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

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

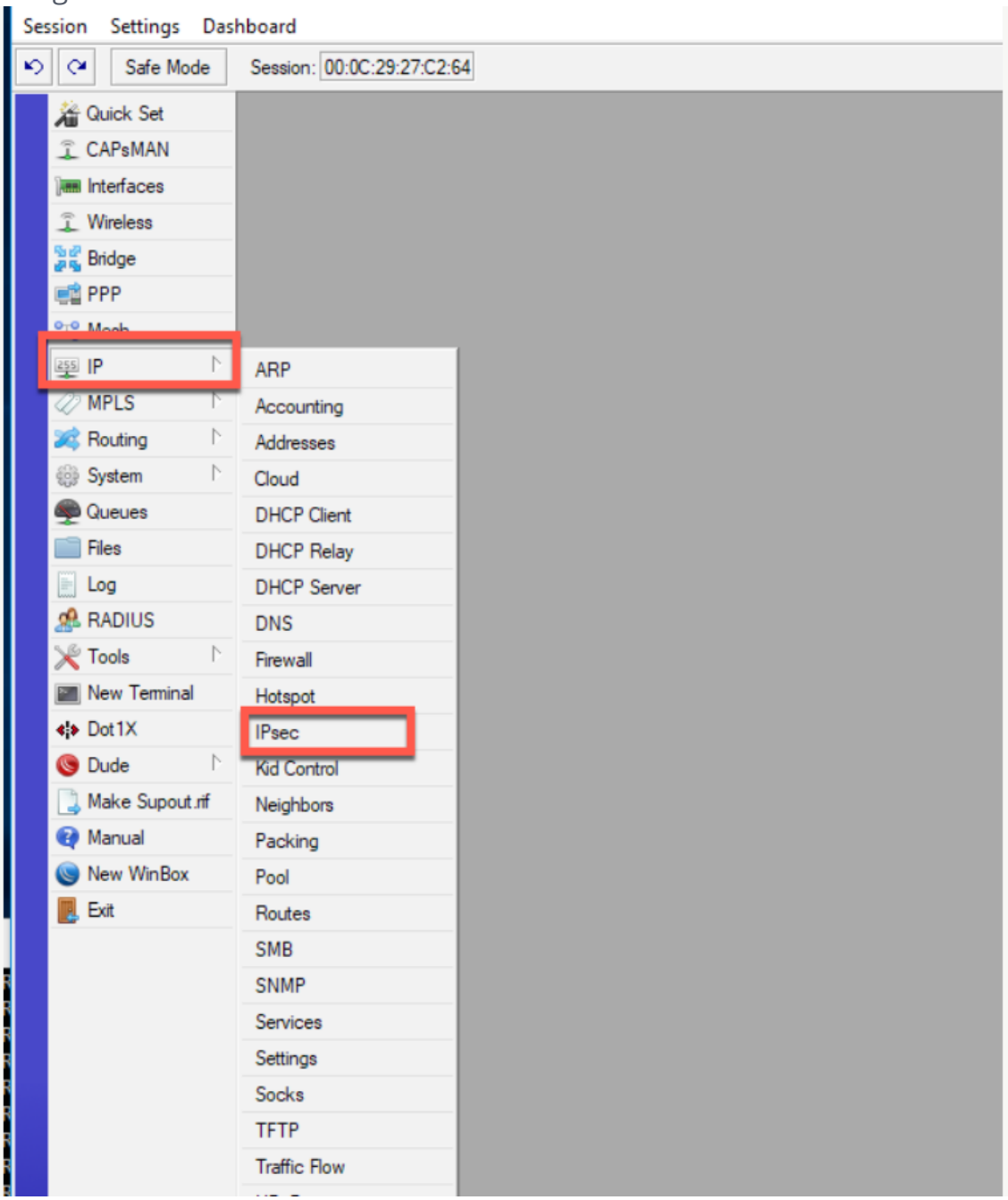
1. Log in to your tenant. Switch to **Disaster Recovery** -> **Connectivity**.
2. Create a **Cloud network** and click **Add connection**.
3. Enter the name of your MikroTik and public IP.

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

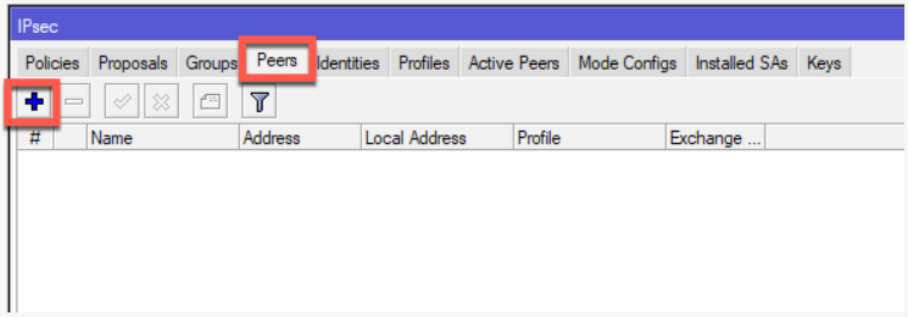
1. Log in to MikroTik Web interface console.

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

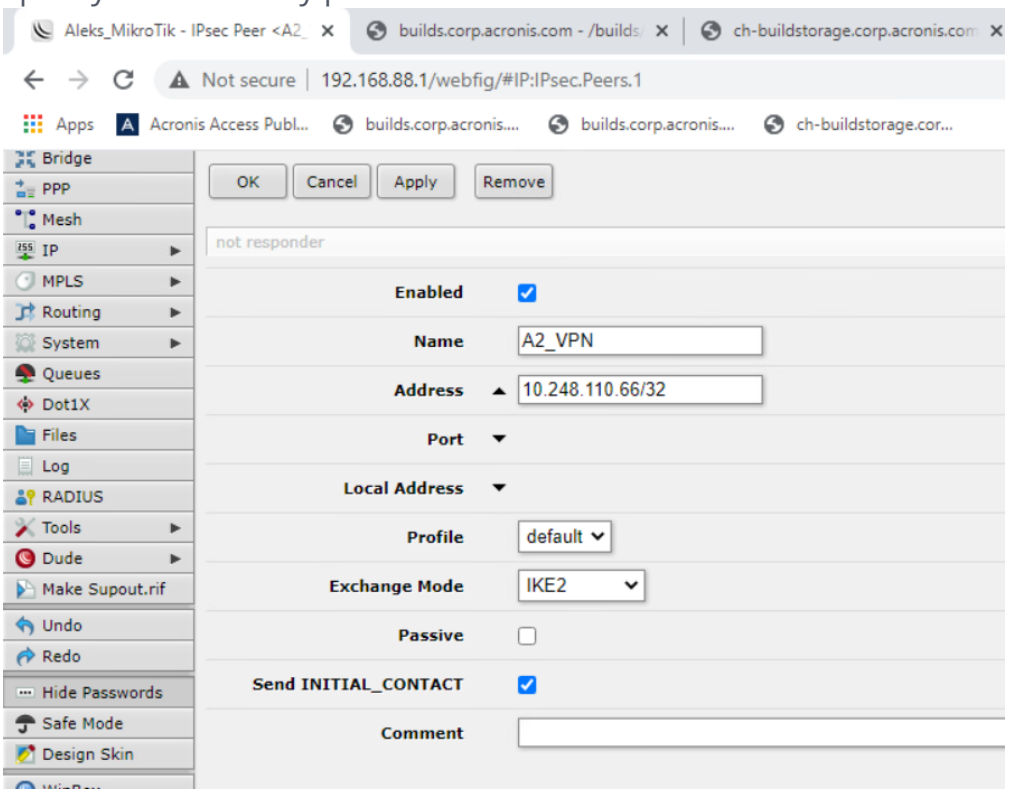


3. First, you need to define Peer (VPN_Server). Navigate to the **Peers** tab and click the **+** sign to add a new Peer:

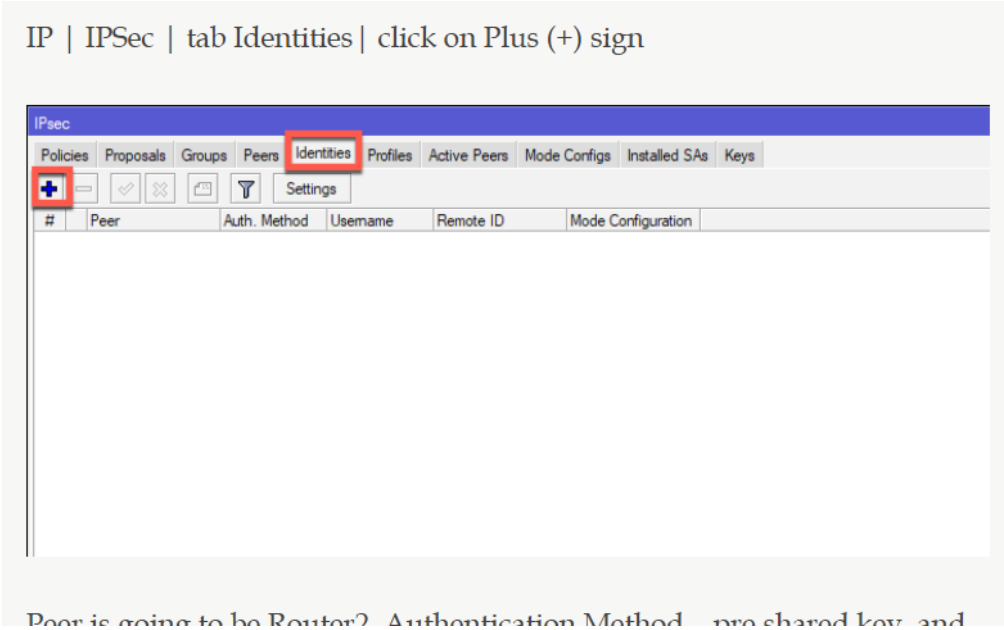
IP | IPSec | tab Peers | click on Plus (+) sign



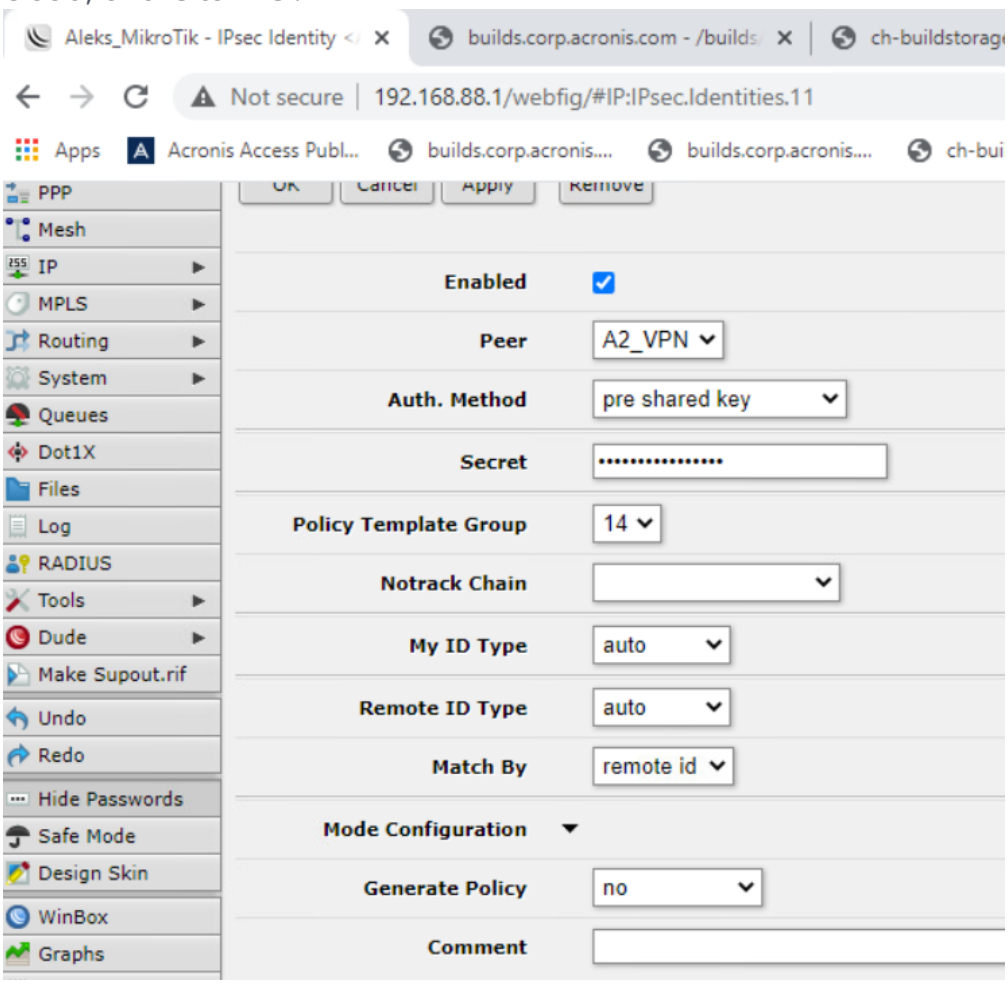
4. Set up Peer configuration as shown on the screenshot. In **Address**, specify VPN Gateway public IP address.



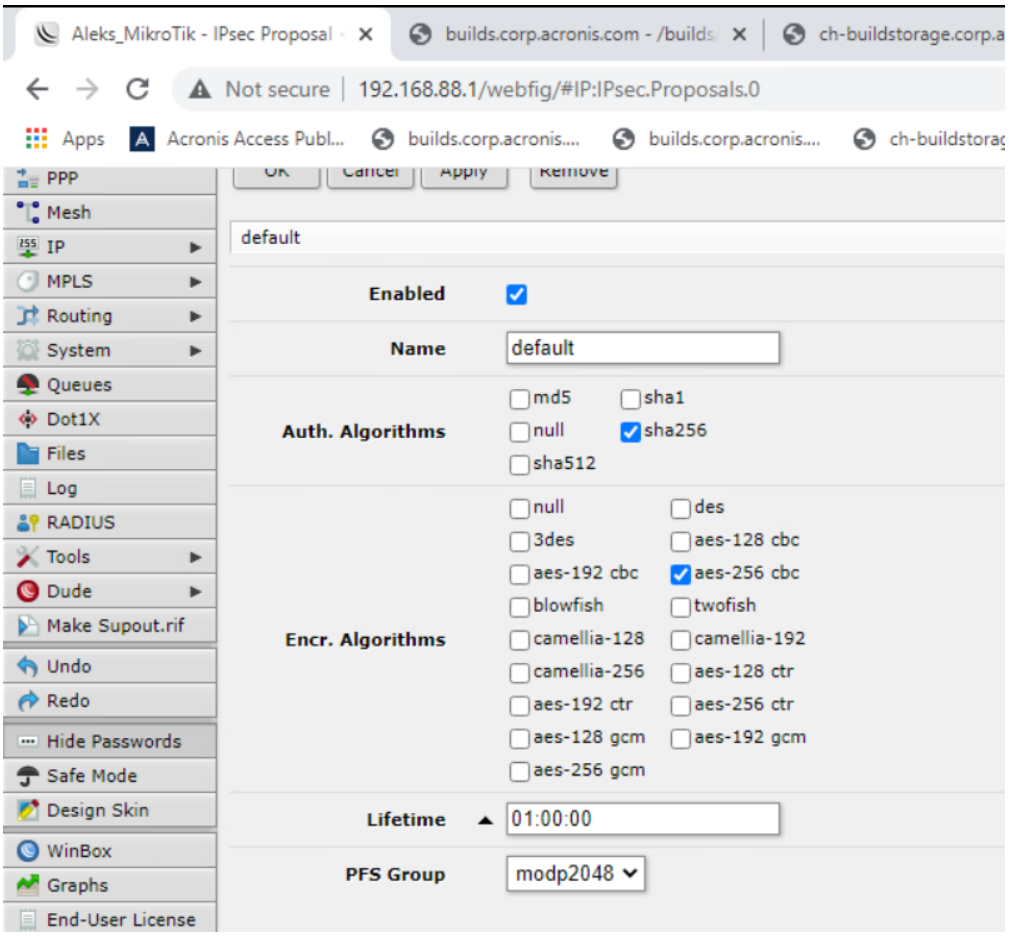
5. Switch to the **Identities** tab:



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.

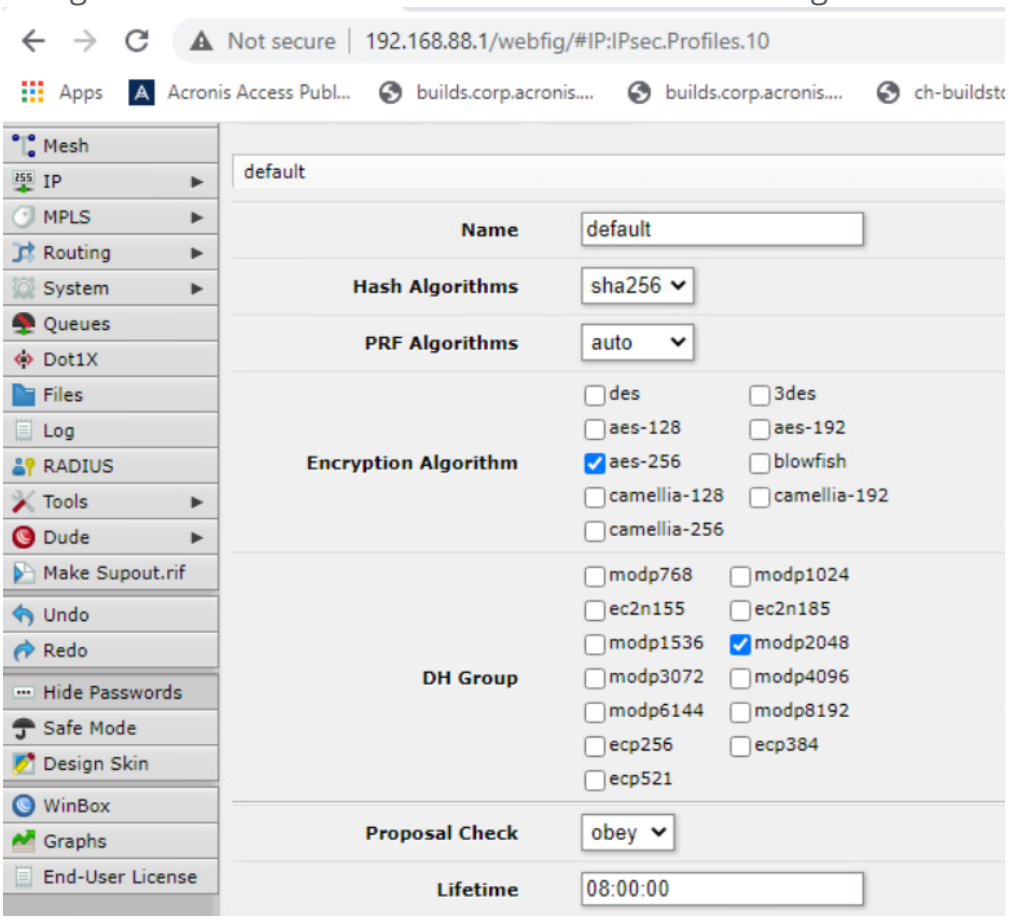


7. Navigate to the **Proposals** tab. Click on the **default** configuration to edit it:



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:



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.

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