#### <36 Networks>

## **Mikrotik Security**

## IP -> Services

- Disable unused services
- Set Available From for appropriate hosts
- Secure protocols are preferred (Winbox/SSH)

IP Service List									
<b>~</b>	* 7							Find	
	Name	Δ	Port		Available From		Certificate		-
	api		8	728	0.0.0.0/0				
				21	0.0.0.0/0				
	ssh			22	0.0.0.0/0				
	telnet			23	0.0.0.0/0				
	winbox		8	291	0.0.0.0/0				
	www			80	0.0.0.0/0				
Х	www-ssl			443	0.0.0.0/0		none		

# IP -> Neighbors

- Disable Discovery Interfaces where not necessary. All interfaces that don't directly connect to your own infrastructure.
- Note: Winbox discovery won't work if you disable neighbor discovery.

📑 Neighbo	or List		×
Neighbors	Discovery Interfaces		
+ -	× × 7	Find	
Interfa	ace /		-
🔔 bri	dge1		
📜 🚺 etł	ner1		
🛛 🗶 🛝 wla	an1		

## Tools -> Btest Server

 By default the bandwidth test server is enabled. Be sure to only activate this when necessary.

🔲 BTest 9	5erver						×
- 7	BTest S	erver Setti	ngs	]		Find	
Addre	ess	A Protoc	col I	Direction	User		-
BT	act Sarua	er Setting	6			X	
Alloca	ite UDP Po Max S	rts From: [ dessions: [	2000 10	nabled uthenticate		OK Cancel Apply	
0 items							

### System -> Users

- Users are assigned to groups.
- Groups specify what access you get.
- User section allows password changes.

🔜 User List		×					
Users Groups Active Users	SSH Keys		User List				×
Name A Group System default user A admin full test read	Name: user Group: read   Allowed Address:	OK       Cancel       Apply       Disable       Comment       Copy       Remove       Password	Users Groups ,	Active Users SSH Keys          New Group         Name:       group1         - Policies       itelnet         issh       ftp         reboot       read         write       policy         test       winbox         password       web         sniff	OK       Cancel       Apply       Comment       Copy       Remove	Find nbox passw web sniff sword web	

## System -> Logging and Log

- Setup special actions to get more detail on a specific subject.
- Send to syslog server (CactiEZ).

	1	_:		V								
L-	Log	ging		스					Log			×
	2. Jac	Actions									al	<b>-</b>
	hules	Actions			Loggi	ing			Les /25 /1970 00:27-50		jones 09.10 DE-29.04.9E/Output: last comparties as because reaction	
	_								Jan/25/1970 06:37:56	wireless into	00.1C.DF.39.64.8E@wiar1. lost connection, no beacons received	
	-    -	-   Y		Find	Rules	Actions			001/20/1010 00.01.01		jones	
					1 P				Jan/25/1970 08:26:58	wireless info	00:1C:DF:39:6A:8E@wlan1: lost connection, no beacons received	
	N	lame 🛆 Ty	pe	<b></b>	- +				Jan/25/1970 08:26:59	wireless info	00:1C:DF:39:6A:8E@wlan1 established connection on 2412, SSID jones	
×	di	isk dis	k						Jan/26/1970 05:15:25	wireless info	00:1C:DF:39:6A:8E@wlan1: lost connection, no beacons received	
×	e	cho ec	ho		Top	pics 🛛 🗚	Prefix	Act	Jan/26/19/0 05:15:42	wireless into	UU:TU:DF:39:6A:8E @wilanT: failed to connect, on 2412, authentical timeout	ion
×	m	nemory me	mory		crit	ical		ech	Jan/26/1970 05:15:55	wireless info	00:1C:DF:39:6A:8E@wlan1 established connection on 2412, SSID jones	
×	te	emote rer	note		erro	or		mer	Jan/26/1970 12:38:34	system info account	user admin logged in from 192.168.222.103 via winbox	
		101				_			Jan/26/1970 12:39:01	system info	Service manager settings changed by admin	
					Info	)		mer	Jan/26/19/012:49:48	system into account	user admin logged in from 192.168.222.103 via teinet	
		Log Action <	<remote></remote>	×	wa	( <u> </u>	1		Jan/26/1970 12:57:46	system into account	SNTP client configuration changed by admin	- <b>T</b>
						New Log Rule			1001/20/1010 12:00:00	system me	of the click configuration changes by damin	
		Name	remote	ок								
		_				Topics: ! ups	∓ ≑	(	DK			
		Туре	remote 🗧 🗧	Cancel								
						Prefix:	•	Ca	ancel			
		Remote Address	0000	Apply								
		Tremote Address.	0.0.0.0			Action: remote	•	A A	pply			
		Remote Port	514	Сору								
								Dis	sable 🛛			
				Bemove								
								l c	opy			
		dofault										
4	items	uerauit						Re	move			
		(										

## **Basic Diagram**



## Packet Flow - Bridging

Via http://wiki.mikrotik.com/wiki/Packet\_Flow



## Packet Flow - Routing

Via http://wiki.mikrotik.com/wiki/Packet\_Flow





## **PAT** Protection

- PAT(Port Address Translation) "NAT Overload"
- This gives you some protection because connections can't be sourced from outside of your network.
- The easiest method is to IP -> firewall -> NAT. Then create a source nat with action of masquerade.

### IP -> Firewall -> Filter

- Lets get down to the nitty gritty, firewall filtering.
- There are 3 chain options:
  - Input The input chain is traffic destined TO the router. This would be someone trying to ping the router or IPSec traffic destined for the router.
  - Output The output chain is traffic sourced from the router heading OUT. This would be an ICMP reply or the router initiating a ping out.
  - Forward The forward chain is traffic moving through the router. This is where most all of our rules will be made.

# • There are 10 action options (here are the most used):

- Accept This stops processing the rule and does nothing.
- Add dst to address list This



- will add the destination address to a specified address list. You can even specify an amount of time for the address to timeout of the list.
- Add src to address list Opposite of dst version.
- Drop This will discard packets that match this rule.
- Log This will put an entry in the log file every time this rule is matched. It will also include the src/dst IP address.
- Tarpit Used with botnet attacks. This will reply to the attack with a SYN/ACK packet and holds open the TCP session. This fools the attacker into thinking he hit the actual server when it is really just the router.

### Allowing Specific SMTP Outbound

- Often you want to allow your users to only use your specific SMTP server. This will prevent users infected with viruses from spamming.
- First. put in an allow for a specific SMTP server.

New Firewall Rule	New Firewall Rule
General Advanced Extra Action St	General Advanced Extra Action
Chain: forward	Action: accept
Src. Address: 192.168.1.0/24	. <u> </u>
Dst. Address: 🗌 1.1.1.1	
Brotocol: 6 (tep)	
Src. Port:	
Dst. Port: 25	

• Now put in the deny for anyone trying to reach any other SMTP.

🔤 New Firewall Rule	New Firewall Rule				
General Advanced Extra Action Statistics	General Advanced Extra Action Statistics				
Chain: forward	Action: drop				
Src. Address:  192.168.1.0/24					
Dst. Address: 0.0.0.0/0					
Protocol: 6 (tcp)					
Src. Port:					
Dst. Port: 25					

## Arranging Rules

- The order of operation is very important. Rules are processed top down. A packet starts at the top of the firewall rules list. It keeps passing down the rules until it finds a match. Once it finds a match, processing is stopped.
- Rules can be dragged and dropped to change the order.

### Address Lists

 Address lists can be lists of individual IP address or subnets. These can be used in filter rules or in mangle rules. These can be built manually or automatically.

Filter Rules NAT Ma	angle Service Ports	Connections	Address Lists
+ - 🖉 💥	≝ 🍸		
Name A A	ddress		
📔 🔤 New Firewall Add	dress List	×	
Name:	₹ 0	к	
Address: 0.0.0.0	Car	ncel	
	Ap	ply	
	Disa	able	
	Com	ment	
	Co	ру	
Ī	Rem	iove	
disabled			
1 2			

## Layer 7 Matching

- L7 matching checks the data portion of the packet. This means the traffic can't be encrypted to be matched.
- The L7 matches in regex (regular expression) format.
- L7 can be used in firewall and mangle rules.

Firewall				
Filter Rules NAT Mangle Service Ports Con	nections A	Address Lists	Layer7 Protocols	
+ - 🗅 🍸				
Name 🛆 Regexp				
New Firewall L7 Protocol		×		
Name: block wordpress	OK			
Regexp:	Cancel			
^.*get.+(/wp-admin/ /wp-login.php).*\$	Apply			
	Commen	ıt		
	Сору			
	Remove			

# **Bridging Interfaces**

- For a 5 port RB, it is common to have a single internet interface and bridge the remaining interfaces together.
- An IP will be assigned to the Bridge interface.



# **Bridging Configuration**

- Create the bridge
- Add ports to the bridge.

		📑 Bridge	
		Bridge Ports Filters NAT Hosts	
Bridge		+ - 🗸 🗶 🎦 🍸	
Bridge Ports Filters NAT Hosts		Interface 🛆 Bridge Price	rity (h Path Cost Horizon F
💠 💳 🗸 Settings		New Bridge Port	×
Interface <bridge1></bridge1>	× B× F	General Status	ОК
B General STP Status Traffic	ОК	Interface: ether4	Cancel
Name: bridge1	Cancel	Bridge: bridge1	Apply
Type: Bridge	Apply	Priority: 80	hex Disable
MTU: 1500	Disable	Path Cost: 10	Comment
MAC Address:	Comment	Horizon:	▼ Сору
ARP: enabled	Сору	Edge: auto	<b>∓</b> Remove
	Remove	Point To Point: auto	
	Torch	External FDB: auto	

## **Enabling Bridging Firewall**

• From bridge, click settings and then choose "Use IP Firewall".

📑 Brid	ge
Bridge	Ports Filters NAT Hosts
+ =	🖉 🖉 🖉 Settings
N	ame 🔺 Type
R ≰≃	bridge1 Bridge
В	ridge Settings 🛛 🔀
	Jse IP Firewall OK
	Jse IP Firewall For VLAN Use IP Firewall For PPPoE
	Apply

# **Rogue DHCP Detection**

- There is a built in rogue detection program, though it gives false positives.
- I prefer to use IP -> DHCP Client, the DHCP Client.
- Be sure you uncheck DNS, NTP and Default route, otherwise a rogue can introduce new routes into your routing table.

DHCP	Client				
+ -			<b>7</b> Release	Rene	W
New	DHCP Clie	nt			×
DHCP	Status				OK
	Inte	rface:	ether1	₹	Cancel
	Hostr	name:		-	Apply
	Clie	nt ID:		]▼	Disable
			Use Peer DN	S   P	Сору
			Add Default f	Route	Remove
Default	Route Dist	ance:	0		Release
					Renew
disabled				stopped	l

## SSH Tunnel

• Allows you to tunnel any traffic through the MTK into a network.



## Resources

- Awesome Site <u>http://GregSowell.com</u>
- Mikrotik Video Tutorials -<u>http://gregsowell.com/?page\_id=304</u>
- Mikrotik Support Docs-<u>http://www.mikrotik.com/testdocs/ros/3.0/</u>
- CactiEZ <u>http://cactiez.cactiusers.org/download/</u>
- Cacti Video Tutorials <u>http://gregsowell.com/?page\_id=86</u>
- Great Consultant ;)-<u>http://gregsowell.com/?page\_id=245</u>