

Зачем IKEv2?

Сравнение клиент-серверных типов VPN (RouterOS)



	L2TP	L2TP/IPSEC + psk	OpenVPN	РРТР	SSTP	IPSec IKE2
Протокол	UDP	UDP over UDP/ESP	TCP	GRE	TCP	UDP, ESP
Скорость работы	Быстро	Средне	Медленно	Быстро	Медленно	Очень быстро
Скорость подключения	Средне	Медленно	Медленно	Средне	Средне	Очень быстро
Требуется мощный CPU	Нет	Да	Да	Нет	Да	Да
Балансируется между ядрами СРU	Да	Да	Нет	Да	Да	Да
Безопасность	Низкая	Высокая	Высокая	Низкая	Высокая	Очень высокая
Доставка маршрутов	Нет	Нет	Нет	Нет	Нет	Да
Работа через NAT	Да	Да	Да	Да	Да	Да
Наличие интерфейса	Да	Да	Да	Да	Да	Нет
Популярность	Высокая	Очень высокая	Высокая	Очень высокая	Низкая	Высокая

Зачем IKEv2?

- 1. Очень высокая скорость работы
- 2. Мгновенное подключение
- 3. Очень высокий уровень безопасности
- 4. Поддержка аппаратного шифрования
- 5. Поддерживается большинством современных операционных систем
- 6. Доставляет маршруты клиентам
- 7. Работает через NAT
- 8. Адаптирован для хаотичных мобильных каналов связи

Сетевая диаграмма













Никита Тарикин

Сертифицированный сетевой инженер MikroTik PRO, Россия



Никита Тарикин

Сертифицированный сетевой инженер MikroTik PRO, Россия







Сетевая диаграмма



Сетевая диаграмма

Общий план презентации

- 1. Подготовка к работе
- 2. Настройка VPN сервера в главном офисе
- 3. Подключение Windows 10
- 4. Подключение MacOS, iOS, Android
- 5. Подключение филиала через роутер MikroTik
- 6. Конкурс

Подготовка к работе

- 1. Наличие знаний уровня МТСNA (рекомендуется)
- 2. RouterOS 6.45 или новее
- 3. Все испытания строго в лабораторных условиях (настоятельно рекомендую)
- 4. Дефолт конфигурация 6.45+



Пожалуйста! Не применяйте методологию **раз-раз-продакшн** на исправно работающих сетях!

Nikita Tarikin / nikita@tarikin.com

O'REILLY*

Россинский Е.Б. & Ахметов С.Ю.

Обновляем RouterOS до версии 6.45 или новее





2. Заливаем пакет в корень файловой системы

No

Сбрасываем RouterBoard к заводской v6.45+ конфигурации

ession Settings Dashb	admin@192.168.88	1 (MikroTik) - Win	Box v6.44.3 on mAP lite	e (mipsbe)	
Safe Mode	Session: 192.168.88.1				CPU: 4% 🔳 🛅
🔏 Quick Set					
CAPSMAN					
im Interfaces	Package List				
🚊 Wireless	T Check For U	dates Enable	Disable Uninstall	Unschedule Downgrade	Check Installation
Sig Bridge	Name	Version	Build Time	Scheduled	
PPP	@routeros-mipsb	6.44.3	Apr/23/2019 12:37:03	3	
🛫 Switch	advanced-t	ools 6.44.3	Apr/23/2019 12:37:03		
°t <mark>8</mark> Mesh	e hotspot	set Configuration		×	
IP D	mpls	Kee	ep User Configuration	teset Configuration	
🧱 Routing 🛛 🗈	@ppp		PS Mode	Cancel	
😳 System 🗈	Auto Upgrade		Not Radium		
Queues	Certificates	un After Darrh			
Files	Clock	un Arter Reset:	' · /		
E Log	Console				
🧟 RADIUS	Disks				
🔀 Tools 🛛 🗈	History				
📰 New Terminal	Identity	_		_	
E MetaROUTER	LEDs				
🏉 Partition	License				
📃 Make Supout.rif	Logging	/			
😧 Manual	Packages				
🔘 New WinBox	Password				
	Ports	/			
	Reboot		Sustem ->	> Reset co	nfigurati
	Reset Configuration		Jystem /	Reset CC	milyurati
	Resources				
	Routerboard				
	SNTP Client				

Сброс на заводской конфиг применит обновленные правила файрволла, интерфейс листов, улучшенные настройки безопасности итп..

The following default	t configuration has been installed on your router:	
RouterMode:		
* WAN port is prote	cted by firewall and enabled DHCP dient	
* Wireless and Ethe	rnet interfaces (except WAN port ether1)	
are part of LAN bri	dge	
wlan1 Configuration:		
mode: ap	p-bridge;	
band: 2g	jhz-b/g/n;	
tx-chains: 0	())	
rx-chains: U	ijij ooldoh uu	
AN Configuration:	20/40mnz-XX;	
ID address 192 16	8 88 1/24 is set on bridge (LAN port)	
DHCD Server: ena	bled:	
WAN (gateway) Con	figuration:	
gateway: ether1	:	
ip4 firewall: enabl	led;	
NAT: enabled;		
DHCP Client: enab	oled;	•
		_

Общие системные настройки

План действий:

- 1. WAN IP/DNS адреса
- 2. Часовой пояс
- 3. Дата/время через NTP
- 4. Loopback bridge
- 5. IP pool

Адреса WAN IP и DNS для IKE2 VPN сервера

	e e admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)						
Ses	sion Settings Dashbo	pard					
Ю	😋 🛛 Safe Mode	Session: 192.168.88.1	CPU: 1%				
OS WinBox	Puick Set CAPSMAN Interfaces Wireless Bridge PPP Switch Pop System Piles Piles Piles Piles Pools Routing Piles Piles Math CUTER Partition Make Supout.rif	DHCP Client DHCP Client DHCP Client Options					
utel	🥶 Manual	2 items					
9							

123.45.67.8 на WAN интерфейсе

Проверяем записи DNS: Имя: **vpn.ike2.xyz** Адрес: **123.45.67.8**

	<u>ヽ_(ツ)_</u> Γ	~ (zsh)	
Last login: Tu	e May 7 11:04:11 c	on ttys001	
🔶 ~ nslookup	/pn.ike2.xyz		
Server:	192.168.88.1		
Address:	192.168.88.1#53		
Name: vpn.ik Address: 123.4 → ~	5.67.8		

* DNS записи настраиваются через панель управления хостинг провайдера или регистратора доменного имени Нет денег на свой домен? 😎

•••	admin@10.0.88.	.1 (vpn.ike2.xyz) - V	VinBox v6.44.5 or	n CHR (x86_64)	
Session Settings Dashb	oard				
Safe Mode	Session: 10.0.88.1				CPU: 0% 📕 🛅
🔏 Quick Set					
Interfaces	1				
💦 😹 Bridge					
ei PPP					ОК
ିଅଟି Mesh		DDNS Update Interval:		•	Cancel
IP D	ARP		Update Time		Apply
🏹 Routing 🛛 🗎	Accounting	Public Address:	34.87.15.122		Former the data
💮 System 🗈	Addresses	DNS Name:	6b3a0c358bf8f1f5.s	sn.mynetname.net	Force Update
🙊 Queues	Cloud		Use Local Addres	s	
Files	DHCP Client	stod		outor is babind a NOT	Domoto connecti
Log	DHCP Relay	ateu		Codcer is bening a NAT	. Remote connect
🙆 🥵 RADIUS	DHCP Server				
🗧 🔀 Tools 📃	DNS				
new Terminal	Firewall				
🧕 🗋 Make Supout.rif	IPsec				
🔮 😯 Manual	Kid Control				
🗟 🕒 New WinBox	Neighbors				
	Packing				
	Pool				
	Routes				
	SMB				
	SNMP				

IP -> Cloud

Проверяем записи DNS: Имя: *blabla*.sn.mynetname.net Адрес: **34.87.15.122**

Настраиваем часовой пояс

🔴 🕘 🔵 admin	n@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)
Session Settings Dashbo	bard
Safe Mode	Session: 192.168.88.1
Quick Set CAPSMAN Im Interfaces Wireless Bridge PPP Switch Switch Set Mesh IP	Clock Time Manual Time Zone OK Cancel Date: Jan/01/1970 Apply Time Zone Name: Europe/Moscow ✓
Routing System Outly Queues Dot1X Files Log RADIUS Tools New Terminal	GMT Offset: +03:00 Auto Upgrade DST Active Certificates
Make Supout.rif	License Logging Packages Password Ports Reboot Reset Configuration
	Resources



/system clock <mark>set</mark> time-zonename=Europe/Moscow

name=Europe/Moscow

Настройка автоматической синхронизации даты и времени

• Ses	e admir	n@192.168.88.1 (I oard	MikroTik) - WinBox vê	8.45.2 on hAP lite (sm	ips)
5	Safe Mode	Session: 192.168.88.	1		a
	à Quick Set				
	🚊 CAPsMAN		SNTP Client		
	🔚 Interfaces			Enabled	ОК
	🚊 Wireless		Mode:	broadcast	Cancel
	😹 Bridge		Primary NTP Server:	0.0.0.0	
	📑 PPP		Secondary NTP Server:	0.0.0.0	
	🛫 Switch		Service DNS Namocu	0 ru pool ptp. org	_
	°t <mark>8</mark> Mesh		berver bivo walles:	on a poor nep or g	
	IP 🗅			1.ru.pool.ntp.org	₹
	😹 Routing 📃 🗎			2.ru.pool.ntp.org	\$
	🎲 System 🗅	Auto Upgrade	Dynamic Servers:		
	룢 Queues	Certificates	Dell Tekenvelv	0.0	
	Dot1X	Clock	Poli Interval:	US	
	Files	Console	Active Server:		_
	Log	History	Last Update From:		
	2 RADIUS	Identity	Last Update:		
š	🔀 Tools 🗈	LEDs	Last Adjustment:		
n B	New Terminal	License	b De d De de la Crease		
N	Make Supout.rif	Logging	t Bad Packet From:		_
v	😧 Manual	Packages	Last Bad Packet:		
5	S New WinBox	Password	ad Packet Reason:		_
Ę	🛃 Exit	Ports			
ş		Reboot			
		Reset Configuration			
		Resources	Δrm	UBUDVOM N	ITP client
		Routerboard		MIDNIDACM I	TT CTTCIII
		SNTP Client			
		Scheduler			

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

1.ru.pool.ntp.org,2.ru.pool.ntp.org

Nikita Tarikin / nikita@tarikin.com

ЭТО ВАЖНО

Добавляем новый loopback bridge

/interface bridge add
name=bridge-loopback

Задаём IP адрес для loopback bridge



10.0.88.1

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

network=10.0.88.0

Добавляем новый пул IP адресов для IKEv2 VPN клиентов

-			
•	e admin	@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)
Ses	ssion Settings Dashb	oard Session: 192.168.88.1	CPU: 0% 📕 📴
outerOS WinBox	Quick Set Image: CAPsMAN Image: CAPS	IP Pool Pools Used Addresses Image: Image	Find

10.0.88.2-254

/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

Генерируем правильные SSL сертификаты

План действий

- 1. Генерируем главный СА
- 2. Генерируем серверную пару сертификат+ключ
- 3. Генерируем клиентские цифровые подписи
- 4. Экспортируем клиентские подписи

•	admin@192	.168.88.1 (Mikro	oTik) - WinBox v	6.45.2 on hAP lite (si	nips)	
n Settings Dashb	Section: 192 168 88 1					
	Jession. [192.100.00.1]	_	_			CP0.0%
Quick Sec	Certificates					
	Certificates SCEP Ser	New Certificate				
Wireless	+ - 7 Im	General Key Lican	e Statuc			
2 Bridge	Name	North Star	Că ilea eee			ОК
PPP		Name:	CA.IK82.XYZ			Cancel
Switch	Auto Upgrade				<u> </u>	Apply
8 Mesh	Certificates				-	
IP D	Clock	Issuer:	,			Сору
Routing	Console	Country:	RU			Remove
System	History	State:	Moscow Oblast			Sign
Queues	Identity	Locality:	Scolkovo			Sign via SCEP
Dot1X	LEDs	Organization:	IKE2.xvz			Import
Files	License	Units	[Card Reinstal
Log	Logging					
RADIUS	Packages	Common Name:	CA.ike2.xyz			Card Verity
🖁 Tools 🛛 🗅	Password	ubject Alt. Name:	DNS	∓ : ca.ike2.xyz	\$	Set CA Passphrase
New Terminal	Ports					Export
Make Supout .nif	Reboot	Key Type:				Revoke
👌 Manual	Reset Configuration	Key Size:	4096		₹	
New WinBox	Resources	Days Valid:	3650			
Exit	Routerboard	-				
	SNTP Client	vate key crl	authority		card trusted	
	Scheduler		1			
	Scripts					
	Shutdown					
	Special Login					
	Users					
	Watchdog					



/certificate add name=CA.ike2.xyz country=RU state="Moscow Oblast" locality=Scolkovo organization=IKE2.xyz commonname=ca.ike2.xyz subject-altname=DNS:ca.ike2.xyz key-size=4096 days-valid=3650 trusted=yes keyusage=digital-signature,keyencipherment,data-encipherment,keycert-sign,crl-sign

Само-подписываем новый CA SSL сертификат (Certificate Authority)

	admin@103	169 99 1 (Mikro	Tik) - WinBox v6 45 2 on bAP lite (smins)		
sion Settings Dashb	oard		(amps)		
Safe Mode	Section 102 169 99	1			CPU/100% 📕 🕀
Sale Mode	Jession: 192.100.00			_	CP0: 100 % 🎽 🛄
🔏 Quick Set	rtificates				
I CAPSMAN	artificates SCED Serve		arte OTB CBI		
🔚 Interfaces		IS DEF RA REQUE			
🧘 Wireless	· · · · Impo				
💥 Bridge	Name /	General Key Usage	e Status	r	
E PPP	CHINGENTE	Name:	CA ike2 ywz		ОК
🛫 Switch		Nume.	CHINGER/E		Cancel
°t8 Mesh					Apply
IP D		Taguari			
🎉 Routing 🛛 🗎		Issuer:	,		Сору
💮 System 🗅		Count Sig	n (Running)		Remove
👳 Queues		Sta	Certificate: CA ike2 xyz 🐱 Start		Sign
Dot1X		Locali			Sign via SCEP
Files		Organizatio	CA: Stop	51	Import
E Log			A CRL Host: Close	= }	Cond Defended
🥵 RADIUS	em (1 selected)		Progress: /		Card Reinstall
🄀 Tools 🛛 🗎		Common Name:	ca.ike2.xyz		Card Verify
📰 New Terminal		Subject Alt, Name:	DN5 T : ra.ike2.xvz	•	Set CA Passphrase
[Make Supout.rif				<u> </u>	Export
🤁 Manual		Key Type:	RSA		Revoke
S New WinBox		Key Size:	4096	Ŧ	
🛃 Exit		Days Valid:	3650		
		private key cri	authority expired smart card	trusted	

/certificate sign CA.ike2.xyz

Само-провозглашение себя главным авторитетом в банановой корпорации

) 🔵 🛛 adn	nin@192.168.88.1 (MikroTik) - WinBox v6.45.2	on hAP lite (smips)
ion Settings Dashboard Safe Mode Sessio	in: 192.168.88.1	CPU: 1% 📕 🗂
Quick Set Certal CAPsMAN Certal Therfaces Wireless Sridge Switch Switch Switch Routing IP Queues Queuess Dot1X Certal Ce	icates if cates if cates if cates General Key Usage Status Name: Vpn.ike2.xyz Issuer: Country: RU State: Moscow Oblast Locality: Scolkovo	OK Cancel Apply Copy Remove Sign Sign via SCEP
Files Log RADIUS Tools	Organization: IKE2.xyz Unit: Common Name: vpn.ike2.xyz Sociect Alt. Name: DNS F: vpn.ike2	Card Reinstall Card Verify Set CA Passphrase
New Terminal Make Supout.rif Manual New WinBox	Key Type: Key Size: 2048	Export Revoke

New Certificate		
New Certificate General Key Usage Gigtal signature Key encipherment Key agreement Cri sign Gigtal signature	content commitment data encipherment key cert. sign encipher only dvcs ocsp sign ipsec user ipsec end system code sign v tis server	Cancel Apply Copy Remove Sign Sign via SCEP
-		Import

/certificate add name=vpn.ike2.xyz
country=RU state="Moscow Oblast"
locality=Scolkovo organization=IKE2.xyz
common-name=vpn.ike2.xyz subject-altname=DNS:vpn.ike2.xyz key-size=2048
days-valid=1095 trusted=yes keyusage=tls-server

vpn.ike2.xyz

Подписываем серверный сертификат у авторитета CA.ike2.xyz

•••	admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)
Session Settings Dashb	oard	
🔊 🍳 🛛 Safe Mode	Session: 192.168.88.1	CPU: 100% 📕 🛅
CAPsMAN CapsMa	Certific Certificate <vpn.ike2.xyz> Certif General Key Usage Status Name: vpn.ike2.xyz</vpn.ike2.xyz>	
Switch Switch Ses IP	Issuer:	Apply Copy Remove
Routing P System P Queues shot1X	Locality CA: CA: (ke2.xyz) Stop Organizatior CA CRL Host: ↓ Unit Progress: /	Sign via SCEP Import Card Reinstall
Log	Common Name: vpn.ike2.xyz 2 item Subject Alt. Name: DNS F: vpn.ike2.xyz	Card Verify Set CA Passphrase
New Terminal	Key Type: R5A Key Size: 2048 Days Valid: 1095	Revoke
New WinBox	private key cri authority expired smart card trust	ed

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

са=са.ткег.хуг

Создаем шаблон для тиражирования клиентских подписей

edmin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)					
essior	n Settings Dashbo	oard			
0	🎽 🛛 Safe Mode	Sessio	on: 192.168.88.1		CPU: 3%
Â	guick Set	Certi			
Ĵ	CAPSMAN	Cert	New Certificate		
1	Interfaces		General Key Usag	e Status	
Ĵ	Wireless	+	Name:	~client-template@vpn.ike2.xyz	
50	🕻 Bridge	KAT		A	Cancel ster 🔻
¢,	PPP	KI			Apply
	Switch		Issuer:		Сору
°t	8 Mesh		Couptry:	PU .	Remove
255	IP D		Country.		Cirr.
2	Routing D		State:	Moscow Oblast	Sign
6	System D		Locality:	Scolkovo	Sign via SCEP
9	Queues		Organization:	IKE2.xyz	Import
<¦	Dot1X		Unit:		Card Reinstall
	Files		Common Name:	vclient-template@vpp_ike2_xvz	Card Verify
	Log	• 2 itor	- Lu - Lu - Lu		Set CA Passphrase
õ 🖉	RADIUS		Subject Alt. Name:	Email Client-template@vpn.ikg	Evport
2×	Tools D		Key Type:		Export
	New Terminal		Key Sizer	2048	Revoke
νĿ	Make Supout.rif		Key bize:		
2 🕄) Manual		Days Valid:	365	
	New WinBox				
ğ 🖪	Exit		private key crl	authority expired smart card trust	ed
<u>-</u>					

New Certificate	
General Key Usage Status	
Key Usage: digital signature content commitment	СК
key encipherment data encipherment	Cancel
key agreement key cert. sign	Apply
cri sign encipher only	
decipher only dvcs	Сору
server gated crypto ocsp sign	
timestamp ipsec user	Remove
ipsec tunnel ipsec end system	Sign
email protect code sign	
✓ tis client Its server	Sign via SCEP

/certificate add name=~clienttemplate@vpn.ike2.xyz country=RU state="Moscow Oblast" locality=Scolkovo 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

Создаем первую клиентскую подпись из заготовленного шаблона

	admin@192.168.88.1 (MikroTik) - Win	Box v6.45.2 on hAP lite (smips)		
tings Dashb	oard			
Safe Mode	Session: 192.168.88.1		CPU: 1% 📕 🔒	
k Set sMAN ·faces	Certificates Certificates Certificates SCEP Servers SCEP Mane: Certificates SCEP SCEP	late@vpn.ike2.xyz> itatus ient-template@vpn.iky2.xyz	ОК	leartifi
less je :h	KAT General Key Usage Status KI Name: admin@vpn.ike2.xyz			template name=adm
ing P	Issuer:	Apply Copy	Sign Sign via SCEP	name=adm name=ema
Jes X	Country: RU State: Moscow Oblast Locality: Scolkovo	Remove Sign Sign via SCEP	Import Card Reinstall Card Verify	_
IUS	Organization: IKE2.xyz Jiter Unit:	Import Card Reinstall	Set CA Passphrase Export	
; D Terminal e Supout.rif	Common Name: admin@vpn.ike2.xyz Subject Alt. Name: Email 🟹 : admin@	Card Verify Set CA Passphrase Export	Revoke	
Jal WinBo×	Key Type: Key Size: 2048 Days Valid: 365	Revoke rush		- adm:
	private key crl authority expired	smart card trusted		

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

admin@vpn.ike2.xyz
Подписываем клиентскую подпись у авторитета CA.ike2.xyz



/certificate sign admin@vpn.ike2.xyz ca=CA.ike2.xyz

Создаем остальные клиентские подписи из шаблона (по аналогии)

CA Safe Mode	Session: 192.168.88.1						CPU: 1%
🔏 Quick Set	New Certificate						
I CAPSMAN	General Key Usage Stat	s					
🛲 Interfaces	Name: frontd	or@rkp.gov.ru		Certificate <alex@n< th=""><th>sc.ru></th><th></th><th></th></alex@n<>	sc.ru>		
Wireless				General Key Usag	je Status		ОК
😹 Bridge		New Certificate		Name:	alex@nsc.ru		Cancel
📑 PPP	Iccupy	General Key Usag	ge Status			<u>^</u>	
🛫 Switch	155061.)	Name:	webmaster@yasdelie.ru				
°T¦8 Mesh	Country: RU			Issuer:]		Сору
255 IP	State: Mosco	v		Country:	RU		Remove
🙈 Routing 🗈	Locality: Mosco	v Issuer:]	State:	Novosibirsk oblast		Sign
💮 System 🔹	Organization: RKN	Country:	RU	Locality	0 kademoorodok		Sign via SCEP
Sueues	Unit:	States	Kaliningrad	Localicy:			
Dot1X		State:	Kaliningrad	Organization:	IKE2.×yz		Import
Files	Common Name: frontd	oor@rl Locality:	Kaliningrad	Unit:			Card Reinstall
Log	Subject Alt. Name: Email	Organization:	YaSdelie web development	Common Name:	alex@nsc.ru		Card Verify
RADIUS	Kautura	Unit:		Subject Alt Name:	Email Enail		Set CA Passphrase
Navy Tayasia al	Key Type:	Common Name:	webmaster@vasdelie.ru		- I dioxenseria		Export
Make Supput rif	Key Size: 2048	Subject Alt Mamou	Email En under	Key Type:	RSA		Revoke
Manual	Days Valid: 3650	Subject Ait, Name:	Linai ▼ : webma	Key Size:	2048	₹	
New WinBox		Кеу Туре:		Days Valid:	365		
Exit	private key crl	auth Key Size:	2048				
		Days Valid:	365	private kev	authority expired smart carr	d tructer	d
				private resy	addroney expired smart card	a in falascoi	

Экспортируем клиентскую подпись + приватный ключ в файл .p12

admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)								
ession Settings Dashboard								
🔊 🍳 🛛 Safe Mode	Session: 192.168.88.1	CPU: 1% 📕 🛅						
🔏 Quick Set	Certificate <admin@vpn.ike2.xyz></admin@vpn.ike2.xyz>							
I CAPSMAN	General Key Usage Status]						
🛲 Interfaces	Name: admin@vpn.ike2.xvz	ОК						
🤶 Wireless		Cancel						
😹 Bridge		Apply						
📑 PPP	Issuer:	Conu						
🛫 Switch		Сору						
°t <mark>%</mark> Mesh	Country: RU	Remove						
255 IP D	State: Moscow Oblast	Sign						
🌌 Routing 🛛 🗋	Export							
🌐 System 🗈	Certificate: admin@vpn.ike2.xyz	Export						
👳 Queues	Type: PKC512							
∢i> Dot1X								
Files	Export Passphrase:							
🔀 🖹 Log	Subject Alt. Name: Email : admin@vpn.ike2.xyz	Set CA Passphrase						
🞽 🧟 RADIUS		Export						
늘 🄀 Tools 🛛 🖻	Key Type: RSA	Revoke						
👩 🔚 New Terminal	Key Size: 2048							
🧿 🗋 Make Supout.rif	Days Valid: 365							
👰 🕢 Manual	Trusted							
🗟 🕓 New WinBox	private key or authority licened evolved evolves by	rustad						
🕰 📕 Exit	privace key ich auchoncy issued expired ismart ca ic	usteu						

При экспорте **обязательно** указываем пароль. Пустой пароль экспортирует **сертификат без ключа**.

Пароль храним в секрете.

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

export-passphrase=keepinsecret

Экспортируем сертификат авторитета СА в .crt файл

admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)							
Safe Mode	Session: 192.168.88.1	CPU: 2% 📕 🔒					
VOUNT Set CAPSMAN CAPSMAN CAPSMAN CAPSMAN CAPSMAN CAPSMAN Solution Solution Solution Solution Solution Solution Solution Comparison Solution Comparison Compa	Certificate <ca.ike2.xyz> General Key Usage Status Name: CA.ike2.xyz Issuer: Country: RU State: Moscow Oblast Export Certificate: CA.ike2.xyz Type: PEM Export Passphrase: БЕЗПАРОЛЯ ▼ Subject Alt. Name: DNS : ca.ike2.xyz Key Type: RSA Key Size: 4096 Days Valid: 3650 ▼ Trusted</ca.ike2.xyz>	Cancel Cancel Apply Copy Remove Sign Sign Cancel stall ify Set CA Passphrase Export Revoke					
Sou	private key cri authority expired smart card truste	ed					

При экспорте ни в коем случае не указываем пароль. Экспорт ключа СА самопровозглашенного авторитета УГРОЖАЕТ БЕЗОПАСНОСТИ ВСЕМ ЖИТЕЛЯМ БАНАНОВОЙ КОРПОРАЦИИ

/certificate

export-certificate CA.ike2.xyz type=pem

Скачиваем с роутера экспортированный СА сертификат + клиентские подписи

•••	admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)		
Session Settings Dashb	pard second s		
🔊 🍳 🛛 Safe Mode	Session: 192.168.88.1	CPU: 6%	
🔏 Quick Set			
CAPSMAN			
Interfaces	Certificates SCEP Servers SCEP RA Requests OTP CRL		
1 Wireless	💠 🖻 🍸 Import Card Reinstall Card Verify Revoke Create Cert. Request Settings Find		
Se Bridge	Name 🔺 Issuer Common Name Subject Alt. Name Key Size Days Valid Trusted 🔽		
	KAT CA.ike2.xyz ca.ike2.xyz DN5:ca.ike2.xyz 4096 3650 yes VI admin@urp.ike2.xyz bin@urp.ike2.xyz 2048 245 pe		
Cuitch	KI alex@nsc.ru alex@nsc.ru Email:alex@nsc.ru 2048 365 no		
	KI frontdoor@rkn.gov.ru frontdoor@r Email:frontdoor@rkn.gov.ru 2048 3650 no		
"lä Mesh	KI office-spb@vpn.ike2.xr office-spb@vpn.ike2.xr 5000 bit VI use ike2 was File List		
IP D	KI webmaster@yasdelie.r		
🌌 Routing 🕒	vclient-template@vpn	ind	
💮 System 🗈	File Name △ Type Size Creation Time	T	
🙊 Queues	Cert_export_CA.ike2.xyz.crt .crt nie 2061 B Aug/01/2019 10:17:14	9	
∢¦> Dot1X	Cert_export_alex@nsc.ru.p12 .p12 file 4456 B Aug/01/2019 10:35:56	6	
Files	☐ cert_export_frontdoor@rkn.gov.ru.p12 .p12 file 4490 B Aug/01/2019 10:35;4;	1	
	Cert_export_orrice-spo@vpn.ike2.xyz.p12 .p12 file 4528 B Aug/01/2019 10:35:27	4	
	8 items directory Jan/01/1970 03:00:0-	4	
New Terminal	7 items 8.4 MiB of 16.0 MiB used 47% free		
Q 🔝 Make Supout.rif			
🕘 🥶 Manual			
🗟 🔘 New WinBox			



Настройка IPSec

- 1. Настройка Mode Configs
- 2. Hacтройкa Peer Profiles
- 3. Настройка Peers
- 4. Настройка Proposals
- 5. Настройка Policy Groups
- 6. Настройка Policy Template
- 7. Hастройка 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;

Ключевые изменения в 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. Наст	ройка нового IPSec mode config	Name: modeconf vpn.ike2.xy	ок
	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 Dashb	pard	ess Prefix Length: 32	
Safe Mode	Session: 192.168.88.1 CPU: 2%		
http://www.com/com/com/com/com/com/com/com/com/com/	IPsec 🔲	Split Include: 192.168.88.0/24	
	Policies Proposals Groups Peers Identities Profiles Remote Peers Mode Configs Installed SAs Keys	Static DNS, 10.0.92.1	
	Find	State DNS: 10.0.88.1	
Bridge	Name △ Resp Address Pool Address Address Prefi Split Include Sy	▼	
PPP	request-only no		
📟 Switch			
°t¦8 Mesh	New Three Made Confin		
255 IP D			
Routing	Name: modeconr vpn.ike2.xyz OK	/ip ipsec m	ode-config
System D	Cancel		
	Address Pool: pool vpn.ike2.xyz 🔽 🔺 Apply	add address	-pool="pool
- Log	Address: Copy	vnn ike? vv	z" address_prefix_
A RADIUS	Address Prefix Length: 32 Remove	vpn i ikcz i ky	
🗙 🄀 Tools 🗈 🗈	◆ Split Include: 0.0.0.0/0 ◆	length=32 n	ame="modeconf
🔏 🕅 New Terminal	1 item System DNS		
Set MetaROUTER	Static DNS: 10.0.88.1	vpn.ike2.xy	z" split-
Partition		include=0.0	.0.0/0 static-
Q 🛄 Make Supout.rif			
Manual		dns=10.0.88	<pre>.1 system-dns=no</pre>

2. Настройка нового IPSec peer profile (фаза 1)

Safe Mode Session: 192.168.88.1 CPU: 0% Quick Set Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 CAPSMAN Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 CAPSMAN Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.88.1 Image: Session: 192.168.168.168.168.168.168.168.168.168.168	Tik) - WinBox v6.44.3 on mAP lite (mipsbe)	admin@192.168.88.1 (MikroTik) - \ pard	e e e	Ses
Quick Set CAPsMAN Interfaces Proposals Grou Wireless Proposals Grou Wireless Proposals Grou Wireless Proposals Grou Proposals Grou Proposals Grou Proposals Grou Proposals Grou Proposals Grou Proposals Grou Proposal Grou Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal C Proposal Check: Propo	СРU: 10% 📃 💼	Session: 192.168.88.1	ର୍ଚ୍ଚ 🖓 Safe Mode	ю
MetaROUTER 1 item NAT Traversal DPD Interval: 120 F s DPD Maximum Failures: 5	e Carcel Name: vofile vpn.ke2.xyz OK orithms: sha256 Carcel gorithm: des 3des Apply ✓ aes-128 ✓ aes-192 Apply ✓ aes-256 blowfish Copy Carcellia-128 Carcellia-192 Remove Carcellia-256 Copy Carcellia-256 Copy Carcellia-256 Copy Carcellia-256 Copy Copy Carcellia-256 Copy Remove 4 Group: modp768 ✓ modp1024 ec2n155 € con2048 Modp1536 ✓ modp2048 Modp1536 ✓ modp2048 Modp1536 € ecp384 ecp521 4 Check: obey Ifetime: 1d 00:00:00 Febytes: ▼ NAT Traversal Interval: 120 Failures: 5	IPsec Name: Proposals Grou Image: Second	Quick Set CAPsMAN CAPsMAN Interfaces Wireless Still PPP Switch Switch System Part Queues Files Log ADJUS New Terminal MetaROUTER Partition MetaROUTER Partition Make Supout.rif Manual New WinBox	outerOS 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

3. Создание нового IPSec peer на публичном IP адресе (режим IKE2)

🛑 😑 🛑 ad	min@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)							
Session Settings Dashbo	ession Settings Dashboard							
Safe Mode	Session: 192.168.88.1 CPU: 2%							
Quick Set CAPsMAN Interfaces Wireless Signinge PPP	IPsec Image: Section of the section							
Section 2017 Secti	New IPsec Peer Name: peer 123.45.67.8 OK Address: Port: Profile: profile: profile: profile: Profile: Profile: Profile: Profile: Profile: Passive Postive: Passive: Profile:							

Принимаем клиентов со всех адресов 0.0.0.0/0

Принимаем клиентов только на адрес **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. Настройка нового IPSec proposal (фаза 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% 📕 🛅
Image: CAPSMAN Image:	Image: Proposals Groups Peers Identities Profiles Remote Peers Mode Configs Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Image: Proposal Proposal Image: Proposal </th <th>Installed SAs Find</th>	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. Добавление новой IPSec policy group

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

	6. Ha	стройка нового шаблона II	Sec policy
•	• •	admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)
5es N	sion Settings Dasht	Session: 192.168.88.1	CPU: 294
terOS WinBox	Quick Set CAPsMAN CAP	Policies Proposals Groups Peers Identities Profiles Active Peers Mode	Configs Configs Configs Concel Apply Disable Comment Copy Remove
Rou	S New WinBox	enabled Template Active	

New IPsec Policy General Action Status ОK Action: encrypt Cancel IPsec Protocols: esp Ŧ Apply Ŧ Proposal: proposal vpn.ike2.xyz Disable Comment Copy Remove enabled

/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. Внимательно создаем IPSec identities для каждого клиента

e admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)										
sion Settings Dashbo	n Settings Dashboard									
Cafe Mode	Session: 192.168.88.1									CPU: 2% 📕 🛅
A Quick Set	IPsec Identity <peer 123<="" th=""><th>3.45.67.8></th><th></th><th></th><th></th><th>IPsec Identit</th><th>y <peer 123<="" th=""><th>.45.67.8></th><th></th><th></th></peer></th></peer>	3.45.67.8>				IPsec Identit	y <peer 123<="" th=""><th>.45.67.8></th><th></th><th></th></peer>	.45.67.8>		
🛲 Interfaces	Peer:	peer 123.45.	IPsec Identity <peer 123<="" th=""><th>3.45.67.8></th><th></th><th></th><th>Peer:</th><th>peer 123.45.67.8</th><th>Ŧ</th><th>ОК</th></peer>	3.45.67.8>			Peer:	peer 123.45.67.8	Ŧ	ОК
🗊 Wireless	Auth. Method:	digital signatu	Peer:	peer 123.45.67.8	Ŧ	ОК	h. Method:	digital signature	₹	Cancel
훭릁 Bridge	Certificate:	vpn.ike2.xyz	Auth. Method:	digital signature	Ŧ	Cancel	ertificate:	vpn.ike2.xyz	Ŧ \$	Apply
📑 PPP	Demote Certificate:	frontdoor@rk				- Apply	ertificate:	alex@psc.ru	-	Disable
🛫 Switch	Remote Certificate:	rroncooren	Certificate:	vpn.ike2.xyz	∓ ≑	Арріу	cercificace.	laiex@hisc.rd		
°T <mark>8</mark> 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	y ID Type:	auto	₹	
👰 Queues			Mu ID Tupor	auto	Ξ	Remove				
∢i> Dot1X	Remote ID Type:	user fqdn	Hy ID Type.	3300			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@vpn.ike2.xvz			Match By:	certificate	₹	
🥵 RADIUS			Match Dur		-					
🄀 Tools 🛛 🕑	Mode Configuration:	modecont vpr	Match By:	certificate	•		riguration:	modeconf 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			[ondolog							

method=digitalemote ke2 auth tificate=vpn add identi Ge ipsec signature ip

n@vpn

ad

÷

Внимательно создаем IPSec identities для каждого клиента

.1 (N	/likroTik) - WinBox v6	.45.2 on	hAP lite (sm	ips)		
						CPU: 2%
_			IPsec Identit	y <peer 123<="" td=""><td>3.45.67.8></td><td></td></peer>	3.45.67.8>	
er 123	3.45.67.8>			Peer:	peer 123.45.67.8	OK
eer:	peer 123.45.67.8	₹	ОК	h. Method:	digital signature 🔻	Cancel
hod:	digital signature	₹	Cancel	ertificate:	vpn.ike2.xyz 🗧 🖨	Apply
ate:	vnn.ike2.xvz	∓≜	Apply	ertificate:	alex@nsc.ru	Disable
ate:	admin@vpn.ike2.xyz	- •	Disable	ate Group:	group vpn.ike2.xyz	Comment
		-	Comment	ack Chain:		Сору
oup:	group vpn.ikez.xyz	-	Сору	ID Type:	auto	Remove
ion i			Remove	P LO TYPE.	4400	1
ype:	auto	₹		e ID Type:	user fqdn 두]
		-		emote ID:	alex@nsc.ru]
ype:	admin@upp_ike2_vuz			Match By:	certificate 🗧]
- 10:						
т Ву:	certificate	•		riguration:	modecont vpn.ike2.xyz	1
tion:	modeconf vpn.ike2.xyz	₹ ▲		ate Policy:	port strict	
olicy:	port strict	Ŧ				

/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

Hастройка Firewall

План действий

- 1. Краткий обзор стандартного Firewall
- 2. Правила для подключения к роутеру через IPSec
- 3. Правила для трафика через VPN соединение



Пустой FIREWALL фильтр

		NRO
	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	awn
is Dashbo	pard	20r
e Mode	Session: 192.168.88.1 CPU: 1% 🔳 🎰	
e mode st iN iN iN ises ;	Session: 192.180.00.1 Firewall Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer? Protocols Image: Protocol Sec. Port Dist. Port In. Int Out. Image: Protocol Sec. Port Dist. Port In. Int Out. Image: Protocol Sec. Port Dist. Port In. Int Out. Image: Protocol Sec. Port Dist. Port In. Int Out. Image: Protocol Sec. Port Dist. Port In. Int Out. Image: Protocol Protocol Sec. Port Dist. Port In. Int Out. Image: Protocol Protocol Protocol Sec. Port Dist. Port In. Int Out. Image: Protocol P	Under OS Router HANN
ipout.rif		192.108.88.0/24
	1 item	
nBox		

Пропустить

Фильтровать

Nikita Tarikin / nikita@tarikin.com

WAN

Настройка Firewall

Краткий обзор стандартного фильтра (MTCNA)

Краткий обзор стандартного Firewall фильтра RouterOS 6.45

Firewall																
Filter Rules	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols															
+ -	Ø X		7	00 Reset	: Counters	00 Reset	All Counter:	s							Find	input 🗧
# Ac	ction	Chain	Sri	c. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int	Out. I	In. Int	Out. I	Src. A	Dst. A	Bytes	Packets 🔻
;;; defco	onf: accep	pt establish	hed,re	elated, untra	acked											
1 🖌	/acc i	input													5.5 MiB	61 567
;;; defco	onf: drop	invalid														
2 🔰	≰drop i	input													341 B	6
;;; defco	onf: accep	pt ICMP														
3 🖌	/acc i	input				1 (icmp)									0 B	0
;;; defco	onf: accep	pt to local l	loopb	ack (for CAP	SMAN)											
4 🖌	/acc i	input	İ	,	127.0.0.1										0 B	0
;;; defco	onf: drop	all not com	ning fr	rom LAN												
5 🔰	drop i	input									!LAN				201.2 KiB	1 096
5 items out	of 12															
,																
Firewall																
Flicer Rules	NAT	Mangle	Raw	Service Po	rts Connect	ions Add	ress Lists	Layer7 Proto	cols							
4 -	X		7	00 Reset	: Counters	00 Reset	All Counter	s							Find	forward 🔻
# Ac	ction	Chain	Sri	c. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int	Out. I	In. Int	Out. I	Src. A	Dst. A	Bytes	Packets 🔻
;;; specia	al dummv	rule to sh	ow fa	sttrack cour	nters											
0 D C) pas	forward													190.5 MiB	306 733
::: defco	onf: accer	ot in ipsec	policy													
6 🖌	/acc	forward													0 B	0
;;; defco	onf: accer	ot out ipse	c polic	Y												
7	/acc	forward													0 B	0

;;; defconf: fasttrack ▶ fas... forward 8.0 MiB 53 920 8 ;;; defconf: accept established, related, untracked 9 acc... forward 8.0 MiB 53 920 ;;; defconf: drop invalid Xdrop forward 1060.4 KiB 1 893 10 ;;; defconf: drop all from WAN not DSTNATed 11 Xdrop 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" 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

Hастройка Firewall

- 1. Обзор стандартного фильтра
- 2. Правила для подключения к роутеру через IPSec
- Правила для трафика через VPN соединение



Hастройка Firewall

- 1. Обзор стандартного фильтра
- 2. Правила для подключения к роутеру через IPSec
- Правила для трафика через VPN соединение



Правила фильтра firewall для IPSec трафика (defconf)

	admin@192	2.168.88.1 (MikroTik) - WinBox v6	.44.3 on mA	P lite	(mipsbe)	
ngs Dashb	oard						
fe Mode	Session: 192.168.88.1						CPU: 0% 📕 🛅
iet	Firewall	New Firewall Rule					
AN	Filter Rules NAT Mar	General Advanced E	xtra Action St	atistics		ОК	
ces	+- / *	Chain:	input		₹	Cancel	input Ŧ
is	# Action Chair	Src. Address:			•	Apply	ut. I In. Int 🔻
	;;; defconf: accept es	Dst. Address:	123.45.67.8		•	Disable	
	;;; defconf: drop inva	Protocol:		-		Comment	
	;;; defconf: accept IC	Src. Port:]•	Сору	
1	;;; defconf: drop all n	Dst. Port:	500.4500			Remove	
	4 🗶 drop input	Any, Port:			•	Reset Counters	!LAN
5		In. Interface:			- •	Reset All Counters	
		Out. Interface:		Comment	For Net	u Firewall Dule	
5		In. Interface List:		Allow UDP	9500,4 7.8	500 IPSec for	ОК
Þ		Out. Interface List:					Cancel
erminal		Packet Mark:				<u></u>	
n		Connection Mark:			-		
upout.rif		Routing Mark:			-		
	A items out of 11	Routing Table:			-		•
inBox		Connection Tunor			-		
		Connection Type:					
		Connection State:			•		
		Connection NAT State:			•		
		enabled					
					-		

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"

Правила фильтра firewall для IPSec трафика (defconf)

admin@1	92.168.88.1 (MikroTik) - WinBo	ox v6.44.3 on mAP lite (n	nipsbe)	
Settings Dashboard				
Safe Mode Session: 192.16	8.88.1		с	PU: 1% 📕 🛅
Quick Set	New Firewall Rule			
CAPSMAN	General Advanced Extra Adv	tion Statistics	ОК	
Interfaces Firewall	Chain: input	Ŧ	Cancel	
Wireless Filter Rules N	AT Src. Address:	•	Apply	
Bridge 🕂 🗕 🖌	X Det Address 122	15 67 0		input Ŧ
PPP # Action	0 DSC. Address. [] [23.		Disable	. Out. I 🔻
5witch ;;; derconr: a	ir Protocol: ipsec	-esp 🔻 🔺	Comment	
Mesh ;;; defconf: c	Src. Port:	Ψ	Сору	
(P);;; defconf: a	ccep Dst. Port:		Remove	
Routing 3 Vaco	in if		Reset Counters	
ystem 7 ,,,, derconn. c	p ir			!LA
jij Allow UDP	500, In. Interface:		Reset All Counters	
	Out. Interface:	•		
	In. Interface List:	Comment for New Firev	vall Rule	
Tools	Out. Interface Lict:	Allow IPSec-esp for 12	3.45.67.8	ок
New Terminal 5 items out of 12	2(1 s		G	ancel
MetaROUTER	Packet Mark:		*	
Partition	Connection Mark:			
Make Supout.rif	Routing Mark:	•		
Manual	Routing Table:			
New WinBox	isosang isosof			
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"

Порядок правил фильтра firewall для IPSec трафика (defconf)

INPUT chain

Поднимаем **ассерt** правила выше **drop**

•	admir	n@192	2.168.88	3.1 (N	likroTik)	- WinBox ve	6.44.3 on mA	P lite (mip	sbe)		
Settings Dashb	oard										
Safe Mode	Session: 19	92.168.8	8.1							CP	U:1
Quick Set											
AP <man< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></man<>											
Interfaces	Firewall										
Wireless	Filter Rules	s NAT	Mangle	Raw	Service Po	orts Connect	ions Address Li	ists Layer7	Protocols		
Bridge	+ -	v >	(🖅	7	00 Rese	t Counters	00 Reset All Co	unters		Find	in
PPP	# A	ction	Chain	Sro	. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int	0
Switch	;;; defcc	onf: acce	pt establis	hed,re	elated, untra	acked					-
	1 .	🖉 acc	input								
lesh	;;; defcc	onf: drop	invalid								
P 🖹	2	Kdrop	input								
Routina 🗅	;;; derco	onr: acce	incut				1 (imm)				
Numbers N	defcc	pof: dron	all pot co	mina fr	om LAN		I (icmp)				
bystem	4 3	k dron	input	ining ii	On LAN						
Queues	::: Allow	UDP 50	0,4500 IPS	Sec for	123.45.67	.8					
iles	11 9	acc	input			123.45.67.8	17 (udp)		500,4500		
	;;; Allow	/ IPSec-e	sp for 123	.45.67	7.8						
.og	12 💊	🖌 acc	input			123.45.67.8	50 (ipsec-esp)				
RADIUS											
rools 🗅	•										
New Terminal	6 items out	of 13 (2	selected)								
netaROUTER											
Partition											
Make Supout.rif											
1anual											
New WipBoy											

•		•		adm	in@19	2.168.8	8.1 (N	/ikroTik)	- WinBox v	6.44.3 on mA	P lite (mip	sbe)			
Ses	sion	Settings	Dashb	oard											
Ŋ	0	Safe N	1ode	Session:	92.168.	88.1							CP	U:1%	
	Â	Quick Set													
	7	CAPSMAN		T ime 1											
]	Interfaces		Firewall		-		1						L	
	Î	Wireless		Filter Rule	S NAT	Mangle	Raw	Service Po	orts Connect	tions Address Lis	sts Layer7	Protocols			
	5 6 6 5	Bridge		+ -	*	×	7	00 Rese	t Counters	00 Reset All Cou	unters	[Find	input	₹
	F	PPP		# /	Action	Chain	Sr	c. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int	Out. I	-
		Switch		;;; defo	onf: acc	ept establi	shed,r	elated, untra	acked						
	0_6	Mesh		1 ::: defo	✓ acc… onf: dro	n input									
	255	IP	Þ	2	Xdrop	input									
	200	Routing	Þ	;;; defo	onf: acc	ept ICMP									
	100	Cushara	N	3 Allor	V acc	, input 10.4500 tP	Sec for	r 123,45,67	8	1 (ICMP)					
	833	System		4	Vacc	input	50010	120.10.07	123.45.67.8	17 (udp)		500,4500			
	2	Queues		;;; Allor	v IPSec-	esp for 12	3.45.6	7.8							
		Files		5	Vacc	input			123.45.67.8	50 (ipsec-esp)					
		Log);; deto	:ont: dra Verse	p all not co lipput	oming h	rom LAN							LU A
	00	RADIUS			A arop	inpac									:
\mathbf{x}	<u> </u>	Tools	Þ	4											
õ		New Termin	nal	6 items ou	t of 13 (2 selected))								
i		MetaROUT	FR	1	_		_							_	
\geq		Partition													
S		Make Supo	ut viE												
F		Manual	ucani												
Ë		Manual Naw WieRd													
0	9	Mew Winbo	~												



Nikita Tarikin / nikita@tarikin.com 🚃

Правила для трафика через VPN соединение

Настройка Firewall

Hастройка Firewall

- 1. Обзор стандартного фильтра
- 2. Правила для подключения к роутеру через IPSec
- 3. Правила для трафика через VPN соединение









Правила от VPN абонентов до LAN сети

		New Fires	wall Rule	
		General	Advanced Extra Actio	n Statistics
168.88.1 (MikroTik) - WinBox v6.44	1.3 on mAP lite (mips	be)	Address List:	
			Address List:	•
ion: 192.168.88.1		CPU: 0% 📕 🧯	yer7 Protocol:	•
ew Firewall Rule			Content:	•
Seneral Advanced Extra Action Statis	tics	ОК	nection Bytes:	
Chain: forward	T	Cancel	nection Rate:	
Src. Address: 🗌 10.0.88.0/24		Apply	MAC Address:	
Dst. Address: 🔲 192.168.88.0/24		Disable	t. Bridge Port:	
Protocol:	· · · · · · · · · · · · · · · · · · ·	Comment	h. Bridge Port:	
Src. Port:		Сору	ridge Port List:	
Dst. Port:		Remove	idge Port List:	
Any. Port:		eset Counters	IPsec Policy: in	ipsec i
In. Interface:	▼ Res	et All Counters		
Out. Interface: Comment fo	or New Firewall Rule			
In. Interface List: IKE2: Allow	ALL forward traffic from	🔺 ок		
Out Takenface List	21 CO EMMINECTION	Cancel		
		T		
Packet Mark:	•			
Connection Mark:	•			
Routing Mark:	•			
	-			
nabled				

bard Ses

FORWARD chain

FROM	VPN	to LAN accept
	VPN =	= 10.0.88.0/24
	LAN =	= 192.168.88.0/24

/ip firewall filter add chain=forward src-address=10.0.88.0/24 dstaddress=192.168.88.0/24 ipsecpolicy=in,ipsec action=accept placebefore=[find where comment~"defconf: drop all from WAN not DSTNATed"] disabled=no comment="IKE2: Allow ALL forward traffic from 10.0.88.0/24 to OFFICE network"

OK Cancel

Apply

Disable Comment Copy Remove Reset Counters

Правила от VPN абонентов до WAN

			New Firewall Rule	e	
			General Adva	nced Extra Actio	on Statistics
92.168.88.1 (MikroTi	k) - WinBox v6.44.3 on m	AP lite	(mipsbe)	s List:	
ard				s List:	
Session: 192.168.88.1			CPU: 14% 📕 🚺	tocol:	
New Firewall Rule				ntent:	
General Advanced I	Extra Action Statistics		ОК	Bytes:	
Chain:	forward	Ţ	Cancel	Rate:	
Cur Address			Carles	sifier:	
Src. Address:	10.0.88.0/24	╧╹	Apply	dress:	
Dst. Address:	0.0.0/0	▲	Disable	Port:	
Protocol:		-	Comment	Port:	
Src. Port:		-	Сору	t List:	
Dst. Port:		-	Remove	t List:	
Any. Port:		-	Reset Counters	Policy: in	₹ : ipsec ₹
In. Interface:		•	Reset All Counters	nose.	
Out. Interface:	Comment for New Fire	ewall Rule		3	
In. Interface List:	IKE2: Allow ALL forward 10.0.88.0/24 to ANY	ard traffic network	: from 🛆 OK		
Out. Interface List:					
Packet Mark:		•			
Connection Mark:		-			
Routing Mark:		•			
Dente Tables		-			

FORWARD chain

FROM	VPN	to	0	WZ	٩N	ð	acc	cej	pt
	VPN	=	1	0.	0.	. 8	8.	07	/24
	WAN	=	0	. ().(Ο.	0/	0	

OK Cancel

Apply Disable Comment Copy Remove Reset Counters

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

Правила от VPN абонентов до RouterOS

				New Firewall Rule	
				General Advanced Extra Action S	otistics OK
admi	n@192.168.88.1 (MikroTik) - \	WinBox v6.44.3 on mAP li	te (mipsbe)	Address List:	▼ Cancel
shboar	d			Address List:	▼ Apply
5	ession: 192.168.88.1		CPU: 31	ver7 Protocol:	
- 8	New Firewall Rule				Comment
- 11	General Advanced Extra A	Action Statistics	ОК	Content:	Сору
- 11	Chain: input	Ŧ	Cancel	nection Bytes:	Remove
- 1	Src. Address: 10.	0.88.0/24	Apply	inection Rate:	Reset Counters
	Dst. Address:	▼	Disable	bion Classifier:	F
	Protocol:	-	Comment	MAC Address:	
	Src. Port:		Сору	t. Bridge Port:	▼
	Dst. Port:		Remove	1. Bridge Port:	· / :
	Any, Port:		Reset Counters	idge Port List:	▼
÷	In. Interface:	_	Reset All Counters	idge Port List:	
	Out. Interface:	Comment for New Firewal	Rule		p
		IKE2: Allow ALL incoming	traffic from 📩 OK	TI S Heath	h h
	In. Interface List:	10.0.88.0/24 to this Rout	Cancel		
	Out. Interface List:		*	-	d
- 8	Packet Mark:				2
- 11	Connection Mark:				α.
í	Routing Mark:				i
	Routing Table:				
					t
	Connection Type:	-			
	Connection State:	-			
	Connection NAT State:	•			

INPUT chain

FROM VPN to RouterOS accept VPN = 10.0.88.0/24

/ip firewall filter add chain=input src-address=10.0.88.0/24 ipsecpolicy=in,ipsec action=accept placebefore=[find where comment~"defconf: disabled=no comment="IKE2: Allow ALL incoming traffic from 10.0.88.0/24 to this RouterOS"


Стандартные правила Firewall для любого FORWARD трафика в ipsec упаковке (defconf)



Настройка NAT

Обзор правила NAT стандартного Firewall (defconf)

				NAT Rule <>				
•	😑 🔵 admin@1	92.168.88.1 (Mikro	oTik) - WinBox v6.44.3 on mAP lite	e (mipsbe)	General Advanced Extra Action Statistics		ОК	
Ses	sion Settings Dashb	oard			Src. Address List:	-	Cancel	
ø	Cafe Mode	Session: 192.168.88	.1	CPU: 1%	Dst. Address List:	-	Apply	
	🔏 Quick Set	NAT Rule <>			Laver7 Protocol:	-	Disable	
	I CAPSMAN	General Advanced	Extra Action Statistics	ОК			Comment	
	🛲 Interfaces	Chain:	srcnat 🗧	Cancel	Content:	•	Conv	
	🤶 Wireless	Src. Address		0 contra	Connection Bytes:	-	Remove	
	😹 Bridge	Dit. Address.		- whhix	Connection Rate:		Reset Counters	
	E PPP	Dst. Address:	· · · · · · · · · · · · · · · · · · ·	Disable	Per Connection Classifier:	-	Reset All Counters	
	🙄 Switch	Protocol:	▼	Commen	Src. MAC Address:	•	Reset Mil Counters	
	°13 Mesh	Src. Port:		Сору	Out Bridge Port:			
	IP	Deb Devis		Remove	In Bridge Port			
	🎉 Routing 🛛 🗅	Dst. Port:		Deeph Course	an. bruge Port:			
	System ▷	Any. Port:	_	Reset Coun	In. Bridge Port List:	-		
	👳 Queues	In. Interface:	▼	Reset All Cou	Out. Bridge Port List:			
	Files	Out. Interface:	▼		IPsec Policy: out	T A		
	E Log			-	TI S Horty			
	2 RADIUS	In. Interface List:	*		enabled			
š	💥 Tools 🔹 🗅	Out. Interface List:	WAN ¥					
ĕ	New Terminal	Dacket Mark					psec-out:	
Nir		Fackeci/lank;	· · · · · · · · · · · · · · · · · · ·					
S	🕗 Partition	Connection Mark:	T					
6	📙 Make Supout.rif	Routing Mark:	▼					
te te	🥶 Manual	D						
2	🕒 New WinBox	enabled			Ni	kita '	Tarikin / n	



Обзор правила NAT стандартного Firewall (defconf)

				New NAT Ru	ule Advanced Extra	Action Statistics								
Ma	ickapa	General	a Address Lists	Action Statistics		Capital						(III)		
		Dst	t. Address List:			Apply	New NAT Rule							
								Disable	General Ad	vanced Extra	Action	Statistics		
admin@1	92 168 88 1 (Mik	roTik) - WinBox v6 44 3 on mAP	lite (minshe)	La	ayer7 Protocol:		•	Commer	Action	n: masquerade	•		Ŧ	
n Settings Dashb	oard		ine (impose)		Content:		•	Copy						
Cafe Mode	Session: 192.168.88	3.1	CPU:2%	Con	nnection Bytes:		•	Remove						
4 Ouick Set	New NAT Rule				onnection Rate:		•	Reset Cour	Log Prefix	a			~	
	General Advanced	Evtra Action Statistics			ction Classifier:			Reset All Cou	To Dorb					
Interfaces	Advanced			Src.	. MAC Address:		•		TO PORE	" <u> </u>				
_ Wireless	Chain:	srcnat	Cancel	^	ut. Bridge Port:		•	1						1
🗧 Bridge	Src. Address:	10.0.88.0/24	Apply	I	In. Bridge Port:		•							
PPP	Dst. Address:		Disable	In. B	Bridge Port List:		•							
🗄 Switch	Protocol:		✓ Comment)ut. B	Bridge Port List:		•							
8 Mesh	Src. Port		- Сору		IPsec Policy: out	: Tone	∓ ▲							
E IP D	Det Berti		- Remove	- 10	TLS Host:		-							
🕏 Routing 🛛 🗅	Dsc. Port:		Parah Cauptar		Ingress Priority:	-								
🖟 System 🗈	Any, Port:		Reset Counter:	5	Priority:	/im	, f-	irourl	1 +		200-1	ooforo	-0	
Queues	In. Interface:		Reset All Counte	ers	DSCP (TOS):	/ 1) <u> </u>	LLEWal	I nac	auu pi	ace-i	Jerore	-0	
Files	Out, Interface:		•			cha	ain=	=srcna	it src-	addres	s=10	.0.88.	0/24	
	In Interface List:		•			out		nterfa	ce-lis	+=WAN	inse	<u>~</u> _		
	Out. Tabarface List.		•								-P-0-0	- ,		
New Terminal	Out, Interrace List:	L WAN				bol	llCl	y=out,	none a	ction=	masq	uerade		
	Packet Mark:	Comment for New NAT Rule		×		com	nmer	nt="MS	SQRD IK	E2:10.	0.88	.0/24	>	
Partition	Connection Mark:	MSQRD IKE2:10.0.88.0/24> WAN	I traffic 📩 OK			Ta7 75 151	⊤ + -		. 11					
Make Supout.rif	Routing Mark:		Cancel			WAN		Calll						
Manual	Routing Tables		~											
New WinBox	Koucing rable:							-				-		
Exit	Connection Type:		-											
								N	likita T	arikin /	/ niki	ta@tari	kin.co	m 💻

admin@1	92 168 88 1 (MikroTik) - WinBox v6 44 3 on m4	Plite	(mipshe)	
Settings Dasht	ooard	ir nice i	(mpsbe)	
Safe Mode	Session: 192.168.88.1		CPU: 0% 🔳 🗃	-
Ouick Set	New NAT Rule			dress Li-
CAPSMAN	General Advanced Extra Action Statistics			dress Lis
Interfaces	Chain: except	Ī	Grand	Protoc
Wireless			Cancer	2
Bridge	Src. Address: 10.0.88.0/24		Apply	Conter
PPP	Dst. Address:	•	Disable	tion Byte
Switch	Protocol:		Comment	Classifi
Mesh		-	Copy	Addres
IP D	Src. Port:		Сору	idea De
Routing D	Dst. Port:		Remove	idae Po
System 🔿 👌	Any. Port:		Reset Counters	loge ro
Queues	In. Interface:	-	Reset All Counters	Port Li
Files	Out. Interface: ether1	Ŧ 🔺		Port Li
Log				sec Polic
RADIUS	In. Interface List	rt traffic		TLS Ho
Tools 📃 🗅	Out. Interface List		- <u> </u>	s Priorit
New Terminal			Cancel	Priorit
MetaROUTER	Packet Mark		v	CP (TO:
Partition	Connection Mark:	•		
Make Supout.rif	Routing Mark:	•		ľ
Manual	Routing Table:			

Naw We Dave

New NAT Rule General Advanced Extra Action Statistics Action: src-nat Log Log Prefix: To Addresses: 123.45.67.8 To Ports:

/ip firewall nat add place-before=0
chain=srcnat src-address=10.0.88.0/24
out-interface=ether1 ipsecpolicy=out,none action=src-nat toaddresses=123.45.67.8 comment="SRC-NAT
IKE2:10.0.88.0/24 --> ether1 traffic"

Nikita Tarikin / nikita@tarikin.com

SRC-NAT VPN трафика (рекомендуется)

Поднимаем SRC-NAT или MSQRD NAT правило выше стандартного

	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)
ession Settings Dashb	oard
🔿 🍳 🛛 Safe Mode	Session: 192.168.88.1 CPU: 2% 🔳 🎰
A Quick Set	Firewall
	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Laver7 Protocols
	- Carl Caupters Do Recet All Coupters
T Wireless	
Ster Decides	# Action Chain Stc. Address Dsc. Address Proc Stc. Port Dst. Port In. Int Out. I In. Int Out. I. ▼
and bridge	70 ≓ll ma… srcnat 10.0.88.0/24 WAN
PPP	;;; defconf: masquerade
🛫 Switch	1 Filma srcnat WAN
°t¦8 Mesh	
255 IP 🗅	
😹 Routing 🛛 🗅	
💮 System 🔹 🗅	
🙊 Queues	
Files	
E Log	
🧟 RADIUS	
< 🏹 Tools 🔹 🕅	
📰 New Terminal	
🔜 MetaROUTER	
Partition	
A Make Supout.rif	
	1

Hастройка TCP MSS

План действий

- 1. Объяснение MTU и фрагментации IP пакетов
- 2. Объяснение IPSec MTU
- 3. Объяснение TCP MSS
- 4. Настройка TCP MSS через IKE2









IP packet

IP	DATA
20 bytes	1492 bytes

IPSec ESP packet (tunnel mode)



IPSec ESP packet (tunnel mode)



IPSec ESP packet with NAT-T (tunnel mode)



IPSec ESP packet with NAT-T (tunnel mode)



TCP Segment size = MTU - 40 bytes









om 📒



Коррекция TCP MSS от IPSec IKE2 адресов

					🗧 😑 🗧 admin	n@19	2.168.88.1 (MikroTik) - WinBox v6.44.3 o	n mAP	lite (mipsbe)
		0 4 0 0 0 4 (MilmaTile	N/1-D0.44.0		Session Settings	Dashb	pard		CD11 001
 aur 	nin@19	2.168.88.1 (MIKFOTIK	.) - WINBOX V0.44.3 OI	n map iii	e (mipsbe)	Jae	Session: 192.106.00.1		CPU:0%
Setting	s Dashb	oard					General Advanced Extra Action Statistics	,	OK
Safe	e Mode	Session: 192.168.88.1		(:PU: 2%		Str. Address List:	1.	Cancel
Quick Sel	t	New Mangle Rule			E ×		Dst. Address List:		Annly
CAPsMA	N	General Advanced Ex	ktra Action Statistics		OK				- apper
Interface	85	Chain:	forward	I	Cancel		Layer7 Protocol:	•	Disable
Wireless		Src. Address:	10.0.88.0/24		Apply		Content:	•	Comment
Bridge					UPP17	Þ	Connection Bytes:]• }	Demove
PPP		Dst. Address:			Disable	Þ	Connection Rate:	-	Reset Counte
Switch		Protocol:	tcp Ŧ	1 4 [Comment		Per Connection Classifier:	•	Reset Al Count
Mesh		Sec. Borts			Copy		Src. MAC Address:]• }	
IP	\square	Sic. Porc.			Demous		Out. Bridge Port:	-	
Routing	Þ	Dst. Port:		. -	Remove		In. Bridge Port:	•	
System	Þ	Any, Port:		- _	Reset Counters	₽.	To Riidas Dart List	-	/ i
Queues		In. Interface:		▼ F	Reset All Counters	al R	Out, Bridge Port List:	-	
Files		Out. Interface:		-					ms
Log						t.rif	IPsec Policy: in 🔻 : ipsec 🔻	^	2
RADIUS		In. Interface List:		-			TLS Host:	•	au
Tools	Þ	Out. Interface List:		-			Ingress Priority:	-	fl
New Terr	minal			1			Priority:	•	
MetaROl	JTER	Packet Mark:		~			DSCP (TOS):]•	po
Partition		Connection Mark:		-			TCP M55: 1 0-1360	•	co
Make Sup	oout.rif	Routing Mark:		-			Packet Size:	•	
Manual		Routing Table:		-			Random:	•	10
New Win	Box						TCP Flags: Syn	•	
Exit		Connection Type:		-			Invert		
		Connection State:		-			■ ICMP Options		
		Connection NAT State:		-					

General Advanced Extra Action Statistics CAP\$MAN 0% OK Β× Interfaces Action: change MSS Ŧ Cancel T Wireless OK Apply Log 🗧 Bridge Cancel Log Prefix: -Disable 💼 PPP Apply 🙄 Switch Comment New TCP MSS: 1360 Ŧ Disable 12 Mesh Passthrough Copy omment 5 IP Comment for New Mangle Rule Copy 🙉 Routing IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY OK Remove 💮 System 🗬 Queues Cancel et Counters Files All Counters Log DADE /ip firewall mangle add action=changemss chain=forward new-mss=1360 srcaddress=10.0.88.0/24 protocol=tcp tcpflags=syn tcp-mss=!0-1360 ipsecpolicy=in, ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY"

Session: 192,168,88,1

Session

C⁴

🖀 Quick Set

5

Settings Dashboard

Safe Mode

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

CPU: 3%

Ы×

Коррекция TCP MSS до IPSec IKE2 адресов

_			😑 😑 🔵 admin@1	92.168.88.1 (MikroTik) - WinBox v6.	.44.3 on mAP
admin@19	2.168.88.1 (MikroTik) - WinBo	x v6.44.3 on mAP I	ite (mipsbe)	hoard	
Settings Dashb	oard			Session: 192.168.88.1	
Safe Mode	Session: 192,168,88,1		CPU:2%	New Mangle Rule	
				General Advanced Extra Action Sta	tistics
Quick Set	New Mangle Rule			Src. Address List:	•
CAPSMAN	General Advanced Extra Action	n Statistics	ОК	Dst. Address List:	•
Interfaces	Chain: forward	₹	Cancel	Layer7 Protocol:	-
Wireless	Src. Address:		Apply	Content:	
Bridge		ala4	- 1997-17	Corportion Bytes:	
PPP	Dst. Address: 10.0.00	.0/24	Disable	Connection Bate:	
Switch	Protocol: 6 (tcp)		Comment	Per Concection Classifier:	
Mesh	Size Boxti		Conv	Srr. MAC Address:	
IP D	Srt. Port:				
Routing D	Dst. Port:	▼ [Remove	Out. Bridge Port:	-
System	Any. Port:	▼	Reset Counters	In. Bridge Port:	•
Oueues	In. Interface:	•	Reset All Counters	In. Bridge Port List:	•
Files	Out Interface:			Out. Bridge Port List:	•
Log				These Delivery as A The	
PADIUS	In. Interface List:	•		TIS Hort	Sec
Tools	Out. Interface List:				
New Townload				Ingress Priority:	•
New Terminal	Packet Mark:			Priority:	•
MetaROUTER	Connection Mark:			DSCP (TOS):	-
Partition				TCP MSS: 1 0-1360	^
Make Supout.rif	Routing Mark:	•		Packet Size:	-
Manual	Routing Table:	•		Random:	•
New WinBox				TCP Flags	T A
E×it	Connection Type:			Invert	•
	Connection State:	•			
	Connection NAT State:	•			

🔴 😑 🌒 admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)										
Ses	Session Settings Dashboard									
Ю	C¥ Safe Mode	Session: 192.168.88.1	CPU: 1% 📕 🛅							
	http://www.com/action/a	New Mangle Rule	D×							
	CAPSMAN	General Advanced Extra Action Statistics	ОК							
	🕅 Interfaces	Action: change MSS	Cancel							
	🧵 Wireless		Apply							
	😹 Bridge	Log								
	📑 PPP	Log Prefix:	Disable							
	🙄 Switch	New TCP MSS: 1360	Comment							
	ଂଧ୍ୱ Mesh	✓ Passthrough	Сору							
	🚳 IP 🛛 🗅									
	🔀 Routing 🛛 🗈	Comment for New Mangle Rule								
	💮 System 🗈	IKE2: Clamp TCP MSS from ANY to 10.0.88.0/24	OK punters							
	룢 Queues		Cancel Counters							
	📄 Files	<u> </u>								
	📄 Log									
	O DADTUS									

CPU: 1%
CPU: 1%
CPU: 1%
CPU: 1%
COK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset Counters

/ip firewall mangle add action=changemss chain=forward new-mss=1360 dstaddress=10.0.88.0/24 protocol=tcp tcpflags=syn tcp-mss=!0-1360 ipsecpolicy=out,ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from ANY to 10.0.88.0/24"

Настройка клиентов

Nikita Tarikin / nikita@tarikin.com

Windows 8 / 8.1 / 10

План действий

- 1. Импорт SSL сертифкатов
- 2. Настройка IKEv2 соеденения
- 3. Проверка маршрутов IKEv2



Скачать .p12 сертификат



Выбрать Local Machine хранилище —> Далее

		ອັ Windows 10 x64	ð
ecycle B	Certificate Import Wizard	×	
	Private key protection		
	To maintain security, the private key was protected with a p	password.	
	Password:		
	Import options: Enable strong private key protection. You will be pron private key is used by an application if you enable this Mark this key as exportable. This will allow you to back keys at a later time. Protect private key using virtualized-based security(N	mpted every time the is option. ck up or transport your Non-exportable)	
	☑ Indude all extended properties.	Next	
		TVEXL Cancel	
Q		へ 回 即 (J)) ^{2:24 PM}	



->Далее

••			জ Windows 10 x64	ð
cycle B ←	🐓 Certificate	Import Wizard	×	
	Certificate Sto Certificat	ore e stores are system areas where certificates a	are kept.	
	Windows the certif	can automatically select a certificate store, or icate.	you can specify a location for	
		ce all certificates in the following store rtificate store:		
			Browse	
			Next Cancel	
Q	Hi 🏒		へ 回 臣 (小) 2:24 PM [

Автоматический выбор —> **Далее**



SSL сертификат успешно импортирован —> **OK**

Nikita Tarikin / nikita@tarikin.com

Windows 10: Импорт SSL сертификатов

Network and Sharing Center		- 0	×				
🕂 🔿 👻 🛧 🙀 " Network	> Network and Sharing Center	Search Control Panel	Q				
Control Panel Home	View your basic network in connections	formation and set up					
Change adapter settings Change advanced sharing	View your active networks	View your active networks					
settings	Network 6	Access type: Internet					
Media streaming options	Private network	Connections: <i>I</i> Ethernet0					
	Troubleshoot problems Diagnose and repair netw information.	ork problems, or get troubleshooting	I				
See also							
Infrared							
Infrared Internet Options							



-> Панель управления -> Сеть и интернет -> Центр управления сетями

Создание нового подключения







へ 🗉 🖫 🖤

Q ∐i

.

II G & · · B P · · · · · · · · · · · · · · · ·	Windows 10 x64 Image: Organization - Image: Organization	Свойства -> Безопасность
Par ← → ~ ↑ ✿ * Network > Network and Sharing Center ✓ O Search ad Control Pan ↓ C @vpn.ike2.xyz Properties × ad Change add Orga General Options Security Networking Sharing tree Change add Orga Type of VPN: KEv2 ✓ ✓	Control Panel	Шифрование данных:
Media streat Advanced settings Data encryption: Data encryption (disconnect if server declines) Authentication Use Extensible Authentication Protocol (EAP) Properties	Internet C1@vpn.ike2.xyz No Internet access Ethernet0	Самое стойкое Проверка подлинности: Использовать
Use machine certificates	or set up a router	сертификаты компьютеров
O See also Infrared Internet Op Windows D 3 iter Windows D	oubleshooting	—> OK

へ 💷 হ 🗤 2:45 PM

 \Box

Явный выбор сертификата для IKEv2 соединения

Set-VpnConnection -Name "cl@vpn.ike2.xyz" MachineCertificateIssuerFilter 'C:\mycerts\CA.crt'

Через уточнение издателя авторитета СА
Windows 10: проверка IKEv2 VPN соединения



Windows 10: проверка IKEv2 VPN маршрутов

р Ц

	3 ↔	⊟ @ »	🖻 Wir	ndows 10 x€	64 🗇	route -4 p	rint.	
🔤 Command Prompt				-	o ×	10000 1 p		
C:\Users>route -4	print				^			
Interface List 900 Oc 29 e6	e6 ceIntel(R) 82574L Gigabit	t Network Connect	tion		Destination		
25 600 50 56 fc 1	с1@vpn fe e4Вlueto Softwa	.1Ke2.xyz oth Device (Perso re Loopback Inter ====================================	onal Area Networl rface 1	<) 			0.0.0.0/0	(default)
IPv4 Route Table						Gateway:		
Active Routes:							On-link	
Network Destinatio	n Netmask	Gateway	Interface	Metric			-	
<u> </u>	aaaa	192 168 88 1	192 168 88 252	4250				
0.0.0.0	0.0.0.0	On-link	10.0.88.2	26				
10.0.88.2	255.255.255.255	UN-IINK	10.0.88.2	281		Interface:		
123.45.67.8	255.255.255.255	192.168.88.1	192.168.88.252	4251				
127.0.0.0	255.0.0.0	On-link	127.0.0.1	4556			10.0.88.2	
127.0.0.1	255.255.255.255	On-link	127.0.0.1	4556			10000002	
127.255.255.255	255.255.255.255	On-link	127.0.0.1	4556				
192.168.88.0	255.255.255.0	On-link	192.168.88.252	4506				
192.168.88.252	255.255.255.255	On-11nk	192.168.88.252	4506		Motric (dist	ance).	
192.168.88.255	255.255.255.255	On-link	192.108.88.252	4506				
224.0.0.0	240.0.0.0	On link		4556			26	
224.0.0.0	240.0.0.0	On-link	10 0 99 2	4500			20	
255 255 255 255	240.0.0.0	On-link	127 0 0 1	4556				
255.255.255.255	255.255.255.255.255	On-link	192.168.88.252	4506				
255.255.255.255	255.255.255.255	On-link	10.0.88.2	281				
					~			

へ 🖻 🏷 🗤 2:55 PM

 \Box

Windows 10: проверка IKEv2 VPN маршрутов

	admin@192.168	3.88.1 (MikroT	ik) - Winl	Box v6.4	4.3 on mAP	lite (mipsbe)			
ashbo	ard									
de	Session: 192.168.88.	1						CPL); 1% 📕 🖥	
	IPsec									
	Policies Proposals	Groups	Peers	Identities	Profiles	Remote Peers	Mode Configs	Installed SAs	Keys	
_	4 - 7								Find	
	Name 🖌	Resp	Addres	ss Pool	Address	Address Pr	Split Include	Syste	em Sr 🔻	
	modeconf vpn.ik	yes	pool v	pn.ike2.xyz		32	192.168.99.0/2	24, 17 yes		
	request-only	no								
		IPsec	: Mode (Config <mod< th=""><th>leconf vpn</th><th>.ike2.xyz></th><th></th><th>×</th><th></th><th></th></mod<>	leconf vpn	.ike2.xyz>		×		
				Name	modecon	Funn ike? yuz	OK	1		
\land				riamo.	Doctoria	ndor		-		
\square					I Kespui	luer	Cancel			
⊳			Ad	dress Pool:	pool vpn.	ike2.xyz 👅 🔺	Apply			
	•	-		Address:		•	Сору	1	•	
	2 items (1 selected)	Add	ress Pre	fix Length:_	32		Remove	i		
	<u>'</u>		Sr	lit Include:	192,168.	99.0/24				ĺ
Þ					172.16.0	.0/22	;			
					10.20.0.0)/21	;			
				Ľ	Systen	n DNS				
·										

.rif

•••	\$ ↔	»	🖻 Wir	ndows 10	x6
👞 Command Prompt				_	ć
IPv4 Route Table					
Active Routes:					
Network Destinatio	n Netmask	Gateway	Interface	Metric	
0.0.0.0	0.0.0.0	192.168.88.1	192.168.88.252	4250	
0.0.0.0	0.0.0.0	On-link	10.0.88.2	26	
10.0.88.2	255 255 255 255	On-link	10 0 88 2	281	
10.20.0.0	255.255.248.0	On-link	10.0.88.2	26	
16.20.1.200	200,200,200,200	On-link	10.0.00.2	7 97	
123.45.67.8	255.255.255.255	192.168.88.1	192.168.88.252	4251	
127.0.0.0	255.0.0.0	On-link	127.0.0.1	4556	
127.0.0.1	255.255.255.255	On-link	127.0.0.1	4556	
127.255.255.255	255 255 255 255	On link	127 0 0 1	1000	
172.16.0.0	255.255.252.0	On-link	10.0.88.2	26	
172,16,3,255	255.255.255.255	On-⊥1nk	10.0.88.2	281	
192.168.88.0	255.255.255.0	On-link	192.168.88.252	4506	
192.168.88.252	255.255.255.255	On-link	192.168.88.252	4506	
1 <mark>92 168 88 255</mark>	255 255 255 255	On-link	197 168 88 757	4506	
192.168.99.0	255.255.255.0	On-link	10.0.88.2	26	
192.108.99.200	255.255.255.255	Un-link	10.0.00.2	201	
224.0.0.0	240.0.0.0	On-link	127.0.0.1	4556	
224.0.0.0	240.0.0.0	On-link	192.168.88.252	4506	
224.0.0.0	240.0.0.0	On-link	10.0.88.2	26	
255.255.255.255	255.255.255.255	On-link	127.0.0.1	4556	
255.255.255.255	255.255.255.255	On-link	192.168.88.252	4506	
255.255.255.255	255.255.255.255	On-link	10.0.88.2	281	

Persistent Routes:

None

Windows 10: проверка IKEv2 VPN маршрутов

-0.0.0/0 **???**

Address:		Сор
Address Prefix Length:	32	Remo
Split Include:	192.168.99.0/24 🔷	
	172.16.0.0/22 🗢	
	10.20.0.0/21	
	System DNS	

••	• 11 6	₹} ↔>	_ @ »	🖻 Wir	ndows 10 :	x64	Ō
es. Com	mand Prompt				_	٥	×
IPv4 R	oute Table						
====== Active	Routes						
Networ	k Destination	n Netmask	Gateway	Interface 192 168 88 252	Metric 4250		
	0.0.0.0	0.0.0.0	On-link	10.0.88.2	26		
	10.0.88.2	255.255.255.255	UN-11NK	10.0.88.7	281		
	10.20.0.0	255.255.248.0	On-link	10.0.88.2	26		
	10.20.7.255	255.255.255.255	Ūn-link	10.0.88.2	281		
	123.45.67.8	255.255.255.255	192.168.88.1	192.168.88.252	4251		
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	4556		
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	4556		
127.	255.255.255	255.255.255.255	<u>On-link</u>	127.0.0.1	4556		
	172.16.0.0	255.255.252.0	On-link	10.0.88.2	26		
1	72.16.3.255	255.255.255.255	On-link	10.0.88.2	281		
1	92.168.88.0	255.255.255.0	On-link	192.168.88.252	4506		
192	.168.88.252	255.255.255.255	On-link	192.168.88.252	4506		
192	168.88.255	255.255.255.255	<u>On-link</u>	192.168.88.252	4506		
1	92.168.99.0	255.255.255.0	On-link	10.0.88.2	26		
192	.168.99.255	255.255.255.255	On-link	10.0.88.2	281		
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	4556		
	224.0.0.0	240.0.0.0	On-link	192.168.88.252	4506		
	224.0.0.0	240.0.0.0	On-link	10.0.88.2	26		
255.	255.255.255	255.255.255.255	On-link	127.0.0.1	4556		
255.	255.255.255	255.255.255.255	On-link	192.168.88.252	4506		
255.	255.255.255	255.255.255.255	On-link	10.0.88.2	281		
Persis	tent Routes:						

None

Windows 10: отключаем пересылку всего трафика через IKEv2 VPN



Windows 10: отключаем пересылку всего трафика через IKEv2 VPN

Network Connections Internet Protocol Version 4 (TCP/IPv4) Properties This con Internet Protocol Version 4 (TCP/IPv4) Properties This con Internet Protocol Version 4 (TCP/IPv4) Properties Advanced TCP/IP Settings You can get IP settings assigned automatically if your network administrator for the appropriate IP settings. Obtain an IP address automatically Obtain an IP address automatically Obtain DNS server address automatically Obtain DNS server address automatically Ouse the following DNS server addresses: Outomatic metric Automatic metric Automatic metric	•••		◙ Windows 10 x64
Image:	Network Conn cl@vpn. C General O This con	ike2.xyz Properties X v pptions Security Networking Sharing tion Internet Protocol Version 4 (TCP/IPv4) Properties	→ □ × Search Network Connections ♪
wide a	inis con	General You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. O Utain an IP address automatically Use the following IP address: IP address: IP address: Use the following DNS server addresses:	Advanced TCP/IP Settings IP Settings DNS WINS This checkbox only applies when you are connentwork and a dial-up network simultaneously, data that cannot be sent on the local network is dial-up network. Use default gateway on remote network Disable class based route addition
Alternate DNS server:	vide e acrost	Preferred DNS server:	Interface metric:

Свойства -> Сеть

Свойства TCP/IPv4 Получить IP адрес автоматически
 Получить адрес DNS автоматически

->

Дополнительно

Дополнительные параметры TCP/IP

Использовать основной шлюз

Подключение non-Windows

MacOS iOS Android RouterOS



Apple MacOS

≥ 10.11 El Capitan

План действий

- 1. Импорт SSL сертификатов
- 2. Настройка IKEv2 VPN соединения
- 3. Проверка IKEv2 VPN маршрутов

MacOS: Импорт SSL сертификатов



Скачать .p12 сертификат

MacOS: Импорт SSL (сертификатов	
		Export Certificate: c1@vpn.ike2.xyz Cancel Export Passphrase: ++++++ Keep in secret mn.ike2.xyz
Add Certificates		: ct@vpn.ke2
Certificate(s) fro "c2@vpn.ike2.xyz.p12" to a keychain?	Enter the password for "c2@vpn.ike2.xyz.p12": Password: Show password Cancel OK	Keychain: login (default)
Keychain:	login ᅌ	Type your
View Certificates	Cancel Add	SSL certificate password
		—> OK





Keychain access

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



• • •	ca.ike2.xyz
Certificate Certi	z te authority day, May 29, 2029 at 7:48:56 PM Indochina Time z ^e certificate is not trusted
▶ Irust	
Details Subject Name	
Country or Persion	MY
State/Province	Selanger
Locality	Cuberiava
Organization	IKF2.xvz
Common Name	ca.ike2.xvz
	een nom ny m
Issuer Name	
Country or Region	MY
State/Province	Selangor
Locality	Cyberjaya
Organization	IKE2.xyz
Common Name	ca.ike2.xyz
Serial Number	5701666201070268944
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Saturday, June 1, 2019 at 7:48:56 PM Indochina Time
Not Valid After	Tuesday, May 29, 2029 at 7:48:56 PM Indochina Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : E3 BB 56 44 1C 84 EE F4
Exponent	65537
Key Size	2,048 bits
	Frances Marile Marr

Signature 256 bytes : A8 3F AF 12 D3 AF 15 87 ...



Keychain access

Verify CA certificate details







Сверяем **отпечатки** СА сертификата







Keychain access







		ca.ike	2.xyz				
Certificate	ca.ike2.xyz Root certificate au Expires: Tuesday, & "ca.ike2.xyz" ce	uthority May 29, 202 ertificate is r	29 at 7:48:56 P not trusted	M Indoc	china Time		
Wh	en using this certifi	icate: Use	Custom Setting	gs 🗘	?		
Secu	re Sockets Layer (SSL) Nev	er Irust				
	Secure Mail (
Extensibl	e Authenticati						
	IP Securit Code		You are mak Trust Settin Enter your pas	t ing ch a gs. sword to	anges to you	r Certificate	
	X.509 Bas		User Name:	Vicky			
Details			Password:	••••		•••••	
					Cancel	Update Settings	



Keychain access

Type your MacOS password -> Update settings

● ● ○ **〈** 〉 Ⅲ Q VPN 8 System Preferences VPN options VPN on Demand Advanced VPN options Connect or disconnect VPN THE R. L. Network 11 (1:



System preferences -> Network



Unlock to make changes

) • 0 < >	Network Select the interface and enter a name for the new service	Q VPN 😵	Create new connection
• Wi-Fi Connected	Interface: VPN VPN Type: IKEv2 Service Name: c2@vpn.ike2.xyz	 Ni-Fi Off and has the 	
	Cancel Cr Automatically join Ask to join new new Known networks will b no known networks ar to manually select a n	eate	Interface: VPN VPN Type: IKEv2 Service name: c2@vpn.ike2.xyz -> Create
+ - *	✓ Show Wi-Fi status in menu bar	Advanced ?	
Click the loo	k to prevent further changes.	Revert Apply	Nikita Tarikin / nikita@tarikin.com

	Network	Q VPN	8				
Location:	Automatic	0		New IPsec Identity			
• Wi-Fi Connected	Status: Not Connected			Peer: Auth. Method:	peer 123.45.67.8 rsa signature	¥	Ok Can
• c2@vpn.ike2.xyz Not Connected				Certificate: Remote Certificate:	vpn.ike2.xyz c2@vpn.ike2.xyz	= \$	App Disal
	Server Address: vpn.ike2.xyz			Policy Template Group: Notrack Chain:	group vpn.ike2.xyz	Ŧ	Comm
	Remote ID: vpn.ike2.xyz	7	<	My ID Type:	auto	-	Rem
	Authentication	Settings		Remote ID Type:	user fqdn c2@vpn.ike2.xyz	T	
	Connect			Match By: Mode Configuration:	certificate modeconf vpn.ike2.xy;	z ∓ 🔺	
				Generate Policy:	port strict	•	
+ - *	Z Show VPN status in menu bar	Advanced ?					
Click the lock to prevent fur	ther changes.	Revert Apply					

••• • • •	Network	Q VPN	Oreste nour connection
Locat	tion: Automatic	3	Create new connection
• Wi-Fi Connected	Status: Not Connected		
c2@vpn.ike2.xyz Not Connected			Server Address:
			vpn.ike2.xyz
	Server Address: vpn.ike2.xyz		Remote ID:
	Remote ID: vpn.ike2.xyz		vpn.ike2.xvz
	Local ID: c2@vpn.ike2.xyz		Local ID:
	Authentication Set	tings	c2@vpn.ike2.xyz
	Connect		
			✓ Show VPN status in menu bar
			-> Apply
+ - *	✓ Show VPN status in menu bar	Advanced ?	
Click the lock to prevent	t further changes.	Revert Apply	
			Nikita Tarikin / nikita@tarikin.com

	Network Q. VPN Authentication Settings: None	Authentication Settings
Wi-Fi Connected c2@vpn.ike2.xyz Not Connected	Shared Secret: Certificate: Select None selected Cancel OK OK OK	
	Remote ID: vpn.ike2.xyz Local ID: c2@vpn.ike2.xyz Authentication Settings Connect	Authentication Settings: None Certificate: -> Select
+ - *·	Show VPN status in menu bar Advanced prevent further changes. Revert	



Authentication Settings

Select machine auth certificate: c2@vpn.ike2.xyz

-> Continue



MacOS: Проверка IKEv2 VPN маршрутов

CPU: 1%	
CPU: 1%	
CPU: 1%	
SAs Ke	ys
Fil	nd
System	St 🔻
yes	
	•
	SAs Ker System yes

🔳· 🛄 00:02:49 🔶 💄

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz

✓ Default

Show Time Connected

✓ Show Status While Connecting

Open Network Preferences...

[➔ ~ netstat -nr g	grep ipsec				
default	link#23	UCSI	0	0	ipsec0
10.0.88.254	10.0.88.254	UH	3	0	ipsec0
10.20/21	10.0.88.254	UGSc	0	0	ipsec0
172.16/22	10.0.88.254	UGSc	0	0	ipsec0
192.168.99	10.0.88.254	UGSc	0	0	ipsec0
224.0.0/4	link#23	UmCSI	0	0	ipsec0
255.255.255.255/32	link#23	UCSI	0	0	ipsec0
→ ~					

MacOS: Проверка IKEv2 VPN маршрутов

admin(@192.168.88.1	(MikroTik) - WinBox	v6.44.	3 on m/	AP lite (mip	osbe)		
s Dashbo	pard								
e Mode	Session: 192.168.	88.1					CPU	3%	1
:	IPsec								×
J	Peers Identities	Profiles	Remote Peers	; Mode	Configs	Installed SA	s Keys		
s	+ - 7							Find	
	Name	Resp	Address Poo	ol	Address	Address Pr.	Split Inc	lude	-
	modeconf vpn.ik	yes	pool vpn.ike	2.xyz		3	32 0.0.0.0	/0	
	request-only	no							_
		IPsec Mode	e Config <moc< th=""><th>leconf vp</th><th>on.ike2.xy</th><th>/z></th><th></th><th>×</th><th></th></moc<>	leconf vp	on.ike2.xy	/z>		×	
			Name:	modeco	nf vpn.ike	e2.xyz	ОК		
Þ				🖌 Resp	onder		Cancel	1	
Þ		ρ	ddress Pool:	pool vp	n.ike2.xy;	2 🔻 🔺	Apply		
▶			Address:			•	Copy		
	•	Address P	refix Length:	32			Remove	1	•
	2 items (1 selected		Split Include:	0.0.0.0	/0	+	L	⁻╞	
				575	em DNS				
Þ			Static DNS:	10.0.88	3.1	\$			
ninal									
JTER									
out.rif	l	_							
Box									

🎟 00:02:49 🔶 💄

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz

✓ Default

•

Show Time Connected

✓ Show Status While Connecting

Open Network Preferences...

					-		
[→ ~ n	etstat -nr	grep ipsec					1
defaul	t	link#23	UCS	1614	0	ipsec0	
1.	9	link#23	UHW3I	0	1	ipsec0	!
1.	159	link#23	UHW3I	0	1	ipsec0	!
1.	.112	link#23	UHW3I	0	1	ipsec0	
1.	.222	link#23	UHW3I	0	1	ipsec0	1
1.	.131	link#23	UHW3I	0	1	ipsec0	· · !
1.	.22	link#23	UHW3I	0	1	ipsec0	
1.	31	link#23	UHW3I	0	1	ipsec0	!
1.	143	link#23	UHW3I	0	1	ipsec0	1
2.	156	link#23	UHW3I	0	1	ipsec0	2
2.	64	link#23	UHW3I	0	1	ipsec0	1
2.	27	link#23	UHW3I	0	1	ipsec0	!
2.	01	link#23	UHW3I	0	1	ipsec0	!
2.	204	link#23	UHW3I	0	1	ipsec0	1
2.	23	link#23	UHW3I	0	1	ipsec0	1
2.	5	link#23	UHW3I	0	1	ipsec0	1
2.	53	link#23	UHW3I	0	1	ipsec0	
2.	21	link#23	UHW3I	0	1	ipsec0	!
2.	33	link#23	UHW3I	0	1	ipsec0	1
2.	.111	link#23	UHW3I	0	5	ipsec0	1
2.	.62	link#23	UHW3I	0	1	ipsec0	!
2.	100	link#23	UHW3I	0	1	ipsec0	2
2.	95	link#23	UHW3I	0	1	ipsec0	!

Apple iOS

≥ версия 9

План действий

- 1. Импорт SSL сертификатов
- 2. Настройка IKEv2 VPN соединения

iOS: Загрузка SSL сертификатов



Download CA certificate .crt

Download client certificate .p12

iOS: Импорт SSL сертификата авторитета CA



iOS: Импорт SSL сертификата авторитета CA

18:4	5	(■ \$ h.	
Set	ttings		
Q Se	earch		
	Nikita Tarikin	18:45	ati 🗢 🔳
20	Apple ID, iCloud, iTunes & App S	Cancel Insta	all Profile Install
Profile	e Downloaded	ca.ike2.xvz	18:45
			Install Profile on iko2 war
	Airplane Mode	Signed by ca.ike2.xyz	Ca.ikez.xyz
_		Not Verified	CERTIFICATE
?	Wi-Fi	Contains Certificate	ca.ike2.xyz
*	Bluetooth	More Details	Issued by: ca.ike2.xyz Expires: 29 May 2029
((₁))	Mobile Data		_
-		Remove Do	wnloaded Profile
ල	Personal Hotspot		

18:46	ail 🗢 🔳	18:46	-
Ca.ike2.xyz	ca.ike2.xyz	<pre><ca.ike2.xyz ca.ike2.xyz<="" pre=""></ca.ike2.xyz></pre>	
SUBJECT NAME		Signature Data	
Country or Region	MY	a8 3f af 12 d3 af 15 87 66 9f 2b 89 a5 1f 35 8e 64	b4
State/Province	Selangor	c4 6a a3 c1 89 c0 2b 55 75 d3 c9 0e d7 ee 90 9b	2b
Locality	Cyberjaya	2b 15 e8 fc f3 bb e8 1e df 77 64 82 fa 02 87 bc 57 42 a1 cb 54 3a 78 e7 a0 e1 d1 77 11 eb 54 b3 06 c	79 6 b
Organisation	IKE2.xyz	5a 65 2b 5e 87 39 6f 2f cb c9 48 5b 7f 6c d0 16 8 7d 64 8f ba 17 25 58 4f 0a 5c 51 05 66 ec dc 42 5	3d 55
Common Name	ca.ike2.xyz	c7 8e 64 fc a3 b5 f5 4b 89 0b da 6d ea ec 3c 80 d ad 8f 10 59 09 dc 66 83 7f ad 80 0d 8e 38 45 02	cb 04
ISSUER NAME		77 66 e3 30 21 e7 74 1e 30 d6 b0 c2 07 60 dc 4a a4 2b 18 3c bd ee 16 01 0e cd 02 a9 cc 66 08 bd	9e ef
Country or Region	MY	3c 7c 4a f1 d9 8f 83 a0 40 04 f4 2f 49 2f 0e 98 fa	6f
State/Province	Selangor	e6 4f 20 e8 5b c1 64 a7 78 c1 39 15 7b 56 7e 52 9	30
Locality	Cyberjaya	29 15 34 55 ad 9c be 11 73 3a d6 21 9d 35	
Organisation	IKE2.xyz	FINGERPRINTS	
Common Name	ca.ike2.xyz	SHA-256	
SERIAL NUMBER		b5 7c af 68 13 b3 52 a0 ab ab aa 4e 42 f8 c5 69 4 87 57 ee da f8 30 b9 3e 4b 05 c6 d7 33 d9 4b	14
Serial Number	5701666201070268944	SHA-1	
VALIDITY PERIOD		6b a4 71 8b 3f 22 4e 3d c7 83 05 69 bf d8 94 c3 56 87 d8	38
Not Valid Before	2019-06-01, 19:48:56		
Not Valid After	2029-05-29, 19:48:56	Version	2
PUBLIC KEY INFO			

iOS: Импорт SSL сертификата авторитета CA



iOS: Импорт SSL сертификата клиента



Airplane Mode	\bigcirc		
🔊 Wi-Fi	vpn.ike2.lab	>	
Bluetooth	On 2	>	
Mobile Data	2	>	
Personal Hotspot		>	_
	Date & Time		>
Notifications	Keyboard		>
Sounds & Haptics	Language & Region		>
Do Not Disturb	Dictionary	18:55	
Screen Time		〈 General	VPN
	iTunes Wi-Fi Sync		
General	VPN	Add VPN Config	uration
Control Centre	Profiles		11 >

19:08		ail 🗢 🔳
Cancel	Add Configura	tion Done
Туре		IKEv2 >
Description	c3@vpn.ike2.xyz	
Server	vpn.ike2.xyz	
Remote ID	vpn.ike2.xyz	
Local ID	c3@vpn.ike2.xyz	*
AUTHENTICATI	ON	
User Authen	tication	None >
Use Certific	ate	
Certificate		c3@vpn.ike2.xyz >
PROXY		
Off	Manual	Auto



iOS: Подключение IKEv2 VPN



19:08		.ul 🗢 🔳
< VPN	c3@vpn.ike2.xyz	Edit
Туре		IKEv2
Server		vpn.ike2.xyz
Server Addres	S	123.45.67.8
Address		10.0.88.253
Connect Time		0:11
	Delete VPN	

Nikita Tarikin / nikita@tarikin.com

Android

версия 9 <

План действий

- 1. Установка приложения StrongSwan
- 2. Импорт SSL сертификатов
- 3. Настройка IKEv2 VPN подключения

Android: Установка StrongSwan

÷						Q	:
	stro co	ongSwan ngSwan Proj mmunication	VPN Cli ect	ent			
					IN	STALL	
Rate this	арр						
Tell others	what you t	think					
Tell others	what you t	think	\overleftrightarrow	$\widehat{\Sigma}$	Δ		
Tell others	what you t	think think W		₹ Ew	\$		
Tell others	what you the second sec	think V		£∵ w	\$		^
Develope	r contact	w	RITE A REVI	ew	1		^
Develope © W © E	r contact Vebsite	think	RITE A REVI	ж ew			^
Developer	r contact Vebsite mail	think	RITE A REVI	Ъ́.	\$		^

Найти и установить StrongSwan

через Google Play

Android: Импорт SSL сертифкатов

File Manager	4	Q	:
CATEGORIES	STO	RAGE	
STORAGE > ial storage	> Do	wnload	\rightarrow
<pre>cert_export_CA 1.36 KB 2019.06.10</pre>	.ike2.	xyz.ci	t
Extract certific	ate		
Type the password to	extrac	t the	
certificates.			
certificates.			I



Download and install

user certificate .p12
Android: Настройка IKEv2 VPN соединения





Choose certificate

The app strongSwan VPN Client has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.

- c4@vpn.ike2 CN=c4@vpn.ike2.xyz
- + Install certificate

DENY SELECT

Android: Подключение IKEv2 VPN



ADD VPN PROFILE

Status: No active VPN

c4@vpn.ike2.xyz Server: vpn.ike2.xyz User certificate: c4@vpn.ike2

Connection request

strongSwan VPN Client wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

• appears at the top of your screen when VPN is active.

CANCEL OK



ADD VPN PROFILE

Status: Connected Profile: c4@vpn.ike2.xyz

DISCONNECT

c4@vpn.ike2.xyz Server: vpn.ike2.xyz User certificate: c4@vpn.ike2

Подключение RouterOS



Загрузка и установка клиентского SSL сертификата

• Ses	el admin@19: sion Settings Dashbo	168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on	mAP lite (mipsbe)
ю	CH Safe Mode	5ession: 192.168.188.1	a
	Quick Set CAPSMAN Im Interfaces Wireless Bridge PPP	File List Image: Size File Name Type Size Cert_export_office-spb@vpn.ike2 flash disk flash/pub directory flash/skins	Find Find Creation Time B Aug/08/2019 16:38:11 Jan/01/1970 07:00:06 May/24/2017 02:38:22 Jan/01/1970 07:00:02
	Switch Switch Constant Switch Swi	Certificates Certificates SCEP Servers SCEP RA Requests OTP CRL TIMPort Card Reinstall Card Verify Revoke	Create Cert. Request Setting
	 i System i Queues i Files 	Name △ Issuer Common Name Subject	Alt Key Size Days Valid
	Log RADIUS X Tools	4 Passphrase: *******	Import Cancel
nBox	New Terminal New Terminal New Terminal		
eros Wi	Partition Make Supout.rif Manual	O items	
oute	S New WinBox		

/certificate import filename=cert_export_officespb@vpn.ike2.xyz.p12

Переименовываем установленные SSL сертификаты

		• •	admin@	192.	168.188.1	(MikroTik off	ice-spb.ike2.	xyz) - WinBo	x v6.45.3 on	mAP lite (m	ipsbe)	
	admin@102.169.199.1 (MikraTik office, onb.ike2.vvz) - WinPey v6.45	Session	Settings Dash	hboard								
ashb	oard	6	Safe Mode	Se	ssion: 192.168	8.188.1						-
	session: 192.168.188.1 File Ust File Name Certificates Certificates Certificates SCEP Servers SCEP RA Requests OTP CRL Certificates Certificates Certific		Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP Routing System Queues Files Log		ie List ie List cert_export flash flash/pu flash/ski Certificates Certificates AT ca KT of	Confice-spb@vp SCEP Servers SCEP Servers Import ame .ike2.xyz Fice-spb@vpn.ik	kup Restore Type on.ike2 p12 f disk direct direct direct SCEP RA Rec Card Reinsta Issuer C=RU,t ke2.xyz C=RU,t	Upload ile ory ory quests OTP (all Card Verif ET=Moscow O ST=Moscow O	ize 4528 E RL y Revoke Common Name ca.ike2.xyz office-spb@vp	Creation Time Aug/08/201 Jan/01/197 May/24/201 Jan/01/197 Create Cert.	<i>Find</i> 9 19 16:38:11 70 07:00:06 17 02:38:22 70 07:00:02 . Request . Request . Subject Alt. DNS:ca.ike2 Email:office-	Settings Key Siz 4096 2048
riF	Passphrase: Cancel Cancel Zitems	uterOS WinBox	Tools New Terminal Dot1X MetaROUTER Partition Make Supout.rif Manual		♦ 2 ltems	_	_	_		_	_	

Настройка нового IPSec peer profile (фаза 1)

Safe Mode Session: 192.168.88.1 CAPSMAN Image: CAP	Ses	e sion Settings Dashb	admin@192.16 nard	8.88.1 (MikroTik) - \	VinBox v6.44.3 on mAP lite	mipsbe)	
Quick Set C CAPsMAN Interfaces Proposals Grou Proposals Grou Proposals Grou Proposals Grou Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Odd Proposal Check: Proposal Check: Proposal Check:	5	Cafe Mode	Session: 192.168.8	8.1			CPU: 0% 📕 🛅
Make Supput.rif DPD Interval: 120 \$ s Image: Manual Structure DPD Maximum Failures: 5	outerOS WinBox	Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Interfaces PP Switch Interfaces Pop Switch Interfaces Pop Newsh Interfaces Pop Pop <	IPsec Proposals Grou Proposals Grou Name default 1 item	New IPsec Profile Name: Hash Algorithms: Encryption Algorithm: DH Group: Proposal Check: Lifetime: Lifebytes: DPD Interval: DPD Maximum Failures:	vrofile vpn.ike2.xyz sha256 des 3des aes-128 aes-192 aes-256 blowfish camellia-128 camellia-192 camellia-256 modp1024 modp1536 modp2048 modp3072 modp4096 modp3072 modp4096 modp144 modp8192 ecp521 ecp384 obey ▼ MAT Traversal 120 \$ s 5 5	Copy Remove	Keys Find oposal C ▼ 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

Добавление нового клиентского IPSec peer (инициатор)

/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'

Настройка нового IPSec proposal (фаза 2)

Ses	e esion Settings Dashbo	admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)	
ю	Cafe Mode	Session: 192.168.88.1	CPU: 1% 📕 🛅
outerOS WinBox	Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch PP Mesh PP Routing Queues Files Log RADIUS New Terminal MetaROUTER Partition Make Supout.rif Manual New WinBox	IPsec Policies Proposals Groups Peers Identities Profiles Remote Peers Mode Configs I Image: Im	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

Добавление новой IPSec policy group

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

Добавление нового шаблона IPSec policy

sion securitys Dasho			
C Safe Mode	Session: 192	2.168.188.1	
🔏 Quick Set	10		
I CAPSMAN	IPsec		
🛲 Interfaces	Policies	Proposals Groups Peers Identities Profiles Active Peers	
🧘 Wireless	+ -	Statistics	Find
凝 Bridge	#	Peer Tunnel Src. Address Src. P	. Dst. Addre 🔻
E PPP	0 *T		::/0
🛫 Switch		New These Deline	
°t8 Mesh		New IPsec Policy	
255 IP		General Action Status OK	
😹 Routing 👘 🗅		Src. Address: 10.0.88.0/24 Cance	el
🎲 System 🗈		Src. Port: Apply	/
🙊 Queues		Dst. Address: 0.0.0.0/0	
📄 Files	• 1.itom	Dist Port:	
📄 Log	Titem	Comme	ent
🧟 RADIUS		Copy	·
🄀 Tools 🛛 🗅		Template Remov	/e
📰 New Terminal		Group: group vpn.ike2.xyz	
«¦> Dot1X			
🔜 MetaROUTER			
🏉 Partition		enabled Template Active	_
🛄 Make Supout.rif		Templete Jactive	
Manual			

😒 New WinBox

New IPsec Policy			
General Action	Status		ОК
Action:	encrypt	Ŧ	Cancel
IPsec Protocols:	esp	₹	Apply
Proposal:	proposal vpn.ike2.xyz	Ŧ	Disable
			Comment
			Сору
			Remove
enabled	Template	Active	

/ip ipsec policy

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

src-address=i0.0.88.0/24 temptate=yes

Добавление нового списка LAN сетей в firewall address list

🛑 😑 🔵 admin@	019	2.168.18	8.1 (N	/likroTik offi	ce-spb.ike2	.xyz) – WinBo	ox v6.45.3	on mA	P
session Settings Da	ashbo	oard							
🗢 🍳 🛛 Safe Mod	е	Session: 1	92.168	.188.1					
🔏 Quick Set									
🚊 CAPsMAN		Firewall						[٦×
🔚 Interfaces		Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Proto	ocols	
🧘 Wireless		4 -		× =	7		Eind	al	Ţ
😹 Bridge		Name				limeout	Creation	Time	
📑 PPP									
🙄 Switch									
°t¦8 Mesh			New	v Firewall A <u>ddr</u>	ess List				
255 IP				Name:	AN-address-lis		OK		
🙈 Routing				Address 4					
💮 System				Address:	192.100.100.0		Cancel		
👰 Queues				Timeout:			Apply		
Files			Cre	eation Time:			Disable		
Log							omment		
🥵 RADIUS							-		
💥 Tools	Þ	0 items	-				Сору		
🗙 🔚 New Terminal			-			I	Remove	_	
🖞 🖇 Dot1X			ena	bled					
MetaROLITER									

/ip firewall address-list
add address=192.168.188.0/24
list=LAN-address-list

ISC=LAN-address-LISU

Добавление нового клиента IPSec modeconf (инициатор)

admin@19	92.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on mAP lite (mipsbe)
ettings Dashb	oard
Safe Mode	Session: 192.168.188.1
ick Set	
PsMAN	Firewall
erfaces	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols
eless	
lge	Name
)	Address A
itch	IPsec
sh	Policies Proposals Groups Peers Identities Profiles ActivePeers Mode Configs Installed SAs Keys
Þ	
uting D	
item D	Name △ Resp Address Pool Address Address Prefi Split Include ▼ request-only no Include
eues	
s	
1	Name: modecont office-spb@vpn.ike2fxyz OK
DIUS	Responder Cancel
ols D	Connection Mark:
w Terminal	Src. Address List: LAN-address-list
:1X	Сору
taROUTER	Remove
tition	
ke Supout.rif	◆ ◆
nual	
w WinBox	

/ip ipsec mode-config
add name="modeconf officespb@vpn.ike2.xyz" responder=no srcaddress-list=LAN-address-list

address-list=LAN-address-list

Добавление нового удостоверения IPSec identity

ession Settings Dashbo	rd	
Safe Mode	5ession: 192.168.188.1	
Quick Set	IPsec Peers Identities Profiles Active Peers Mode Configs Installed SAs The New IPsec Identity	• Keys
Bridge	# Peer: peer vpn.ike2.xyz Auth. Method: digital signature F	OK
Switch C Mesh S IP	Certificate: office-spb@vpn.ike2.xyz	Apply Disable
Routing System Queues	Policy Template Group: group vpn.ike2.xyz	Comment
Files	● O it My ID Type: user fqdn	Remove
Tools	Remote ID Type: fqdn Remote ID: vpn.ke2.xyz]
Alpha Dot1X MetaROUTER	Match By: remote id	
Make Supout.rif	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-spb@vpn.ike2.xyz"
my-id=user-fqdn:office-spb@vpn.ike2.xyz
peer="peer vpn.ike2.xyz" policy-templategroup="group vpn.ike2.xyz" remoteid=fqdn:vpn.ike2.xyz

id=tqdn:vpn.ike2.xyz

dLonb=_dLonbNikita Tarikin / nikita@tarikin.com

Сверка удостоверений IPSec identity

Сервер

Клиент



Проверка связи IKEv2

Active peers state: established <

	IPsec													×
	Policies	Proposals	Groups	Peers	Identities	Profiles	Active Peers	Mode Configs	Installed SAs	Keys				
1	- 1	Kill Co	nnections										Find	
	ID	St St	ate	Loca	l Address	Remot	e Address 🛛 🛛	ynamic Address	Side	Uptime		PH2 Total	Tx Bytes	-
	vpn.ike2	.xyz es	tablished	123.	45.67.9	123.4	5.67.8 0).0.0.0	initiator		01:00:31		1	0

PH state: established	0
динамическая policy	#
Генерирована	4
	Polic

IPsec																×
Policies	Proposals	Groups	Peers	Identities	Profiles	Active P	eers M	ode Configs	Installed	SAs	Keys					
+	- 🖉 🛛	1	7	Statistics											Find	
#	Peer		Tunn	el Src. Ado	lress	Sr	c. P D	st. Adaress		Dst. P	Prot	ocol	Action	Level	PH2 State	•
0 *T				::/0				/0			25	5 (all)	encrypt			
1 T				10.0.88	.0/24		0.	0.0.0/0			25	5 (all)	encrypt			
2 DA	peer vp	n.ike2.xyz	z yes	10.0.88	.254		0.	0.0.0/0			25	5 (all)	encrypt	unique	established	ł

Peer:	aut	thorized
Addres	ss:	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

Проверка связи IKEv2

Генерировано **динамическое**

src-nat правило

Firewall									
Filter R	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols								
+ -	- 🖉 🖾 🍸 0	Reset Counters OO Re	eset All Counters			Find srcnat 🔻			
#						•			
0 D	;;; ipsec mode-config ⊮Ir Action: Dst. Address List: Bytes: Packet Rate:	src-nat !LAN-address-list 168 B 0	Chain: Log: Packets:	srcnat no 4	Src. Address List: To Addresses: Rate:	LAN-address-list 10.0.88.254 0 bps			
1	;;; defconf: masquerade ≓∥ Action: IPsec Policy: Packets:	masquerade out:none 1 033	Chain: Log: Rate:	srcnat no 0 bps	Out. Interface List: Bytes: Packet Rate:	WAN 64.2 KiB 0			

FROM:	LAN-address-list	192.168.188.0/24
TO:	NOT- LAN-address-list	NOT-192.168.188.0/24

```
Action: SRC-NAT
TO-address: 10.0.88.254
```



Проверка связи IKEv2: В Интернет



Те	rminal							×
[a	dmin@office-spb] > /too.	traceroute 1.2	l src-	address=	192.168.	188.1		+
#	ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	
1	10.0.88.1	0%	53	1.3ms	1.2	1	2.7	
2	123.45.67.1	0%	53	1.2ms	1.3	1.1	3.3	
3	172.16.102.254	0%	53	5.4ms	62.4	1.7	813.7	
4	10.252.35.2	0%	53	3ms	40.4	1.6	765.5	
5	43.252.157.43	0%	53	17.3ms	37.7	2.1	787.1	
6	10.251.1.197	0%	53	5.3ms	79.9	3.2	880.3	
7	43.252.157.90	0%	53	3.6ms	28.3	2.6	427.1	
8	43.252.157.57	28	53	3.3ms	42.7	2.9	559	
9	124.195.38.8	5.8%	52	34.9ms	107.1	34.5	699.9	
10	27.111.228.132	5.8%	52	36.7ms	93	35	764.9	
11	1.0.0.1	3.8%	52	41.6ms	126.3	33.7	963.5	
-	[Q quit D dump C-z pau:	se]						+

FROM: NOT-LAN-address-list



Tei	rminal] ×
[a	dmin@office-spb] > /tool	traceroute 1.	1					+
#	ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	
1	123.45.67.1	0%	25	0.3ms	0.3	0.2	0.6	
2	172.16.102.254	0%	25	0.8ms	53.3	0.8	563.9	
3	10.252.35.2	0%	25	0.8ms	100.9	0.8	787.1	
4	43.252.157.43	0%	25	l.9ms	70.4	1	601.7	
5	10.251.1.197	12%	25	3ms	120.5	2.2	647.2	
6	43.252.157.90	0%	25	14.8ms	52.2	1.9	355.9	
7	43.252.157.57	4%	25	3.6ms	43.9	1.9	391.5	_
8	124.195.38.8	8%	25	36.6ms	153.8	33.5	920.1	
9	27.111.228.132	12%	25	35.5ms	130.8	34.4	609.8	
10	1.0.0.1	4%	25	34ms	122.2	33.4	641.6	
	[Q quit D dump C-z pause	:]						•



Проверка связи IKEv2: из главного офиса в филиалы

erminal	כ	×
admin@MikroTik] > ping 192.168.188.1 src-address=192.168.88.1 SIZE TIL TIME STATUS 0 123.45.67.1 84 64 0ms net unreachable 1 123.45.67.1 84 64 0ms net unreachable 2 123.45.67.1 84 64 0ms net unreachable 3 123.45.67.1 84 64 0ms net unreachable 4 123.45.67.1 84 64 0ms net unreachable 5 123.45.67.1 84 64 0ms net unreachable 6 123.45.67.1 84 64 0ms net unreachable		•
7 123.45.67.1 84 64 Oms net unreachable		+







RouterOS IKEv2 site-to-site

Двусторонняя связь между офисами

192.168.188.0/24







Пропускаем входящие IPSec-esp пакеты на клиенте (на всякий случай)

192.16	2.168.188.1 (office-spb) - WinBox v6.45.3 on mAP lite (mipsbe)									
ard	d									
Session:	192.168.188.1]								
Firewall										×
Filter Ru	ules NAT Ma	angle	Raw	Service Ports	Connection	IS	Address Lists	Layer7 P	rotocols	;
+ –	New Raw Rule			·					pd	a
#	General Ad	lvanced	Extr	a Action :	5tatistics		OK		Port	-
0 D		Chain:	prero	uting	Ŧ	-	Cance	el		
	Src. Ad	ddress:			•		Apply	,		
	Dst. Ad	ddress:				•	Disabl	e		
	Pri	otocol:	🗌 ip:	sec-esp	₹ ▲		Comme	:nt	L	
	Src	. Port:					Copy	,		.
	Dsh	. Ports	Cor	nment for Ne	w Raw Rule					
	0.00	. Dorti		TRACK for A	LL incoming IP:	Sec	c-esp packets		ок	
	MILY	r Porta						C	ancel	
	In. Inte	erface:	<u>ال</u>					-		
	Out. Inte	erface:								
	In. Interfac	ce List:								- 1
	Out. Interfac	ce List:			•					
♥ 1 item										-
)										_

Vew Raw Rule General Advanced Extra Action Stat Climit Climit Nth Climit	tistics	OK Cancel Apply Disable Comment		RAW prerou	iting chain
PSD C	lew Raw Rule General Ad Action Log Prefix	vanced Extra no track Log	Action	Statistics T	Cancel Apply Disable

/ip firewall raw

add action=notrack chain=prerouting protocol=ipsec-esp comment="NOTRACK for ALL incoming IPSec-esp packets" dst-address-type=local Маршрутизируемый трафик через IKEv2: добавление интерфейса



Корректируем клиентский IPSec modeconf

•	😑 🔵 admin@19	2.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on mAP lite (mipsbe)
Ses	sion Settings Dashb	pard
Ю	Cafe Mode	Session: 192.168.188.1
	🔏 Quick Set	
	🧘 Capsman	Firewall
	🛲 Interfaces	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols
12.20		
	💥 Bridge	Name 🛆 Address Timeout Creation Time
	🚅 PPP	● LAN-addr 192.168.188.0/24 Aug/08/2019 17:
	🕎 Switch	IPsec
in the	°t¦8 Mesh	Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys
	😇 IP 🛛 🗅	
	🎉 Routing 💦 🗅	
	🍪 System 🛛 🗅	Name △ Resp Address Pool Address Address Preti Split Include ▼ request-only no
	🙊 Queues	New IPser Mode Confin
	📄 Files	
	📄 Log	Name: modeconf office-spb@vpn.ike2.xyz OK
	🥵 RADIUS	Cancel
×	🎇 Tools 🛛 🗅	Connection Mark: 🛛 🐺 Apply
B	🔤 New Terminal	Src. Address List: LAN-address list
/in	Dot1X	
\leq	🔜 MetaROUTER	Remove
S	😓 Partition	
er	📃 Make Supout.rif	
put	😋 Manual	
R	🔘 New WinBox	

Filter R	ules NAT	Mangle	Raw	Service	Ports	Conne	tions	Ado	dress Lists	Layer7
+ -	• 🖉 🖇	. 🖻	7	00 Re:	set Co	unters	00 F	lesel	t All Counte	rs
#										
0 D	;;; ipsec n →∥^ Action Dst. Addr Bytes: Packet Ra	node-conf : ess List: ate:	ig	<	src-na !LAN-4 168 B 0	it address-	list	1	Chain: Log: Packets:	
1	;;; defcor ≠∥ Action IPsec Poli Packets:	nf: masque : cy:	erade		masqu out:no 1 033	uerade one		1	Chain: Log: Rate:	

/ip ipsec mode-config
add name="modeconf officespb@vpn.ike2.xyz" responder=no

spodvpn.ikez.xyz" responder=no

Nikita Tarikin / nikita@tarikin.com

Открыта до 31 декабря 2019

Демо лаба

Доступна по подписке халявная демо лаборатория в облаке

- 1. Заполнить гугло-форму
- 2. Получить по почте индивидуальный сертификат
- 3. Подключиться к VPN серверу
- 4. Подключиться к лабе через Winbox или SSH

1. Заполнить форму

2. Получить сертификат

- 3. Подключить VPN
- 4. Войти через Winbox

Заполнить эту гугло-форму

https://forms.gle/NxYVAcpgaQfvCSXc6



- 1. Заполнить форму
- 2. Получить сертификат
- 3. Подключить VPN
- 4. Войти через Winbox

Дождаться своего сертификата

Дед Мороз рассылает сертификаты вручную, сорян :)

1. Заполнить форму

2. Получить сертификат

- 3. Подключить VPN
- 4. Войти через Winbox

Подключиться к IKE2 VPN серверу

Адрес сервера: vpn.ike2.xyz

< полученный сертификат вместо логинов и паролей >

- 1. Заполнить форму
- 2. Получить сертификат
- 3. Подключить VPN
- 4. Войти через Winbox

Войти на лабораторный роутер через Winbox

Address 10.0.88.1

Login lab Password lab

Внимание, конкурс!



"Hack the princess "

Открыта до 31 декабря 2019





Чтобы пройти этот квест нужно:

1) подключиться к главному офису и найти проход на филиал

2) подключиться к филиалу и разобраться каким образом

организована связь между зелеными сетями

- обратить особое внимание на шаблоны политик + каким образом формируются динамические политики на клиенте и на сервере
- 4) построить новую политику между своим роутером и целевой сетью по аналогии с политикой между зелеными сетями
- 5) зайти на целевой роутер и вытащить system identity
hacktheprincess@protonmail.com



192.168.**XX**.0/24

192.168.**XX**.YY

/system identity ???

Результаты на почту

	🗕 🔍 🌒 🔥 IKE2	2 LAB certificate request for: × 😫 Inbox hacktheprincess@proton × +		
1	d ⊳ C í	🛛 🖻 mail.protonmail.com/inbox 🛛 🗍	🦻 🙏 💡	2
	🐣 IKE2 LAB certific	ca		
	₽ ProtonMail	Q Search message v C La UPGRADE SETTINGS CONTACTS R	∰ ~ EPORT BUG	наскт
	COMPOSE	□ ~ Ø Ø ÎB Î Ø ÎN ^ Nors ~		<
	🚨 Inbox (3) 🛛 C	rotonMail Welcome to the future of email	246.1 KB	Ø
	Drafts		253.9 KB	Ø
	A Sent	☐ ★ ProtonMail Encrypt your Internet with Proton	224.8 KB	Ø
	Archive			
	⊘ Spam			
	🗊 Trash			
	All Mail (3)			
	Folders / L			
	UPGRADE STORAGE 724.75 KB / 500.00 MB			
	v3.16.3			

Nikita Tarikin / nikita@tarikin.com 🚃

Демо лаба

1. Заполнить форму

2. Получить сертификат

- 3. Подключить VPN
- 4. Войти через Winbox

Заполнить эту гугло-форму

https://forms.gle/NxYVAcpgaQfvCSXc6



Давайте дружить

Пишите на почту:

nikita@tarikin.com

Найти меня в Facebook:



0

Nikita Tarikin

Подписаться:
At a saile in

etarikin

@tropicalengineer

А лучше сразу сюда:



Messenger Nikita Tarikin ~

Nikita Tarikin

nikita@tarikin.com



Nikita Tarikin / nikita@tarikin.com