

Secure & manageable Tiks

Andy Morrison



- 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 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?



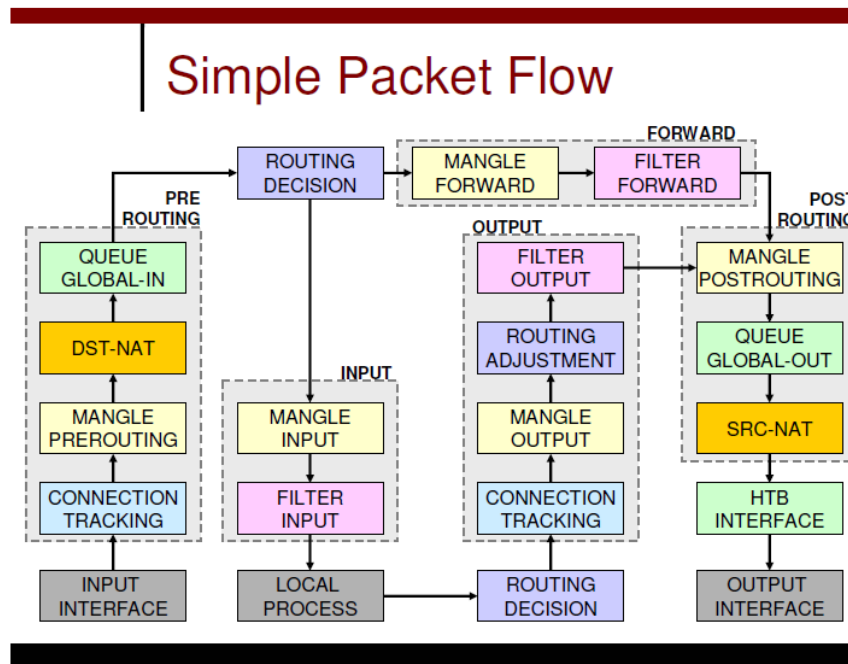
Tiks are nearly perfect but somebody has to program them.

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.

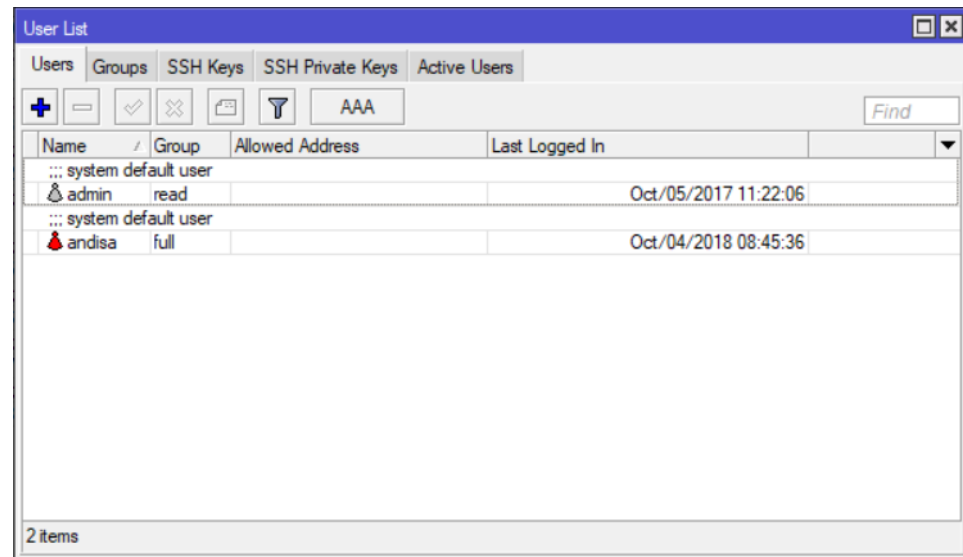


FIRST LINE OF DEFENSE

Everyone knows the default

Copy admin and then admin a “read only”

/system users



The screenshot shows the 'User List' window in Mikrotik WinBox. It displays a table of users with columns for Name, Group, Allowed Address, and Last Logged In. The table contains two entries: 'admin' with group 'read' and 'andisa' with group 'full'. The 'admin' user was last logged in on Oct/05/2017 at 11:22:06, and the 'andisa' user was last logged in on Oct/04/2018 at 08:45:36. The window also shows tabs for Users, Groups, SSH Keys, SSH Private Keys, and Active Users, along with a search bar and a 'Find' button.

Name	Group	Allowed Address	Last Logged In
admin	read		Oct/05/2017 11:22:06
andisa	full		Oct/04/2018 08:45:36

WHERE TO ALLOW ACCESS FROM.



1.

Name	Address	Timeout	Creation Time
AndisaVPN	10.0.0.0/24		Sep/26/2017 19:...
AndyHome	192.168.0.0/24		Oct/04/2017 21:...
HostingCentre	192.168.0.0/24		Sep/26/2017 19:...
MyLAN	10.0.0.0/24		Sep/26/2017 10:...
MyLAN	10.0.24.1/24		Sep/26/2017 14:...
MyLAN	10.0.0.0/24		Oct/03/2017 22:...
MyLAN	10.0.0.0/24		Oct/04/2017 21:...
SIP Providers	170.248.30.114		Sep/26/2017 11:...
SIP Providers	0.0.0.0/0		Sep/26/2017 11:...
SIP Providers	0.0.0.0/0		Oct/04/2017 22:...
Workbench	192.168.0.0/24		Oct/06/2017 21:...

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
```

```
SNMP  
/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
```

Trap Target:

Trap Community:

Trap Version:

Trap Generators:

Trap Interfaces:

Src. Address:

Dialog box with OK, Cancel, and Apply buttons.

UPnP Settings dialog box

- Enabled
- Allow To Disable External Interface
- Show Dummy Rule

Buttons: OK, Cancel, Apply, Interfaces

BTest Server Settings dialog box

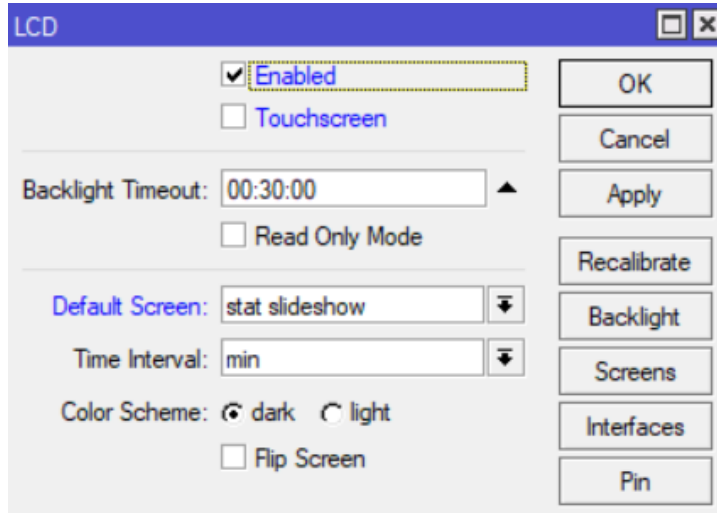
- Enabled
- Authenticate

Allocate UDP Ports From:

Max Sessions:

Buttons: OK, Cancel, Apply, Sessions

PHYSICAL SECURITY?



DR	↔↔<l2tp-andymorr...	L2TP Server Binding	1400	
R	↔↔HostingCentre	L2TP Client	1450	
R	↔↔bridge1	Bridge	1500	6
::: Internet Uplink				
R	↔↔ether1	Ethernet	1500	
::: Backup Uplink to LAN				
R	↔↔ether2	Ethernet	1500	
::: VLAN100				
R	↔↔AndisaLAN	VLAN	1500	
::: VLAN200				
R	↔↔GuestWiFi	VLAN	1500	
::: VLAN101				
R	↔↔Management	VLAN	1500	
::: VLAN201				
R	↔↔Workbench	VLAN	1500	
	↔↔ether3	Ethernet	1500	
X	↔↔ether4	Ethernet	1500	
X	↔↔ether5	Ethernet	1500	
X	↔↔ether6	Ethernet	1500	
X	↔↔ether7	Ethernet	1500	
X	↔↔ether8	Ethernet	1500	
X	↔↔ether9	Ethernet	1500	
X	↔↔ether10	Ethernet	1500	
::: Uplink to LAN				
	↔↔sfp1	Ethernet	1500	

- 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!



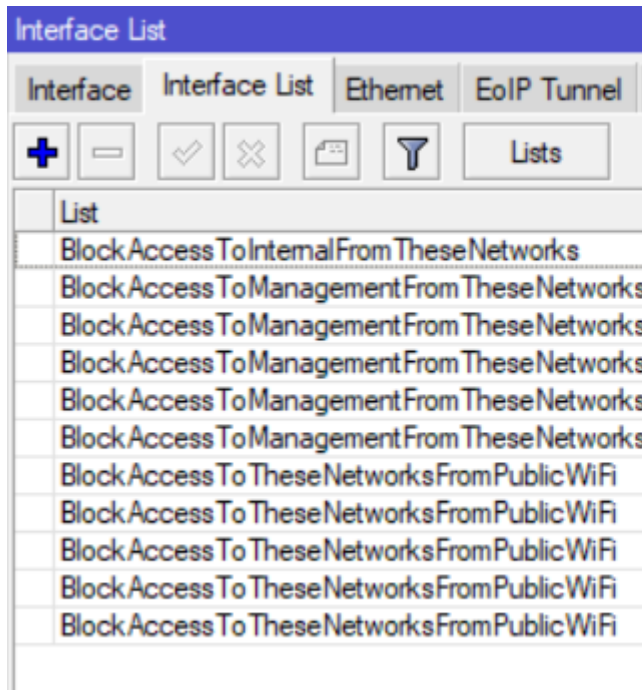
MORE BEST PRACTICES



- 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

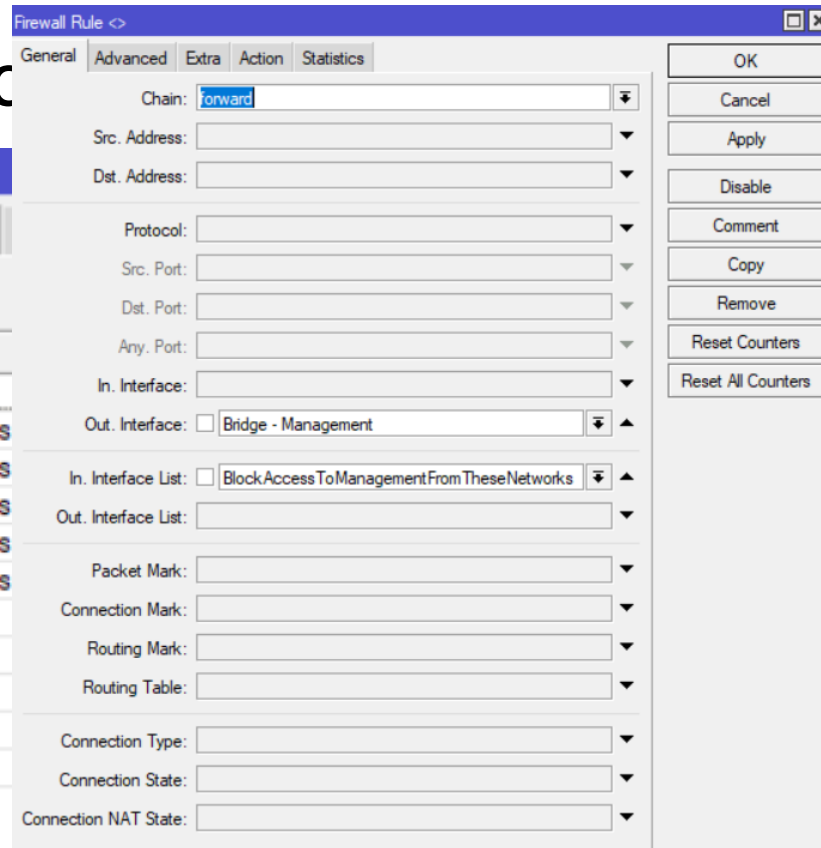
INTERFACE LIST

- /interface interface



The screenshot shows the 'Interface List' window in Mikrotik WinBox. It features a toolbar with icons for adding, deleting, and filtering lists. Below the toolbar is a table with the following entries:

List
Block Access To Internal From These Networks
Block Access To Management From These Networks
Block Access To Management From These Networks
Block Access To Management From These Networks
Block Access To Management From These Networks
Block Access To Management From These Networks
Block Access To These Networks From Public WiFi
Block Access To These Networks From Public WiFi
Block Access To These Networks From Public WiFi
Block Access To These Networks From Public WiFi
Block Access To These Networks From Public WiFi



The screenshot shows the 'Firewall Rule' configuration window in Mikrotik WinBox. The 'Chain' is set to 'forward'. The 'In. Interface' is set to 'Bridge - Management'. The 'In. Interface List' is set to 'Block Access To Management From These Networks'. The 'Out. Interface List' is empty. The 'Connection Type' is set to 'any'. The 'Connection State' is set to 'any'. The 'Connection NAT State' is set to 'any'. The 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Routing Table' are all set to 'any'. The 'Protocol', 'Src. Address', 'Dst. Address', 'Src. Port', 'Dst. Port', and 'Any. Port' are all set to 'any'. The 'Chain' is set to 'forward'. The 'Src. Address' and 'Dst. Address' are both empty. The 'Protocol' is set to 'any'. The 'Src. Port' and 'Dst. Port' are both empty. The 'Any. Port' is set to 'any'. The 'In. Interface' is set to 'Bridge - Management'. The 'Out. Interface' is set to 'any'. The 'In. Interface List' is set to 'Block Access To Management From These Networks'. The 'Out. Interface List' is empty. The 'Packet Mark' is set to 'any'. The 'Connection Mark' is set to 'any'. The 'Routing Mark' is set to 'any'. The 'Routing Table' is set to 'any'. The 'Connection Type' is set to 'any'. The 'Connection State' is set to 'any'. The 'Connection NAT State' is set to 'any'. The 'Chain' is set to 'forward'. The 'Src. Address' and 'Dst. Address' are both empty. The 'Protocol' is set to 'any'. The 'Src. Port' and 'Dst. Port' are both empty. The 'Any. Port' is set to 'any'. The 'In. Interface' is set to 'Bridge - Management'. The 'Out. Interface' is set to 'any'. The 'In. Interface List' is set to 'Block Access To Management From These Networks'. The 'Out. Interface List' is empty. The 'Packet Mark' is set to 'any'. The 'Connection Mark' is set to 'any'. The 'Routing Mark' is set to 'any'. The 'Routing Table' is set to 'any'. The 'Connection Type' is set to 'any'. The 'Connection State' is set to 'any'. The 'Connection NAT State' is set to 'any'.

CALL ME



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