote ID Type:	user fqdn	Hy ID Type.	adto			e ID Type:	user fqdn	₹	
📄 Files	Remote ID:	frontdoor@rk	Remote ID Type:	user fadn	Ŧ		emote ID:	alex@nsc.ru		
📄 Log	Match By:	certificate	Remote ID:	admin@ynn ike2 yyz			Match By:	certificate	∓	
🥵 RADIUS			Neinote ID.						_	
🄀 Tools 🛛 🕑	Mode Configuration:	modeconf vpr	Match By:	certificate	•		riguration:	modecont vpn.ike2.xyz	+ ▲	
📰 New Terminal	Generate Policy:	port strict	Mode Configuration:	modeconf vpn.ike2.xyz	₹ ▲		ate Policy:	port strict	₹	
[ Make Supout.rif	enabled		Generate Policy:	port strict	Ŧ					
😯 Manual			enabled							
🔇 New WinBox										

admi

ficat

rti

Ð

## 7. Carefully assembling IPSec identities for each client

.1 (N	/likroTik) - WinBox v6	.45.2 on	hAP lite (sm	nips)		
						CPU: 2%
			IPsec Identit	:y <peer 12:<="" td=""><td>3.45.67.8&gt;</td><td></td></peer>	3.45.67.8>	
er 123	3.45.67.8>			Peer:	peer 123.45.67.8	ОК
eer:	peer 123.45.67.8	Ŧ	ОК	h. Method:	digital signature 🔻	Cancel
hod:	digital signature	Ŧ	Cancel	ertificate:	vpn.ike2.xyz	Apply
	une the 2 unit		Apply	ertificate:	alex@nsc.ru ₹	Disable
ate:	vpn.ike2.xyz	_ <b>▼</b> ▼	Disable	ate Group	aroup ypp ike? yyz	Comment
ate.	adming vprakezaxyz		Comment	ack Chain:		Сору
oup:	group vpn.ike2.xyz	₹	Copy			Remove
nain:		₹	Remove	y ID Type:	auto	
ype:	auto	₹	Romoro	e ID Type:	user fqdn 🛛 🔻	
				emote ID:	alex@nsc.ru	]
ype:	user fadn			Match By:	certificate	]
e ID:	admin@vpn.ike2.xyz					-
n By:	certificate	₹		figuration:	modeconf vpn.ike2.xyz 🔻 🔺	
tion:	modeconf vpn.ike2.xyz	₹ ▲		ate Policy:	port strict	
olicy:	port strict	₹				

/ip ipsec identity add auth-method=digitalsignature certificate=vpn.ike2.xyz remotecertificate=admin@vpn.ike2.xyz generatepolicy=port-strict match-by=certificate modeconfig="modeconf vpn.ike2.xyz" peer="peer 123.45.67.8" policy-template-group="group vpn.ike2.xyz" remote-id=userfqdn:admin@vpn.ike2.xyz

/ip ipsec identity add auth-method=digitalsignature certificate=vpn.ike2.xyz remotecertificate=alex@nsc.ru generate-policy=port-strict match-by=certificate mode-config="modeconf vpn.ike2.xyz" peer="peer 123.45.67.8" policytemplate-group="group vpn.ike2.xyz" remote-id=userfqdn:alex@nsc.ru

# Setting up Firewall Understanding the default firewall filter



## Empty FIREWALL filter

	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	WAR
gs Dashb	bard	OF
ie Mode	Session: 192.168.88.1 CPU: 1%	
et IN	Firewall OR Raw Service Ports Connections Address Lists Layer? Protocols Action Chain Src. Address Dst. Address Protocol Src. Port Dst. Port In. Int Out. );; special dummy rule to show fasttrack counters O D pas forward EMPTY FIRELWALL = ALLOW ALL OUTPUT	U23.45.67.8/24 NPUT LAN 192.168.88.0/24
	1 item	
nBox		

Accept

Drop

WAN

## RouterOS 6.45+ default configuration firewall overview

Firewall																	×
Filter Rules	5 NAT	Mangle	Raw	Service Po	orts Connec	tions Add	iress Lists	Layer7 Proto	cols								
+ -	Ø 3	8 🖻	7	00 Rese	t Counters	00 Reset	: All Counte	rs							Find	input	Ŧ
# A	ction	Chain	Sre	. Address	Dst. Address	s Protocol	Src. Port	Dst. Port	In. Int	Out. I	In. Int	Out. I	Src. A	Dst. A	Bytes	Packets	•
;;; defcc	onf: acce	ept establis	shed,re	elated, untra	acked												
1 🗳	/acc	input													5.5 MiB	61 567	
;;; defcc	onf: drop	o invalid															
2 🔰	<b>K</b> drop	input													341 B	ť	,
;;; defcc	onf: acce	ept ICMP															
3 💊	/acc	input				1 (icmp)									0 B	(	J
;;; defcc	onf: acce	ept to local	lloopba	ack (for CA	PsMAN)												
4 💊	/acc	input			127.0.0.1										0 B	(	,
;;; defco	onf: drop	o all not co	ming fr	om LAN													
5 👂	尾 drop	input									!LAN				201.2 KiB	1 096	,
5 items out	of 12																
Firewall																	×
Filter Rules	S NAT	Mangle	Raw	Service Po	orts Connec	tions Add	iress Lists	Layer7 Proto	cols								
+ -	2	8 🖻	7	00 Rese	t Counters	00 Reset	: All Counte	rs							Find	forward	Ŧ

÷	-	1	× 🖻 !	T	00 Rese	t Counters	00 Reset	All Counters								Find	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	ŀ
;	;; spe	ecial dumm	y rule to sho	w fas	ttrack cou	nters												
0	D	🗅 pas	forward													190.5 MiB	306 73	3
;	;; def	iconf: acc	ept in ipsec p	olicy														
6		✓acc	forward													0 B	1	0
)	;; def	fconf: acc	ept out ipsec	polic	Y													
7		✓acc	forward													0 B	1	0
)	;; def	iconf: fast	track															
8		Ì≱fas…	forward													8.0 MiB	53 92	0
;	;; def	iconf: acc	ept establishe	ed,re	lated, untr	acked												
9		✓acc	forward													8.0 MiB	53 92	0
;	;; def	iconf: drop	o invalid															
10		X drop	forward													1060.4 KiB	1 893	3
- ;	;; def	iconf: drop	o all from WA	N no	: DSTNATe	:d												
11		💢 drop	forward									WAN				0 B	1	0
7 ite	ems o	ut of 12																

#### #Input Chain Rules

/ip firewall filter

add action=accept chain=input comment="defconf: accept established,related,untracked" connectionstate=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" connectionstate=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





#### INPUT chain

### + UDP 500 + UDP 4500

/ip firewall filter add placebefore=[ find where comment~"defconf: drop all not coming from LAN" ] protocol=udp dstport=500,4500 dstaddress=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)

•	admin@192.	168.88.1 (MikroTik)	- WinBox v6	6.44.3 on	mAP lite (r	nipsbe)	
Settings Dashb	pard						
Safe Mode	Session: 192.168.88	.1					CPU: 1% 📕 🛅
Quick Set		New Firewall Rule					]
CAPsMAN		General Advanced E	xtra Action	Statistics		ОК	
Interfaces	Firewall	Chain:	input		₹	Cancel	
Wireless	Filter Rules NAT	Src. Address:			-	Apply	
Bridge	+ - <b>*</b> ×	Det Address	122 45 67	0			input Ŧ
PPP	# Action C	DSC. Address.	123.43.07	.0		Disable	. Out. I 🔻
Switch	1 vacc ir	Protocol:	ipsec-esp		₹ ▲	Comment	
Mesh	;;; defconf: drop i	Src. Port:			~	Сору	
IP P	;;; defconf: accep	Dst. Port:			-	Remove	
Routing	3 Vacc ir	Any Ports			_	Reset Counters	
System /	4 Xdrop ir	Any, Port.				Recet All Coupters	!LA
Queues	;;; Allow UDP 500,	In. Interface:				Reset Air Counters	
Log	II Geen a	Out. Interface:			•		
RADIUS		In. Interface List:		Comment	for New Firev	vall Rule	
Tools	•	Out. Interface List:		Allow IPS	ec-esp for 12	3.45.67.8	OK
New Terminal	5 items out of 12 (1 s		ļ	1		(	Tancel
MetaROUTER		Packet Mark:				<b>v</b>	
Partition		Connection Mark:			-		
Make Supout.rif		Routing Mark:			-		
Manual		Routing Table:			-		
New WinBox							
Exit		Connection Type:			•		
		Connection State:			•		
		Connection NAT State:			•		
		enabled					

#### INPUT chain

### + IPSec-esp (protocol 50)

/ip firewall filter add placebefore=[ find where comment~"defconf: drop all not coming from LAN" ] protocol=ipsecesp 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**

Safe Mode	Session: 192.	168.88.1							CP	U:
uick Set										
AP <man< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></man<>										
terfaces	Firewall									
icon acco	Filter Rules	Mangle	D and	Service Do	vtc Copped	tions Address L	iche Lavor7	Protocole		
lireless		NAT Mangle	Raw	Der vice PC	ins connec	LIOITS AUDIESS L	ISIS Layer/	Protocols		
ridge	+ - *	' 🗶 🖆	T	00 Rese	t Counters	00 Reset All Co	unters		Find	in
PP	# Actio	n Chain	Src	. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int	0
witch	;;; defconf:	accept establ	ished,rel	lated, untra	acked					
ech	1 🗸 a	cc input								
	;;; derconr:	orop invalid								
P.	::: defconf:	accept ICMP								
outing 🗅	3 🗸 a	cc input				1 (icmp)				
vstem 🗅	;;; defconf:	drop all not co	oming fro	m LAN						
	4 🗙 d	rop input								
ueues	;;; Allow UD	P 500,4500 IF	Sec for 1	123.45.67	.8					
les	11 🗸 a	cc input			123.45.67.8	17 (udp)		500,4500		
a	;;; Allow IP	Sec-esp for 12	3.45.67.	.8	100 45 45 0	F0 (in				
ADTUC	12 Va	cc input			123.45.67.8	50 (ipsec-esp)				
40105										
bols 🗈	•									
ew Terminal	6 items out of	13 (2 selected	)							
		_	-	_	_		_	_		-
CONCILIC										
artition										
ake Supout.rif										
anual										

•	•	•		â	admin	@192	2.168.8	8.1 (	MikroTik)	- WinBox v	6.44	.3 on mAl	P lite (mip	sbe)			
iess	ion	Settings	Dashb	oard													
0	0	Safe M	ode	Sessio	on: 19	2.168.8	88.1								CP	U:1%	•
	Â	Quick Set															
	î	CAPSMAN															
	]	Interfaces		Firewa	all												
	Ĵ	Wireless		Filter	Rules	NAT	Mangle	Raw	Service P	orts Connec	tions	Address Lis	ts Layer7	Protocols			
	5 P P 5	Bridge		4	-	* >	۳	T	00 Rese	et Counters	<b>00</b> F	Reset All Cou	Inters	[	Find	input	Ŧ
	<b>P</b>	PPP		#	Ac	tion	Chain	S	rc. Address	Dst. Addres:	s Prol	tocol	Src. Port	Dst. Port	In. Int	Out. I.	🔻
		Switch			defco	nf: acce	ept establi	shed,i	related, untr	acked							
	°78	Mesh			defcor	nf: drop	input invalid										
	255	IP	$\sim$	2	3	drop	input										
	×	Routing	⊳	3	defcor	nt: acce acc	ept ICMP				1 (ir	rmn)					
	63	System	⊳		Allow	UDP 50	0,4500 IP	Sec fo	r 123.45.67	7.8	- 11						
		Queues		4	0llow	acc	input	2 4 5 6	70	123.45.67.8	17 (	(udp)		500,4500			
	ñ	Files		5	Allow	acc	input	5.45.0	17.0	123.45.67.8	50 (	(ipsec-esp)					
	-	100		- 333	defco	nf: drop	all not co	ming l	from LAN								
1		RADIUS		6		drop	input										!LA
		Tools	Þ														_
õ		Nou Tormin	-1	• 6 item	ns out i	of 13 (2	' selected'	1									•
Ë			а р					, 			_					_	
			.к														
Л		Partition															
2		Make Supou	it.rif														
Ш	4	Manual															
đ	0	New WinBo:	<														

# RouterOS IPSec IKEv2 server ready



# Setting up client RouterOS 🔌

## Upload and install client SSL certificate



🔌 Client

/certificate import filename=cert\_export\_office-01@v pn.ike2.xyz.p12

## Rename installed SSL certificates: CA and client



	🌭 admin@35.247.134.1	47 (office-01) - WinBox v6.45.6 on CHR (x86_64)	
	Session Settings Dashbo	pard	
	Safe Mode	Session: 35.247.134.147	<b>a</b>
.147 (office-01) - WinBox v6.45.6 on CHR (x86_64) nboard	📕 🔏 Quick Set		
Session: 35.247.134.147	Interfaces	Certificates	
	Se Bridge	Certificates SCEP Servers SCEP RA Requests OTP CRL	
Certificates SCEP Servers SCEP RA Requests OTP CRL	🚅 PPP	🛉 🗕 🍸 Import Card Reinstall Card Verify Revoke Create Cert. Request	Settings
💠 🗕 🍸 Import Card Reinstall Card Verify Revoke C	ିଅଟି Mesh	Name 🛆 Issuer Common Name	Subject Alt. 💌
Name 🛆 Issuer Co	😇 IP 🛛 🖻	AT ca.ike2.xyz C=RU,ST=Mosco ca.ike2.xyz	DNS:ca.ike2.xy
KT cert_export_office-01@vpn.ike2.xyz.p1 C=RU,ST=Moscow 0 offi AT cert_export_office-01@vpn.ike2.xyz.p1 C=RU,ST=Moscow 0 ca	🥰 Routing 🛛 🗅	K1 office-U1@vpn.ike2.xyz U=HU,S1=Mosco office-U1@vpn.ike2.xyz	Email:office-UT(
	∰ System D		I
Import	S Queues		I
Only File: cert_export_office-01@vpn.ike2.xyz.p12   Baconkrace: ####################################	Files		I
	E Log		
	🔀 🧟 RADIUS		I
	🔏 🎇 Tools 🔹 🗅		I
2 items (1 selected)	듣 🔤 New Terminal		I
	Not1X		
	🔘 ] Make Supout.rif	2 items (2 selected)	
	🤠 😯 Manual		
	🗟 🕓 New WinBox		

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



•	• •	admin@192.16	8.88.1 (MikroTik) - V	VinBox v6.44.3 on mAP lite (	mipsbe)	
Ses	sion Settings Dashbo	pard				
ю	Cafe Mode	Session: 192.168.8	8.1			CPU: 0% 📕 🕯
Sox 5	Safe Mode       Interfaces       CAPSMAN       Interfaces       Wireless       Bridge       PPP       Switch       Bridge       PP       Switch       Routing       Piles       Itel       Files       Log       RADIUS       Tools       New Terminal	Session: 192.168.8	8.1 New IPsec Profile Name: Hash Algorithms: Encryption Algorithm: DH Group: Proposal Check: Lifetime: Lifetytes:	yrofile vpn.ike2.xyz         sha256       ▼         des       3des         v aes-128       aes-192         aes-256       blowfish         camellia-128       camellia-192         camellia-128       camellia-192         camellia-256       modp768       modp1024         ec2n155       ec2n185       ✓         modp1536       modp2048       modp4096         modp6144       modp8192       ecp521         obey       ▼       ▼         1d 00:00:00       ▼       ▼	Cancel Apply Copy Remove	CPU: 0%
Wi	HetaROUTER	1 item		✓ NAT Traversal		
0S	Make Supout.rif		DPD Interval:	120 🔻 s		
ter	😲 Manual		DPD Maximum Failures:	5		
ou	Sew WinBox					

/ip ipsec profile add dhgroup=modp2048,modp1536,modp10
24 encalgorithm=aes-256,aes-192,aes128 hash-algorithm=sha256
name="profile vpn.ike2.xyz"
nat-traversal=yes proposalcheck=obey

## Adding new client IPSec peer (initiator)





/ip ipsec peer
add address=vpn.ike2.xyz exchangemode=ike2 name="peer vpn.ike2.xyz"
profile="profile vpn.ike2.xyz"

profile="profile vpn.ike2.xyz"

## Setting up new IPSec proposal (phase 2)



admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)         Session       Settings         Session       Session:         Interfaces       CPU: 1%         Wireless       Policies         Proposals       Groups         Person       Find         Name       Proposal         Name       Proposal         Name       Proposal         Name       Proposal         Name       Name:         Name       Proposal         Name       Name:         Name       Name:         Name       Name:         Name       Name:         Name       Statistics         Pidefault       Name:         Name       Statistics         Name       Statistics         Name       Statistics         Pidefault       Name:         Name       Statistics         System       System         Queues       Camella-128         Log       Item         Log       Log         New Terminal       PFS Group:         PFS Group:       Name         PFS Group:       Name			
Session       Safe Mode       Session: 192.168.88.1       CPU: 1% <ul> <li>Quick Set</li> <li>Quick Set</li> <li>CAPSMAN</li> <li>Ploicies</li> <li>Proposals</li> <li>Groups</li> <li>Perce</li> <li>Verieless</li> <li>Wireless</li> <li>Wireless</li></ul>		admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	
Safe Mode       Session: 192.168.88.1         Quick Set       Quick Set         CAPsMAN       Policis         Policis       Proposals         Groups       Peers         Minister       Peers         Wireless       Policis         Wireless       Peers         Wireless       Peers         Name       Proposal         Very       Statistics         Pill       Peers         Peers       Name         Proposal       Person         Wireless       Peers         Wireless       Peers         Peers       Name         Proposal       Person         Name       Proposal         Peers       Name         Proposal       Person         Name       Proposal         Proposal       Person         Name       Proposal         Pass       Person         Switch       Person         Person       Person         Person       Person         Person       Person         Person       Person         Person       Person         Person       Person<	Session Settings Dashbo	bard	
Quick Set       IPsec         CAPSMAN       Policies         Policies       Proposals         Groups       Peers         Interfaces       Image: Statistics         Image: Wireless       Image: Statistics         Image: Switch       Image: Smitch         Image: System       Image: Smitch         Image: Switch       Image: Smitch     <	🔊 🍳 🛛 Safe Mode	Session: 192.168.88.1	CPU: 1% 📕 🛅
	Quick Set         CAPSMAN         Im Interfaces         Wireless         Bridge         PPP         Switch         Bridge         PP         System         Piles         I.og         RADIUS         New Terminal         Partition         Make Supout.rif         Manual         New WinBox	IPsec         Policies       Proposals       Groups       Peers       Identities       Profiles       Remote Peers       Mode Configs         Image:       Image: <t< th=""><th>Installed SAs Find</th></t<>	Installed SAs Find

/ip ipsec proposal add authalgorithms=sha512,sha256,sha1 enc-algorithms=aes-256cbc,aes-256-ctr,aes-256gcm,aes-192-ctr,aes-192gcm,aes-128-cbc,aes-128ctr,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

34.1	47 (office-01)	- WinBox v6.4	5.6 on CHR (x86	_64)			
ashbi	oard						
le	Session: 35.24	7.134.147					🔳 🛅
	IPsec						
	Policies Prop	osals Groups	Peers Identities	Profiles	Active Peer	s Mode Config	gs
	+ - •	• 🗙 🗖	T Statistics				Find
	# P	eer	Tunnel Src. Ad	dress	Ste J	Port Dist. Addres	s 🔻
	0 *T		::/0	0/24		::/0	
			1 10.0.00			0.0.0.0/0	
$\triangleright$		IPsec Policy <1	0.0.89.0724:0->0.0	.0.0/0:0>			
Þ		General Acti	ion Status			OK	
		Src. Address:	10.0.88.0/24			Cancel	
		Src. Port:				Apply	
		Dist. Address:	0.0.0/0			Disable	
Þ		Dist. Port:			<b>▼</b>	Comment	
		Protocol:	255 (all)		₹	Сору	
~	•		Template			Remove	•
rit	2 items (1 selec	Group:	group vpn.ike2.xy	z	₹		
		enabled	Template		Active		

New IPse	c Policy					
General	Action	Status				ОК
	Action:	encrypt			₹	Cancel
IPsec Pro	otocols:	esp			₹	Apply
Pr	roposal:	proposal	l vpn.ike2.xyz		₹	Disable
						Comment
						Сору
						Remove
enabled		Т	femplate	4	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

src-address=iv.v.88.v/24 temptate=yes

## Carefully assembling client's IPSec identity

247.134.1	47 (offi	ice-01) - WinBox v6.45	5.6 on CHR (x86_64)		<u>_                                    </u>
gs Dashb	oard				
e Mode	Sessio	on: 35.247.134.147	<b>a</b>		
et	IPsec	IPsec Identity <peer th="" vpn.<=""><th>ike2.xyz&gt;</th><th></th><th></th></peer>	ike2.xyz>		
es	Group	Peer:	peer vpn.ike2.xyz	OK	Keys
	+	Auth, Method:	digital signature	Cancel	Find
	# 0	Certificate:	office-01@vpn.ike2.xyz 🔻 🜩	Apply	Mode Configur 🔻
Þ		Remote Certificate:	none	Disable	
↑ ↑		Policy Template Group:	group vpn.ike2.xyz	Comment	
		Notrack Chain:	<b>•</b>	Сору	
		My ID Type:	user fqdn 🗸 🗸	Remove	
		My ID:	office-01@vpn.ike2.xyz	]	
Þ		Remote ID Type:	fqdn 두	]	
rminal		Remote ID:	vpn.ike2.xyz	]	
upout rif	•	Match By:	remote id 두	]	•
ap out in	1 item	Mode Configuration:	request-only ∓ 🔺		
nBox		Generate Policy:	port strict	]	



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

### id=fqdn:vpn.ike2.xyz

dLonb= dLonbNikita Tarikin / nikita@tarikin.com

### Cross-check IPSec identity (example)





IPsec Identity <peer 123.45.67.8=""></peer>			IPsec Identity <	peer vpn.ike2.xyz>		
Peer: peer 123.45.67.8	<b>T</b>	ок		Peer: peer vpn.ike2.xyz	Ŧ	ОК
Auth. Method: digital signature	₹ Ca	ancel	Auth. N	Method: digital signature	₹	Cancel
Certificate: vpn.ike2.xyz	<b>₹</b> \$ A	pply	Cert	tificate: office-spb@vpn.ike2.xyz	∓ \$	Apply
Remote Certificate: office-spb@vpn.ike2.x	yz 🗧 🛡 Dis	able	Remote Cert	tificate: none	₹	Disable
Policy Template Group: group vpn.ike2.xyz	Ţ Con	nment	Policy Template	Group: group vpn.ike2.xyz	Ŧ	Comment
Notrack Chain:	₹ C	ору	Notrack	k Chain:	₹	Сору
Multo Turan Cada	Rer	move		D Turpou lucor fodo	Ξ	Remove
My ID Type: rgan My ID: vpn.ike2.xyz				My ID: office-spb@vpn.ike2.xyz		
Remote ID Type: user fqdn	Ŧ	$\land$	Remote II	D Type: fqdn	₹	
Remote ID: office-spb@vpn.ike2.x	yz 🚽		Rem	note ID: vpn.ike2.xyz		
Match By: certificate	₹		Ma	atch By: remote id	₹	
Mode Configuration: modeconf vpn.ike2.xyz	2 ∓ 🔺		Mode Configu	uration: modeconf office-spb@vp	n.ike2.xyz ∓ 🔺	
Generate Policy: port strict	Ŧ		Generate	e Policy: port strict	₹	
enabled			enabled			

## Testing the IKEv2 connectivity

🔌 Client

Active peers state: established



Dynamic Active (DA)							
IPSec policy							
generated from							
Template ( <b>T</b> )							
PH2 state:							
established							

Peer: authorized Address: acquired

I	Psec													J×
	Policies	Proposals	Groups	Peers	Identities	Profiles	Active Peers	Mode Configs	Installed SAs	Keys				
	+ -		1	7	Statistics								Find	
	#	Peer		Tunr	nel Src. Add	lress	Src. P.,	. Dst. Address	Dst.	P Protoc	ol 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 vp	n.ike2.xy	z yes	10.0.88	.254		0.0.0.0/0		255 (	all) encrypt	unique	established	Ŀ

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



Sadmin@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	IPsec		IP address	10.0.88.254
Interfaces	Policies Proposals Groups Peers Identities Profiles Active Peers Mode C	onfigs	Interface	ether1
😹 Bridge	🗣 💳 🛷 🖄 🖅 Statistics	Find		
🚅 PPP	# Peer Tunnel Src. Address Src. Port Dst. Ad	dress		
ଂଅଟ୍ର Mesh	0 *T ::/0 ::/0			
E IP	1 T 10.0.88.0/24 0.0.0.0 2 DA peer vpn.ike2.xyz ves 10.0.88.254 0.0.0.0	/0		
💦 🔀 Routing 🛛 🗈				
🎲 System 🗈	Address List			
🙊 Queues	🕂 🗕 🖉 🖾 🔽 🛛 🖌 Find			
📄 Files	Address 🔺 Network Interface 🔻			
E Log	D 守10.0.88.254 10.0.88.254 ether1 D 令10.148.0.7 10.148.0.1 ether1			
🔀 🥵 RADIUS	🖶 192.168.199.1/24 192.168.199.0 bridge			
🔓 🎇 Tools 🔹 🗅				
🚝 🔚 New Terminal				
Not1X				
🁸 🗋 Make Supout.rif	3 items     3 items	•		
🧑 😯 Manual				
🗟 🔘 New WinBox				


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





#### OSPF works

No TCP MSS issues

Easy to configure and understand

Routable

Has interface

# Option 1 (easy)

Decreased MTU due to extra encapsulation overhead

Takes longer to connect and reconnect







# Create new ipsec modeconf with static IP address

7.15.122	(office-main ypn.	ike2.xyz) - WinBox v	6.45.6 on CHR	(x86_64)		
s Dashbo	pard					
e Mode	Session: 34.87.15.	122				🗖 🖻
et						
s	IPsec					
	Peers Identities	Profiles Active Peers	Mode Configs	Installed SAs	Keys	
	+ - 7				F	ind
<u> </u>	Name modecopf office	IPsec Mode Config <m< th=""><th>odeconf office-01</th><th>@vpn.ike2.xyz;</th><th></th><th></th></m<>	odeconf office-01	@vpn.ike2.xyz;		
	modeconf office- modeconf vpn.ik	Name:	modeconf offic	e-01@vpn.ike2	.xyz	ОК
▶	* request-only		Responder			Cancel
		Address Pool:			•	Apply
		Address	10.0.88.3		<b></b>	Сору
		Split Include:	0.0.0/0		\$	Remove
Þ			System DNS	i		
minal		Static DNS:			<u></u>	
ipout.rif	4 A items (1 selected)					
					_	
вох						

10.0.88.3

/ip ipsec add

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

# Select new ipsec static modeconf for the client identity



Server

# Reconnect ipsec peer and check new static IP address



Client

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







# 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)	admin@34.87.15.122 (office-main) - WinBox (64bit) v6.45.6 on CHR (x86_64)
n Settings Dashb	pard	Session Settings Dashboard
Cafe Mode	Session: 35.247.134.147	Safe Mode Session: 34.87.15.122
Quick Set  Interfaces Bridge Bridge PPP Mesh SPP Routing System Queues Files Log RADIUS RADIUS New Terminal Dot1X Make Supout.rif Manual New WinBox Exit	Address <10.1.1.3>         Address:       10.1.1.3         Address:       10.1.1.1         Cancel         Interface:       ipip-main-office         Address:       192.168.88.0/24>         General       Attributes         Ok       Ok         Dst. Address:       192.168.88.0/24         Gateway:       10.1.1.1         Gateway:       10.1.1.1         Type:       unicast         Obstance:       1         Scope:       30         Target Scope:       10         Routing Mark:	Y   Y   Y   Y   Y   Y   Y   Y   Y   Y     Y   Y     Y   Y          Y     Y     Y     Y     Y     Y     Y     Y     Y     Y     Y     Y     Y     Y     Y



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

😋 🛛 Safe Mode	Session: 35.	.247.134.147	
Quick Set       Im Interfaces       Bridge       PPP       % Mesh       IP       IP       X       Routing	Address Lis	st       Interface List         iss       △ Network       Interface       Interface       Interface List       Ethernet       EoIP Tunnel       IP Tunnel       GRE Tunnel          10.0.88.3       10.0.88.3       ether1       Image: Constraint of the state of the	ind
Queues Include Log		Route List Routes Nexthops Rules VRF	
ARDIUS       Tools       New Terminal       Image: Contract of the second	4 items (1	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           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	
Make Supout.rif		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	lms					
192.168.88.1	56	64	Oms	Sederin Reddine maint a minur 100 100 1		- 10		
192.168.88.1	56	64	Oms	[admin@office-main] > ping 192.168.1	.99.1 src-addres	8=19.	2.168. <b>mm</b>	88.1
192.168.88.1	56	64	Oms	SEQ HUST	SIZE	TTL	TIME	STAT
192.168.88.1	56	64	Oms	0 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	1 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	2 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	3 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	4 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	5 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	6 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	7 192.168.199.1	56	64	Oms	
ent=12 received=12 packet-loss=0% min-ri	tt=Oms	avg-i	rtt=Om	з 8 192.168.199.1	56	64	Oms	
x-rtt=1ms					; min-rtt=Oms av	g-rt	t=Oms	max-r





No MTU overhead -> performs faster

Connects and reconnects much faster

Much more **stable**, less reconnects

# **Option 2 (advanced)**

# 100% policy based ipsec ike2

OSPF <del>works</del>

Harder to configure and understand

Has no routable interface

Need to adjust TCP MSS manually





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

Nikita Tarikin / nikita@tarikin.com



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

<pre>htc=main vpn.ikc2.xyz) - Winitiox v6.45.6 on CHR (xdt6_64)</pre>		New IPsec Policy		
secon: 34.87.15.122	fice-main vpn.ike2.xyz) - WinBox v6.45.6 on CHR (x86_64)		Status	ОК
ession: <u>348715122</u>		Action:	encrypt 💌	Cancel
boold process (process) (p	ssion: 34.87.15.122	tocols:	esp	Apply 192.168.88.0/24
c       initial Proposals       Groups       Peers       Identities       Profiles       Action       Status       initial       initial       Status       initial       initial       Status       initial       initia       initial       initial		oposal:	proposal vpn.ike2.xyz	Disable
<pre>kitics Proposals Groups Peers Identitie Profiles Active Peers Mode Confige Installed SAs Keys General Action Status General Composition Status General Action Status General Composition Status General General Composition Status General Composition Status</pre>	ec			Comment
Find Find Centeral Action Status          Image: General Action Status       Image: Cancel Concel	Dicies Proposals Groups Peers Identities Profiles Active Peers Mode Co	onfigs Installed SAs Keys		Сору
General Action Status       OK       st. Address:       Dzt. Port       192.168.199.0/24         Stc. Address:       192.168.199.0/24       0.88.0/24       255 [         Dst. Address:       192.168.199.0/24       0.88.23       255 [         Dst. Address:       192.168.199.0/24       0.88.23       255 [         Dst. Address:       192.168.199.0/24       0.88.23       255 [         Dst. Address:       192.168.199.0/24       0.88.253       255 [         Dst. Port       Comment for IPsec Policy (192.168.88.0/240-5192)       Image: Comment for IPsec Policy         Protocodt       255 [all]       Policy template for group vpn ike2.xyz       0K         Group:       group vpn.ike2.xyz       0K       Cancel         Group:       group vpn.ike2.xyz       0K       add ress=192.168.88.0/24       proposal="proposal="proposal="proposal="proposal vpn.ike2.xyz"         ee enabled       Template       Octive       Image: comment for IPsec Policy       Image: comment for IPsec Policy	IPsec Policy <192.168.88.0/24:0->192.168.199.0/24:0>	Find		
stc. Address: 192168 88.0/24 Stc. Port Dst. Address: 132168 193.0/24 Dst. Address: 132168 193.0/24 Dst. Address: 132168 193.0/24 Dst. Port Protocot 255 (all) Template Group. group vpn.ike2.xyz remember enabled Template Poly template for group vpn.ike2.xyz Cancel Group. group vpn.ike2.xyz Cancel	General Action Status OK Ist. Add	dress Dst. Port Proto 💌		192,168,199,0/24
Src. Port Apply 0.88.0/24 255 ( Dst. Address: 192.168.199.0/24 Comment for IPsec Policy <192.168.88.0/24:0.3192 X add peer="peer vpn.ike2.xyz" src- 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	);; Src. Address: 192.168.88.0/24 Cancel	200 [		
<pre> Jost Address: 192.168.199.0/24 Jost Port Dote: 255 (all) Dote: 255 (all)</pre>	1 Src. Port	.0/24 255 (		
Jost. Port       Comment for IPsec Policy <192 168 88.0/24:0>192       Image: Comment for IPsec	2 0.0.00 3 Dst. Address: 192.168.199.0/24 0.0.88.	.253 255 (		_
Protocol 255 (all) Protocol 255 (all) Template Group: group vpn.ike2.xyz Protocol: 255 (all) Template Group: group vpn.ike2.xyz Protocol: 255 (all) Template Group: group vpn.ike2.xyz Protocol: 255 (all) Template Group: group vpn.ike2.xyz Protocol: 255 (all) Active	4 Dst. Port Comment for IPsec Policy <	192.168.88.0/24:0->192 🗖 🗙	/ip ipsec pc	olicy
address=192.168.199.0/24 dst- address=192.168.88.0/24 proposal="pro posal vpn.ike2.xyz" tunnel=yes level= unique	Protocol: 255 (all)	on.ike2.xyz 🔼 OK	add peer="pe	eer vpn.ike2.xyz" src-
Image: Template       Image: Group: group vpn.ike2.xyz       Image: Group: group vpn.ike2.xyz       Image: Group: Group vpn.ike2.xyz       Image: Group vpn.ike2.xyz	6 [site-to-site]	Cancel	address=192.	168.199.0/24 dst-
Group: group vpn.ike2.xyz enabled Template Active Template Active Template Active Template Active Template Active Template Active Template Active Template Tem	7 Template		address=102	168 88 0/24  proposal="pro
enabled Template Active	Group: group vpn.ike2.xyz			
er enabled Template Active unique			posal vpn.ik	<pre>kez.xyz* tunnel=yes level=</pre>
	enabled Template Active		unique	



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

			IPsec Po	<u>licy</u> <192	192.168.199.0/24:0->192.168.88.0/24:0>
7.134.1	47 (office-C	01) - WinBox v6.45.6 on CHR (x86_64)	>		tion Status
Dashbo	bard				
Mode	Session: 3	5.247.134.147	🔳 🔂	ction:	on: encrypt Cancel
				evel:	vel: unique F Apply
	IFSEC			peols:	ols: esp 💿 🐨 Disable 192 168 199 0/24
	Policies	Proposals Groups Peers Identities Profiles Active F	eers Mode Configs	posal:	sat proposal vpn.ike2.xyz
	+ -	🖉 💥 🖾 🍸 Statistics	Find		
	#	New IPsec Policy	dress 🔻		
	0 *T	General Action Status	ОК		102 169 00 0/24
1	2 DA	Peer: peer vpn.ike2.xyz	Cancel 10		192.100.00.0/24
			Applu		
		Stc. Address: 192168199.0/24			
			Disable		(in income nolice)
		Src. Port:	Comment		/ip ipsec policy
		Dst. Address: 192.168.88.0/24			<pre>add peer="peer vpn.ike2.xyz" src-</pre>
		Dst. Port:			address=192.168.199.0/24 dst-
$\triangleright$		Protocol: 255 (all)	Remove		$addross = 102$ 160 00 $\alpha/24$ tuppel = vos
inal					auuress-192.100.00.0/24 tunnet-yes
		Template			<pre>proposal="proposal vpn.ike2.xyz"</pre>
iout.rif	•		•		
	3 items	enabled Template Active			
lox					

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





s Dashboard	
Mode Session: 35.247.134.147	
Immode       Session       Session	Image: Keys         Find         Image: Find         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (         255 (

		, , , , , , , , , , , , , , , , , , , ,							
ettings Dashb	oard				Mode	Session: 34.87.15.12	22		<b>a</b>
Safe Mode	Session: 3	35.247.134.147		🔳 🛅			-		
uick Set	IPsec					IPsec			
erfaces	Policies	Proposals Groups Peers Identities Profiles	Active Peers Mode C	Configs		Policies Proposals	IPsec Policy <192168 88 0/24:0->192168 199 0/24:0-		stalled SAs Keys
idge op	+ -	🗸 💥 🖾 🍸 Statistics		Find		+ - 🖉 🐹	General Action Status	ОК	Find
esh	# 0 *T	General Action Status		dress 🔻		# Peer	Src. Address: 192.168.88.0/24	Сору	Dst. Port Proto
4	1 T 2 DA	Peer: peer vpn.ike2.xyz	■      Cancel		Þ	;;; Policy template	Src. Port	Remove	255 (
outing D		Tunnel	Annly			2 DA peer 34	Dst. Address: 192.168.199.0/24		255 (
istem D		Src. Address: 192.168.199.0/24				3 DA peer 34	Dst. Port:		255 (
leues		Src. Port	■ Disable			4 T	Protocol: 255 (all)		255 (
es		Dat Address: 192 168 88 0/24	Comment			;;; Policy template			255 (
		Dat Date	Сору			;;; Policy template	L I emplate		200 [
ADIUS			Remove		$\sim$	6 T Z Dó Deer 34			) 255 ( 255 (
uu Torminal		Protocot: 255 (all)			ninal				200 [
switenninar st1V		Template				<b>4</b>	dynamic enabled Template Ac	tive	•
ake Supout.rif	•			•	out.rif	8 items (1 selected)	<u> </u>		· · · · · · · · · · · · · · · · · · ·
anual	3 items	enabled Template	Active			-			
ew WinBox				J	вох				





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

Colo Mada	Consider DE (	247 124 147							-
Sare Mode	Session: 35.2	247.134.147							_
🔏 Quick Set	Address List			Interface	List				
🔚 Interfaces				Interfac	e Interface	lict Ethernet	FoID Turpel ID Turpe	cDE Turnel	
😹 Bridge			Find						
📑 PPP	Addres	s 🛆 Network	Interface	- ++	- 🗸 🗙		Detect Internet		Find
°t¦s Mesh	X 10.0	1.1.3 10.1.1.1	ipip-main-office	Nar	ne	∆ Type	Actual MT	TU L2 MTU 1	x 🔻
255 TP	D 🕆 10.1	148.0.7 10.148.0	.1 ether1	R 11	bridge otbor1	Bridge	1	500 65535	
Routing	宁192	.168.199.1/24 192.168.3	199.0 bridge	X 🔶	ipip-main-offic	e IP Tunnel	1	386 65535	
Curtury N									1
System /		Route List							4
🕎 Queues		Routes Nexthops Rules	VRF						
Files		4 <b>- / x -</b>	T				Find		
							- rerve		
E Log			( Catoway		Distance	Routing Mark	Drof. Source		
📃 Log		Dst. Address	△ Gateway 10.148.0.1 reachable eth	er1	Distance	Routing Mark	Pref. Source		
Log RADIUS Y Tools		Dst. Address           DAS         ▶ 0.0.0.0/0           DAC         ▶ 10.0.88.3	▲ Gateway 10.148.0.1 reachable eth ether1 reachable	er1	Distance	Routing Mark	Pref. Source	<b>▼</b>	
E Log		Dst. Address           DAS         0.0.0.0/0           DAC         10.0.88.3           DAC         10.148.0.1	▲ Gateway 10.148.0.1 reachable eth ether1 reachable ether1 reachable	er 1	Distance	Routing Mark	Pref. Source 10.0.88.3 10.148.0.7	· · · · · · · · · · · · · · · · · · ·	
Log ARADIUS Cools New Terminal	4 items (1	Dst. Address           DAS         0.0.0.0/0           DAC         10.0.88.3           DAC         10.148.0.1           VS         192.168.88.0/24           DAC         192.168.99.0/2	Gateway     10.148.0.1 reachable eth     ether1 reachable     ether1 reachable     10.1.1.1     bridge reachable	ler1	Distance	Routing Mark	Pref. Source 10.0.88.3 10.148.0.7		
Log ARADIUS Tools New Terminal Dot1X	4 items (1	Dst. Address           DAS         0.0.0.0/0           DAC         10.0.88.3           DAC         10.148.0.1           XS         192.168.88.0/24           DAC         192.168.199.0/24	Gateway     10.148.0.1 reachable eth     ether1 reachable     ether1 reachable     10.1.1.1     bridge reachable	er1	Distance	Routing Mark	Pref. Source 10.0.88.3 10.148.0.7 192.168.199.1		
Log       ADIUS       Tools       New Terminal       ◆ Dot1X       Make Supout.rif	4 items (1	Dst. Address           DAS         ▶ 0.0.0.0/0           DAC         ▶ 10.0.88.3           DAC         ▶ 10.148.0.1           XS         ▶ 192.168.88.0/24           DAC         ▶ 192.168.199.0/2*	Gateway     10.148.0.1 reachable eth     ether1 reachable     ether1 reachable     10.1.1.1     bridge reachable	er1	Distance	Routing Mark	Pref. Source 10.0.88.3 10.148.0.7 192.168.199.1		-
Log       ADIUS       Tools       New Terminal       → Dot1X       Make Supout.rif       Anual	4 items (1	Dst. Address           DAS         ▶ 0.0.0.0/0           DAC         ▶ 10.0.88.3           DAC         ▶ 10.148.0.1           XS         ▶ 192.168.88.0/24           DAC         ▶ 192.168.199.0/24	Gateway     10.148.0.1 reachable eth     ether1 reachable     ether1 reachable     10.1.1.1     bridge reachable	er1	Distance	Routing Mark	Pref. Source 10.0.88.3 10.148.0.7 192.168.199.1		•



## 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 Dashbo	pard	
い 🖓 🛛 Safe Mode	Session: 35.247.134.147	
Quick Set  Im Interfaces  Redge  PPP  Set Mesh  Set PP  Set Routing  System  Set System Set System  Set System  Set System  Set System Set System Set System Set System Set System Set System Set System Set System Set System Set System	Dession jobe minimized         IPsec         Policies       Proposals       Groups       Peers       Identities       Profiles       Active Peers       Mode Configs       Installed SAs       Keys         Image: Proposals       Groups       Peers       Identities       Profiles       Active Peers       Mode Configs       Installed SAs       Keys         Image: Proposals       Groups       Peers       Identities       Profiles       Active Peers       Dst. Address       Dst. P       Prot       Action       Level       PH2 State       Image: Profiles         Image: Proposals       Src. Address       Src. P       Dst. Address       Dst. P       Prot       Action       Level       PH2 State       Image: Profiles         Image: Profiles       Src. Address       Src. P       Dst. Address       Dst. P       Prot       Action       Level       PH2 State       Image: PH2 State         Image: Peer       Tunnel       Src. Address       Src. P       Dst. Address       Dst. P       Prot       Action       Level       PH2 State       Image: PH2 State         Image: Profiles       Src. Address       Src. P       Dst. Address       Dst. P       Prot       Action	
Queues  Files  Cog  Amount And Content of the second of t	Routes         Nexthops         Rules         VRF         Terminal           Image: Construction of the state of th	•



## 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)									
Sess	sion Settings Dashb										
ø	😋 🛛 Safe Mode	ession: 35.247.134.147									
	http://www.com/com/com/com/com/com/com/com/com/com/										
	Interfaces	viicies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys									
	Sridge	Find									
	📑 PPP	Peer Tunnel Src. Address Src. P Dst. Address Dst. P Prot Action Level PH2 State 🔽									
	°t¦e Mesh	0 *T ::/0 ::/0 255 encrypt									
	🐺 IP 🔹 🕨	2 DA peer vpn.ike2.xyz yes 10.0.88.3 0.0.0.0/0 255 encrypt unique established									
	🎉 Routing 💦 👌	3 A peer vpn.ike2.xyz yes 192.168.199.0/24 192.168.88.0/24 255 encrypt unique established									
	🎲 System 👘 🗅	Route List									
	룢 Queues	Routes Neutres Dulas VDE	IX.								
	📄 Files	8 192.168.88.1 timeout									
	E Log	9 192.168.88.1 timeout									
$\times$	🧟 RADIUS	Dst. Address 🛆 Gateway Distance									
8	🛫 💥 Tools 🔹 🗅	DAS ▶ 0.0.0.00 10.148.0.1 reachable ether1 1 [admin@office=01] > ping 192.168.88.1 src=address=192.168.199.1									
1	New Terminal	DAC ▶10.148.0.1 ether1 reachable 0 0.192.168.68.1 56.64 lms									
$\geq$	dia Dot1X	X5 ▶ 192.168.88.0/24 10.1.1.1 1 1 192.168.88.1 56 64 0ms									
S	Maka Supaut vit	DAC         P 192,168,199,0/24         Druge reachable         0         2 192,168,88,1         56         64 0ms           2         192,168,09,0/24         56         64 0ms         56         64 0ms									
2		$\begin{array}{cccccccccccccccccccccccccccccccccccc$									
Ę	🥶 Manual		•								
б	Sew WinBox	5 items (1 selected)									

### 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	lms					
192.168.88.1	56	64	Oms	Federic Reference in 1 a minur 100, 100	100 1	- 10	0 1/0	
192.168.88.1	56	64	Oms	[admingorrice-main] > ping 192.168	.199.1 src-addres	8=19	2.100.	00.1
192.168.88.1	56	64	Oms	SEQ HUST	SIZE	TTL	TIME	STAT
192.168.88.1	56	64	Oms	0 192.168.199.1	56	5 64	Oms	
192.168.88.1	56	64	Oms	1 192.168.199.1	56	5 64	Oms	
192.168.88.1	56	64	Oms	2 192.168.199.1	56	5 64	Oms	
192.168.88.1	56	64	Oms	3 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	4 192.168.199.1	56	5 64	Oms	
192.168.88.1	56	64	Oms	5 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	6 192.168.199.1	56	64	Oms	
192.168.88.1	56	64	Oms	7 192.168.199.1	$5\epsilon$	64	Oms	
ent=12 received=12 packet-loss=0% min-rtt	=0ms	avo-:	rtt=Om	a 8 192.168.199.1	$5\epsilon$	64	Oms	
<pre></pre>				sent=9 received=9 packet-loss=	0% min-rtt=Oms av	g-rt	t=Oms	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)

ttings Dashboard			angle Rule <192.168.199.0/24->192.168.88.0/24>			
Safe Mode	Session: 34.87.15.122	📕 🛅	Seneral Advanced Extra Action Statistics	ОК	ngle Rule <192.168.88.0/24->192.168.199.0/24>	
ck Set	Mangle Rule <192.168.88.0/24->192.168.199.0/24>		Src. Address List:	Cancel	neral Advanced Extra Action Statistics	ок
erfaces	General Advanced Extra Action Statistics	ОК	Dst. Address List:	Apply	Action: change MSS	Cancel
ge	Chain: forward	Cancel	Layer7 Protocol:	Disable		Apply
	Src. Address: 192.168.88.0/24	Apply	Content:	Comment	Log Prefix:	Disable
ih N	Dst. Address: 192.168.199.0/24	Dicable	Connection Bytes:	Сору		Console
itina 🕑		Commont	Connection Rate:	Remove Reset Counters	New TCP MSS: 1360	Commenc
tem D	Protocol: 6 (tcp)	Continent	Per Connection Classifier:	Reset All Counters	Passthrough	Сору
eues	Src. Port:	Сору	Src. MAC Address:			
5	Dst. Port:	Remove	Out. Bridge Port:			
	Any. Port:	eset Counters	In. Bridge Port:			
DIUS	In. Interface:	set All Counters	In. Bridge Port List:			
IS /	Out. Interface:		Out. Bridge Port List:	/ip	o firewall mangle ad	d action=change-
1X	In. Interface List:		IDrac Policy: in E. Lincar, E. A	mee	chain-forward new-	mcc-1360 crc-
e Supout.rif	Out. Interface List:		TLS Host:	11155		
nual				ado	lress=192.168.88.0/2	4 dst-
v WinBox	Packet Mark:		Ingress Priority:	ado	ress=192.168.199.0/	24 protocol=tcp
	Connection Mark:		DSCP (TOS):	0.0	flage_ovp_top_mag_l	$\begin{array}{c} 1260 \\ 12$
	Routing Mark:		TCP M55: 1 0-1360	cp-	-itags=syn tcp=mss=:	0-1300 lpsec-
	Routing Table:		Packet Size:	pol	licy=in,ipsec passth	rough=yes commen
	Connection Type:		Random:	="1	KF2: Clamp TCP_MSS	from office-
	Connection State:		TCP Flags			
	Connection NAT State:			mai	IN LO OTTICE-01.	
			habled			
	apabled					

## 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)

tings Dashboard			Mangle Rule <192.168.199.0/24->192.168.88.0/24>					
Safe Mode	Session: 34.87.15.122	<b>=</b> 🛅	General Advanced Extra Action Statistics		ОК			
ick Set	Mangle Rule <192.168.199.0/24->192.168.88.0/24>		Src. Address List:	•	Cancel			
erfaces	General Advanced Extra Action Statistics	ОК	Dst. Address List:	•	Apply	Mangle Rule <192.168.88.0/24->192.168.199.0/24>		
dge	Chain: forward	Cancel	Layer7 Protocol:	-	Disable	General Advanced Extra Action Statistics	ОК	
	Src. Address: 192.168.199.0/24	Apply		_	Comment	Action: change MSS	Cancel	
sh	Dst. Address: 192.168.88.0/24	Disable	Content:	<u> </u>	Сору		Apply	
uting D		Disable	Connection Bytes:	Į.	Remove	Log Prefix:	Disable	
stem	Protocol: 6 (tcp)	Comment	Connection Rate:	÷.	Reset Counters		Disable	
eues	Src. Port:	Сору	Src MAC Address:	-	Reset All Counters	New TCP MSS: 1360	Comment	
s	Dst. Port:	Remove		_		Passthrough	Сору	
,	Any. Port:	Reset Counters	Out. Bridge Port:	•				
DIUS	In. Interface:	Reset All Counters	In. Bridge Port:	•				
ols 🗅	Out. Interface:		In. Bridge Port List:	•				
w Terminal	In Interface Lict		Out. Bridge Port List:	•	/ip	firewall mangle add	action=c	hange-
t1X			IPsec Policy: in 🔻 : ipsec 🔻	•	mcc	chain-forward new-m	cc-1360 c	rc-
nual			TLS Host:	-			33-1300 3	
w WinBox	Packet Mark:		Ingress Prioribu	-	add	ress=192.168.199.0/2	4 dst–	
t	Connection Mark:		Priority:	-	address=192.168.88.0/24 protocol=tcp to			
	Routing Mark: 📃 🔻		DSCP (TOS):	-			1200 -	-
	Routing Table:		TCP MSS: 1 0-1360	•	р-т	lags=syn tcp-mss=!0-	1300 1pse	с—
			Packet Size:	-	pol	icy=in,ipsec passthr	ough=yes	comment
	Connection Type:		Random:	-	_0.71	VE2. Clamp TCD MCC f	rom offic	o 01 +o
	Connection State:		TCP Flags	_	= т	KEZ: CLAIIIP ICP MISS I		e-01 to
	Connection NAT State:		TCP Flags: syn 🔻	\$	of	fice-main"		
			enabled	_				
						Nikita Marikin ( n	i ki to Qtori k	
	lenabled					MIKICA IALIKIN / II	INICAULALIK.	

Nikita Tarikin / nikita@tarikin.com

Free live demo is available

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

- 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



- 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 :)

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

# **IKE2 VPN Server address**

vpn.ike2.xyz

- 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



# hacktheprincess@protonmail.com



192.168.**XX**.0/24

192.168.**XX**.YY

/system identity ???

Send results to e-mail

🔍 🔍 🔍 🔥 ікез	2 LAB certificate request for X 2 Inbox   hacktheprincess@proton X +		
a d c i	🕽 👌 mail.protonmail.com/inbox	💱 🔺	P 🐔
🐣 IKE2 LAB certific	ca		
₽ ProtonMail	Q Search messages v c le UPGRADE SETTINGS CONTACTS	REPORT E	BUG HACKT
COMPOSE	□ ~ (④ 《) 🛍 🖬 Ø 🖿 ∿ ∨ More ~		- <
🚨 Inbox (3) 🛛 C	rotonMail     Welcome to the future of email	24	6.1 KB 🗞
Drafts	☐ ★ ProtonMail How to secure your ProtonMail ac	25	3.9 KB 👒
් Starred (3)	rotonMail Encrypt your Internet with Proton	22	4.8 KB 👒
Archive			
⊘ Spam			
🗊 Trash			
All Mail (3)			
Folders / L			
UPGRADE STORAGE 724.75 KB / 500.00 MB			
v3.16.3			

# Let's keep in touch

Send me e-mail: nikita@tarikin.com





0

@tropicalengineer

Direct message me via:

