Using softether to secure your networking kit

Infrastructure management

with examples from Mikrotiks

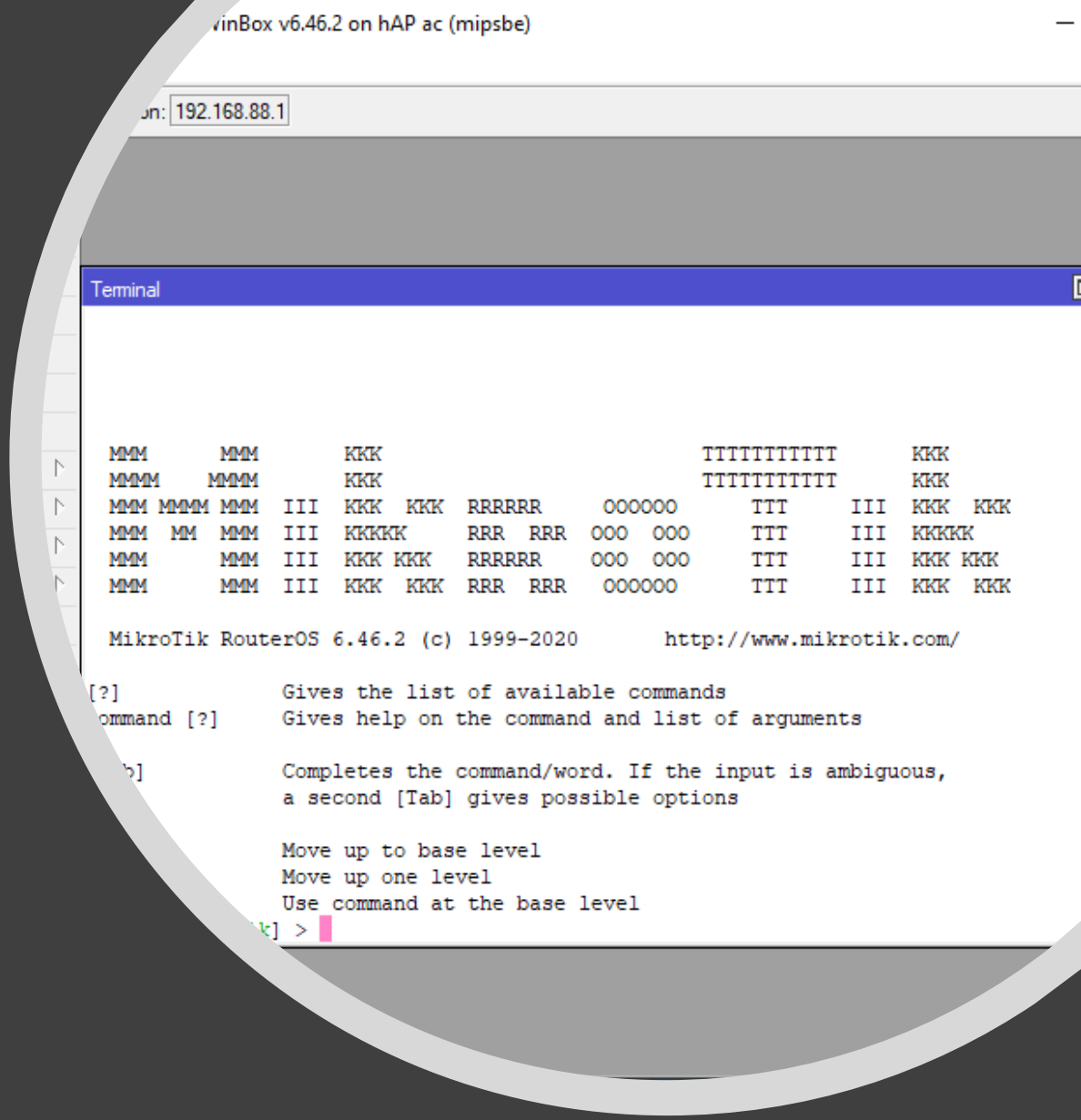
fusion broadband south africa

Ronald Bartels Fusion Broadband

Driving SDWAN adoption in South Africa

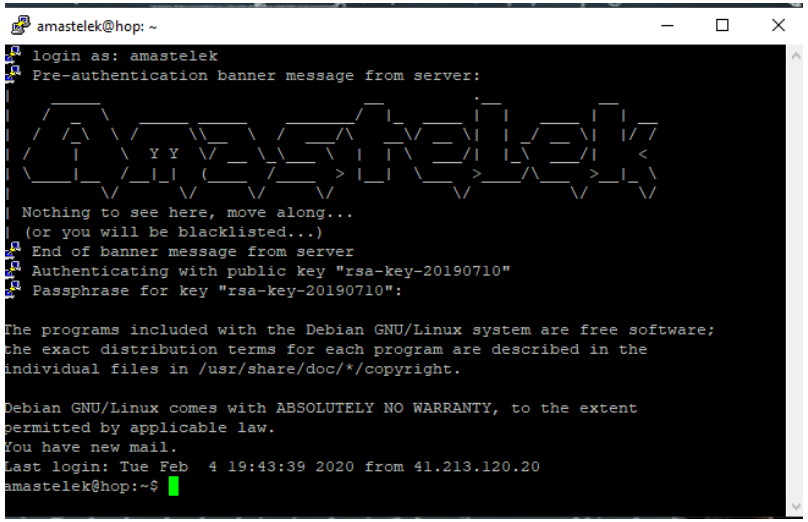
The problem

- Winbox in the Wild https://medium.com/tenable-techblog/winbox-in-the-wild-9a2ee4946add
- There are 600 000 Winbox interfaces open to the Internet without restrictions
- Less than 15% on patched versions
- Shodan is an excellent resources to mine information on your own network
- South Africa is a mess across all ISPs



Mitigation

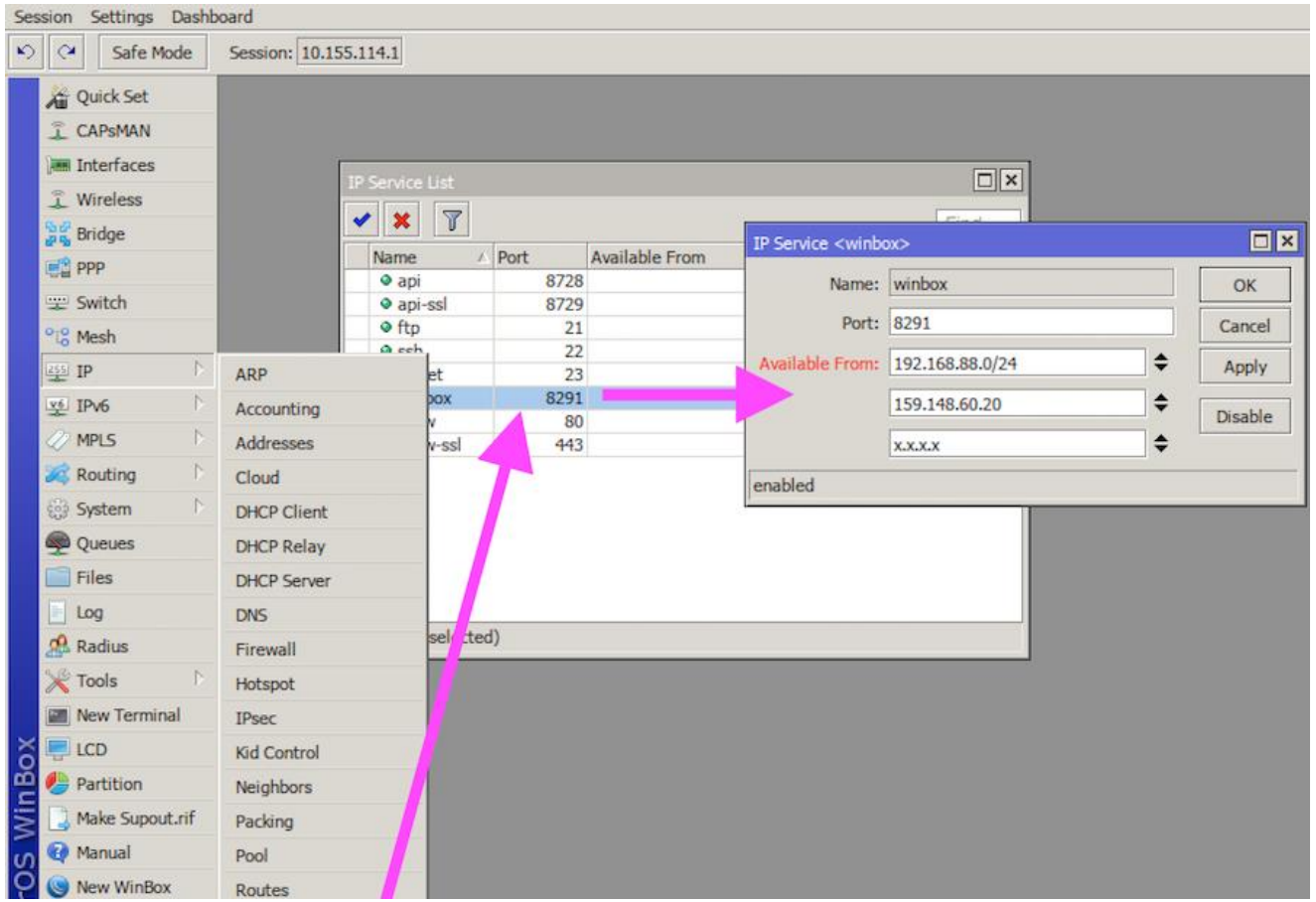
- Whitelist an IP that will manage the infrastructure
- All infrastructure has filters to drop all other IPs
- Install a linux box (I use buster) using the white listed IP – typically the cheapest vps will work
- Typical use case would be to implement as jump server using ssh with certs for login
- But I have a Windows desktop and like using the Windows tools!



Whitelist IP on Mikrotik

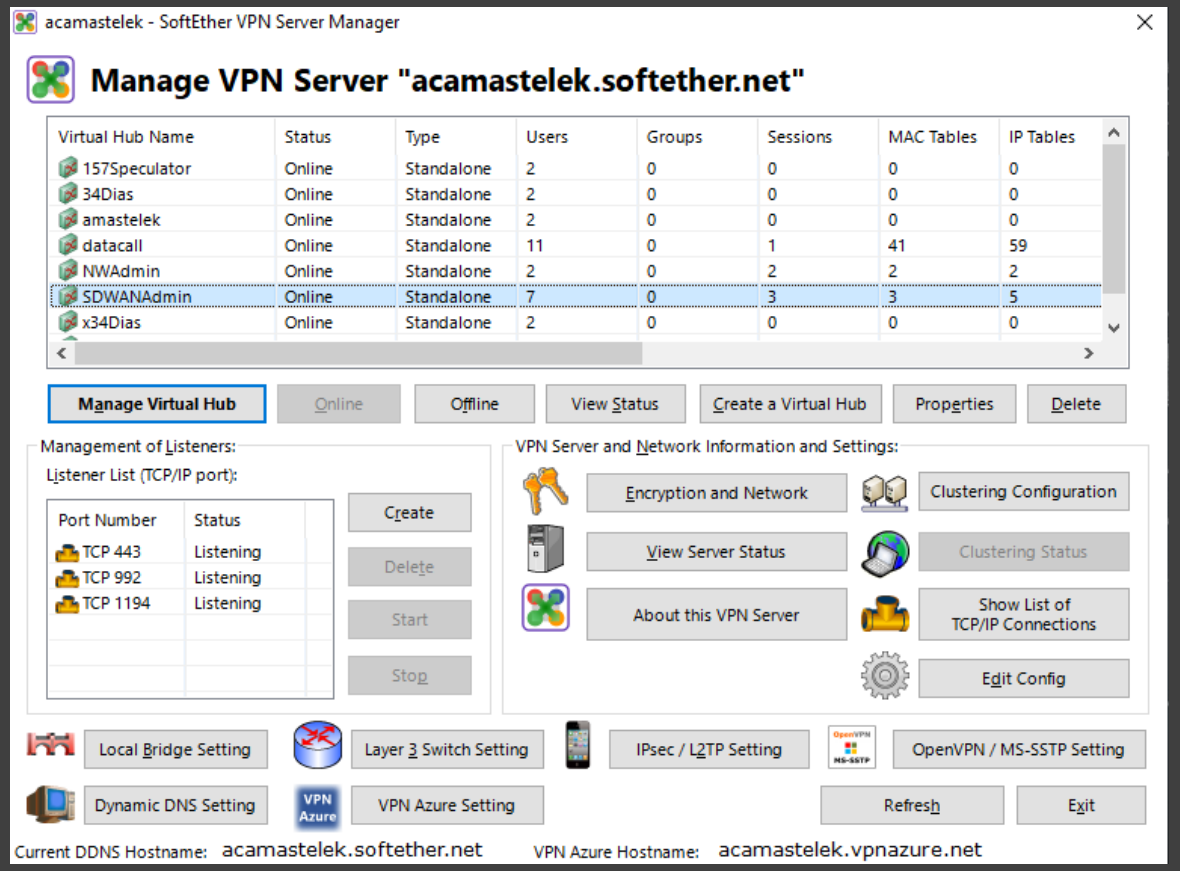
use the "IP -> Services" menu to specify "Allowed From" addresses. Include your LAN, and the public IP that you will be accessing the device from.

- Disable all other services
- Allow 8291 from Internet on the FW



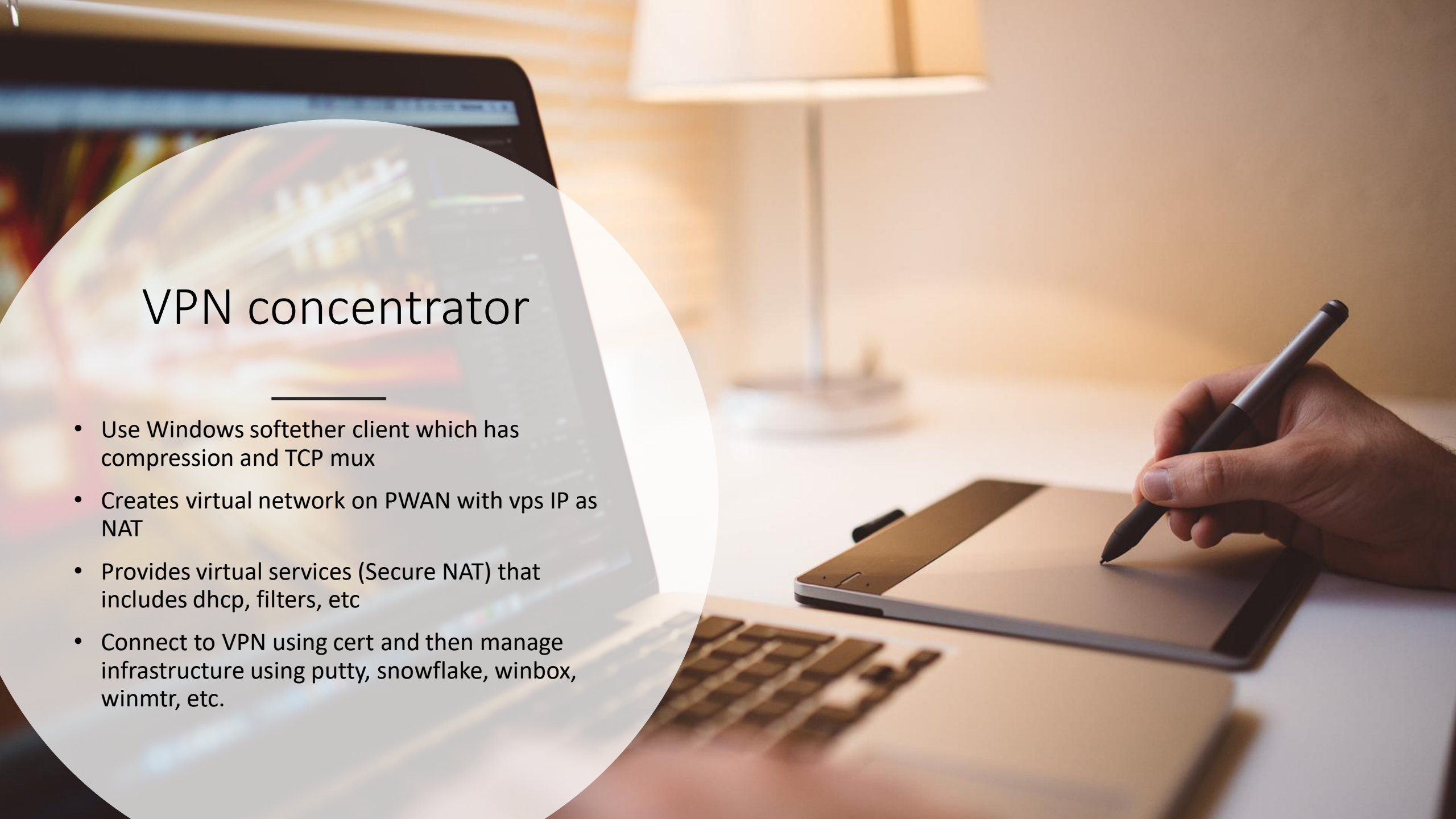
Enter softether

- VPN software available for multiple OS platforms
- Supports multiple VPN protocols as well as its own
- Excellent GUI management tools
- V5 available on github – works with Mikrotiks!
- PS: Punch holes in firewalls and hotspots



VPN concentrator

- Use Windows softether client which has compression and TCP mux
- Creates virtual network on PWAN with vps IP as NAT
- Provides virtual services (Secure NAT) that includes dhcp, filters, etc
- Connect to VPN using cert and then manage infrastructure using putty, snowflake, winbox, winmtr, etc.



Some additional tips

- Don’t use the built-in DNS – use Quad 9
- Use passwords of at least 16 characters and use a master password
- Update your firmware and backup you configs – Unimus https://unimus.net/ will help and save you time and headcount and provide an audit ability – check for a breach

Additional tools

- IPSET blacklist https://github.com/trick77/ipset-blacklist (kills 99% of VPN hack attempts before they even start)
- Fail2ban
- netdata – its just kewl and makes you look like you have an awesome dashboard

Demo of softether

Useful links

- softether vps build: https://github.com/SoftEtherVPN/SoftEtherVPN/blob/master/src/BUILD_UNIX.md
- softether binaries for Windoze: https://github.com/SoftEtherVPN/SoftEtherVPN/releases
- My SDWAN: https://fusionbroadband.co.za
- LinkedIn: https://www.linkedin.com/in/ronaldxbartels/