

# 68150: Acronis Disaster Recovery Cloud: How to configure Acronis IPsec VPN Gateway and MikroTik Firewall

Use Google Translate

Selezione O Idioma ▼

Applies to:

- [Acronis Cyber Disaster Recovery Cloud](#)

Last update: **13-04-2021**

With C21.02 release, we have introduced Multi-site IPsec VPN, bringing a new level of security to Acronis Cyber Disaster Recovery Cloud solution. See [detailed description](#) of the new feature.

Follow the guidelines below to set up IPsec VPN gateway in an environment with MikroTik Firewall.

## Preconditions

1. Two network adapters (WAN and LAN) should be added.
2. One of the LAN address should be assigned to the WebConsole of MikroTik

Make sure that you have connectivity on the local side, local machines have proper connection to the local appliance, before proceeding with setup.

Check **IP > Firewall > NAT** to make sure none of the previously created rules can block the connection.

## Steps on DR side

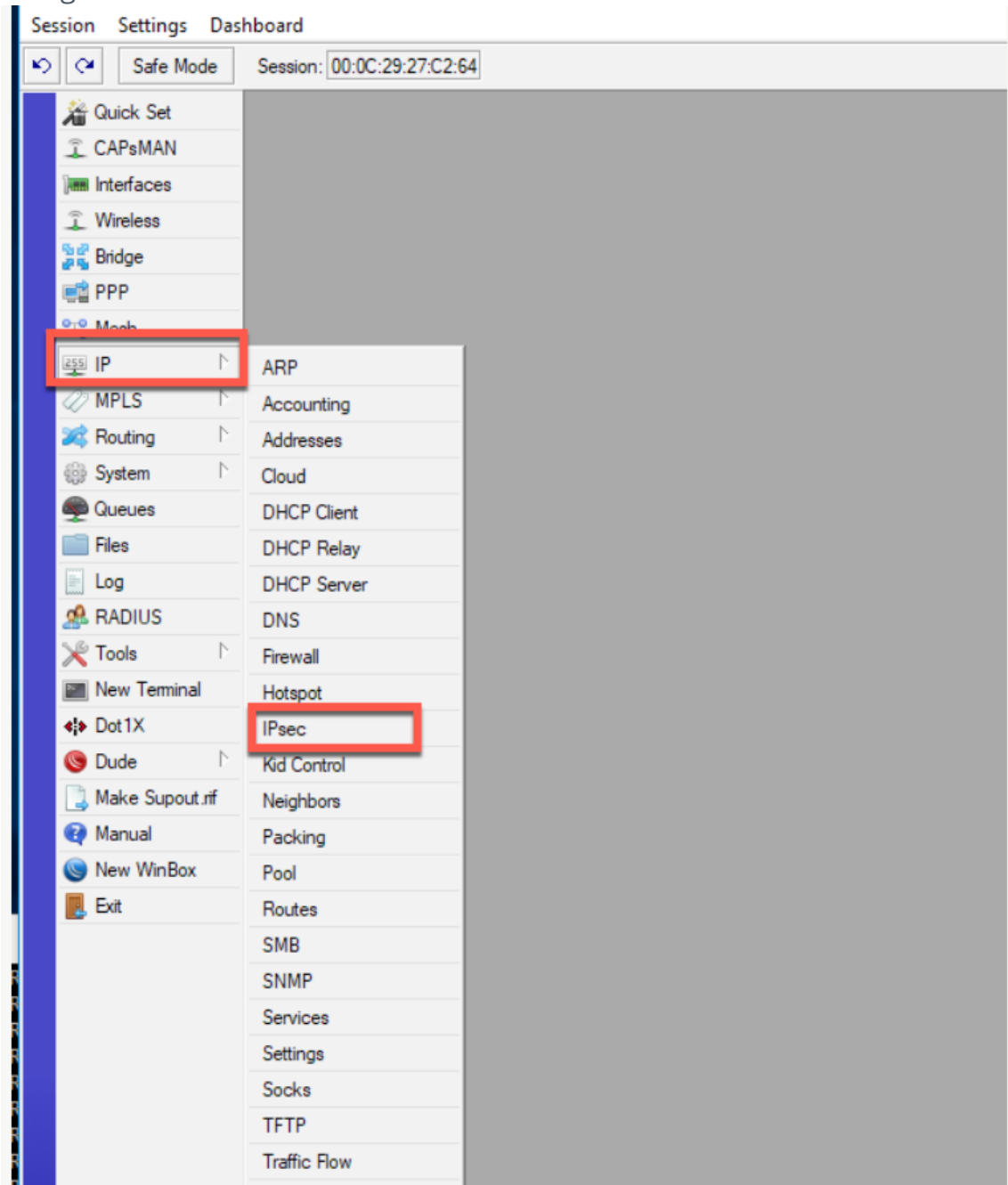
1. Log in to your tenant. Switch to **Disaster Recovery -> Connectivity**.
2. Create a **Cloud network** and click **Add connection**.
3. Enter the name of your MikroTik and public IP.

4. Click **Next**.
5. Generate a **Pre-shared Key** and save the key. You will need this key when setting up MikroTik.
6. Enter your local network and select the newly created Cloud network.
7. Switch to **IPsec/IKE security settings**. In **Startup action**, select **Start**. Click **Save**.

## Steps on MikroTik side

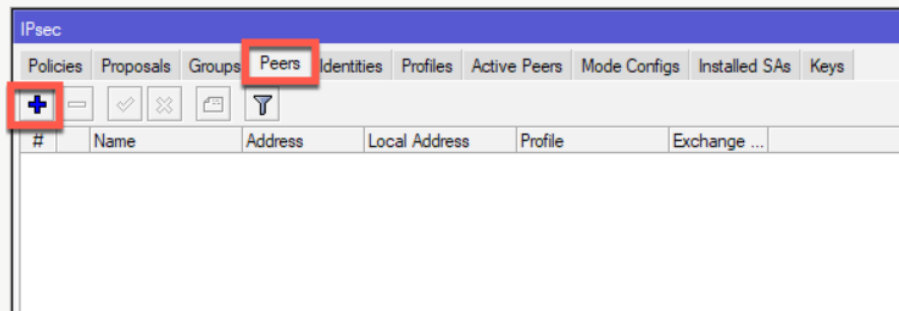
1. Log in to MikroTik Web interface console.

2. Navigate to **IP > IPsec**:

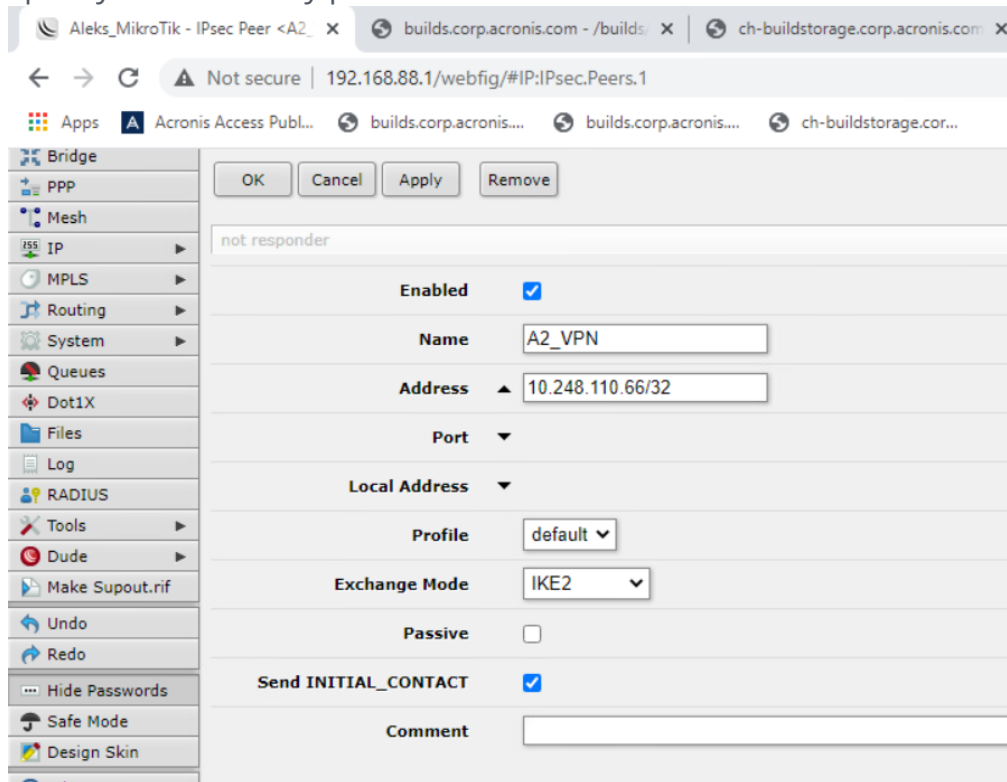


3. First, you need to define Peer (VPN\_Server). Navigate to the **Peers** tab and click the + sign to add a new Peer:

IP | IPsec | tab Peers | click on Plus (+) sign

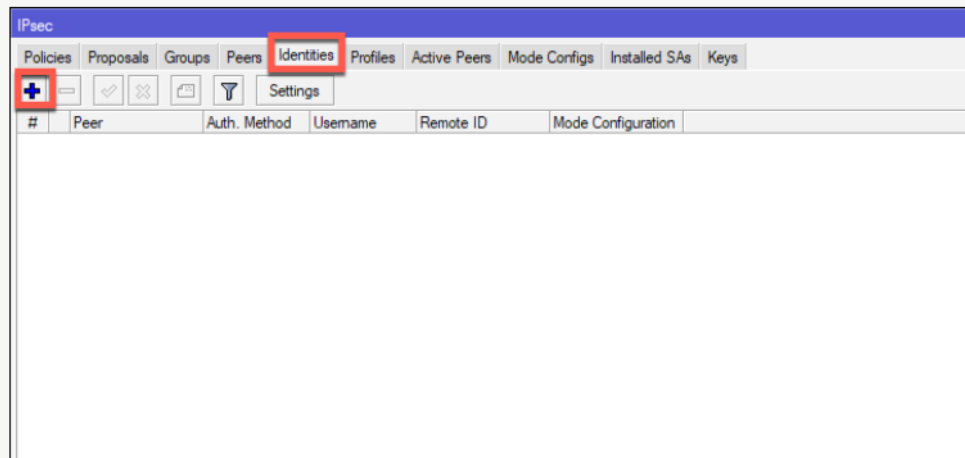


4. Set up Peer configuration as shown on the screenshot. In **Address**, specify VPN Gateway public IP address.



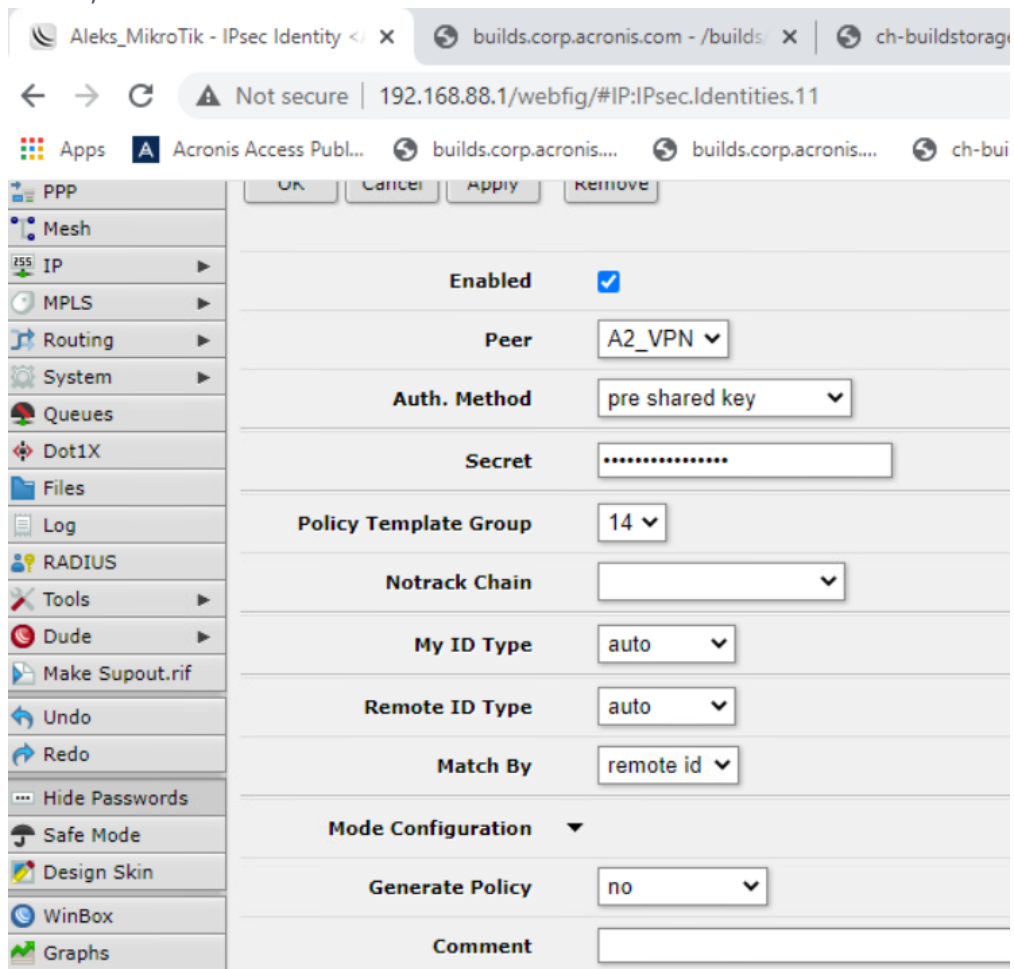
5. Switch to the **Identities** tab:

IP | IPsec | tab Identities | click on Plus (+) sign



Peer is going to be Router2. Authentication Method - pre shared key, and

6. In **Peer**, select the newly created peer (VPN\_Server). **Authentication Method**: pre shared key. In the **Secret** field, provide password. Remember this password, as it is needed on both sides, local and cloud, of the tunnel.



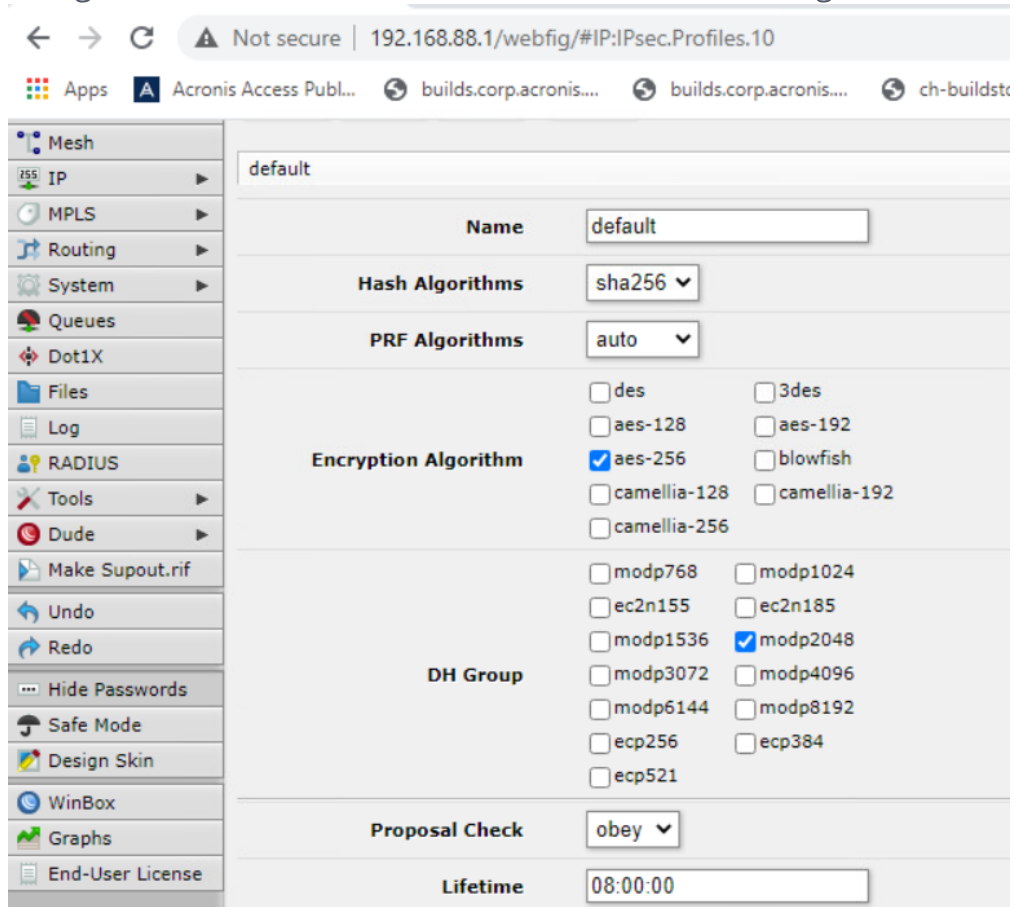
7. Navigate to the **Proposals** tab. Click on the **default** configuration to edit it:

The screenshot shows the Mikrotik WinBox interface with the IPsec Proposal configuration window open. The left sidebar contains a menu with options: PPP, Mesh, IP, MPLS, Routing, System, Queues, Dot1X, Files, Log, RADIUS, Tools, Dude, Make Supout.rif, Undo, Redo, Hide Passwords, Safe Mode, Design Skin, WinBox, Graphs, and End-User License. The main window displays the configuration for the 'default' proposal. The 'Enabled' checkbox is checked. The 'Name' field is set to 'default'. Under 'Auth. Algorithms', 'sha256' is selected. Under 'Encr. Algorithms', 'aes-256 cbc' is selected. The 'Lifetime' is set to 01:00:00. The 'PFS Group' is set to 'modp2048'.

Field	Value
Enabled	<input checked="" type="checkbox"/>
Name	default
Auth. Algorithms	<input type="checkbox"/> md5 <input type="checkbox"/> sha1 <input type="checkbox"/> null <input checked="" type="checkbox"/> sha256 <input type="checkbox"/> sha512
Encr. Algorithms	<input type="checkbox"/> null <input type="checkbox"/> des <input type="checkbox"/> 3des <input type="checkbox"/> aes-128 cbc <input type="checkbox"/> aes-192 cbc <input checked="" type="checkbox"/> aes-256 cbc <input type="checkbox"/> blowfish <input type="checkbox"/> twofish <input type="checkbox"/> camellia-128 <input type="checkbox"/> camellia-192 <input type="checkbox"/> camellia-256 <input type="checkbox"/> aes-128 ctr <input type="checkbox"/> aes-192 ctr <input type="checkbox"/> aes-256 ctr <input type="checkbox"/> aes-128 gcm <input type="checkbox"/> aes-192 gcm <input type="checkbox"/> aes-256 gcm
Lifetime	01:00:00
PFS Group	modp2048

8. Make sure you have the same Proposal configuration on both sides, local and cloud.

9. Navigate to the **Profiles** tab and edit the **default** configuration:



default

Name: default

Hash Algorithms: sha256

PRF Algorithms: auto

Encryption Algorithm:

- ☐ des
- ☐ aes-128
- ☒ aes-256
- ☐ camellia-128
- ☐ camellia-256
- ☐ 3des
- ☐ aes-192
- ☐ blowfish
- ☐ camellia-192

DH Group:

- ☐ modp768
- ☐ ec2n155
- ☐ modp1536
- ☐ modp3072
- ☐ modp6144
- ☐ ecp256
- ☐ ecp521
- ☐ modp1024
- ☐ ec2n185
- ☒ modp2048
- ☐ modp4096
- ☐ modp8192
- ☐ ecp384

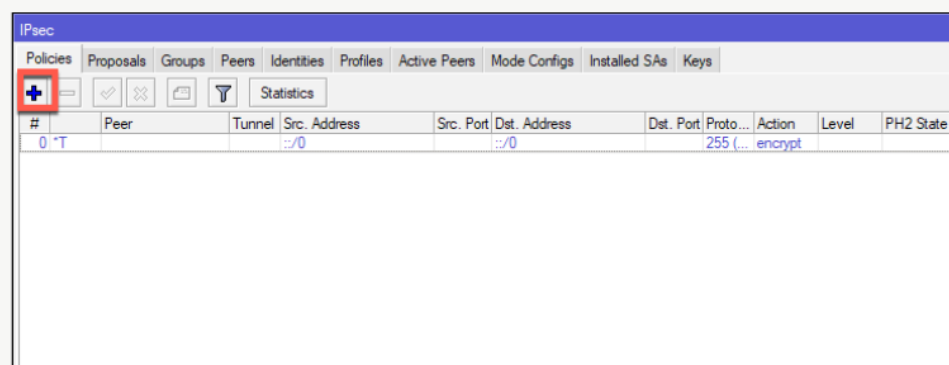
Proposal Check: obey

Lifetime: 08:00:00

10. Make sure you have same settings on both sides, local and cloud.

11. Navigate to the **Policies** tab. Click the + sign to add a new policy.

IP | IPsec | tab Policies | click on Plus (+) sign



IPsec

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

+

#	Peer	Tunnel	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	PH2 State
0	T		:::0		:::0		255 (...)	encrypt		

12. On the **General Tab** of the **New IPsec Policy**, select the newly created VPN\_Server as **Peer**. Navigate to **Tunnel**. In **Src.Address**, provide LAN subnet. In **Dst.Address**, provide remote LAN subnet of the remote side (VPN Gateway). Leave everything else default.
13. Switch Back to DR side and click **Enable connection**. The **Up** state indicates successful connection.

Fonte: <https://kb.acronis.com/content/68150>