



Securing your Mikrotik Network

Andrew Thrift

andrew@networklabs.co.nz

Who am I ?

Andrew Thrift

Mikrotik Certified Consultant

Based in New Zealand

Using Mikrotik RouterOS since around 2002

Working in network security since 1999

Blog with Andrew Cox @ www.mikrotik-routeros.com

Agenda

- Attack Types
- Detecting attacks
- Securing your routers
- Protecting your network
- Question Time

Types of network based attacks

- Attacks on your routers
 - Unauthorised logins
 - Brute force attacks
 - Denial Of Service
- Customer misuse
 - Customers bypassing PPPoE server
 - Rogue DHCP Servers
- Attacks on your networks (customers)
 - Brute force attacks
 - Denial Of Service

Detecting Attacks

Use Intrusion Detection System (IDS/IPS) software

- Snort / Suricata
- Place behind your “border” protection
- Configure alerting

• Use Security Information Events Management (SIEM) software

- Sagan

What is an IDS/IPS

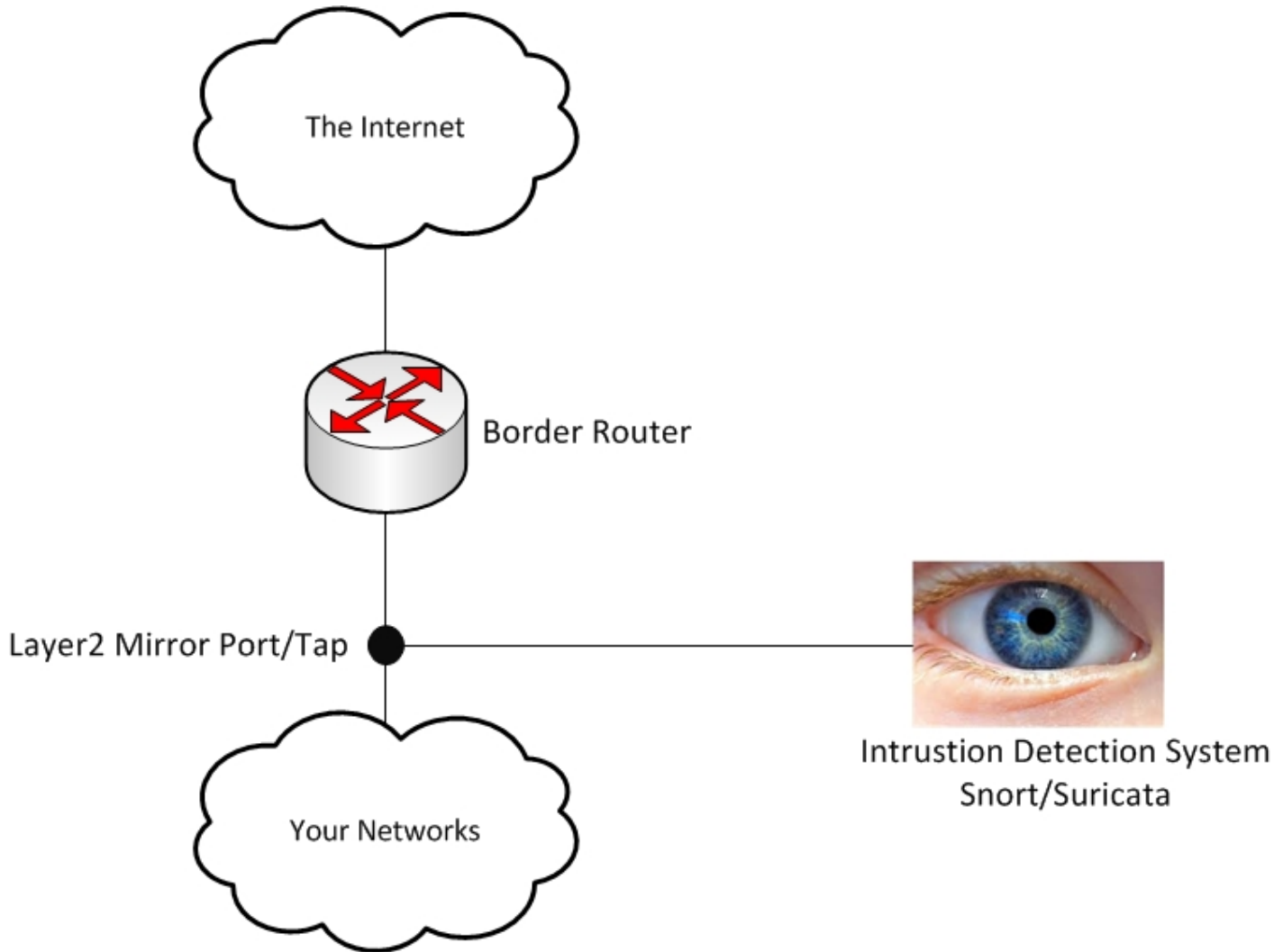
Intrusion Detection System

- Inspects network traffic for “known threats”
- Identifies network threats using:
 - Signatures
 - Behavioural Analysis
 - Heuristics
- Ranks risk severity “Low, Medium, High”
- Common IDS are Snort, Suricata, Bro-IDS

Intrusion Prevention System

- Same as an IDS, but is placed “Inline” and can take actions (drop/mark) based on risk.

Detecting Attacks – Intrusion Detection System



IDS/IPS – What is Suricata

Heard of Snort ?

IDS/IPS - Suricata

Suricata is like Snort, but is better:

- Multi-threaded to scale better on Multi-Core, Multi-Processor systems
- More sane configuration
- Can use existing Snort rule bases
- Fully supported by Emergingthreats.net standard and pro rule bases
- Has been demonstrated doing IPS at wire speed 25 Gigabit on Tiler processors

What is a SIEM ?

Security Information & Events Management

- Inspects log entries and correlates these to “known threats”
- Identifies network threats using:
 - Signatures
 - Behavioural Analysis
 - Heuristics
- Ranks risk severity “Low, Medium, High”
- Common SIEM are Sagan, OSSIM
- Generally require custom rules for RouterOS

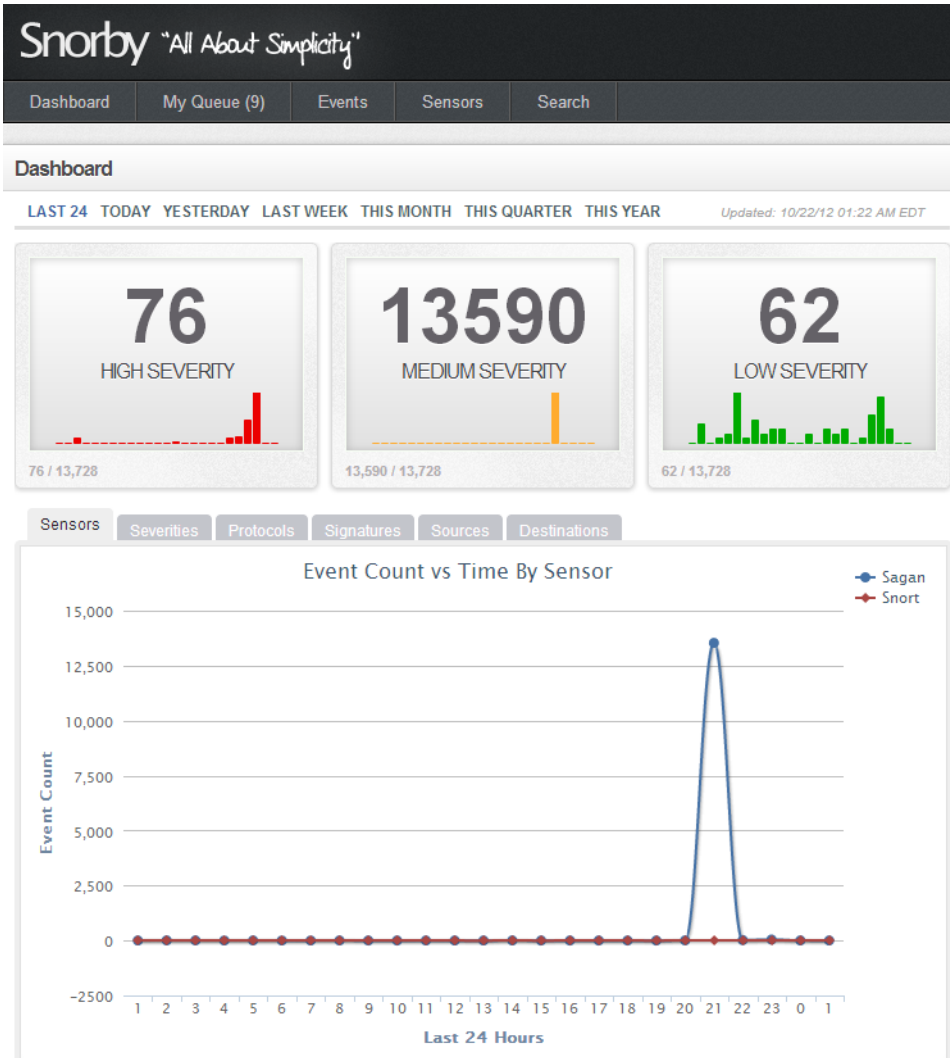
SIEM - Sagan

Sagan is a log analyser:

- Analyses log traffic sent to it via Syslog
- Multi-threaded – Scales well on multi-core/multi-processor systems
- Has flexible “rules” that can correlate multiple different events in to a security event.
- Outputs in Snort format allowing for easy integration

Snorby

Provides a nice Web interface to analyse Suricata + Sagan results



Intrusion Detection for the lazy

Ubuntu + Suricata + Snorby = **SmoothSec**

- Pre-Built “Appliance”
- Works out of the box
- Available from <http://bailey.st/blog/smooth-sec/>
- Can apt-get install sagan for SIEM functionality 😊

What else can you do with an IPS ?

Accurately detect difficult protocols e.g.

- BitTorrent (including DHT/Trackerless torrents)
- Skype (Signalling and media)
- Youtube (Native and embedded)
- VoIP (Signalling and media)

This can be done on standard and non-standard ports.

On match the IPS can change the DSCP tag. Your Mikrotik router can then identify the traffic in mangle using the DSCP tag, and you can then queue this traffic appropriately.

Protecting your routers

Mikrotik Routers have no security configured by default. There are NO firewall policies, all services are accessible from everywhere. You need to protect yourself or it is only a matter of time before your routers are compromised.

How ?

- Disable unused services (WinBox, Telnet, SSH, WebMin)
- Implement “input” IP filters to:
 - Restrict access to router management
 - Minimise the impact of Denial of Service type attack
- Only allow management access within a dedicated Management VRF (RouterOS 6.x + New Routing package)

Protecting your routers - Disabling unused services

Disabling the services you do not use is easy, and once disabled these can not be attacked.

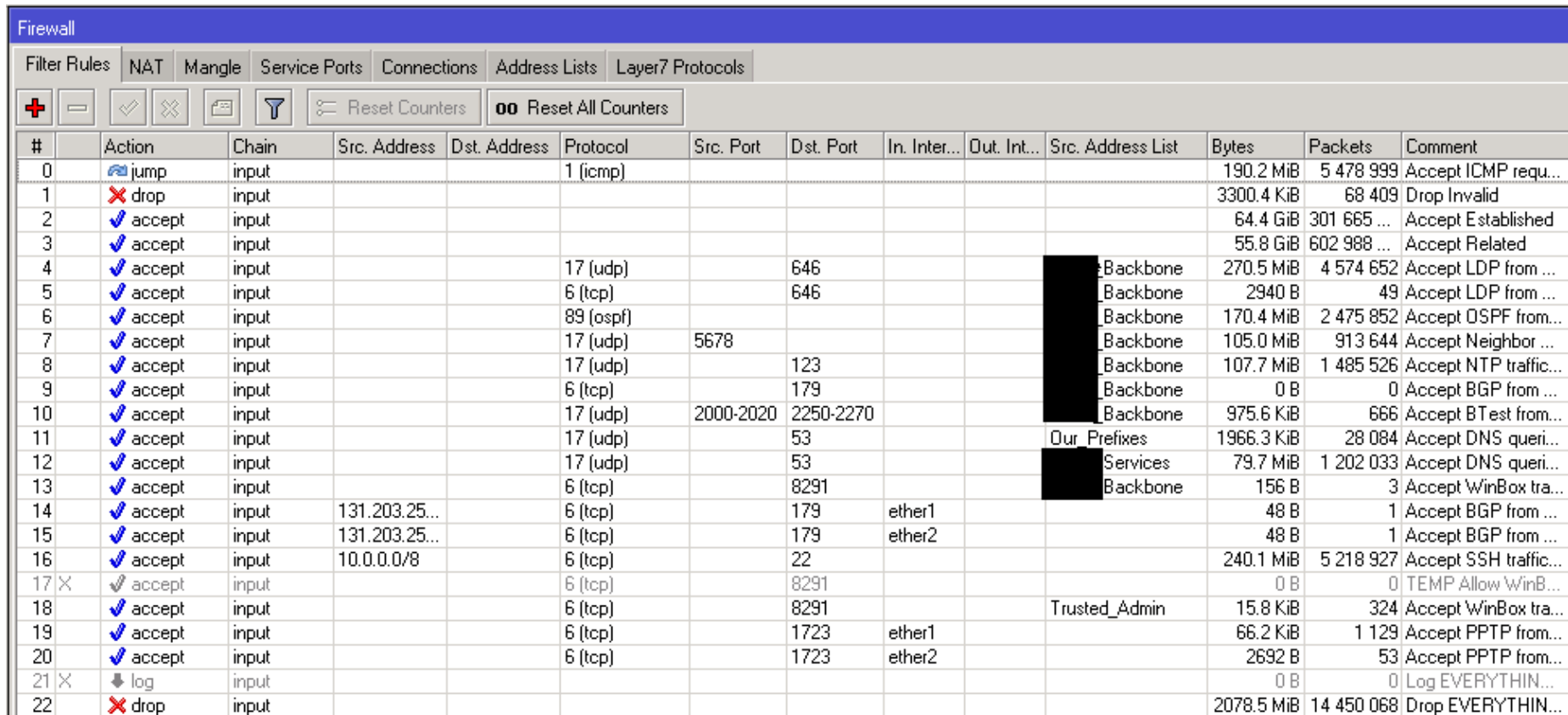
To disable IP services, simply go to:
IP → Services in Winbox and disable the services you do not need.

	Name	Port	Available From	Certificate
<input checked="" type="checkbox"/>	api	8728		
<input checked="" type="checkbox"/>	ftp	21		
<input checked="" type="checkbox"/>	ssh	22		
<input checked="" type="checkbox"/>	telnet	23		
<input checked="" type="checkbox"/>	winbox	8291		
<input checked="" type="checkbox"/>	www	80		
<input checked="" type="checkbox"/>	www-ssl	443		none

7 items

Protecting your routers – IP Filtering

Create “input” policies, accepting the protocols you need. E.g. Winbox, SSH, BGP, OSPF, MPLS LDP, PPTP, DNS. Be specific in your policies, only allow these protocols to enter via a specific interface, or use “Address Lists” to limit these to originate from a group of your subnets.



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Src. Address List	Bytes	Packets	Comment
0	jump	input			1 (icmp)						190.2 MiB	5 478 999	Accept ICMP requ...
1	drop	input									3300.4 KiB	68 409	Drop Invalid
2	accept	input									64.4 GiB	301 665 ...	Accept Established
3	accept	input									55.8 GiB	602 988 ...	Accept Related
4	accept	input			17 (udp)		646			Backbone	270.5 MiB	4 574 652	Accept LDP from ...
5	accept	input			6 (tcp)		646			Backbone	2940 B	49	Accept LDP from ...
6	accept	input			89 (ospf)					Backbone	170.4 MiB	2 475 852	Accept OSPF from...
7	accept	input			17 (udp)	5678				Backbone	105.0 MiB	913 644	Accept Neighbor ...
8	accept	input			17 (udp)		123			Backbone	107.7 MiB	1 485 526	Accept NTP traffic...
9	accept	input			6 (tcp)		179			Backbone	0 B	0	Accept BGP from ...
10	accept	input			17 (udp)	2000-2020	2250-2270			Backbone	975.6 KiB	666	Accept BTest from...
11	accept	input			17 (udp)		53			Our Prefixes	1966.3 KiB	28 084	Accept DNS queri...
12	accept	input			17 (udp)		53			Services	79.7 MiB	1 202 033	Accept DNS queri...
13	accept	input			6 (tcp)		8291			Backbone	156 B	3	Accept WinBox tra...
14	accept	input	131.203.25...		6 (tcp)		179	ether1			48 B	1	Accept BGP from ...
15	accept	input	131.203.25...		6 (tcp)		179	ether2			48 B	1	Accept BGP from ...
16	accept	input	10.0.0.0/8		6 (tcp)		22				240.1 MiB	5 218 927	Accept SSH traffic...
17	accept	input			6 (tcp)		8291				0 B	0	TEMP Allow WinB...
18	accept	input			6 (tcp)		8291			Trusted_Admin	15.8 KiB	324	Accept WinBox tra...
19	accept	input			6 (tcp)		1723	ether1			66.2 KiB	1 129	Accept PPTP from...
20	accept	input			6 (tcp)		1723	ether2			2692 B	53	Accept PPTP from...
21	log	input									0 B	0	Log EVERYTHIN...
22	drop	input									2078.5 MiB	14 450 068	Drop EVERYTHIN...

Protecting your routers – Common Services

Service	Protocol/Port
Winbox	TCP 8291
SSH	TCP 22
Telnet	TCP 23
Webmin	TCP 80 and TCP 443
OSPF	OSPF (Protocol 89)
BGP	TCP 179
MPLS LDP	TCP 646 and UDP 646
Neighbor Discovery	UDP 5678
Btest	UDP 2250-2270

Protecting your network

As well as protecting your routers from attack, you may want to protect your clients from attacks such as:

- Distributed Denial of Service (DDoS)
- Brute Force
- ICMP flooding

And your network from:

- Unauthorised transit
- Customer misuse

Protecting your network – ICMP (Ping) Flooding

This example shows the limiting of ICMP traffic. This works by allowing the various types of ICMP traffic at a rate of up to 5 packets a second.

If ICMP traffic exceeds this, then it will be dropped.

NOTE: This policy will need tuning if you are using it in your “forward” chain.

This policy can be used as-is, for protecting your router in the “input” chain.

```
/ip firewall filter
add chain=forward protocol=icmp action=jump jump-target=ICMP comment="jump to chain ICMP" disabled=no
|
add chain=ICMP protocol=icmp icmp-options=0:0-255 limit=5,5 action=accept comment="0:0 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=3:3 limit=5,5 action=accept comment="3:3 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=3:4 limit=5,5 action=accept comment="3:4 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=8:0-255 limit=5,5 action=accept comment="8:0 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=11:0-255 limit=5,5 action=accept comment="11:0 and limit for 5pac/s" disabled=no
|
add chain=ICMP protocol=icmp action=drop comment="Drop everything else" disabled=no
```

← Send ICMP traffic to the "ICMP" chain

← Allow ICMP up to 5 packets a second

← Drop any remaining ICMP traffic

Protecting your network – SSH bruteforce

This example shows protecting your customers from SSH brute force attacks.

It works by adding the Source IP of the party originating the SSH session to an address list, if this Source party starts another SSH session within a 1 minute timeframe it escalates it up to the next level of address list. If the source party continues to create new SSH sessions, they will be escalated to the “ssh_blacklist” and will not be able to create SSH sessions for 10 days.

```
/ip firewall filter
```

```
add chain=forward protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop \
comment="drop ssh brute forcers" disabled=no
```

← Drop's traffic from any IP in the "ssh_blacklist"

```
add chain=forward protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist \
address-list-timeout=10d comment="" disabled=no
```

← If the IP is in "ssh_stage3" and this is a new connection, add the IP to "ssh_blacklist" with a 10 day timeout

```
add chain=forward protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 \
address-list-timeout=1m comment="" disabled=no
```

← If the IP is in "ssh_stage2" and this is a new connection, add the IP to "ssh_stage3"

```
add chain=forward protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 \
action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no
```

← If the IP is in "ssh_stage1" and this is a new connection, add the IP to "ssh_stage2"

```
add chain=forward protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list \
address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no
```

← Add the IP of SSH src to "ssh_stage1" address list if the connection is new

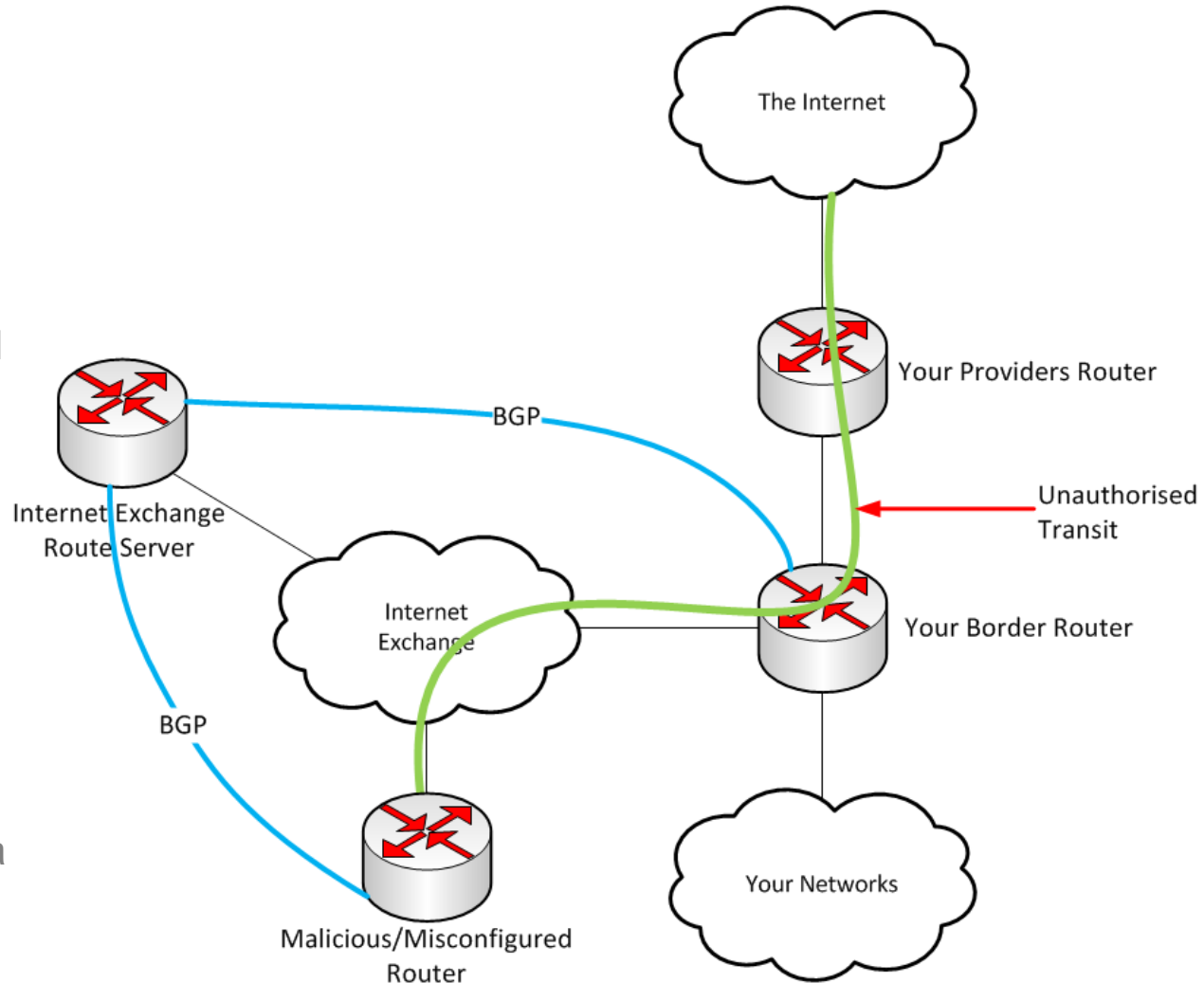
These same techniques can be used for numerous other protocols.

What is unauthorised transit ?

Unauthorised transit is when another party uses your routers to provide transit.

This is common on Internet Exchanges. Your routers will trust the 3rd party as their prefixes will have been received from the trusted IX, the 3rd party will then route traffic via your router which will route it to one of your transit providers.

The 3rd party could now be getting internet bandwidth via your network, at your cost.



Detecting unauthorised transit

This can be done by increasing “visibility” in to your network.

- Use torch on egress port
- Use sflow + analytics software (NTOP/Scruitinizer/Solar Winds)

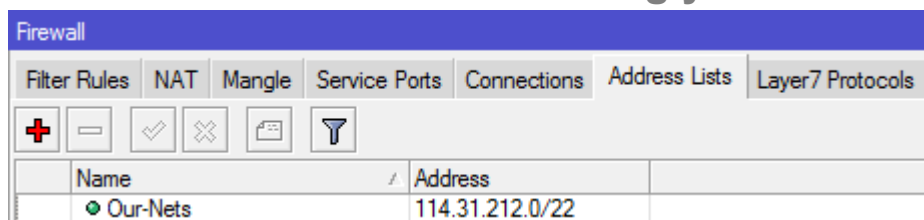
Look for Source addresses that are not within your IP ranges

Preventing unauthorised transit

This can be prevented by restricting L3 forwarding, and controlling your BGP advertisements.

Restrict Layer3 transit (routing) of any networks that are NOT our own

Create an address list containing your subnets



Create 4 IP filter policies

Accept traffic originating from our subnets, to our subnets

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
10	✓ accept	forward								Our-Nets	Our-Nets	336.3 MiB	2 959 131	Our Networks<->Our Networks

Accept traffic originating from our subnets to the Internet

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
12	✓ accept	forward							e10v3201	Our-Nets		28.7 GiB	103 529 ...	Our Networks -> FX National

Accept traffic from the Internet to our subnets

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
13	✓ accept	forward						e10v3201			Our-Nets	36.4 GiB	145 953 ...	FX National -> Our Networks

Drop all other traffic attempting to forward

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
24	✗ drop	forward										2474.6 KB	45 951	

Preventing unauthorised transit

Do NOT advertise prefixes that are NOT your own to upstream BGP peers

Create filter for your upstream peer(s)

- Accept your subnets
- Discard everything else

Route Filters						
#	Chain	Prefix	Prefix Length	Protocol	BGP AS Path	Action
0	as9503-out	114.31.212.0/24				accept
1	as9503-out	114.31.213.0/24				accept
2	as9503-out	114.31.214.0/24				accept
3	as9503-out	114.31.215.0/24				accept
4 X	as9503-out					log
5	as9503-out					discard

BOGON Filtering

A **BOGON** is a Bogus IP address.

BOGON lists contain ranges of IP addresses that are known to have not been allocated by the Regional Internet Registries (APNIC) for use.

These are often used for malicious purposes

BOGON lists can be used on Border Routers as a first line of defence, and can reduce the effect of DOS attacks as well as incoming spam and network scans.

As Regional Internet Registry allocations are constantly changing, BOGON lists should not be static

Using Team CYMRU BOGON BGP feed

1. Request a CYMRU BGP peering session, see www.team-cymru.org
2. Configure your Mikrotik router to peer with Team CYMRU AS65332 (use a loopback!)
3. Configure a routing filter to turn all routes received from CYMRU community 65332:888 in to Black Hole routes

The image shows four panels from the Mikrotik WinBox configuration interface:

- BGP Peer <AS65332-cymru-fullbogons1>**:
 - Name: AS65332-cymru-fullbogons1
 - Instance: default
 - Remote Address: 38.229.66.20
 - Remote Port: [empty]
 - Remote AS: 65332
 - TCP MD5 Key: [empty]
 - Nexthop Choice: default
 - Multihop
 - Route Reflect
 - Hold Time: 180 s
 - Keepalive Time: [empty]
 - TTL: 255
 - Max Prefix Limit: [empty]
 - Max Prefix Restart Time: [empty]
 - In Filter: as65332-cymru-in
 - Out Filter: as65332-cymru-out
 - AllowAS In: [empty]
 - Remove Private AS
 - AS Override
 - Default Originate: never
 - Passive
 - Use BFD
- Route Filter <>**:
 - Chain: as65332-cymru-in
 - Prefix: [empty]
 - Prefix Length: [empty]
 - Match Chain: [empty]
 - Protocol: [empty]
 - Distance: [empty]
 - Scope: [empty]
 - Target Scope: [empty]
 - Pref. Source: [empty]
 - Routing Mark: [empty]
 - Route Comment: [empty]
 - Route Tag: [empty]
 - Route Targets: [empty]
 - Invert Route Targets
 - Site Of Origin: [empty]
 - Invert Site Of Origin
 - Address Family: [empty]
 - OSPF Type: [empty]
 - Invert Match
- Route Filter <>**:
 - BGP AS Path: [empty]
 - BGP AS Path Length: [empty]
 - BGP Weight: [empty]
 - BGP Local Pref.: [empty]
 - BGP MED: [empty]
 - BGP Atomic Aggregate: [empty]
 - BGP Origin: [empty]
 - Locally Originated BGP: [empty]
 - BGP Communities: 65332:888
 - Invert BGP Communities
- Route Filter <>**:
 - Action: accept
 - Jump Target: [empty]
 - Set Distance: [empty]
 - Set Scope: [empty]
 - Set Target Scope: [empty]
 - Set Pref. Source: [empty]
 - Set In Nexthop: [empty]
 - Set In Nexthop Direct: [empty]
 - Set Out Nexthop: [empty]
 - Set Routing Mark: [empty]
 - Set Route Comment: [empty]
 - Set Check Gateway: [empty]
 - Set Disabled: [empty]
 - Set Type: blackhole
 - Set Route Tag: [empty]
 - Set Use TE Nexthop: [empty]
 - Set Route Targets
 - Append Route Targets
 - Set Site Of Origin
 - IPV6

Success

4896 BOGON Subnets will now be blocked at the Border of our networks

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAbB	▶ 0.0.0.0/8		20		
DAbB	▶ 10.0.0.0/8		20		
DAbB	▶ 14.1.96.0/19		20		
DAbB	▶ 14.102.160.0/...		20		
DAbB	▶ 14.192.0.0/19		20		
DAbB	▶ 23.72.0.0/13		20		
DAbB	▶ 23.80.0.0/12		20		
DAbB	▶ 23.96.0.0/11		20		
DAbB	▶ 23.128.0.0/9		20		
DAbB	▶ 24.30.224.0/19		20		
DAbB	▶ 24.41.96.0/19		20		
DAbB	▶ 24.50.32.0/19		20		
DAbB	▶ 24.50.160.0/19		20		
DAbB	▶ 24.51.0.0/19		20		
DAbB	▶ 24.51.224.0/19		20		
DAbB	▶ 24.53.80.0/20		20		
DAbB	▶ 24.53.96.0/19		20		
DAbB	▶ 24.53.192.0/19		20		
DAbB	▶ 24.54.64.0/19		20		
DAbB	▶ 24.55.0.0/18		20		
DAbB	▶ 24.55.128.0/19		20		

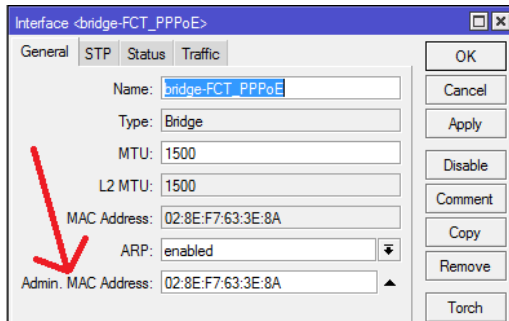
4896 items out of 24674

D = Dynamic, **A** = Active, **b** = BGP, **B** = Blackhole

Preventing Customer Misuse – PPPoE filtering

When backhauling PPPoE to a central concentrator via VPLS/EoIP, you can prevent customers from creating their own networks by using **Bridge Filters**

- Use Admin-Mac to create a static MAC on the bridge on PPPoE concentrator



- Bridge Filter config on router closest to customer

The screenshot shows the Bridge Filter configuration table in WinBox. The table has columns for Chain, Interfaces/Out. Interface, Src. MAC Address, Dst. MAC Address, MAC Protocol (hex), Action, Bytes, and Packets. The table contains 5 rows of configuration.

#	Chain	Interfaces/Out. Interface	Src. MAC Address	Dst. MAC Address	MAC Protocol (hex)	Action	Bytes	Packets
0	forward	vpls1			8863 (pppoe-discovery)	accept	8 712	173
1	forward	vpls1			8863 (pppoe-discovery)	accept	16 568	442
2	forward	vpls1		02:8E:F7:63:3E:8A	8864 (pppoe-session)	accept	774421 306 516	1054 242 926
3	forward	vpls1	02:8E:F7:63:3E:8A		8864 (pppoe-session)	accept	543064 170 974	960 329 280
4	forward					drop	76 074 571	281 947

- Allow pppoe-discovery to ALL destinations
- Allow pppoe-session ONLY to PPPoE Server
- DROP all other traffic

Preventing Customer Misuse – Rogue DHCP Servers

When operating a DHCP based network, it is common to encounter customers who run a DHCP server on their public facing interface. These are called “Rogue” DHCP servers, and can cause outages to other customers by hijacking their DHCP request and responding with settings that differ to your own DHCP server.

Luckily, this is easy to fix using **Bridge Filters**

- Accept Input of DHCP requests
- Accept Output of DHCP responses
- Drop forwarding of all DHCP packets

Questions ?

Stay Secure!

- Comments and feedback: andrew@networklabs.co.nz
- Recommended Reading:
 - wiki.mikrotik.com
- Links:
 - Suricata – <http://www.openinfosecfoundation.org/>
 - Sagan - <http://sagan.quadrantsec.com/>
 - OSSIM - <http://communities.alienvault.com/community/>
 - Team CYMRU - <http://www.team-cymru.org/Services/Bogons/>
 - Tileria/Suricata - http://www.tileria.com/about_tileria/press-releases/tilera%E2%80%99s-tile-gx-delivers-
- Trying to identify P2P / Media? – Email me andrew@networklabs.co.nz