

Using softether to secure your
networking kit

Infrastructure management

with examples from Mikrotiks



IT Blog Awards

hosted by Cisco

**Best
Analysis**

-2018-

FINALIST

 CISCO

Ronald Bartels Fusion Broadband

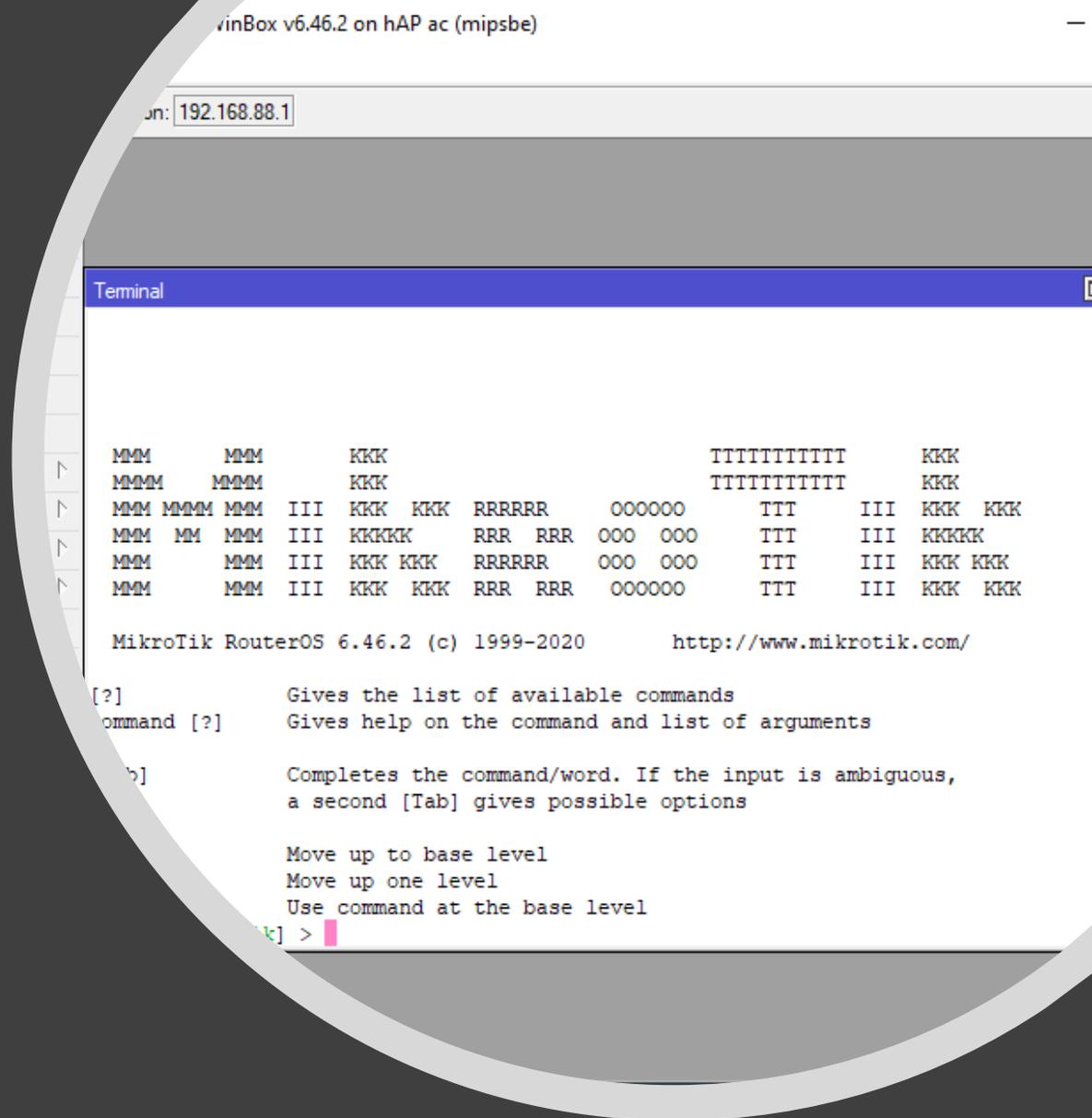
Driving SDWAN adoption in South Africa



on: 192.168.88.1

The problem

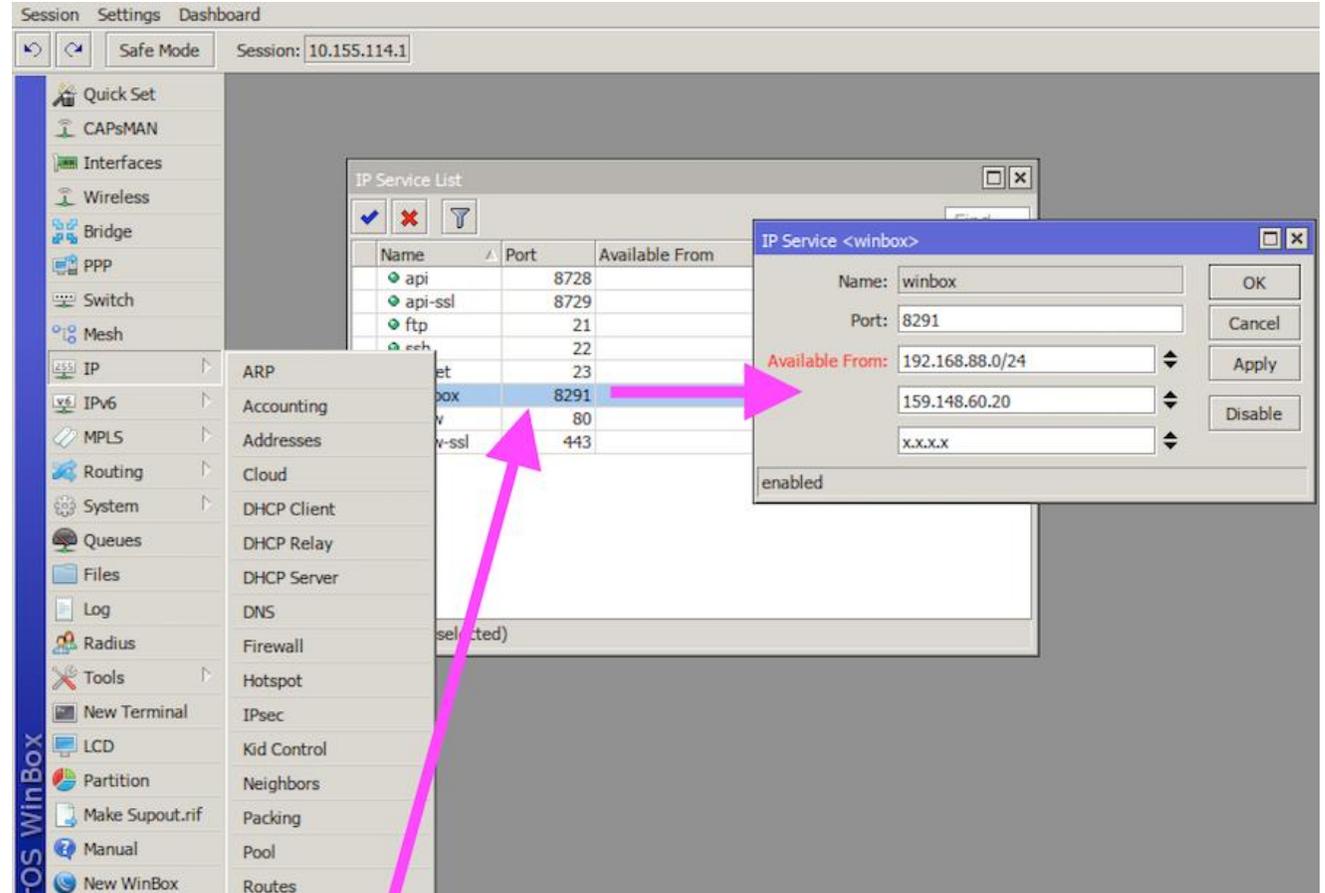
- Winbox in the Wild <https://medium.com/tenable-techblog/winbox-in-the-wild-9a2ee4946add>
- There are 600 000 Winbox interfaces open to the Internet without restrictions
- Less than 15% on patched versions
- Shodan is an excellent resources to mine information on your own network
- South Africa is a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



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

The screenshot shows the 'Manage VPN Server' interface for 'acamastelek.softether.net'. It features a table of Virtual Hubs, a 'Management of Listeners' section with a table of listening ports, and a 'VPN Server and Network Information and Settings' section with various configuration buttons.

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
157Speculator	Online	Standalone	2	0	0	0	0
34Dias	Online	Standalone	2	0	0	0	0
amastelek	Online	Standalone	2	0	0	0	0
datacall	Online	Standalone	11	0	1	41	59
NWAdmin	Online	Standalone	2	0	2	2	2
SDWANAdmin	Online	Standalone	7	0	3	3	5
x34Dias	Online	Standalone	2	0	0	0	0

Management of Listeners:
Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening

VPN Server and Network Information and Settings:

- Encryption and Network
- View Server Status
- About this VPN Server
- Clustering Configuration
- Clustering Status
- Show List of TCP/IP Connections
- Edit Config
- Local Bridge Setting
- Layer 3 Switch Setting
- IPsec / L2TP Setting
- OpenVPN / MS-SSTP Setting
- Dynamic DNS Setting
- VPN Azure Setting
- Refresh
- Exit

Current DDNS Hostname: acamastelek.softether.net VPN Azure Hostname: acamastelek.vpnazure.net

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.

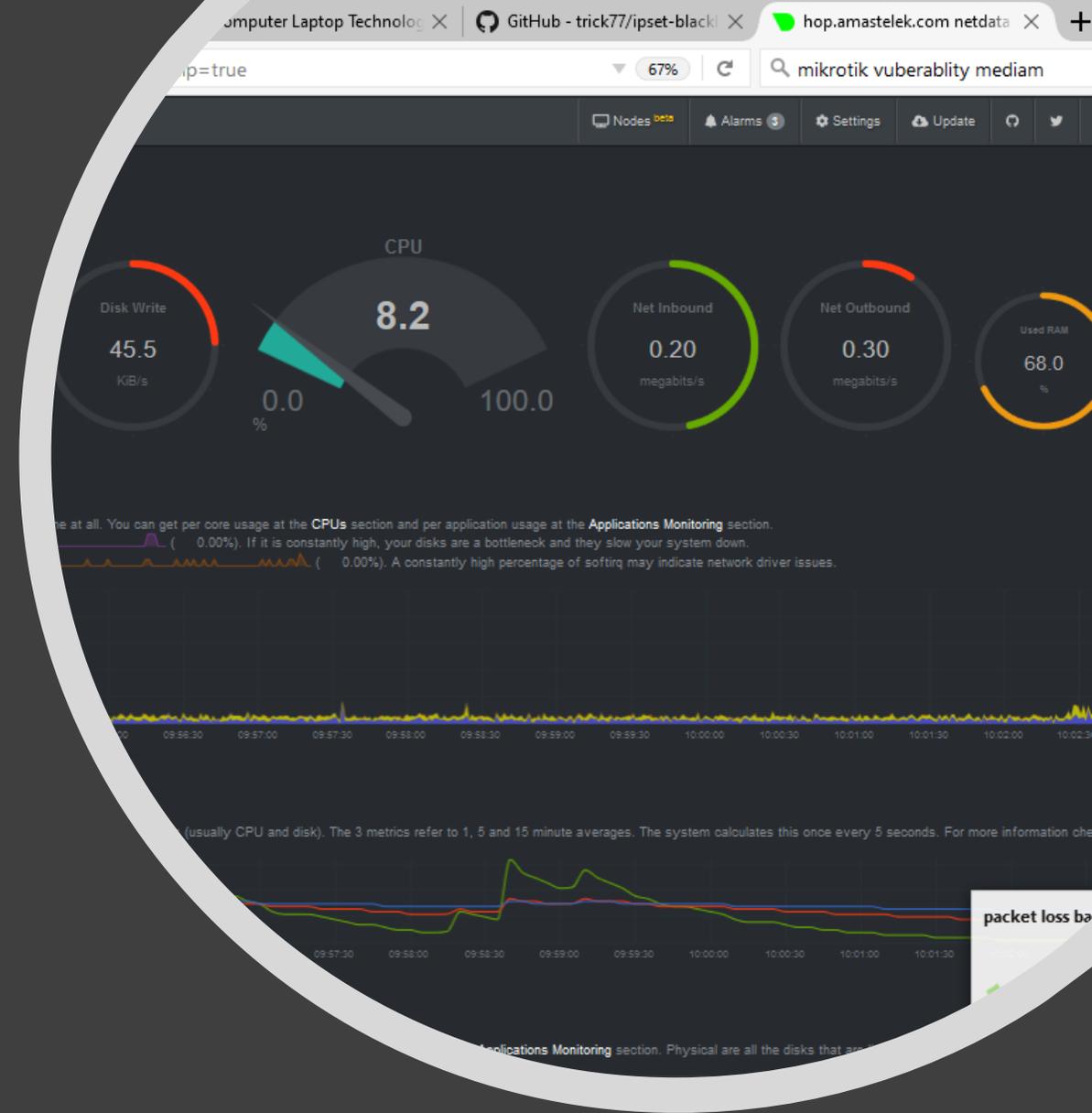
A close-up photograph of a hand holding a white ceramic mug filled with coffee. The coffee has a thick, golden-brown foam on top, with many small bubbles visible. The background is blurred, showing what appears to be a wooden surface and a small brown object.

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/>

