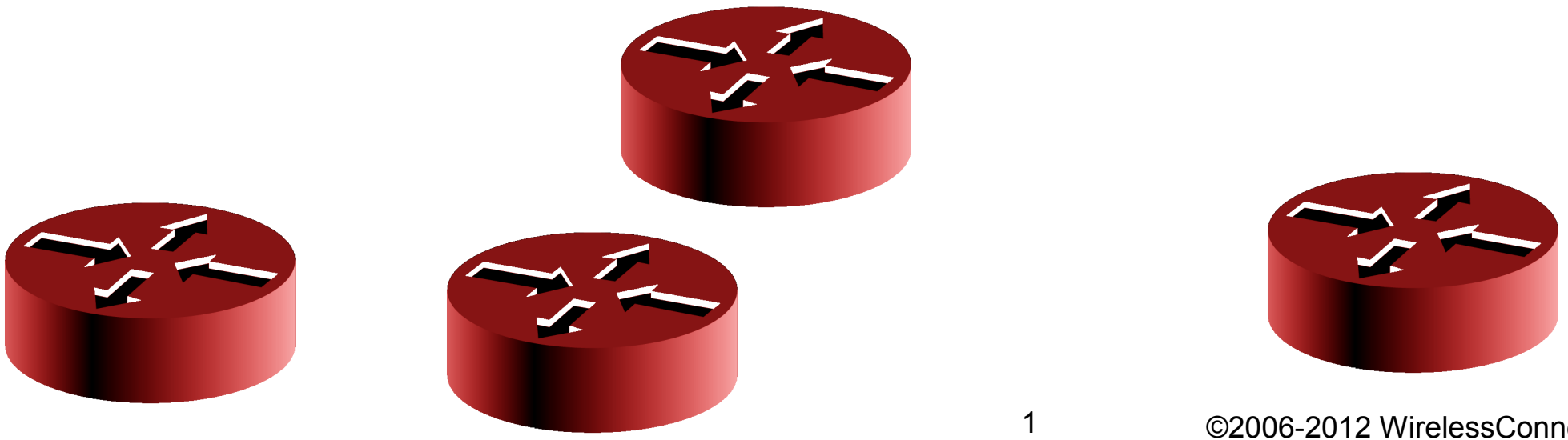
Securing Networks with Mikrotik Router OS

Speaker: ***Tom Smyth, CTO Wireless Connect Ltd.***
Location: ***Dubai***
Date: ***28-08-2012***



Wireless Connect Ltd.

- Irish Company Incorporated in 2006
- Operate an ISP in the centre of Ireland.
- Good Infrastructure Expertise.
- Certified MikroTik Partners
  - Training
  - Certified OEM Integrators
  - Consultants
  - Value Added Reseller

Speaker Profile:

- Studied BEng. Mechanical & Electronic Engineering, DCU,Ireland
- Has been working in Industry since 2000
  - Server Infrastructure Engineer
  - Systems / Network Administrator
  - Internet Security Consultant
- 1st MikroTik Certified Trainer in June 2007 in Ireland

Security Information sources

- ENISA –http://www.enisa.europa.eu/
- OWASP http://owasp.org
- Rits Group – http://www.ritsgroup.com/
- SANS Institute – http://sans.org
- CIS Centre for Internet Security – http://cisecurity.org/
- NIST Computer Security http://csrc.nist.gov/
- Open BSD – http://OpenBSD.org/
- Spamhaus.org – http://spamhaus.org
- nmap.org – http://nmap.org
- ha.ckers.org – http://ha.ckers.org/

Router OS

- Highly Versatile
- Highly Customisable
- Highly Cost Effective
- Allows one to manage Security Threats in many Ways

What Can MikroTik Router OS Do ?

- It is a Stateful Firewall
- It is a Web Proxy
- It is a Socks Proxy
- It is a DNS Cache / Proxy
- It is a Router
- It is an IPSEC Concentrator
- It is an IDS – Intrusion Detection System
- It is an IPS – Intrusion Prevention System

Stateful Firewalls

- Enhance security by monitoring requests and to enforce that only legitimate responses to legitimate requests are allowed.
- All other Traffic is either malicious or due to misconfiguration
- Protect the router / customer from attacks such as DNS Cache Poisoning Attacks
- Every Stateful Firewall must have the the following 9 rules near the top of firewall rule set
  - Allow Established Connections on forward, input and Output Chains
  - Allow Related Connections on forward, input and Output Chains
  - Drop Invalid Connections on forward, input and Output Chains
- All New Requests (non layer 7) will be filtered after the rules above
- See MUM 2010 & MUM 2011 Presentations for More information

Web Proxy

- Web Proxy is an Application Layer Gateway
- Understands HTTP allows one to filter
  - DNS names
  - Urls
  - Filetypes
  - Advanced Filtering with Regular Expression Support
  - Potentially Dangerous Types of Http Requests such as DELETE, TRACE & CONNECT
- Deny or Redirect clients to another page
- Filters Every Request inside a Connection- More secure than Layer 7 Packet Filters

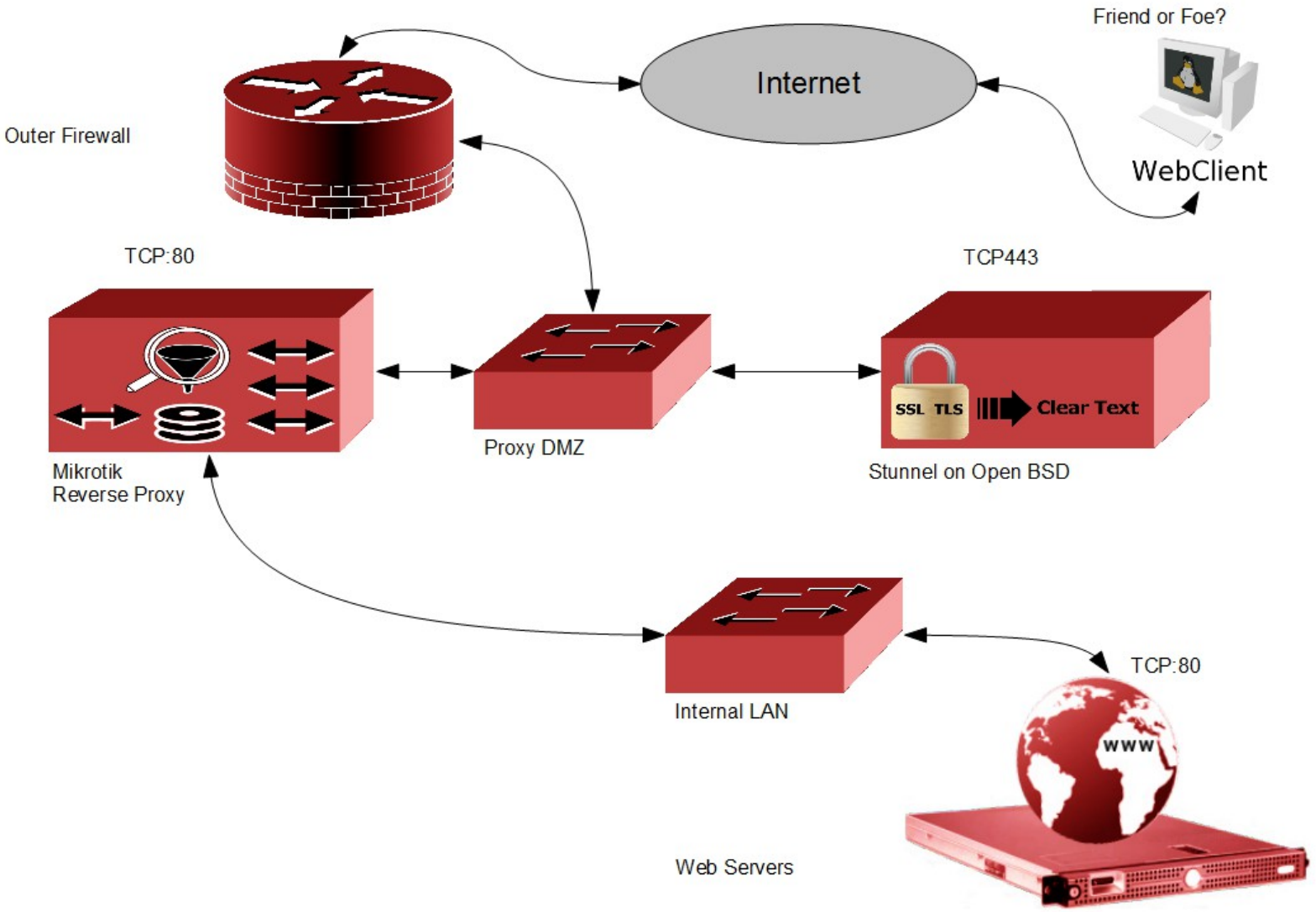
Enforcing a Web Proxy

- Having a Web Proxy is useless if you allow traffic to bypass the firewall.
- Corporate firewalls should
  - Block all traffic from clients directly out of the network
  - Allow Clients to talk to the Proxy (request pages)
  - Allow only the Proxy traffic out of the network
- By blocking direct internet access you force users to use the proxy, where the company has a lot more control over traffic, and can protect the company / user from malicious content

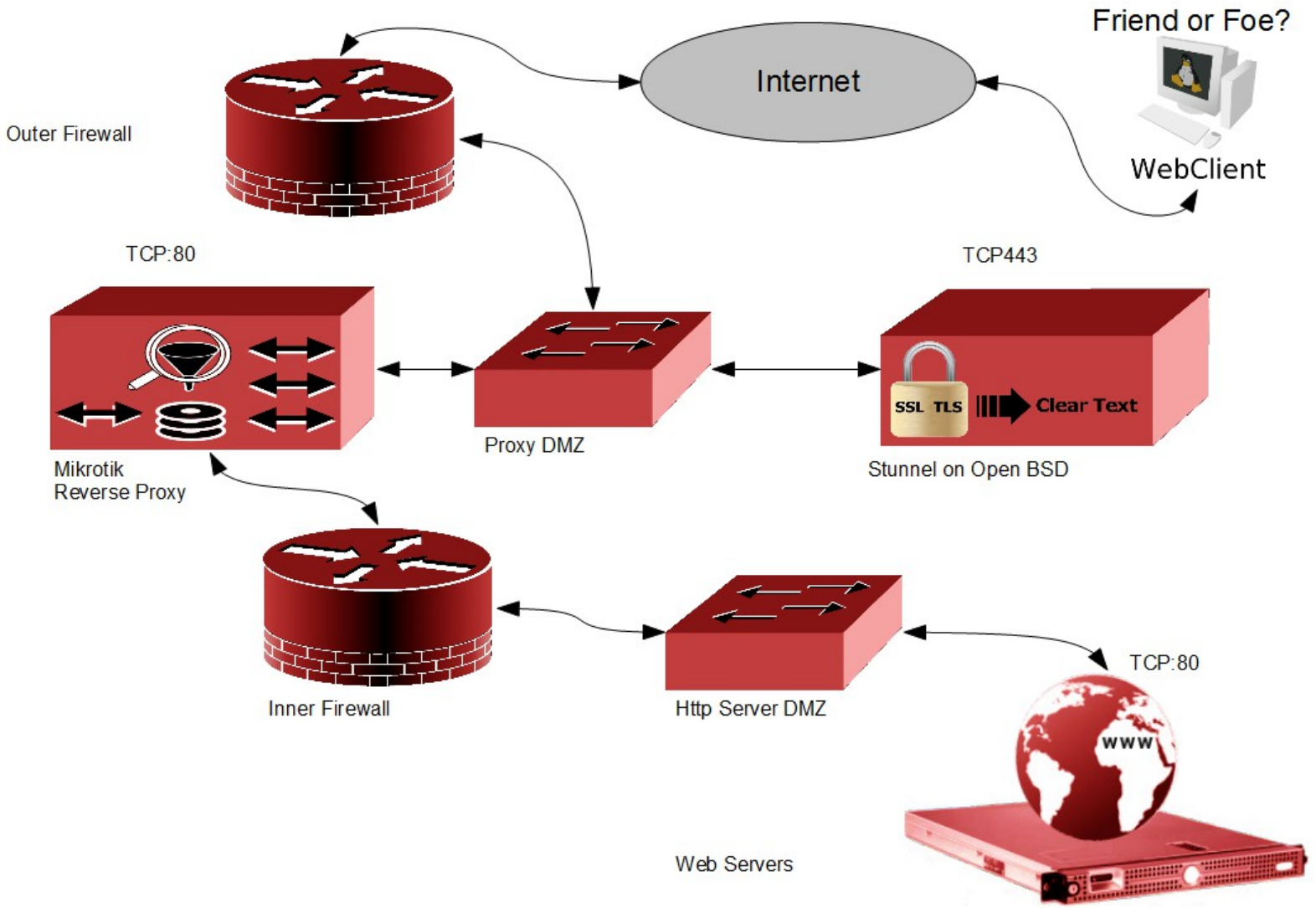
Web proxy Security

- Always filter the External / publicly accessible interface of the Proxy. Other wise you may have an Open Proxy
- Open Proxies are often used by attackers to hide their true identity also can be used in more serious illegal activity
- Reverse Proxies that are open to the public should have a firewall between your internal network and the Proxy.
  - Attackers could use your proxy to bounce to other internal systems administration page

Risky Reverse Proxy Deployment



Internal Network protected by Firewall



MikroTik Socks Proxy

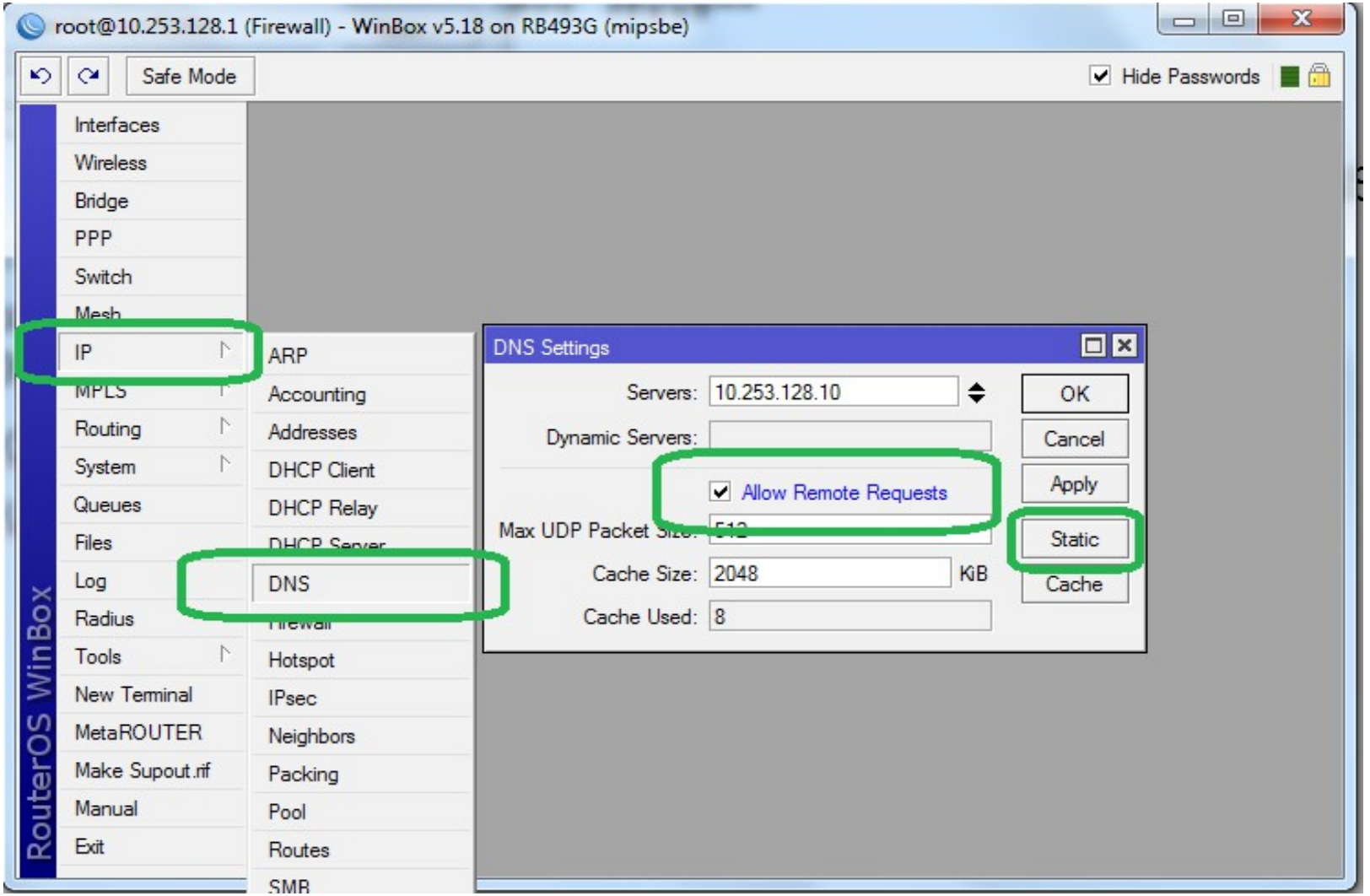
- Allows Proxying of TCP Services
- Operates at Layer 5
- Can offer increased security by breaking the direct connection between a Client and a server
- Useful for TCP Services only
- Can be used to Circumvent Company Policy if Socks Proxy is not sufficiently Protected with
  - Firewall rules
  - Proxy Access List

DNS Cache / DNS Proxy

- MikroTik can not only cache DNS Requests it can provide a DNS Filtering Service
- If combined with a MikroTik Firewall It can enforce a particular DNS policy, can be used in conjunction with
  - OpenDNS
  - URLblacklist

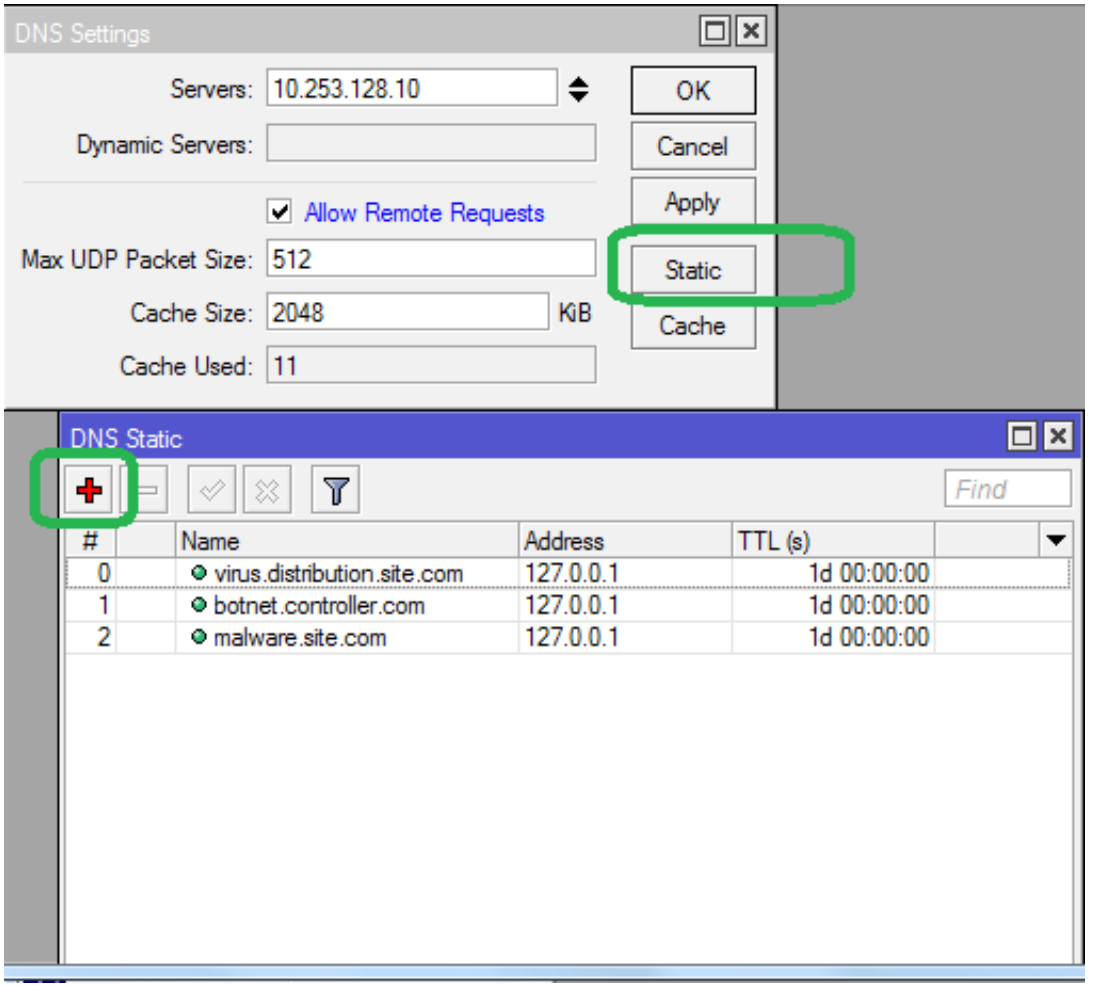
Setting Up a DNS Filter

- Available in the IP / DNS Menu



Filter Known Attack Sites

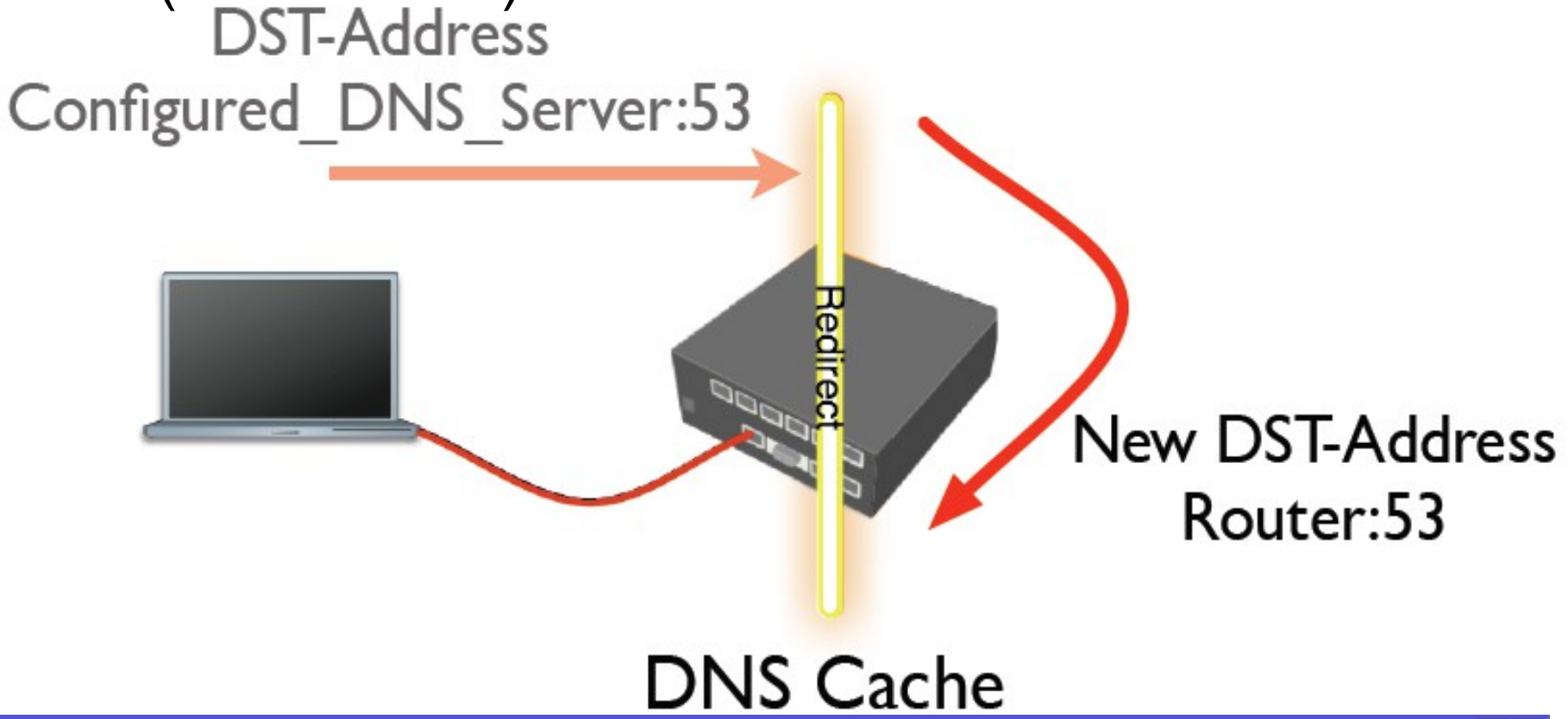
- Users can Opt in by using your DNS Server / Filter
- DNS policy can be Enforced by combining the DNS Server with a Mikrotik Firewall



- When user attempts to connect to a website (accidentally or otherwise) the DNS responds with the loopback address
- Users are prevented / redirected to their own computer

Enforcing a DNS Policy

- Requests to other DNS Servers that traverse the firewall are redirected (DST NATed) to the DNS Filter Server



Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

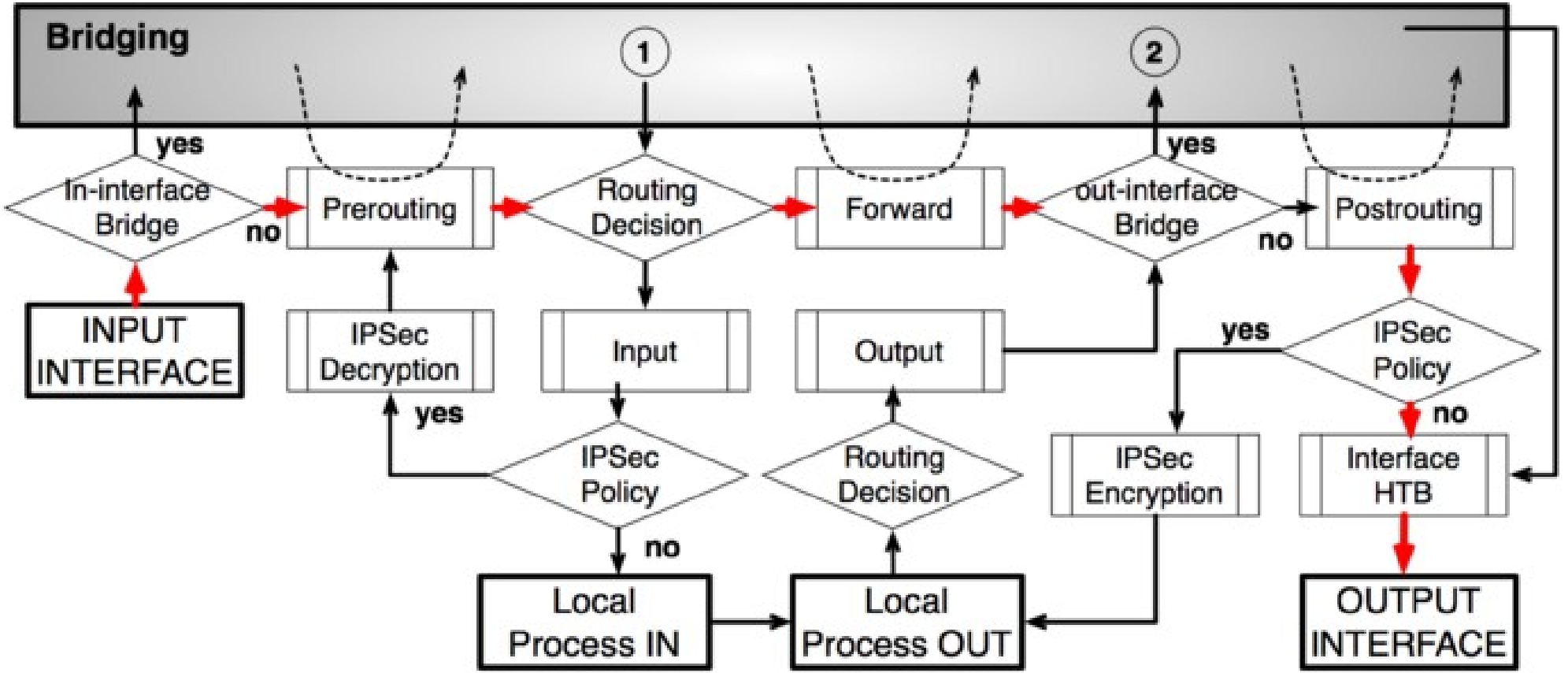
Reset Counters | Reset All Counters | Find | DNS-DSTNAT

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
12	redirect	DNS-DSTNAT			17 (udp)		53			0 B	0
13	redirect	DNS-DSTNAT			6 (tcp)		53			0 B	0

Alternatives to Firewall Filtering

- If we want to filter traffic going towards a destination for example
- Let us take a look at the Kernel where, MikroTik Router OS Does its Magic

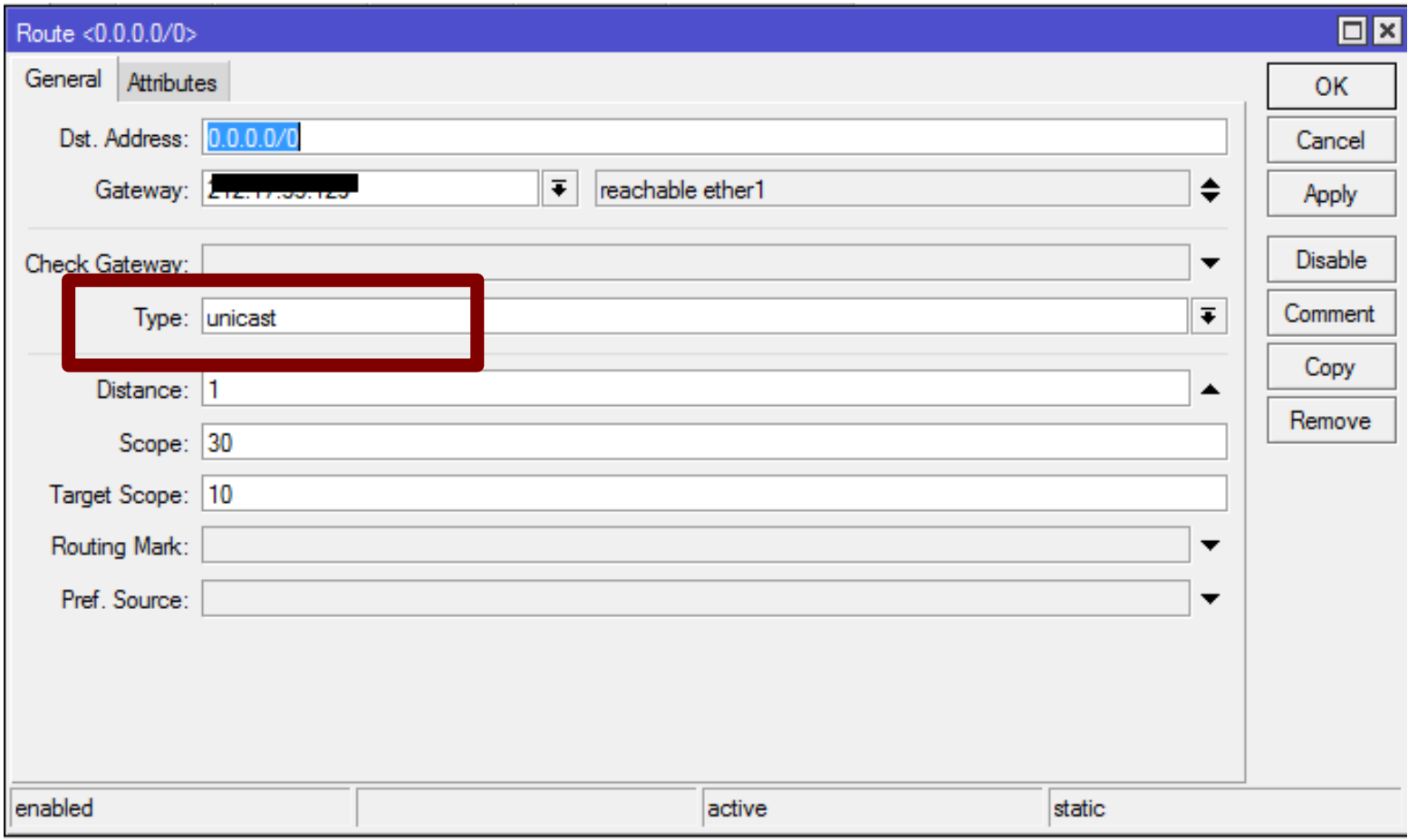
MikroTik Kernel -Packet Flow



- It Seems all packets flowing to / through the router are processed using the routing table

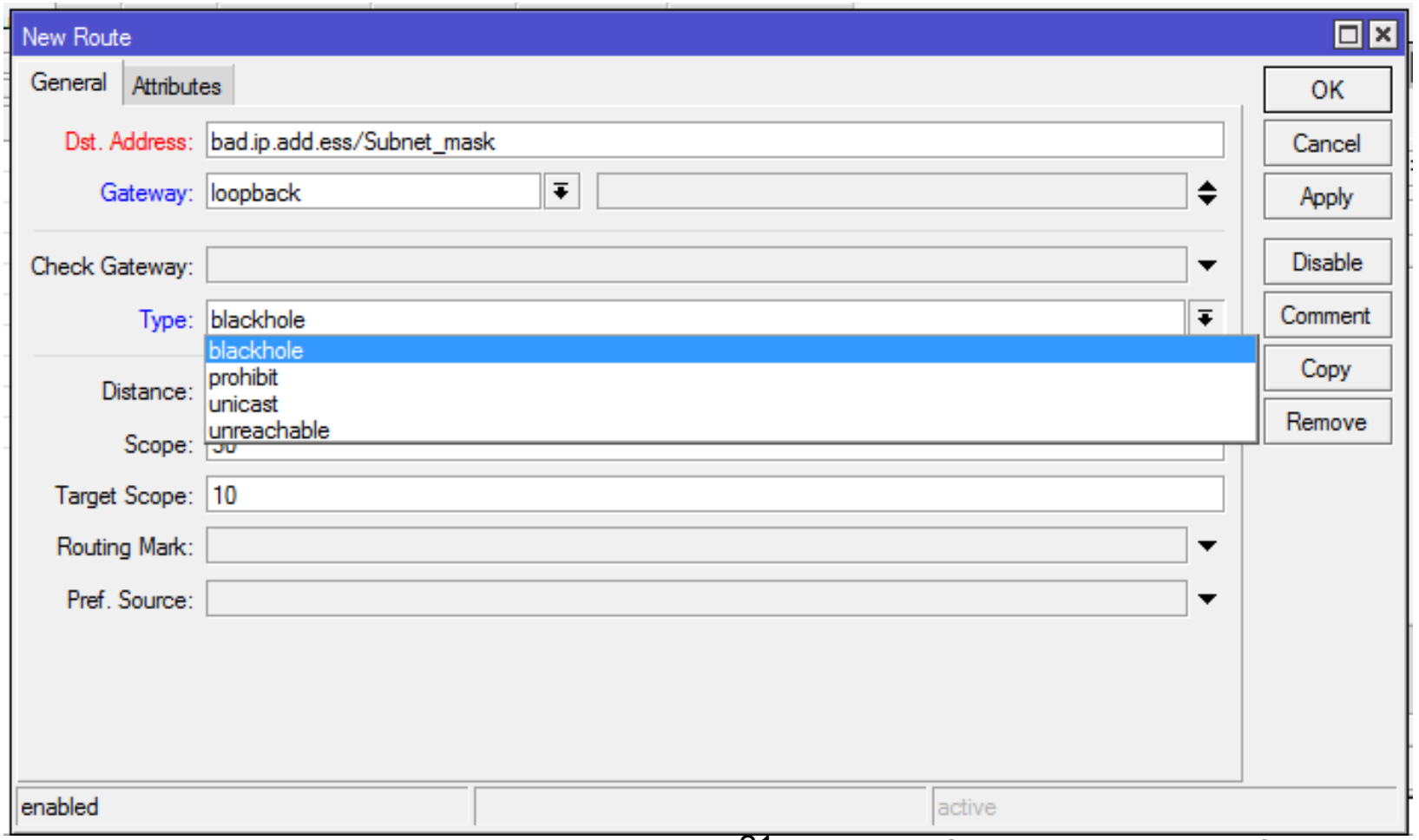
Filtering Using Routes

- Most people are familiar with Routing as a tool to help traffic reach its destination,
- These “Normal” routes are called Unicast routes



Enter the BlackHole Route

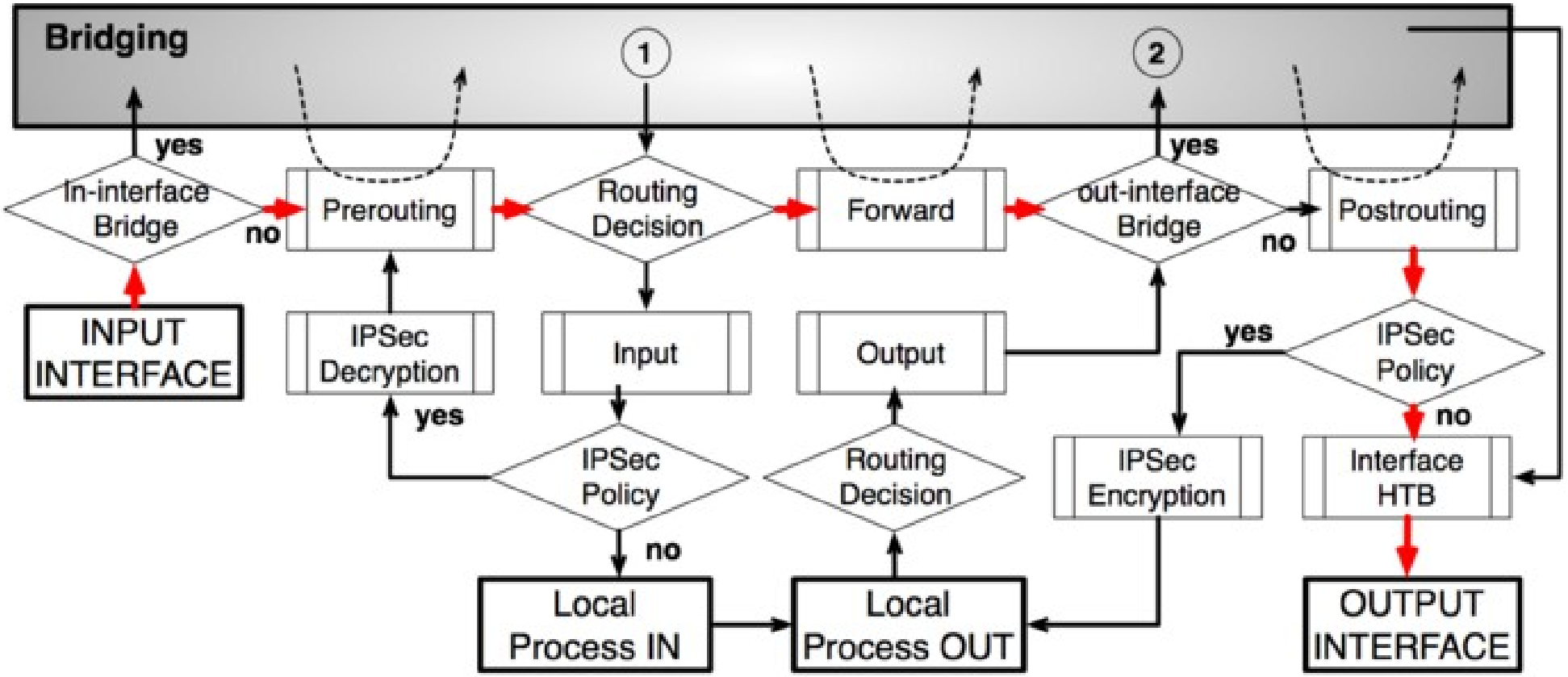
- BlackHole – the name from the astronomical phenomena where any object placed into the BlackHole will never leave.
- BlackHole – Discard the Packet Route



Other types of Discard Routes

- Black-Hole – Discard packet silently (similar to Drop in firewall)
- Prohibit – Discard the packet and Send an ICMP Admin Prohibited msg back to source of the packet (similar to Reject Admin Prohibited)
- Unreachable- Discard Packet and Send an ICMP Host Unreachable message back to the source of the packet
- Black Hole is most secure and incurrs the least load on the router

Benefits of Blackholes over Forward filters



- Forward Filters ... means more processing must be carried out by CPU

Black Hole Hardware Acceleration

- Routers with accelerated hardware for Routing (Express forwarding / Route once Switch many) will see filtering of-loaded from CPU to ASICs.

Automating This Filter Technique

- Routing ... Automating Route Updates ?

Dynamic Routing

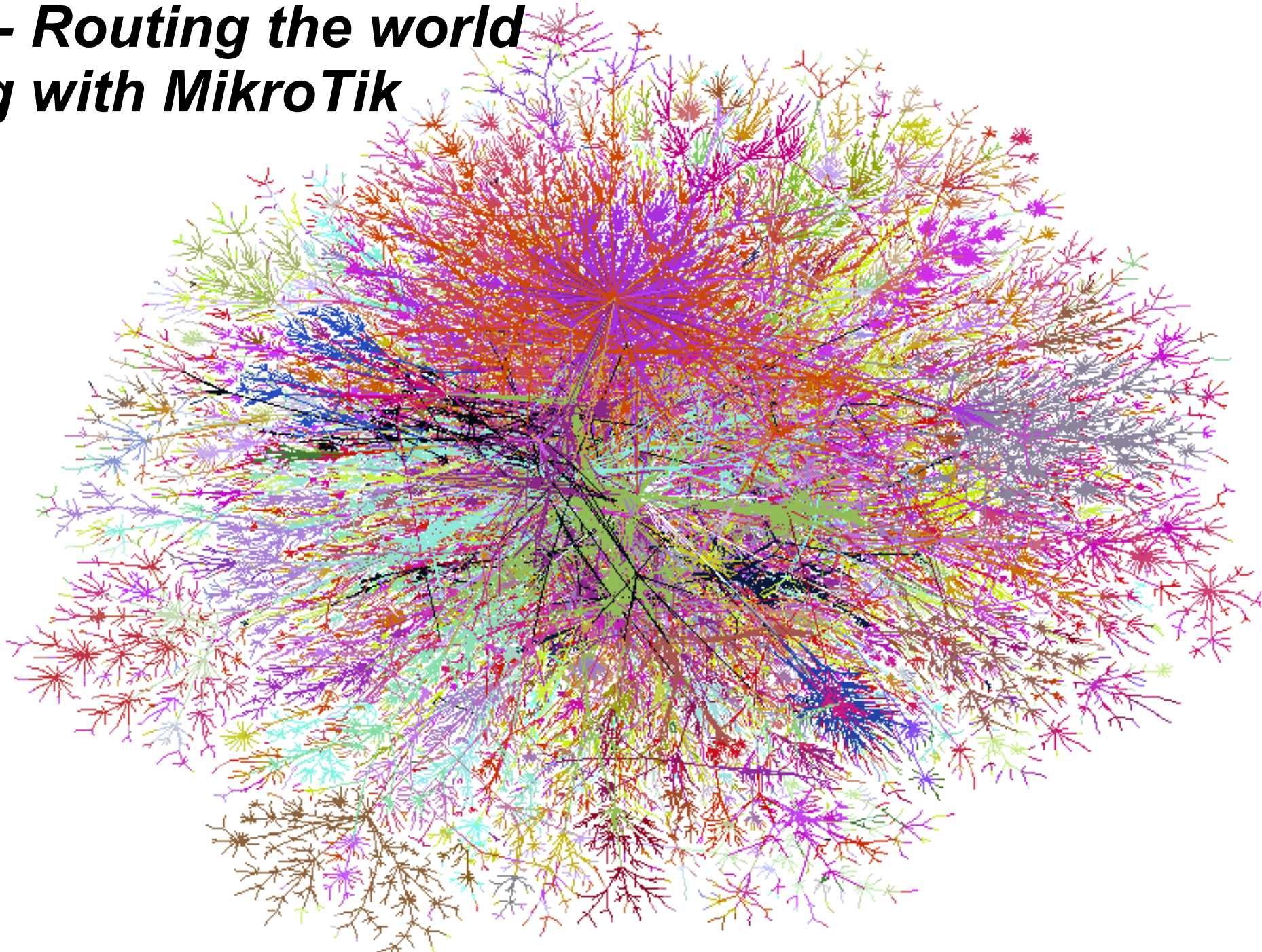
- OSPF... Not a good idea between external parties
- BGP ... Stable Scalable extensive features for filtering and exchanging information about routes

Wireless Connect

Ogma Connect

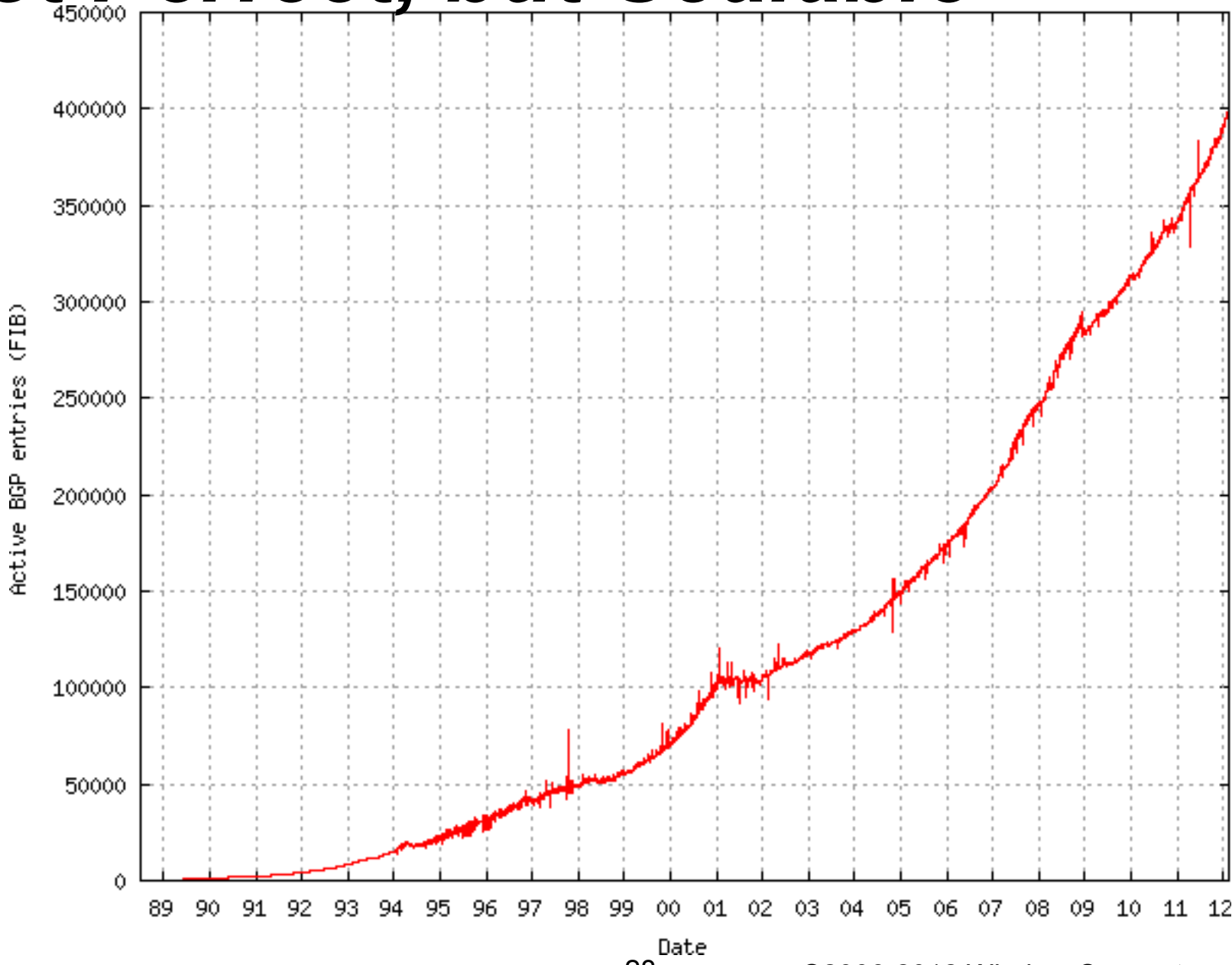
MikroTik

BGP-- Routing the world Along with MikroTik :)



BGP - Not Perfect, but Scalable

- Plot showing Active Routes on Internet
- FIB – Active Routes
- RIB- 2x Active Routes (Redundant Connections)



BGPv4 – Basics

- Stands for Border Gateway Protocol
- Designed as an Inter-AS routing protocol
  - Network topology is not exchanged, only reachability information.
  - *"This Prefix is reachable through my AS"*
  - Only protocol that can handle Internet's size networks
- Uses path vector algorithm
- MikroTik Supports BGPv4 RFC 4271

BGP Transport

- Operates by exchanging NLRI (network layer reachability information).
- NLRI includes a set of BGP attributes and one or more prefixes with which those attributes are associated
- Uses TCP as the transport protocol (port 179)
- Initial full routing table exchange between peers
- Incremental updates after initial exchange
- (maintains routing table version)

Community

- Attribute that groups destinations
- Filters can be easily applied to whole group
- Default groups:
  - No-export – do not advertise to eBGP peer
  - No-advertise – do not advertise to any peer
  - Internet – advertise to Internet community
  - Local-as – do not send outside local AS (in non-confederation network the same as no-export)

BGP Community

- 32-bit value written in format “xx:yy” Where
  - xx= AS Number:
  - yy= Community Option
- Gives customer more policy control
- Simplifies upstream configuration
- Can be used by ISPs for:
  - AS prepending options
  - Geographic restrictions
  - Blackholing, etc.
- Check Internet Routing Registry (IRR)

Communities In a nutshell

- Route Advertiser and Route Reciever (ISP Admins) discuss policies and exchange usefull information meaning of Policies etc.
- Route Advertiser (BGP out) sets communties according to some design / policy
- Various Communties are set and sent out with various routes...
- Route Reciever Admin sets Router Reciever to look for set communities in routes and implement policy based on the community.
- Now each ISP is implementing / continuing a policy as agreed with their peer
- .... BRILLIANT :)

Bogon BGP Feed

- Remember your MTCNA Training ? Remember the defination of a Bogon ?
- If you havent a MTCNA – you could be missing out on lots of tips and techniques to make your job of running and expanding your network easier

Team Cymru --- Cool Internet Security Research Organisation

- Visit http://www.team-cymru.org
- They have lots of services that can be used to increase the security of your network
- They also have a free BGP Feed for IPv4 and IPv6 Bogons
- They are dedicated,helpful, responsive and very inovative
- They even have published examples of BGP Configurations for Mikrotik so that you can peer with them
- Tell your friends about them

Teamcymru's Bogon web page

AUTOMATICALLY FILTERING BOGONS

So how does one use the community **65333:888** or **65332:888** prefixes to generate a bogon filter? There are myriad methods, of course. One possible method is to use a route-map and a route with a next-hop of the null0 (Cisco) interface. We have collected examples below from our own experience and from several helpful contributors, which you may view by following the links below.

Traditional Bogon Examples

- Cisco IOS
- Cisco IOS with peer-groups
- Juniper JunOS
- Force10 router
- OpenBSD bgpd
- Mikrotik RouterOS

Fullbogon Examples

- Cisco IOS IPv4 and IPv6 (IPv4 transport)
- Cisco IOS IPv4 and IPv6 (IPv6 transport)
- Juniper JunOS IPv4 and IPv6
- Quagga IPv6
- Mikrotik RouterOS

If none of these methods will work for you then please contact us for assistance. We are also eager to hear your suggestions on other filtering methods!

HOW DO I OBTAIN A PEERING SESSION?

To peer with the bogon route servers, contact bogonrs@cymru.com. When requesting a peering session, please include the following information in your e-mail:

1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

We will typically provide multiple peering sessions (at least 2) per remote peer for redundancy. If you would like more or less than 2 sessions please note that in your request. We try to respond to new peering requests within one to two business days, but, again, can provide no guarantees for this **free** service.

Remember that you must be able to accomodate up to **100 prefixes** for *traditional bogons*, and up to **50,000 prefixes** for *fullbogons*, and be capable of multihop peering with a private ASN. If you improperly configure your peering and route all packets destined for bogon addresses to the bogon route-servers, your peering session will be dropped.

Bogon Feed Request

Tom Smyth 11/18/11

to bogonrs,

Hello Lads,

We would like to Peer with your selves to get the bogons through BGP,

1. Which bogon types you wish to receive	IPv4 Full bogons
2. Your AS number	4361
3. The IP address(es) you want us to peer with	[redacted] & [redacted]
4. Does your equipment support MD5 passwords for BGP sessions?	Yes select a password of your choosing
5. Optional: your GPG/PGP public key	N/A

Thanks alot and keep up the great work

Cymru response

- We received 5565 bogon prefixes from CYMRU
- We used BGP Bogon community: 65332:888 + no-export
- E-mail contact: noc@cymru.com

RT bogonrs@cymru.com 11/18/11

to me

Hi Tom,

Ok, you're all set for IPv4 fullbogons on our end. The connection details are below. If needed, we have some configuration examples at http://www.team-cymru.org/Services/Bogons/bgp-examples.html#cisco-full-v4trans

Please confirm when you are up and running, and thanks for using our service!

Regards,

Can't connect? here are some things to look at:

1. Clear ip bgp * and verify session details are correct.
2. Entry in peer group (source - update) statement is present and correct.
3. If ping fails verify host route and check ACL's.
4. When pinging make sure it is a source ping, we use host routing.
5. check routing and packet filtering upstream, port 179.
6. Any type of packet shaping that might be corrupting the MD5.
7. Verify your equipment supports MD5 and the password is correctly inputted.
8. Verify you are using enough hops or set to 255

After you have verified these and you still need help please send ping and traceroute output within correspondence.

Here are your Fullbogon session details:

SESSION #1

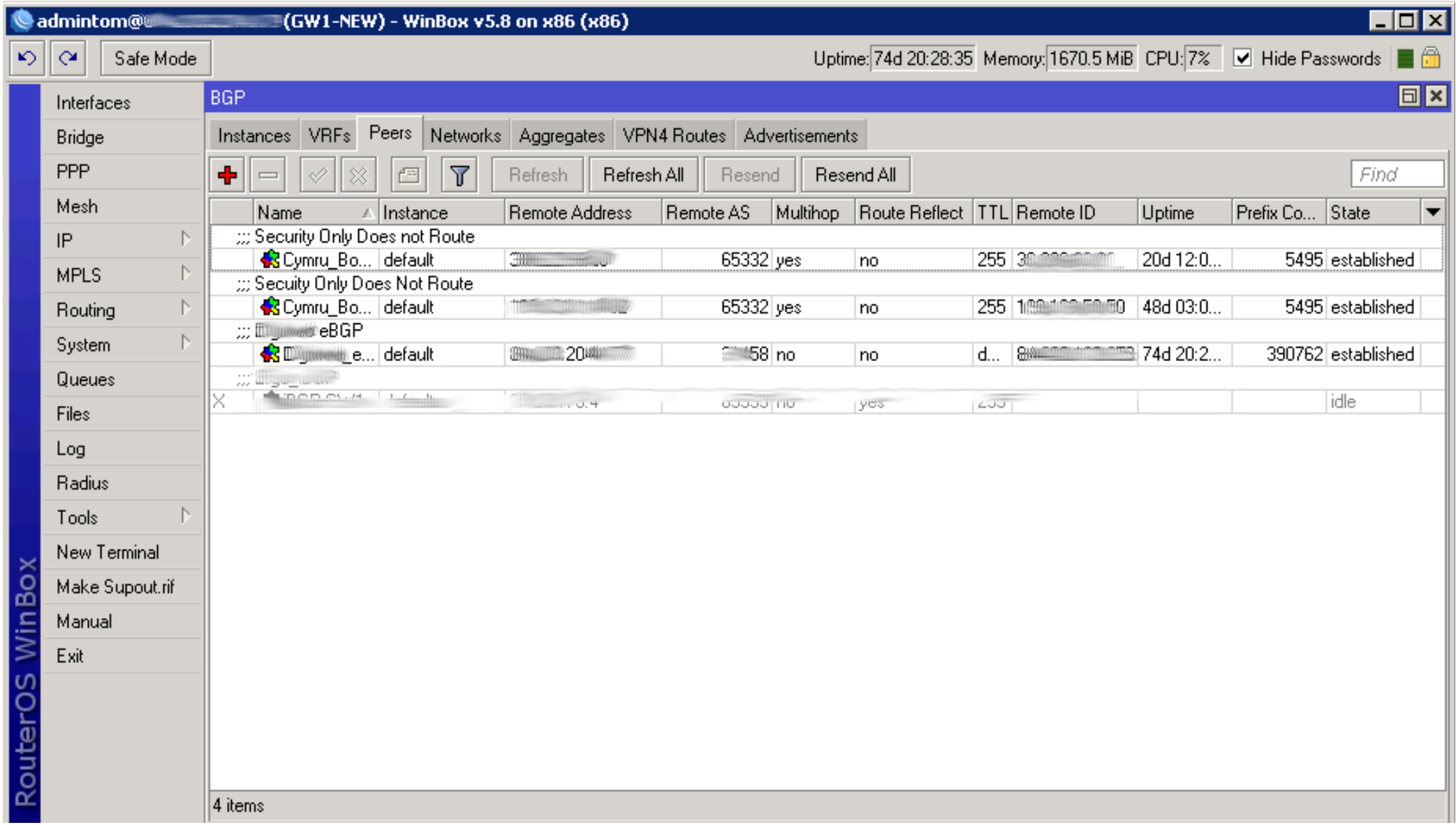
Your IP: [redacted]
Your IP: [redacted]
Your ASN: 436

Our IP: 38.229.66.20
Our ASN: 65332
MD5 Password: upstream,

SESSION #2

Your IP: [redacted]
Your IP: 4.203.204.18

Bogon Feed Installed



Taking BGP Filtering to next Level

- Memory is an issue, full internet table is 800k routes (256Mb Ram needed for it alone) how many routes are being downloaded from your peer ?
- Cost of Memory going down :)
- Can use iBGP to distribute a policy within your entire network
-

Issues with Wide scale deployment

- One could use communities to differentiate between different kinds of threats
- The real question is .. how would these threats be assessed and added to the feed.. Transparency & an speedy appeals process would be an absolute requirement
- The Opt in nature model is good so people could opt to be protected if required. Can be useful for sensitive industries or sensitive collaboration networks

Communities Received from Cogent

- Routes announced to customers by Cogent will have one of the following communities associated with them:

174:22014	Sweden
174:22015	Norway
174:22016	Czech Republic
174:22017	Slovakia
174:22018	Hungaria
174:22019	Ireland
174:22020	Romania
174:22021	Croatia (locally Hrvatska)
174:22022	Slovenia
174:22023	Bulgaria
174:22024	Finland
174:22025	Estonia
174:22026	Ukraine
174:22027	Mexico

Community String	Description
174:21000	Route is learned from NA (North America) non-customer.
174:21001	Route is NA internal or customer route.
174:21100	Route is learned from EU (Europe) non-customer.
174:21101	Route is an EU internal or customer route.
174:22001	Austria
174:22002	Belgium
174:22003	Canada
174:22004	Switzerland
174:22005	Germany
174:22006	Denmark
174:22007	Spain
174:22008	France
174:22009	Italy
174:22010	Netherlands
174:22011	Portugal
174:22012	United Kingdom
174:22013	United States

Thank You

- I hope you enjoyed the Presentation as much as I Did:)
- You are welcome to discuss any questions with me over a cup of tea.