

Jak nastavit L2TP/IPSec na routeru Mikrotik

 torguard.net/article/243/mikrotik-l2tpipsec.html

1. Přihlaste se ke svému routeru pomocí webového rozhraní nebo Winboxu. Pokud používáte webové rozhraní, ujistěte se, že jste v rozhraní WebFig.
2. V levé nabídce klikněte na „IP“ , poté na „IPsec“ a poté proveďte následující:
 - A. Klikněte na kartu „Návrhy“ a poté klikněte na výchozí nabídku.
 - b. Ujistěte se, že je zaškrtnuto „Povoleno“.
 - C. Ujistěte se, že je zaškrtnuto pouze „sha1“ v poli „Auth. pole Algoritmy“.
 - d. Ujistěte se, že je v „ Encr. pole Algoritmy“. Vaše volba závisí na tom, zda chcete svůj provoz šifrovat pomocí AES-128 nebo AES-256. Při použití AES-256 je větší penalizace za výkon.
 - E. Vyberte „none“ z „PFS Group“.

IPsec Proposal <default>

OK Cancel Apply Remove

default

Enabled

Name default

Auth. Algorithms

md5 sha1
 null sha256
 sha512

Encr. Algorithms

null des
 3des aes-128 cbc
 aes-192 cbc aes-256 cbc
 blowfish twofish
 camellia-128 camellia-192
 camellia-256 aes-128 ctr
 aes-192 ctr aes-256 ctr
 aes-128 gcm aes-192 gcm
 aes-256 gcm

Lifetime ▼

PFS Group none

F. Klikněte na „OK“.

Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users **IPsec**

Add New

1 item

		▲ Name	Auth. Algorithms	Encr. Algorithms	Lifetime	PFS Group
-	D	*	default	sha1	aes-128 cbc	none

3. V levé nabídce klikněte na „Rozhraní“.

4. Na kartě „Rozhraní“ klikněte na „Přidat nový“ a poté na „Klient L2TP“.

5. Postupujte takto:

A. Ujistěte se, že je zaškrtnuto „Povoleno“.

b. Pod „General“ vložte jméno do pole „Name“ (např. 'Torguard ').

C. Pod „Dial Out“ přidejte IP adresu vaší VPN do pole „Connect To“ a své uživatelské jméno Torguard do „User“. Kliknutím na šipku vedle „Heslo“ zobrazíte textové pole a do tohoto pole zadejte své heslo Torguard.

The screenshot shows the Mikrotik WinBox configuration window for the 'Torguard' interface. The left sidebar contains a menu with options like Bridge, Switch, PPP, IP, MPLS, Routing, System, Queues, Files, Log, Radius, LCD, Tools, MetaROUTER, Partition, Make Supout.rif, Undo, Redo, Hide Passwords, Safe Mode, Design Skin, WinBox, Graphs, and End-User License. The main configuration area is titled 'Interface <Torguard>' and includes buttons for OK, Cancel, Apply, Remove, and Torch. Below these are status indicators (connected, running, not slave) and an 'Enabled' checkbox which is checked. The configuration is divided into sections: 'General' (Name: Torguard, Type: L2TP Client, Actual MTU: 1200, Max MTU: 1450, Max MRU: 1450, MRRU dropdown) and 'Dial Out' (Connect To: server address, User: Torguard username, Password: Torguard password, Profile: default-encryption, Keepalive Timeout dropdown).

d. Ujistěte se, že je zaškrtnuto „Použít IPsec“. Do pole „IPsec Secret“ zadejte „torguard“.

E. Pokud je tato možnost vybrána, zrušte zaškrtnutí políčka „Vytáčet na vyžádání“ a „Přidat výchozí trasu“.

Use IPsec	<input checked="" type="checkbox"/>
IPsec Secret	<input type="text" value="....."/>
Allow Fast Path	<input type="checkbox"/>
Dial On Demand	<input type="checkbox"/>
Add Default Route	<input type="checkbox"/>
Default Route Distance	<input type="text" value="0"/>
Allow	<input checked="" type="checkbox"/> mschap2 <input checked="" type="checkbox"/> mschap1 <input checked="" type="checkbox"/> chap <input checked="" type="checkbox"/> pap

F. Klikněte na „OK“. Vaše připojení klienta L2TP IPsec k Torguard by se mělo objevit ve vašem seznamu rozhraní. Po krátké chvíli by se nalevo od názvu vašeho připojení L2TP IPsec mělo objevit „R“ – to znamená, že je váš Mikrotik úspěšně připojen k serveru Torguard VPN.

6. V hlavní nabídce na levé straně klikněte na „IP“ a poté na „Firewall“.

7. Na záložce „Pravidla filtrů“ vyhledejte ve sloupci „Akce“ všechna pravidla s „fasttrack connection“. Pokud jsou přítomny, mohou narušovat vaši funkčnost VPN. Pokud přidáváte VPN do routeru Mikrotik s výchozí konfigurací, klikněte na pravidlo označené „fasttrack connection“, zrušte zaškrtnutí „Enabled“ a klikněte na „OK“.

8. Na kartě „NAT“ klikněte na „Přidat nový“ a proveďte následující:

A.

V části „General“ vyberte „srcnat“ z „Chain“ a vyberte „Torguard“ (nebo jakýkoli název, který jste dali svému rozhraní VPN) z „Out Interface“.

not invalid

OK Cancel Apply Remove Reset Counters

Enabled

General

Chain srcnat

Src. Address ▼

Dst. Address ▼

Protocol ▼

Src. Port ▼

Dst. Port ▼

Any. Port ▼

In. Interface ▼

Out. Interface Torguard

In. Interface List ▼

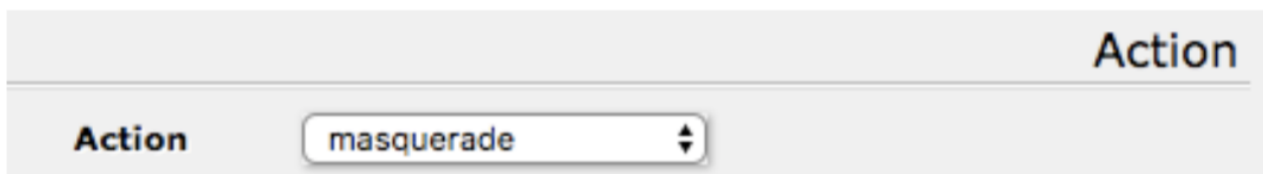
Out. Interface List ▼

Packet Mark ▼

Connection Mark ▼

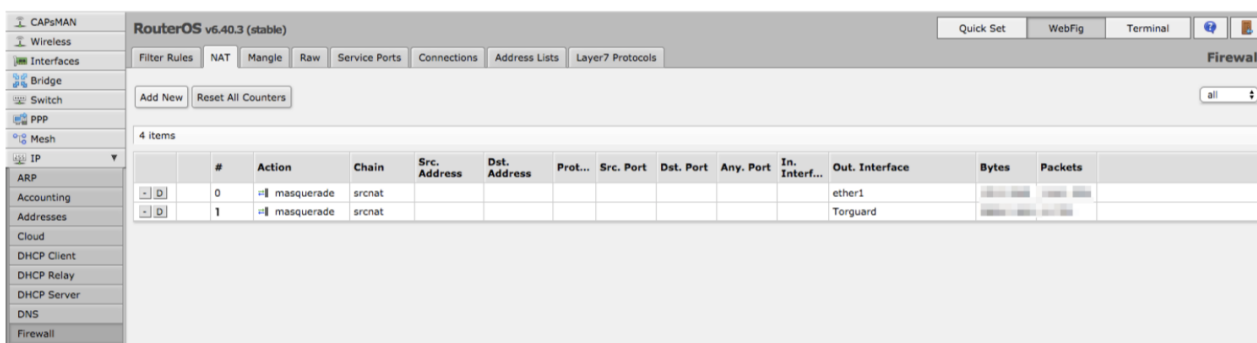
b.

V části „Akce“ vyberte „Maškaráda“.



C.

Klikněte na „OK“. Vaše nové pravidlo NAT by se mělo objevit v seznamu.



9. Na záložce „Mangle“ klikněte na „Add New“ a proved’te následující:

A. Ujistěte se, že je zaškrtnuto „Povoleno“.

b.

V části „General“ vyberte „prerouting“ z „Chain“ a do „Src. Adresa“.

OK Cancel Apply Remove Reset Counters

not invalid

Enabled

General

Chain prerouting

Src. Address Your VPN IP range here

Dst. Address ▼

C.

Pod „Akce“ vyberte „označit směrování“ z „Akce“. Přidejte název (klikněte na šipku a zadejte do textového pole) pro vaši značku směrování VPN (např. 'VPN') v části „New Routing Mark“.

Action

Action mark routing

Log

Log Prefix ▼

New Routing Mark VPN

Passthrough

d. Ujistěte se, že je zaškrtnuto „Passthrough“.

E. Klikněte na „OK“. V seznamu by se mělo objevit vaše nové pravidlo mangle.

F. Tento krok můžete opakovat pro tolik IP adres, rozsahů a pravidel, kolik potřebujete. Pokud používáte více pravidel, pamatujte, že se zpracovávají v pořadí v tabulce Mangle – pokud potřebujete, můžete se vrátit a změnit jejich pořadí kliknutím a přetažením.

10. V hlavní nabídce na levé straně klikněte na „IP“, poté na „Routes“, klikněte na „Přidat nový“ a proveďte následující:

A.

Pod „General“ zadejte „0.0.0.0/0“ do „Dst. Adresa“, potom vyberte dříve vytvořenou směrovací značku pod „Směrovací značka“ (např. ‚VPN‘).

OK Cancel Apply Remove

not invalid active static

Enabled

General

Dst. Address 0.0.0.0/0

Gateway ▼ Torguard reachable ▲

Check Gateway ▼

Type unicast

Distance ▲ 1

Scope 30

Target Scope 10

Routing Mark ▲ VPN

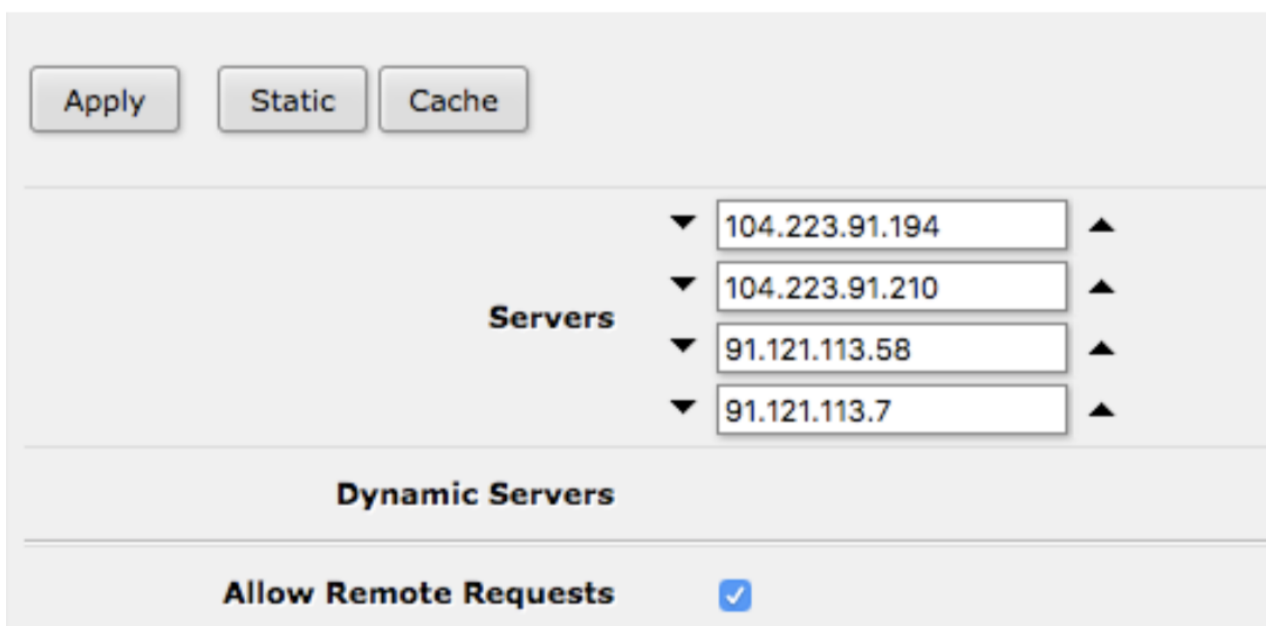
b. Klikněte na „OK“. V seznamu by se měla objevit nová trasa.

11. V tomto okamžiku by vaše připojení VPN mělo fungovat na vámi zvolené IP adrese (adresách). Chcete-li použít servery DNS společnosti Torguard, v hlavní nabídce na levé straně klikněte na „IP“ a poté na „DNS“ a poté proveďte následující:

A. Ujistěte se, že je zaškrtnuto „Povolit vzdálené požadavky“. To umožňuje vašim klientským zařízením používat router vašeho Mikrotiku jako DNS server, který zase bude používat DNS servery Torguardu.

b.

Přidejte aktuální servery DNS Torguardu do „Servery“.



C. Klikněte na „ Použít “.