Secure & manageable Tiks

Andy Morrison

ANDISA IT CONSULTANTS LTD

- Based in Harrogate near Leeds.
- Provide Mikrotik consultancy & IT Consultancy world wide
- Specialising in Mikrotik Router Consultancy, Hosted & On Premise Microsoft systems and VoIP
  - MTCNA,MTCRE,MTCWE, Presented at Kathmandu last year
  - Happy to work “whitebox” along side other IT providers to help improve their own network and infrastructure service.

EXAMPLES OF RECENT PROJECTS

andisa
MAKING I.T. WORK FOR YOU

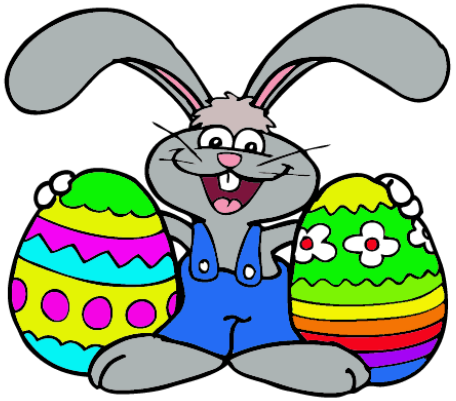
- 400sqkm wireless network in Nepal providing internet to schools
- Multisite LAN linking Ripon Cathedral to its other 5 buildings across the town.
- Wifi for hotels in Accor group managed by Mikrotik devices
- Leeds hosting centre perimeter and client segregation security.

QUESTIONS WE GET ASKED

Can we help show engineers how to set up a Tik so that their company can fix it while out on the road?

YES

How do you catch the Ether bunny



With an Ether net! Boom boom

WHY ATTACK?

Because they can! It's fun. 80%
recent generations have the time, the patience and the knowledge! – don't give them the opportunity!

Theft – 15%
Access to internal systems for information and transactions.

To make a statement – 5%
The "greenpeace" approach. Make a statement in a big way.

SURELEY A TIK IS PERFECT?

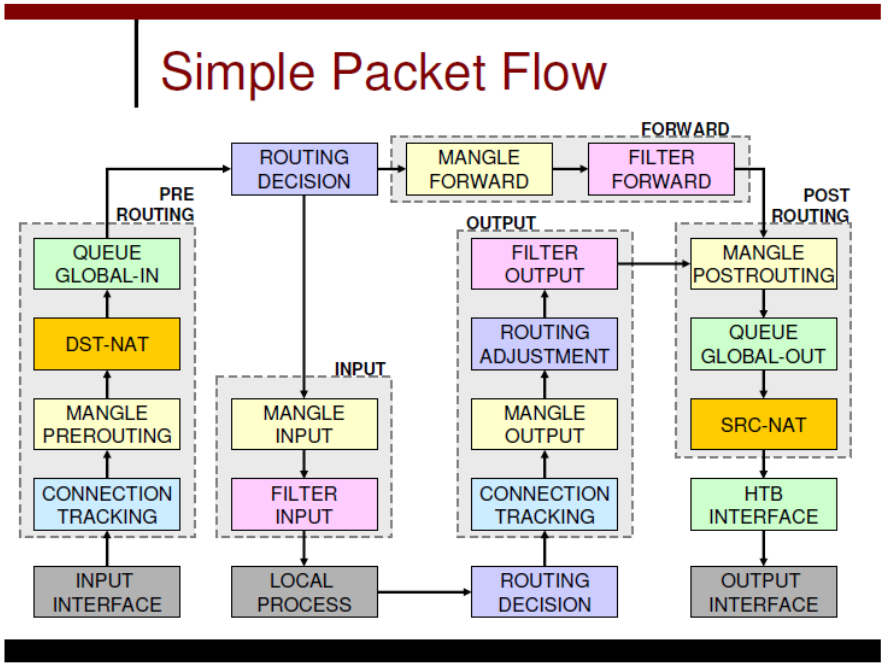
Tiks are nearly perfect but somebody has to program them.

Assume people WILL make mistakes.

1. Block very specifically
2. Add lots of comments
3. Develop your own default config
4. Keep everything up to date.
5. Naming convention – share it.
6. Changelog
7. Prepare

WHICH CHAIN?

1. INPUT CHAIN – earliest point while still allowing FORWARD.

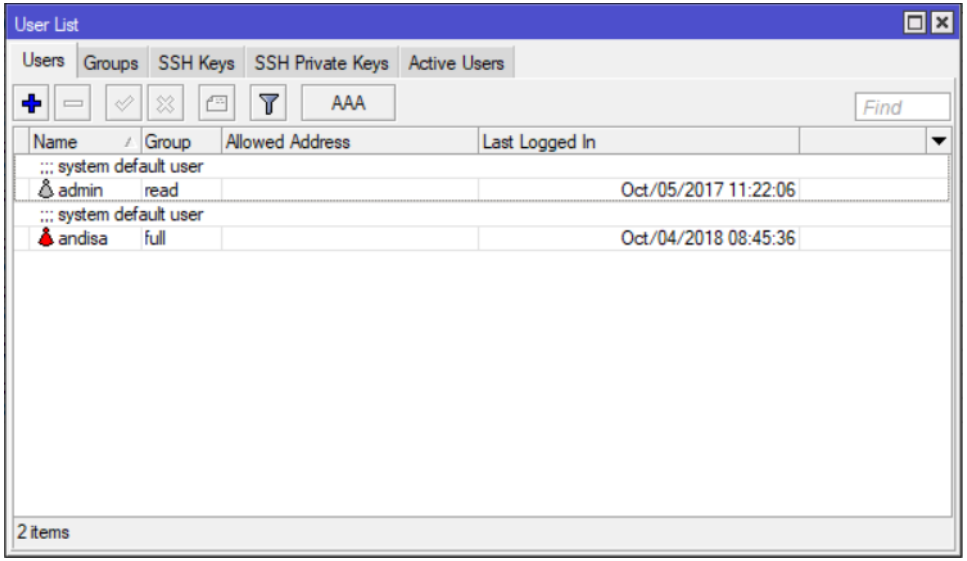


FIRST LINE OF DEFENSE

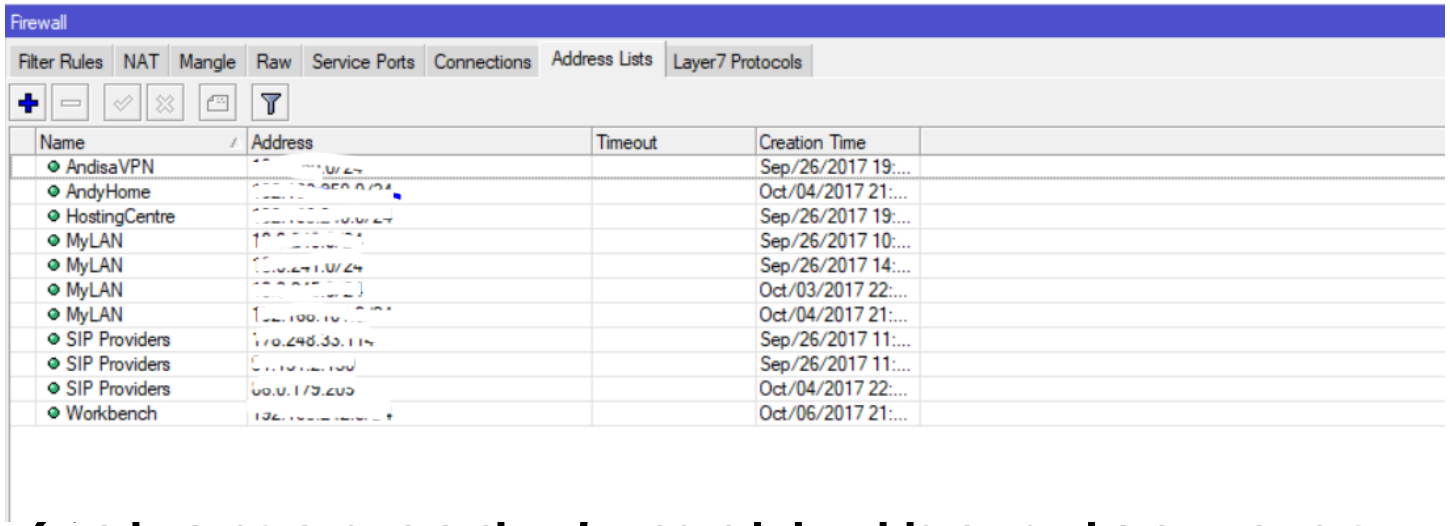
Everyone knows the default

Copy admin and then admin a “read only”

/system users



WHERE TO ALLOW ACCESS FROM.

1. 

2. Get organised - Simplify the rules using address lists
   /ip firewall address-list

CONTROL THE TRAFFIC

1. Block limited traffic
2. Allow limited traffic
3. Block everything else

Don’t forget to allow you first.

/ip firewall filter

```
add action=drop chain=input comment="Rule3 - Block Local Admin from Workbench" src-address-list=Workbench
add action=drop chain=input comment="Rule3 - Block Local Admin from Workbench" in-interface=Workbench
add action=accept chain=input comment="Rule3 - Allow Local Admin from LAN" src-address-list=MyLAN
add action=accept chain=input comment="Rule 4 - Allow Established INPUT" connection-state=established
add action=drop chain=input comment="Rule 5 - Drop all other input INPUT"
```

HALF WAY THERE

- You've got a tik that customers can route through and you can manage from your office.
- You've blocked unwanted addresses.

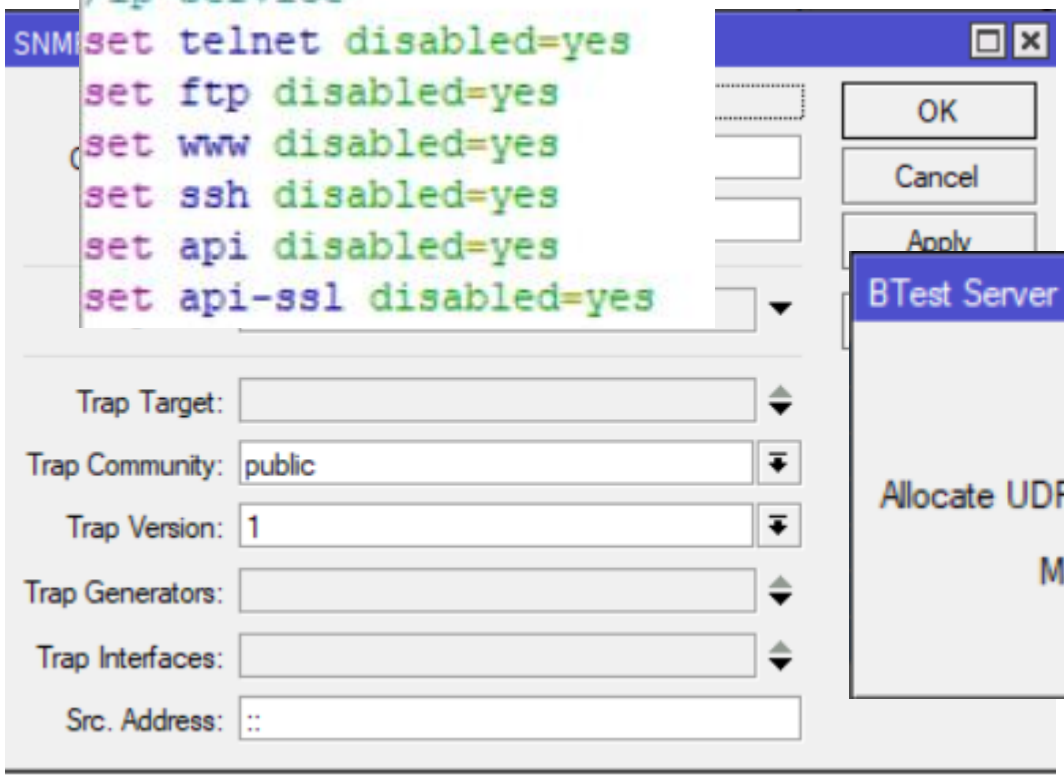
- However some traffic can still get in! Think what might come from the networks you have allowed.

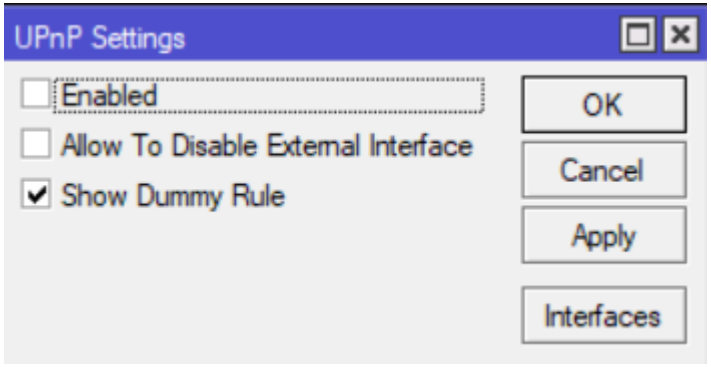
- What about fingers too – physical security

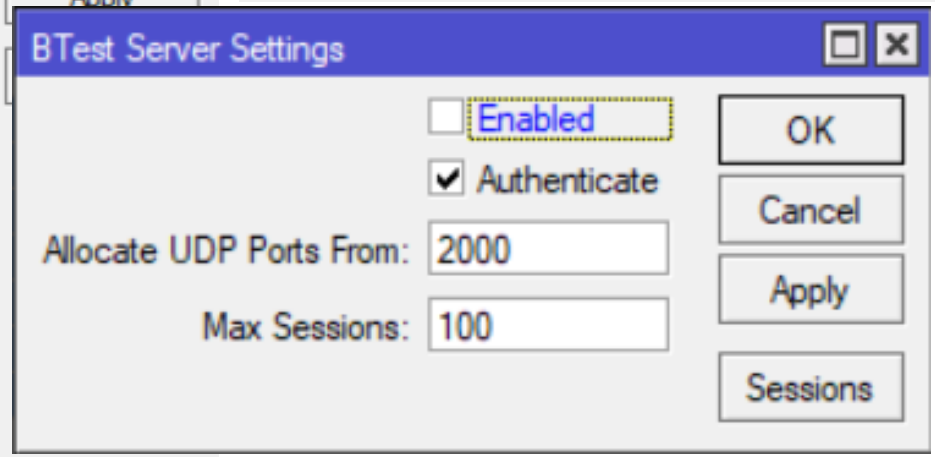
DISABLE UNWANTED SERVICES?

/ip neighbor discovery set [find] discover=no

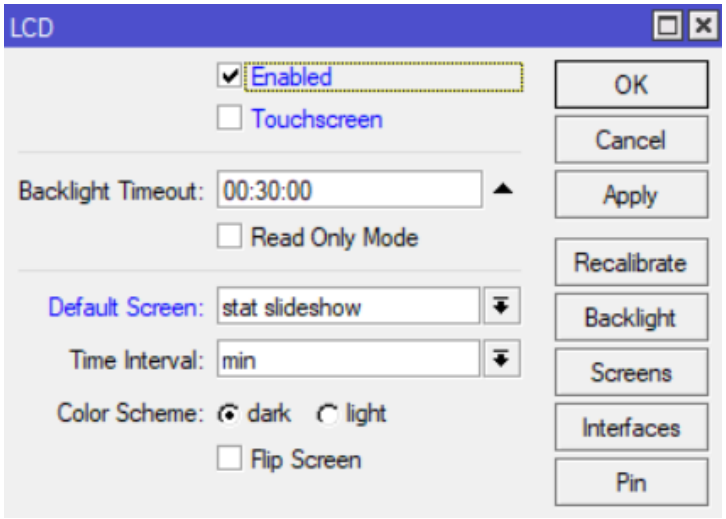
```
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
```

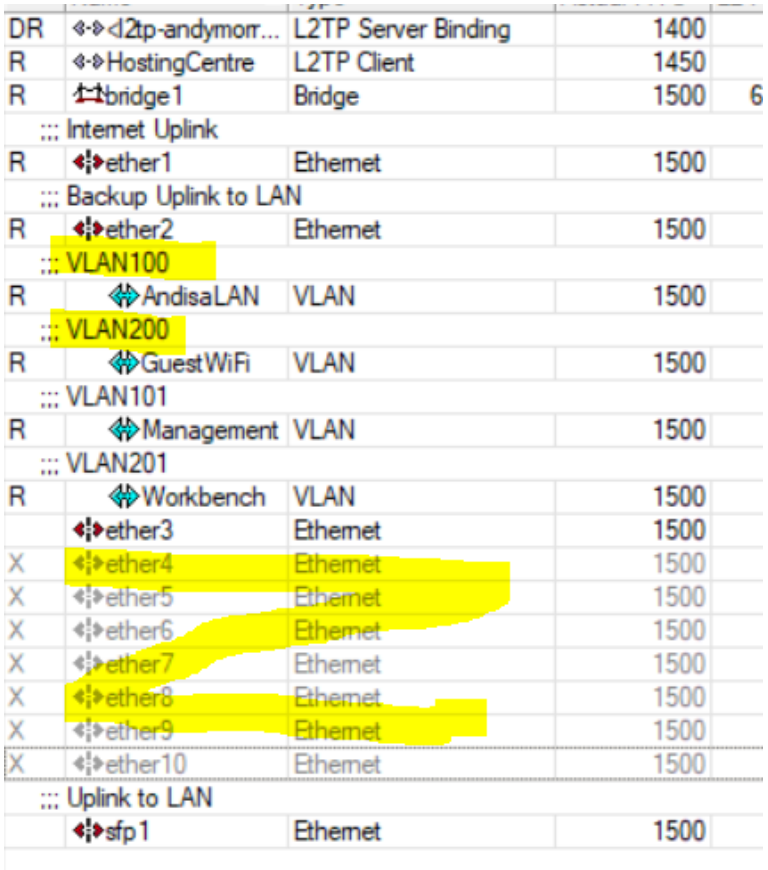






PHYSICAL SECURITY?





- Good documentation and comments
- Disable ports

NEARLY THERE!

Now you've got a Tik that customers can route through !
AND

You can manage it from your office!
AND

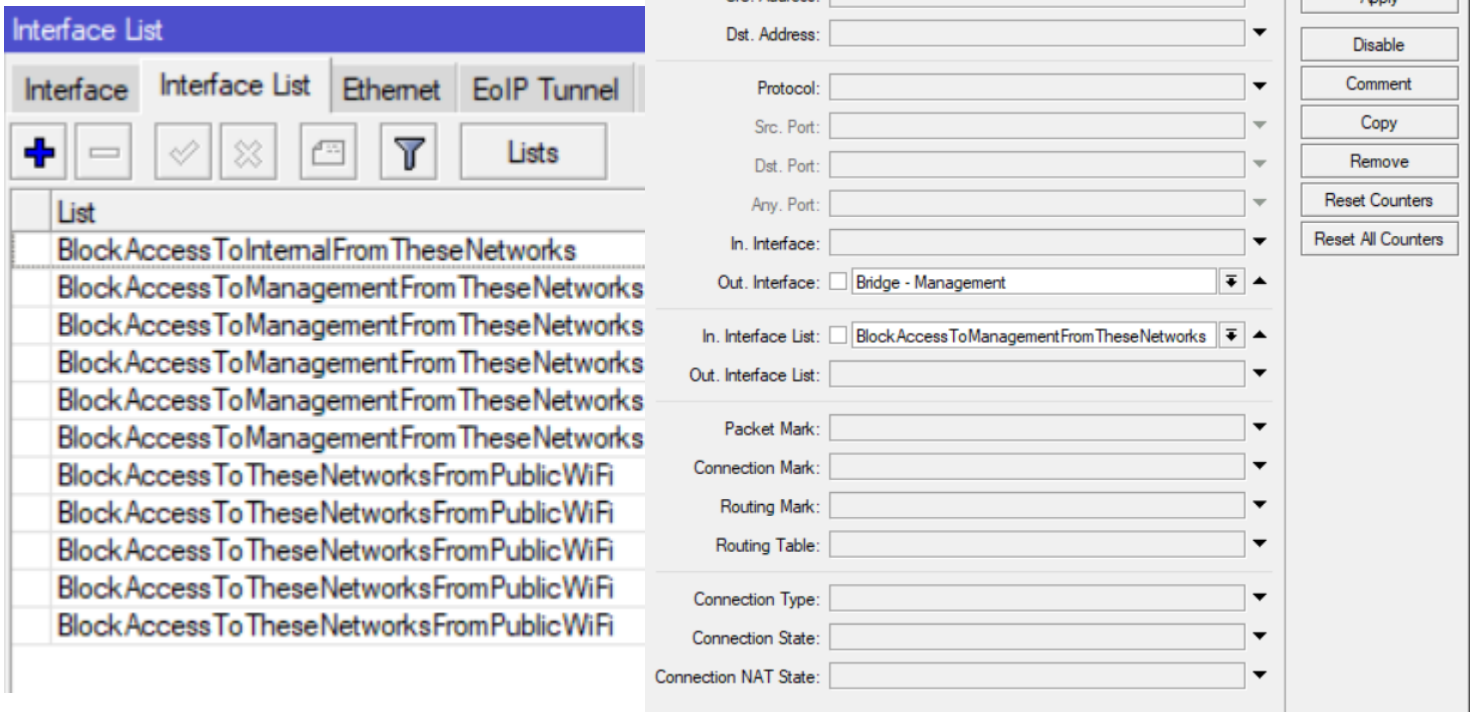
Even if somebody does manage to break your network they still cant browse or discover!

MORE BEST PRACTICES

- Regularly use a port scanner and check you config.
- Use VLANS to separate traffic by purpose / dept.
- Block interVLAN traffic with an INPUT rule and interface list.
- Change SSH keys / strength from defaults – ID the right router!
- Rename SNMP public
- Consider Radius – central user management

INTERFACE LIST

- /interface interfac



CALL ME

- andy@andisa.net
- 01423290029
- www.andisa.net