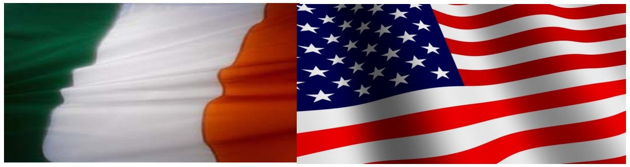
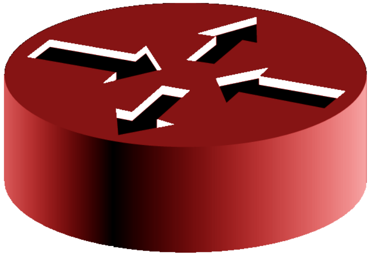
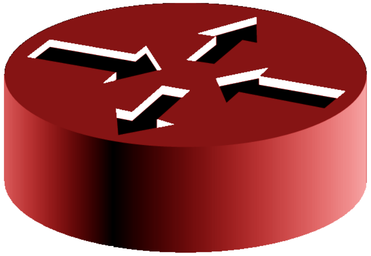
Wireless Connect Ogma Connect MikroTik

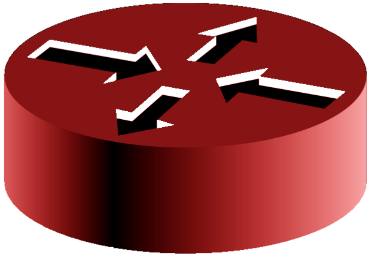
Securing Networks with Mikrotik Router OS

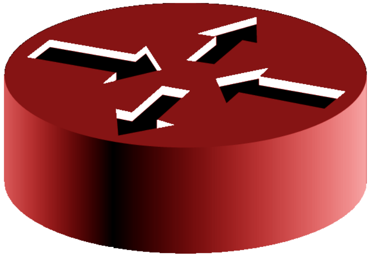


Speaker: Tom Smyth, CTO Wireless Connect Ltd.
Location: New Orleans
Date: 28-09-2012









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/

✓ISAS – http://www.isas.ie/

✓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

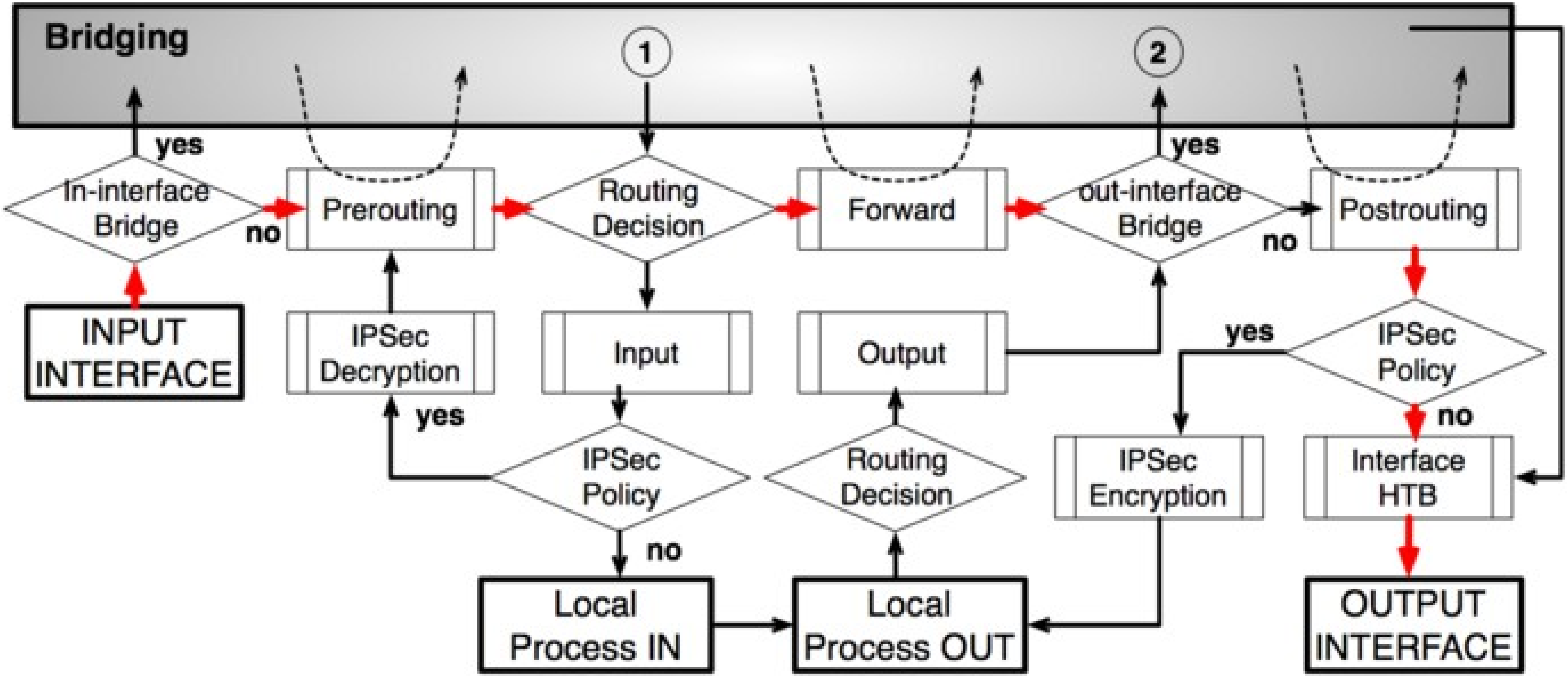
Previous MUM Presentations

- ✓See my presentations from previous mums for more information
  - ·MUM Dubai 2012 --> Blackhole Routing Techniques
  - ·MUM Poland 2010 --> Web Proxy as a Web application firewall
  - ·MUM Budapest 2011 --> Advanced Firewall Strategies
- ✓Check out My good friend Maia Wardner of MD Brazil's Many Presentations on Network Security lots of examples and brilliant illustrations

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

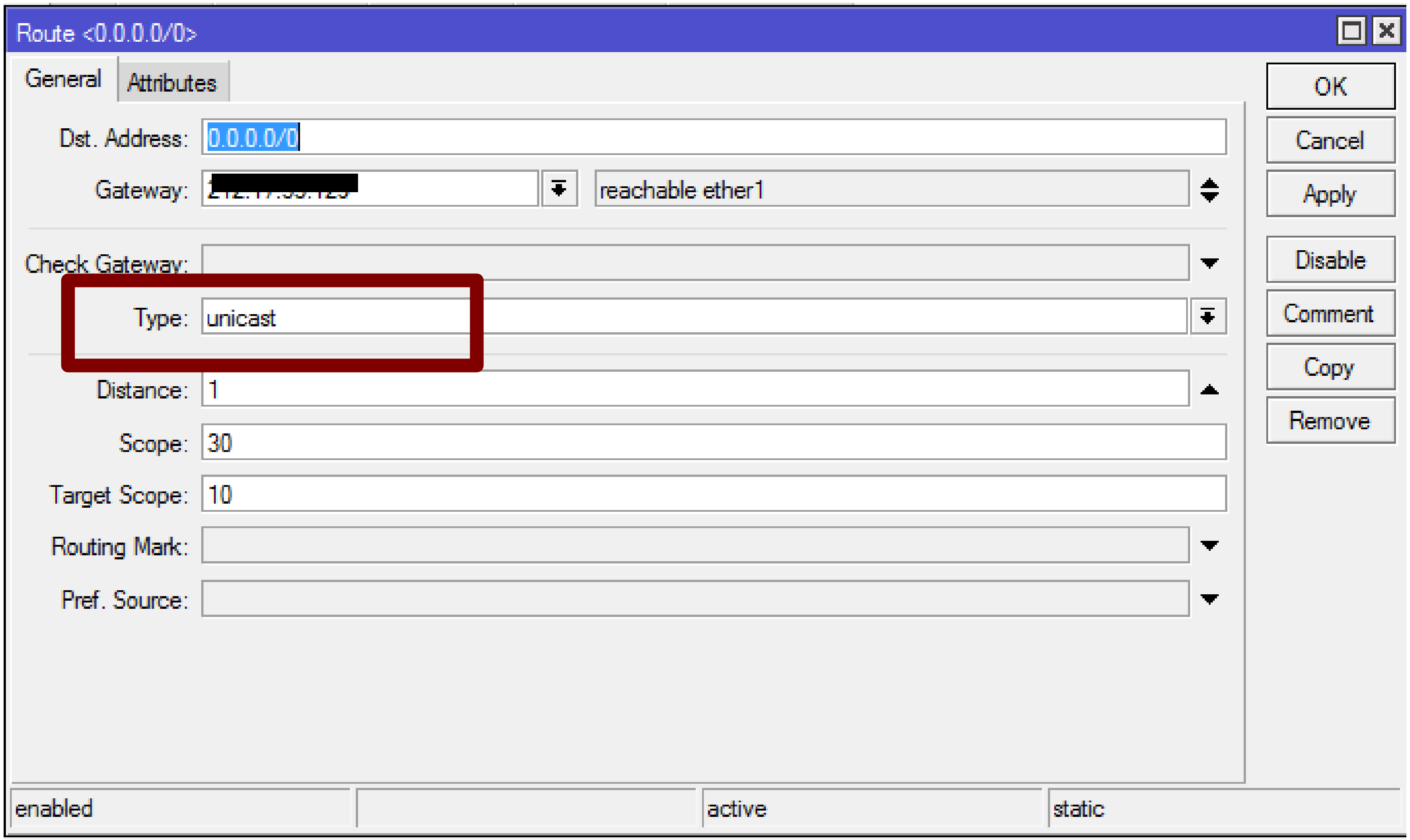
MikroTik Kernel -Packet Flow



- ✓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



Route <0.0.0.0/0>

General | Attributes

Dst. Address: 0.0.0.0/0

Gateway: [redacted] reachable ether1

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

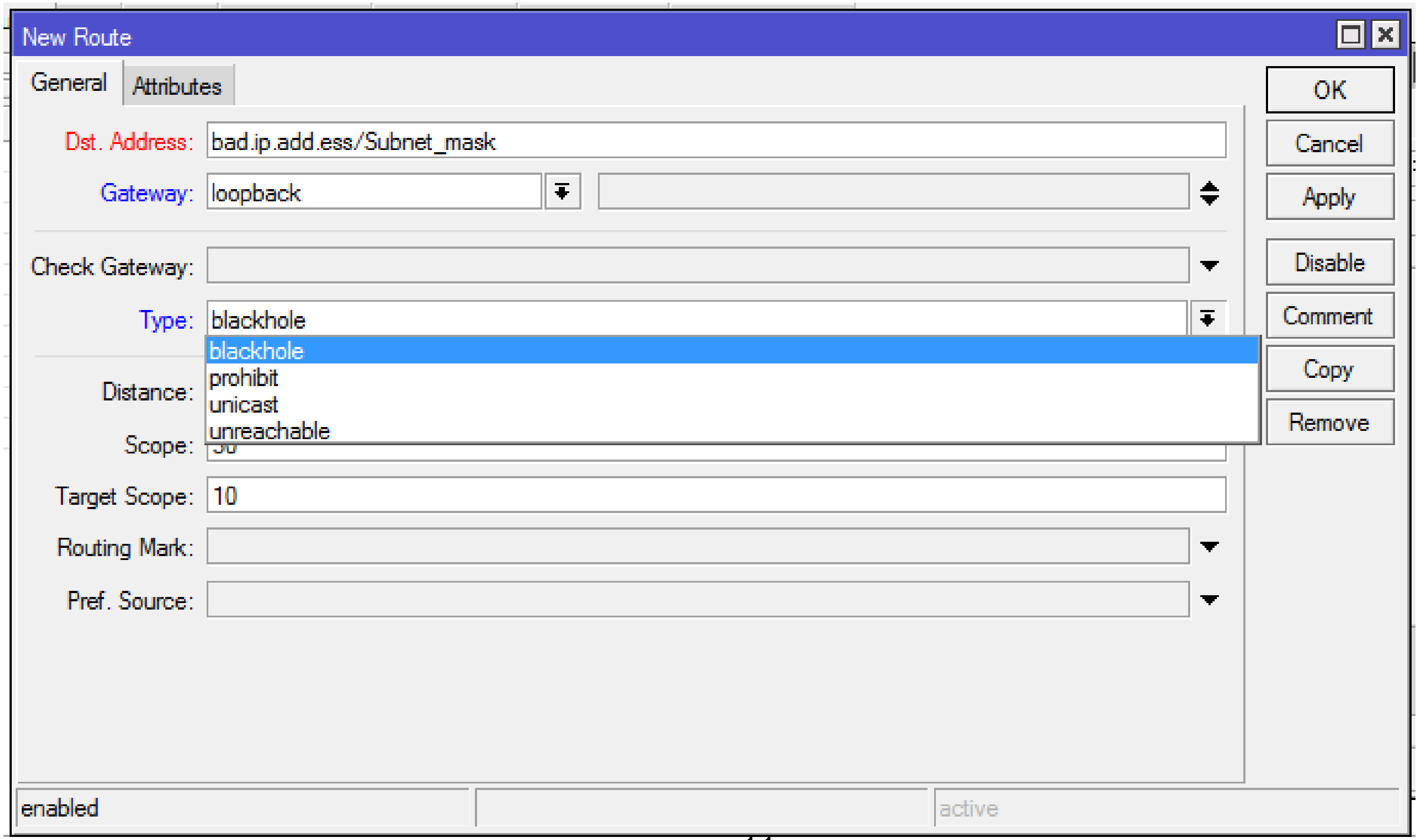
Routing Mark:

Pref. Source:

enabled | active | static

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



New Route

Dst. Address: bad.ip.add.ess/Subnet_mask

Gateway: loopback

Check Gateway:

Type: blackhole

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

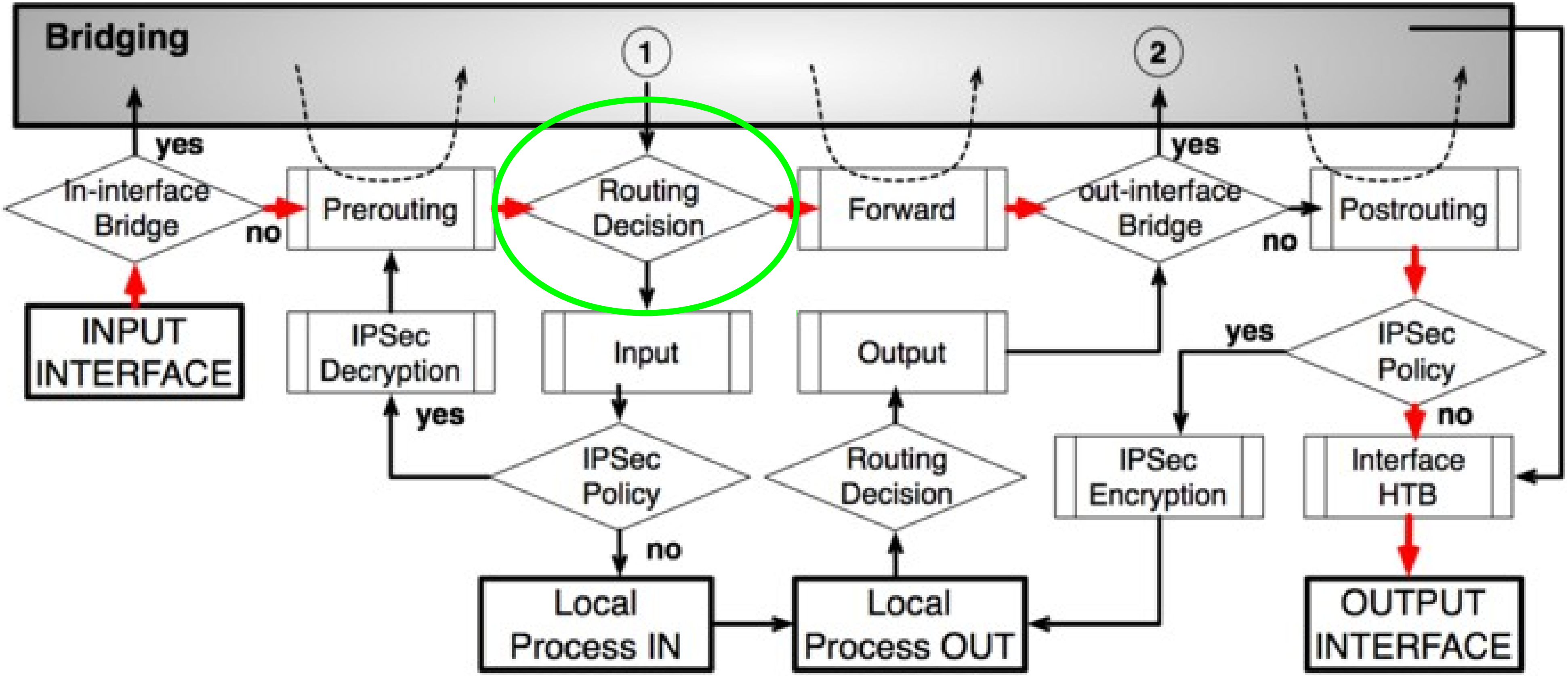
enabled

active

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 incurs the least load on the router

Benefits of Blackholes over Forward filters



- ✓Forward Filters 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.
- ✓CCR1036 Router will have Fast path hardware accelerated routing capability :)

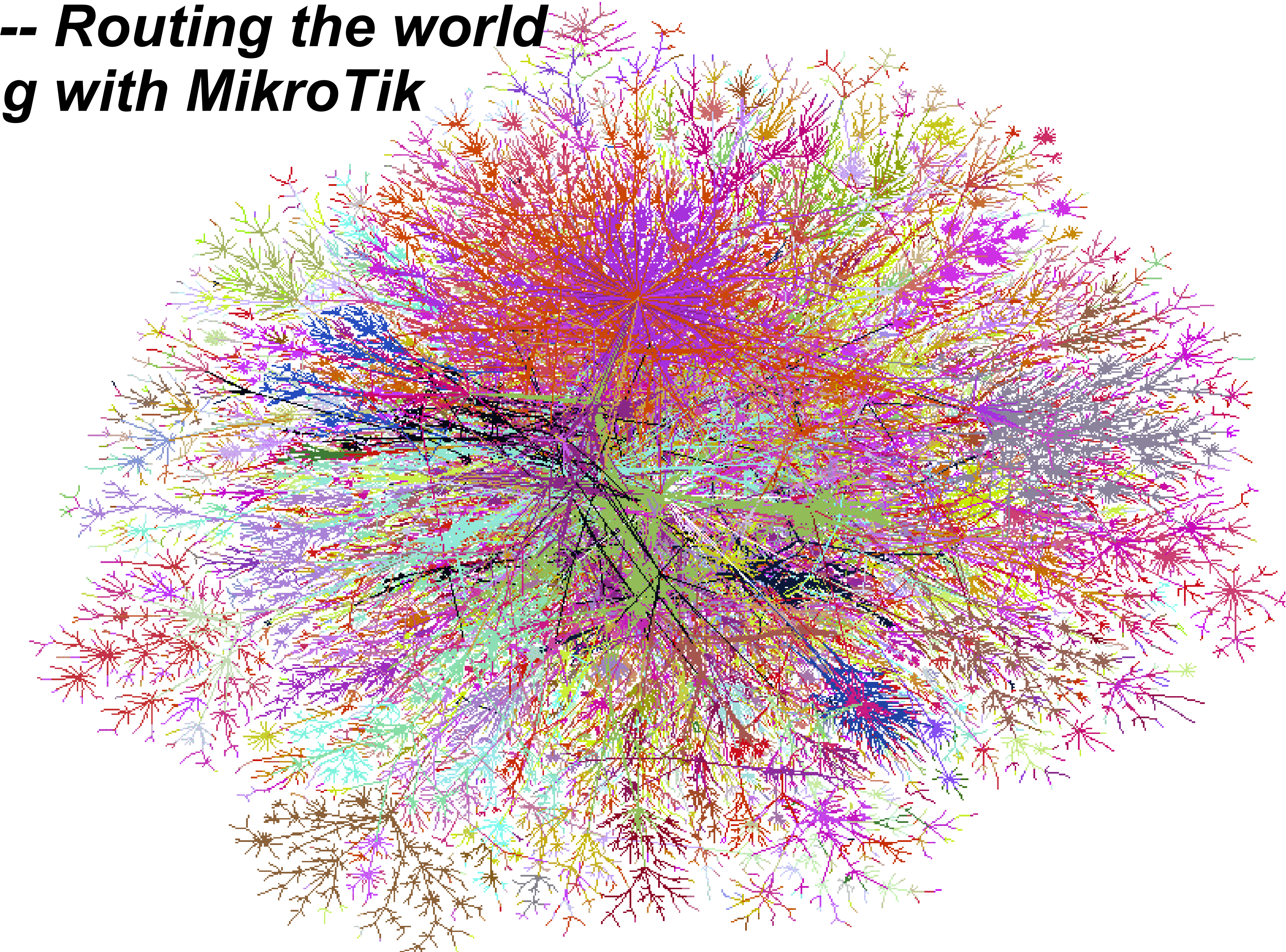
Automating This Filter Technique

- ✓Routing ... Automating Route Updates ?

Dynamic Routing

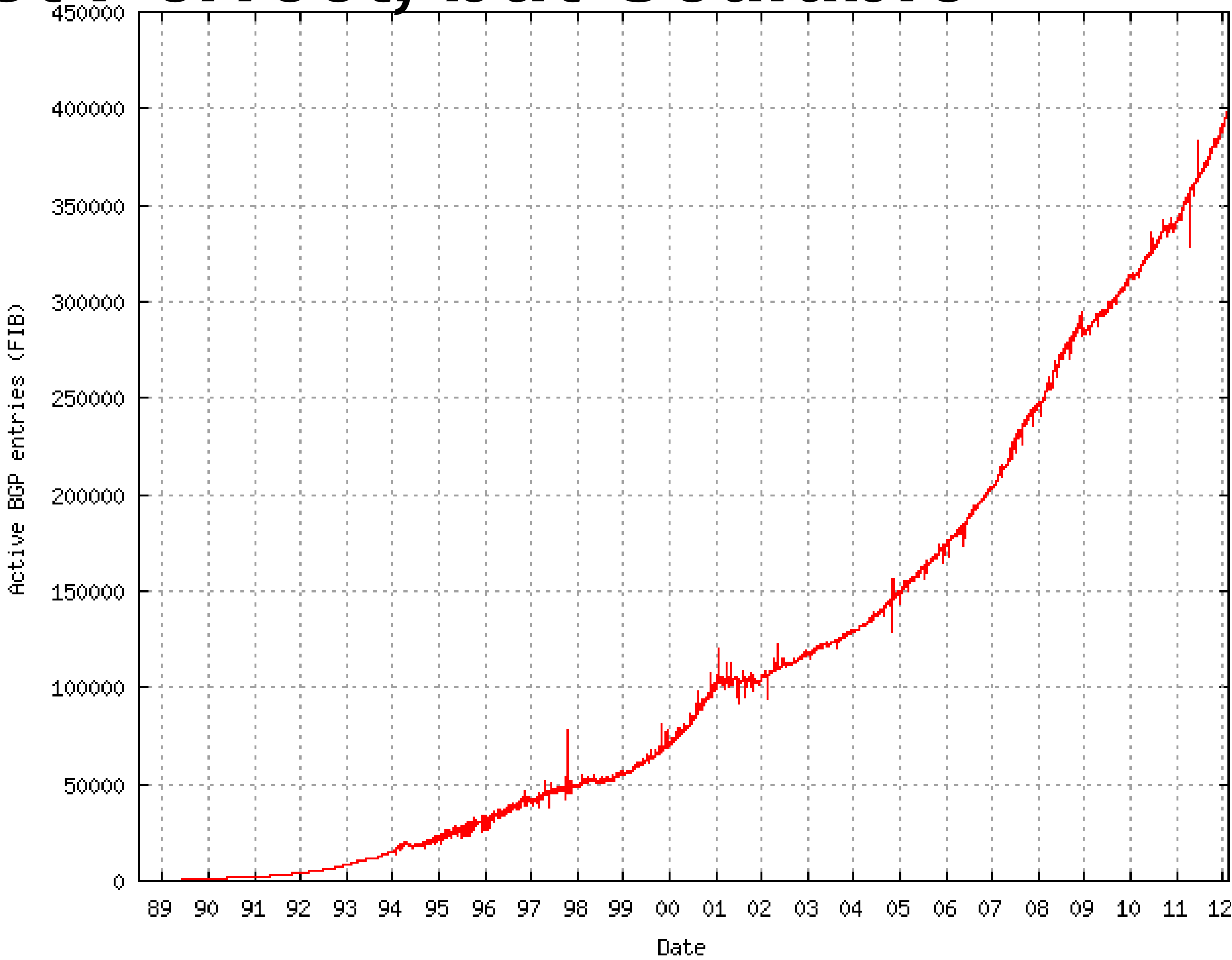
- ✓OSPF--
  - possible to use but OSPF routers need to share at least 1 layer2 segment (either physical or VPN / PPP interface)
  - Very limited Route Attributes can be exchanged between routers
- ✓RIP-- Requiescat in pace...
  - Not scalable not widely deployed
- ✓BGP
  - Stable
  - Scalable
  - Extensive features for filtering
  - Extensive options for exchanging information about routes

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
  - *“This Prefix is reachable through my AS”*
  - Only protocol that can handle Internet's size networks
- ✓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)
- ✓Peers do not have to be directly connected using Multi Hop Configurations :)
- ✓Initial full routing table exchange between peers
- ✓Incremental updates after initial exchange

BGP Community

- ✓Attribute that groups destinations,
- ✓Filters can be easily applied to all routes within one group
- ✓Default groups:
  - ·No-export – do not advertise to eBGP peer
  - ·No-advertise – do not advertise to any peer
  - ·Internet – advertise to Internet community

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 useful information meaning of Policies etc.

- ✓Route Advertiser (BGP out) sets communities according to some design / policy

- ✓Various Communities are set and sent out with various routes...

- ✓Route Receiver Admin sets Router Receiver 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

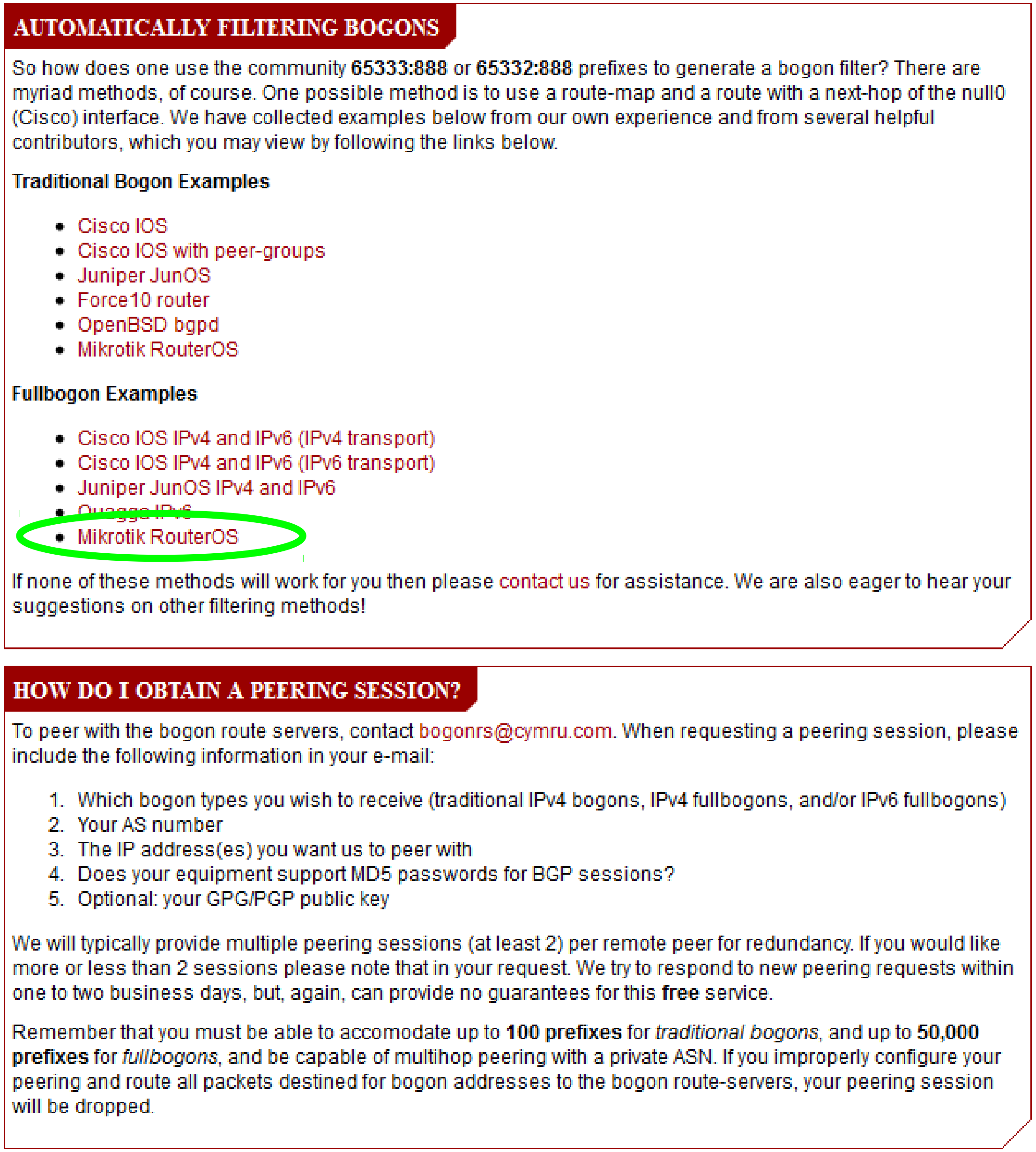
- ✓Remember your MTCNA Training ? Remember the definition of a Bogon ?
- ✓If you haven’t a MTCNA – you could be missing out on lots of tips and techniques to make your job of running and expanding your network easier
- ✓Contact your Prefered Trainer
- ✓Bogon List is constantly reducing – as unassigned Ips get assigned from RIRs to LIRs
- ✓Statically blocking Bogons (with manual Address lists is a very bad Idea)
- ✓We need an automated way of updating our routers bogon filters

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 innovative
- ✓They even have published examples of BGP Configurations for Mikrotik so that you can peer with them
- ✓Tell your friends about them

Team cymru's Bogon web page

- ✓Full Example for Bogon Feed for MikroTik Router OS :)



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:

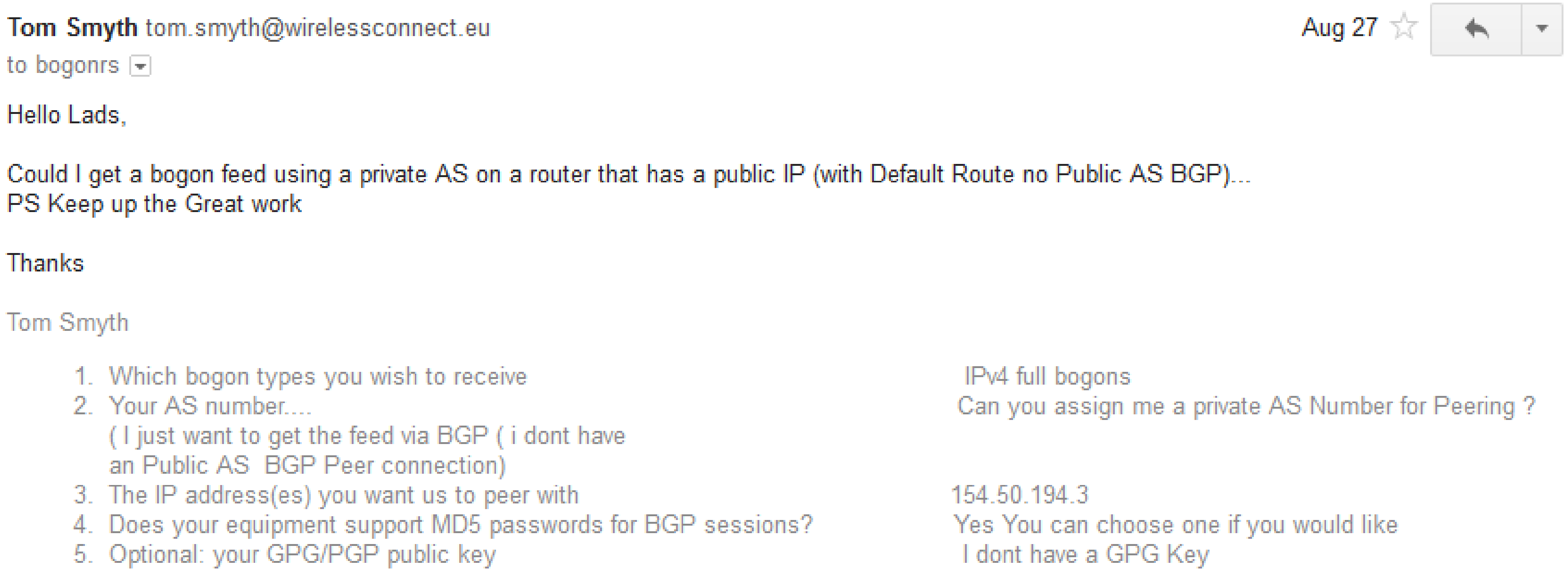
1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

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

- ✓If you dont have a public AS number (not running BGP with your ISP) you can ask for a private AS number
- ✓Just give fill out the request form as shown below
- ✓Give them your AS Number



Tom Smyth tom.smyth@wirelessconnect.eu
to bogonrs

Aug 27

Hello Lads,

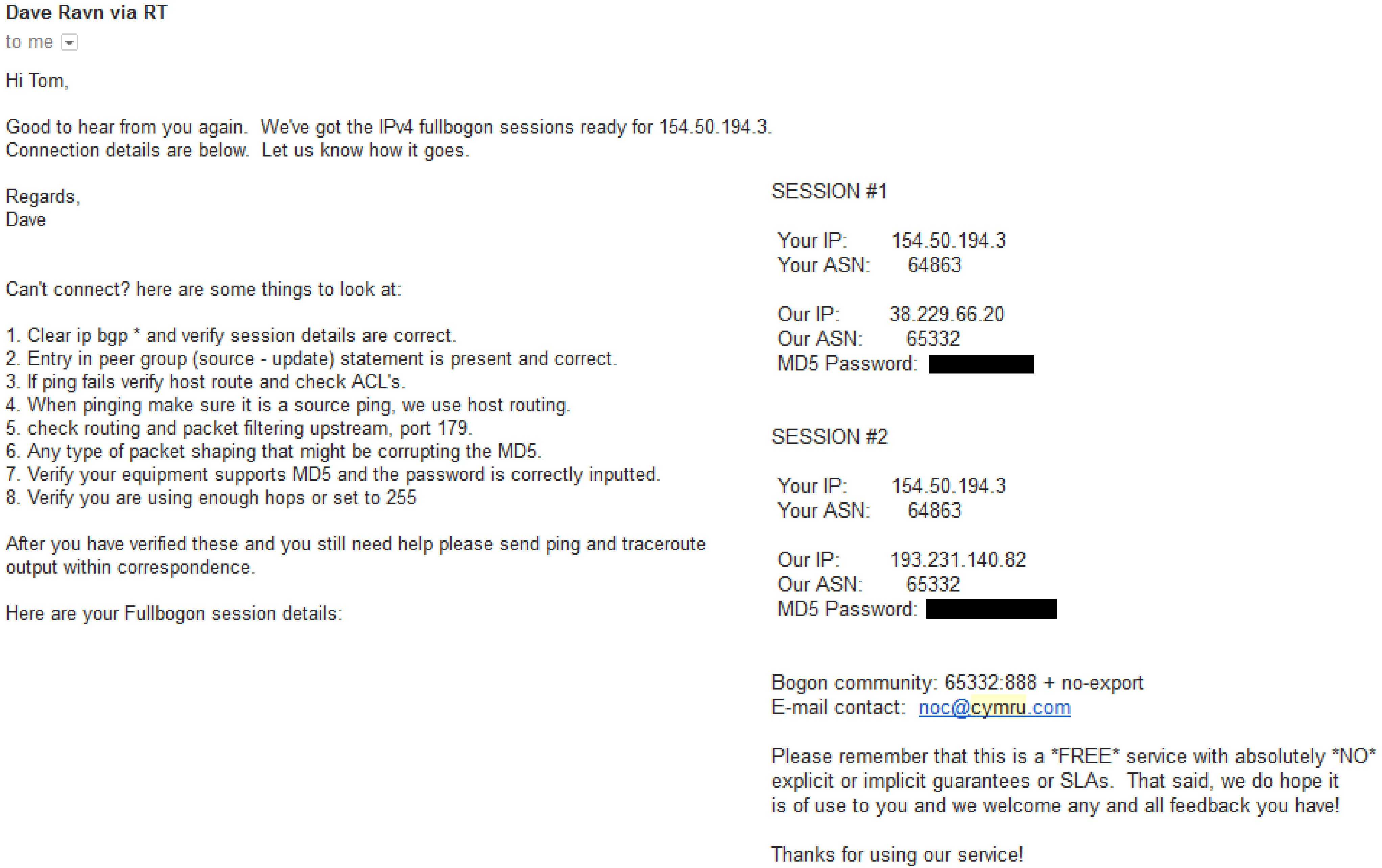
Could I get a bogon feed using a private AS on a router that has a public IP (with Default Route no Public AS BGP)...
PS Keep up the Great work

Thanks

Tom Smyth

1. Which bogon types you wish to receive	IPv4 full bogons
2. Your AS number.... (I just want to get the feed via BGP (i dont have an Public AS BGP Peer connection)	Can you assign me a private AS Number for Peering ?
3. The IP address(es) you want us to peer with	154.50.194.3
4. Does your equipment support MD5 passwords for BGP sessions?	Yes You can choose one if you would like
5. Optional: your GPG/PGP public key	I dont have a GPG Key

Cymru response



Dave Ravn via RT

to me

Hi Tom,

Good to hear from you again. We've got the IPv4 fullbogon sessions ready for 154.50.194.3.
Connection details are below. Let us know how it goes.

Regards,
Dave

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:

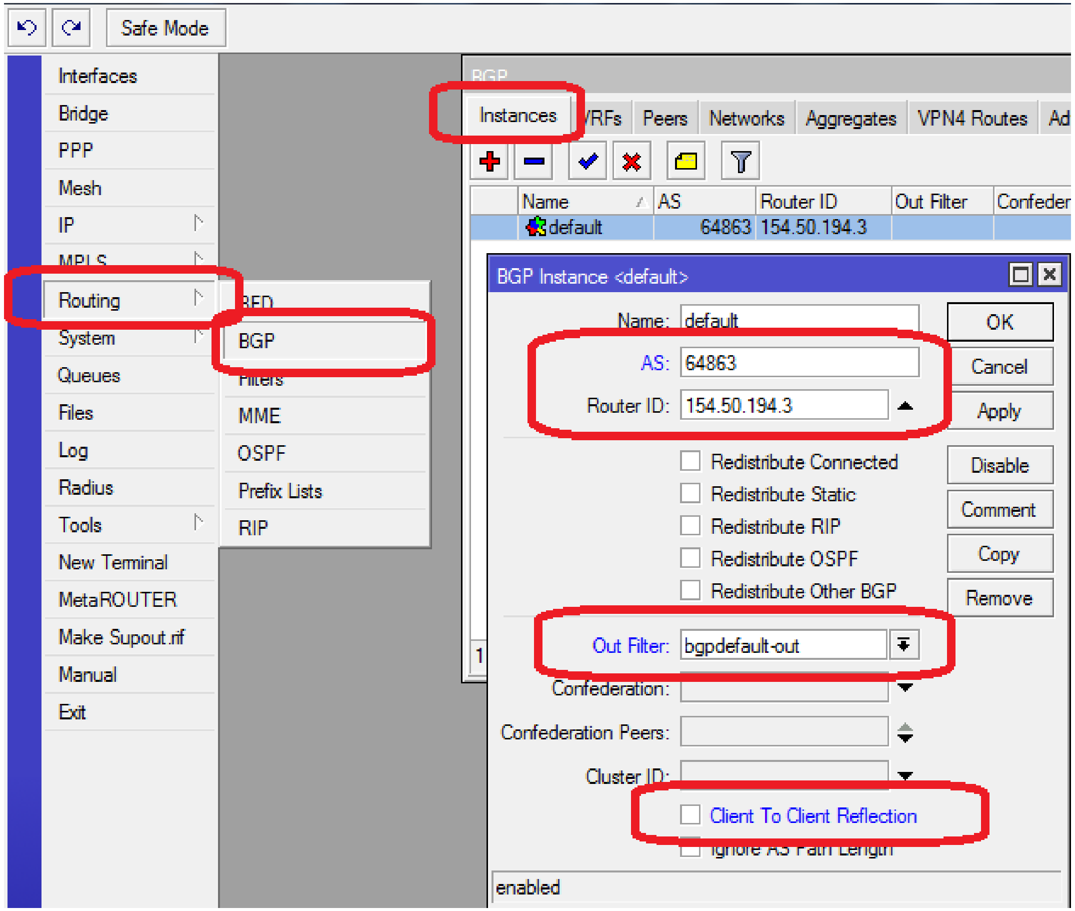
```
SESSION #1

 Your IP:      154.50.194.3
 Your ASN:      64863

 Our IP:       38.229.66.20
 Our ASN:       65332
 MD5 Password: [redacted]


SESSION #2

 Your IP:      154.50.194.3
 Your ASN:      64863

 Our IP:       193.231.140.82
 Our ASN:       65332
 MD5 Password: [redacted]
```

Bogon community: 65332:888 + no-export
E-mail contact: noc@cymru.com

Please remember that this is a *FREE* service with absolutely *NO* explicit or implicit guarantees or SLAs. That said, we do hope it is of use to you and we welcome any and all feedback you have!

Thanks for using our service!

Set up your BGP instance



Name	AS	Router ID	Out Filter	Confeder
default	64863	154.50.194.3		

Name: default

AS: 64863

Router ID: 154.50.194.3

□ Redistribute Connected

□ Redistribute Static

□ Redistribute RIP

□ Redistribute OSPF

□ Redistribute Other BGP

Out Filter: bgpdefault-out

Confederation:

Confederation Peers:

Cluster ID:

□ Client To Client Reflection

□ Ignore AS Path Length

enabled

- ✓Use the Private AS number that Team Cymru assigns you for your router.
- ✓Set the Router ID to be the same as the IP of your router that you gave when requesting the feed
- ✓Set an Out-Filter
- ✓Disable Client to Client Reflection

Setting up Route Filters for BGP

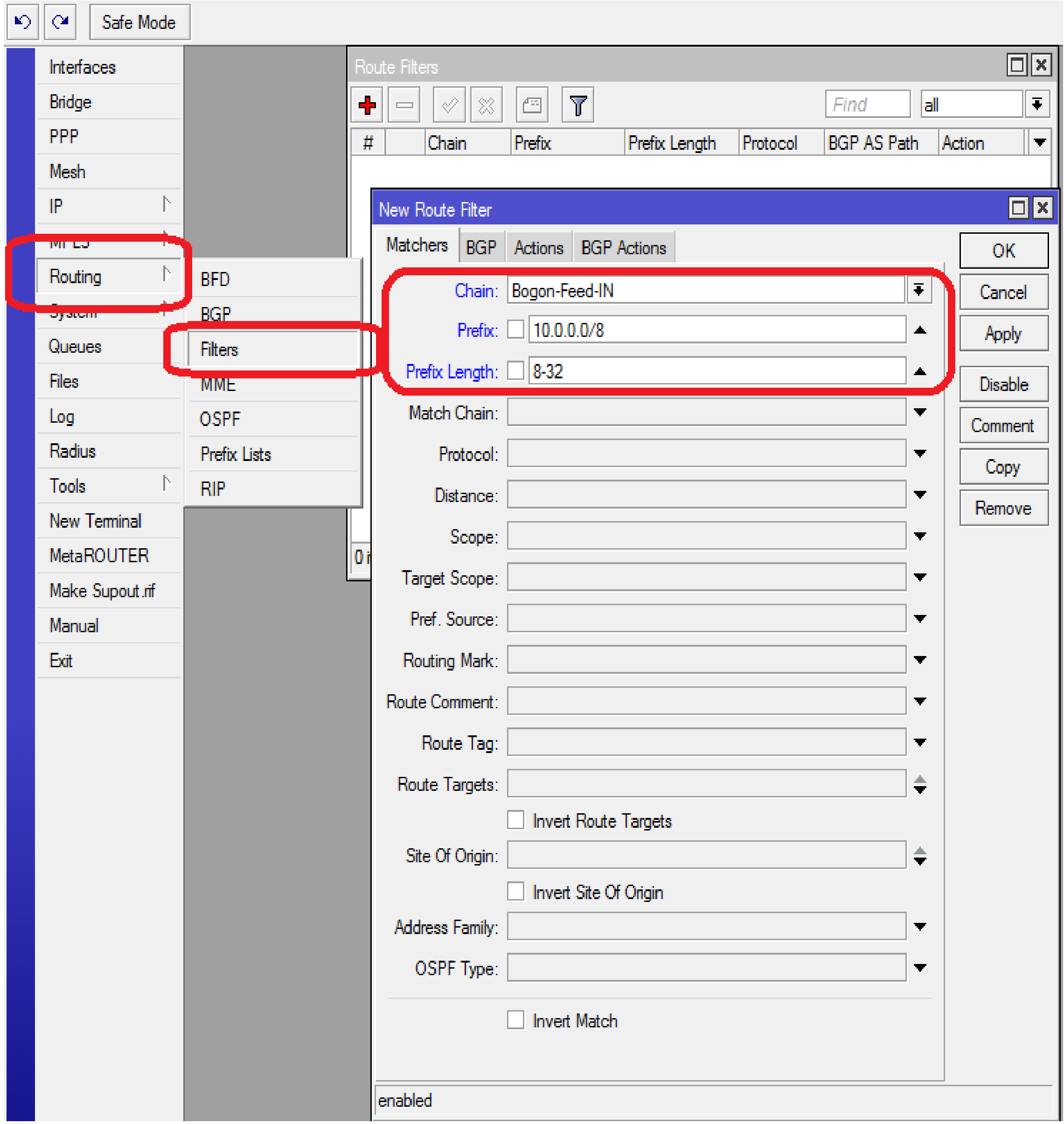
- ✓When Configuring BGP one should always use Route Filters to reduce the impact of mistakes in configuration
- ✓Deny all scenarios you dont want to happen explicitly
- ✓Allow only limited scenarios according to design
- ✓Create a Default Deny rule to prevent any unexpected routes hitting your Router

Bogon Route Filter Requirements

- ✓Reject private IP Black hole routes that conflict with our own private networks
- ✓Allow only Routes with the correct bogon community set and add these routes to the routing table as black hole routes
- ✓Discard all other types of Routes comming from the Bogon Feed (Protect our router from misconfiguration of our Peer)
- ✓Discard all advertisements from our Router to the Bogon BGP Peer (Protect our peer from misconfiguration of our router)

Setting up Route Filters A must for BGP

- Create a new Filter Chain for Bogon Feeds in
- Reject any Private RFC1918 Private addresses (in use on your own network)
- We dont want to blackhole our own networks!



Chain: Bogon-Feed-IN

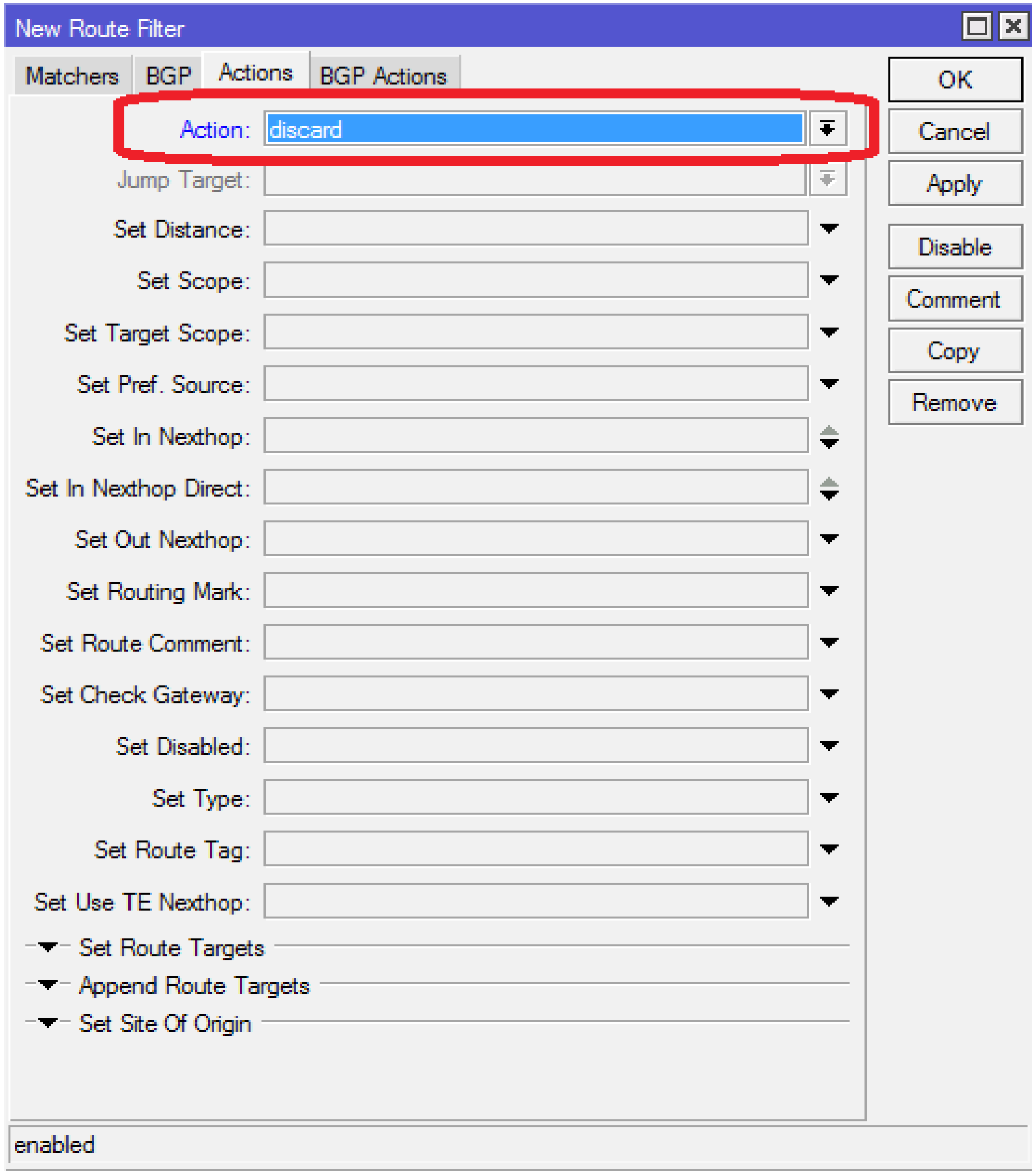
Prefix: □ 10.0.0.0/8

Prefix Length: □ 8-32

enabled

Drop unwanted Bogons

- ✓Set Route Filter Action to Discard



New Route Filter

Matchers | BGP | Actions | BGP Actions

Action: discard

Jump Target:

Set Distance:

Set Scope:

Set Target Scope:

Set Pref. Source:

Set In Nexthop:

Set In Nexthop Direct:

Set Out Nexthop:

Set Routing Mark:

Set Route Comment:

Set Check Gateway:

Set Disabled:

Set Type:

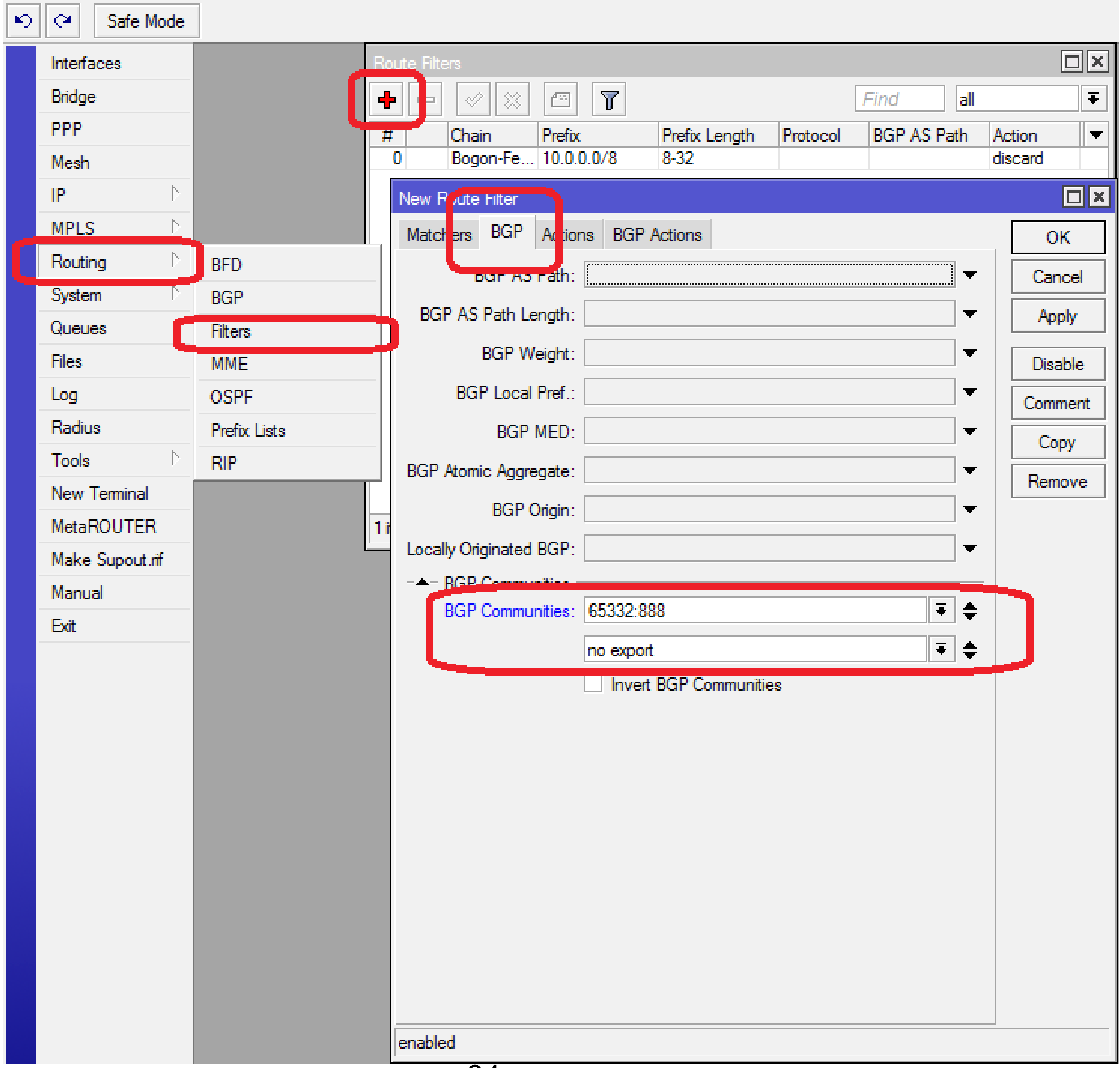
Set Route Tag:

Set Use TE Nexthop:

enabled

Filter to Look for Correct Bogon BGP Community

- Use BGP Matcher Tab to search for routes that have the correct community set
- Check email from Team Cymru for correct bogon communities
- 655332:888 & No Export



#	Chain	Prefix	Prefix Length	Protocol	BGP AS Path	Action
0	Bogon-Fe...	10.0.0.0/8	8-32			discard

BGP Communities: 65332:888

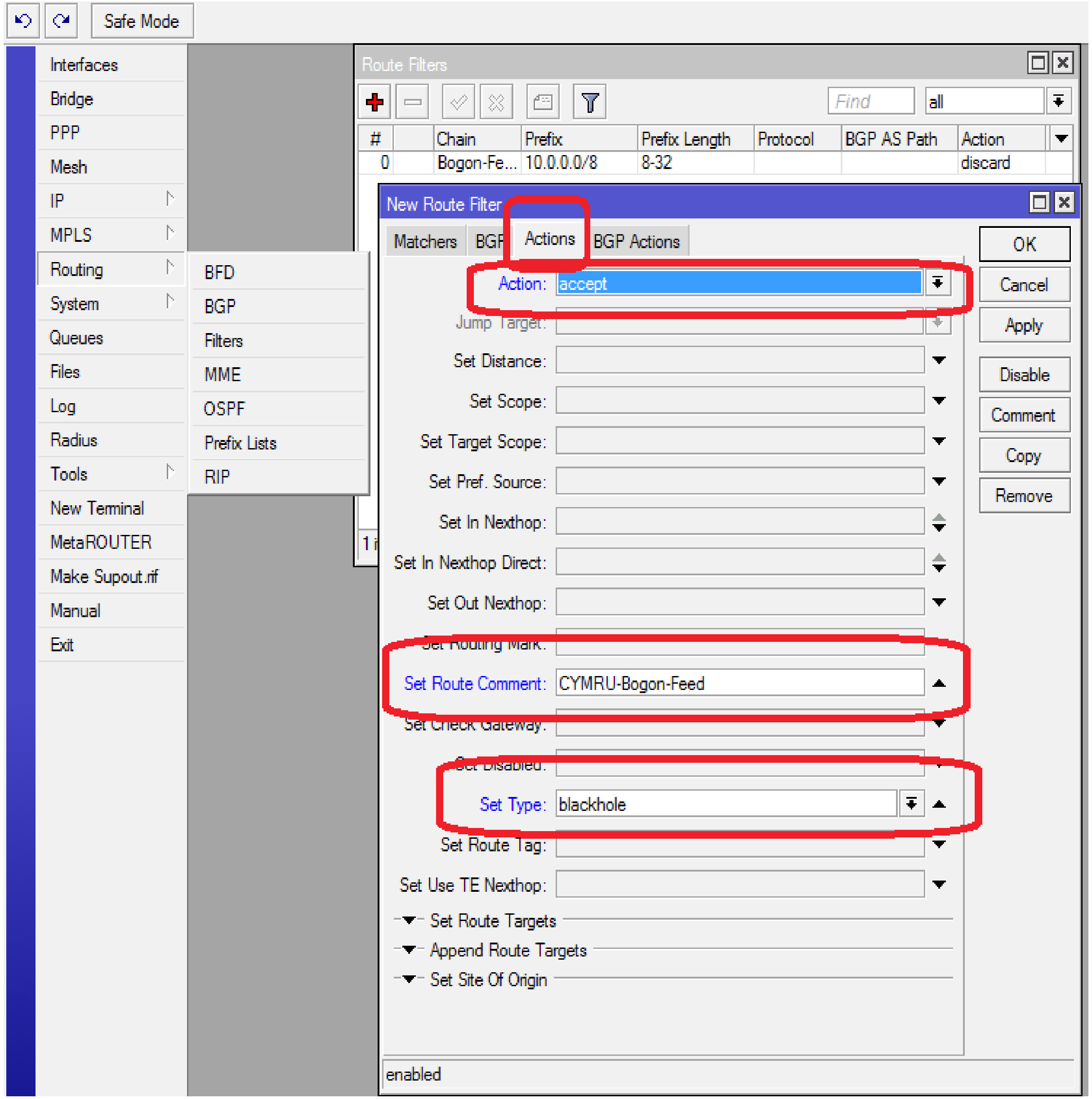
no export

□ Invert BGP Communities

enabled

Accept and Black Hole Bogon prefixes

- ✓Set Action to Accept
- ✓Add Route Comment so that you understand where the routes are comming from
- ✓Set type to Black hole (very Important)



Route Filters

#	Chain	Prefix	Prefix Length	Protocol	BGP AS Path	Action
0	Bogon-Fe...	10.0.0.0/8	8-32			discard

New Route Filter

Action: accept

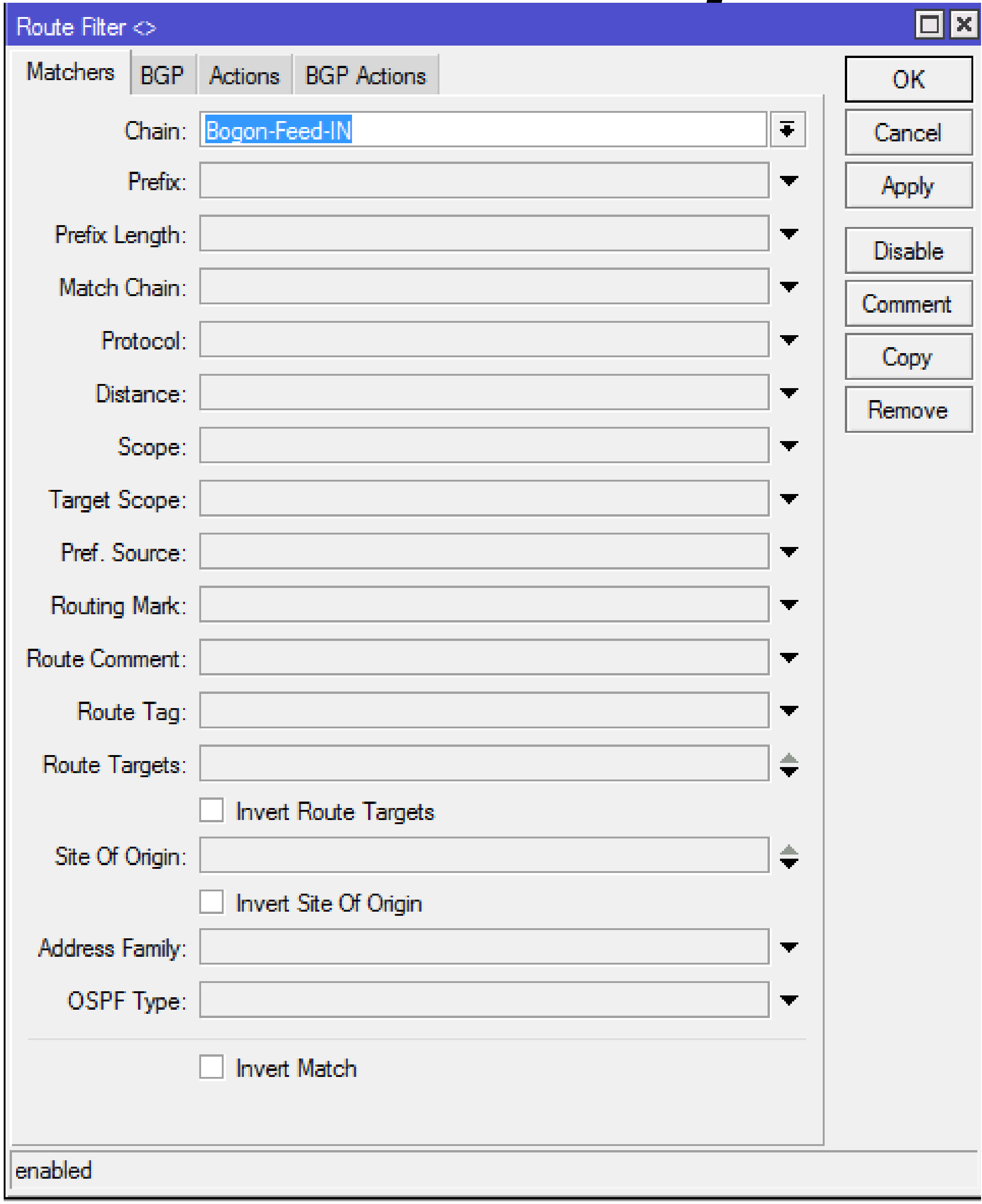
Set Route Comment: CYMRU-Bogon-Feed

Set Type: blackhole

enabled

Drop all other Prefixes from our peer

- ✓Select Bogon-Feed-IN Chain
- ✓Discard all routes by leaving all matcher fields greyed out



Route Filter <>

Chain: Bogon-Feed-IN

Prefix:

Prefix Length:

Match Chain:

Protocol:

Distance:

Scope:

Target Scope:

Pref. Source:

Routing Mark:

Route Comment:

Route Tag:

Route Targets:

□ Invert Route Targets

Site Of Origin:

□ Invert Site Of Origin

Address Family:

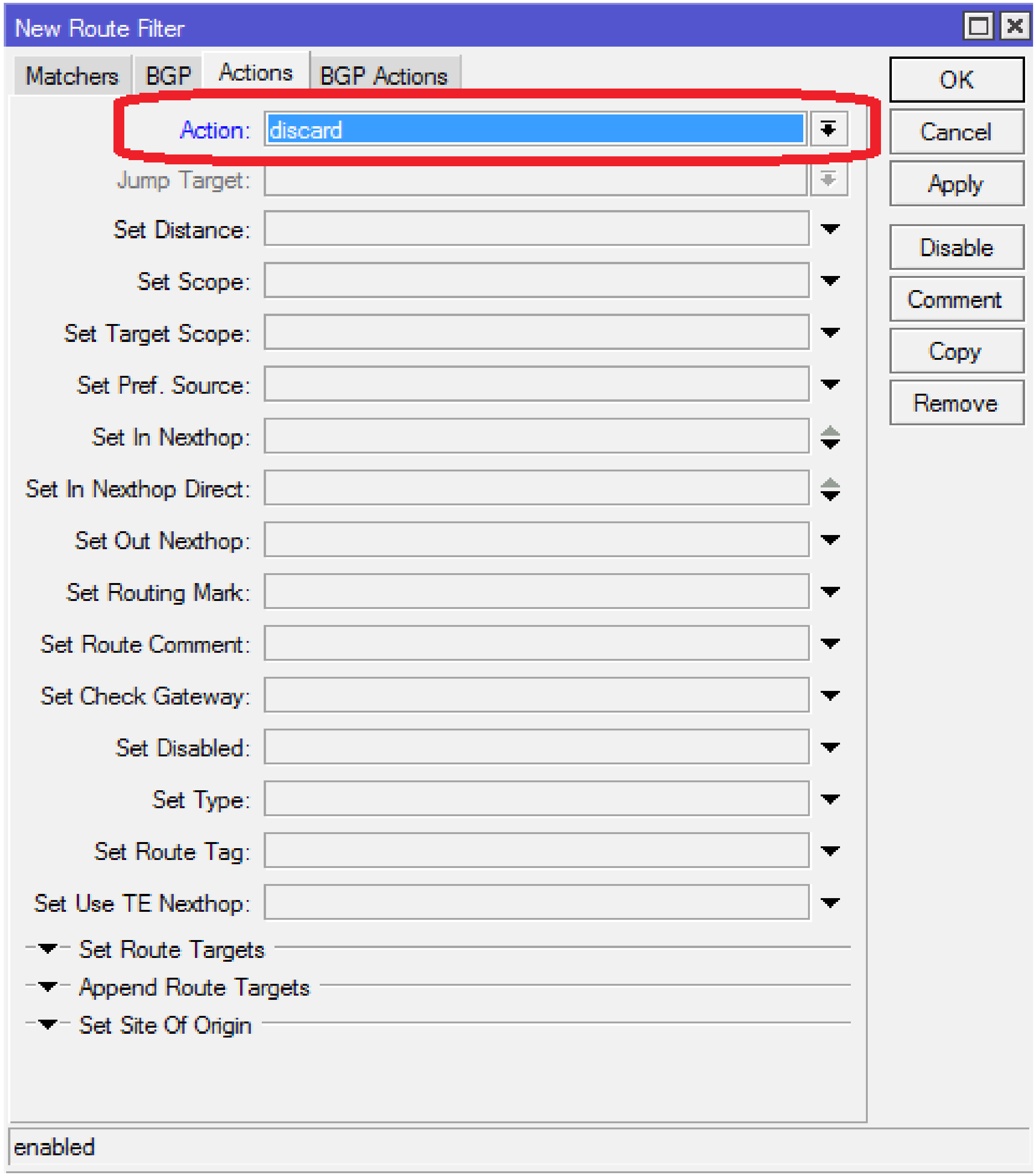
OSPF Type:

□ Invert Match

enabled

Drop All Route Advertisements In

- ✓Discard Routes using the Discard Action in Route Filter Action Tab



New Route Filter

Action: discard

Jump Target:

Set Distance:

Set Scope:

Set Target Scope:

Set Pref. Source:

Set In Nexthop:

Set In Nexthop Direct:

Set Out Nexthop:

Set Routing Mark:

Set Route Comment:

Set Check Gateway:

Set Disabled:

Set Type:

Set Route Tag:

Set Use TE Nexthop:

Set Route Targets

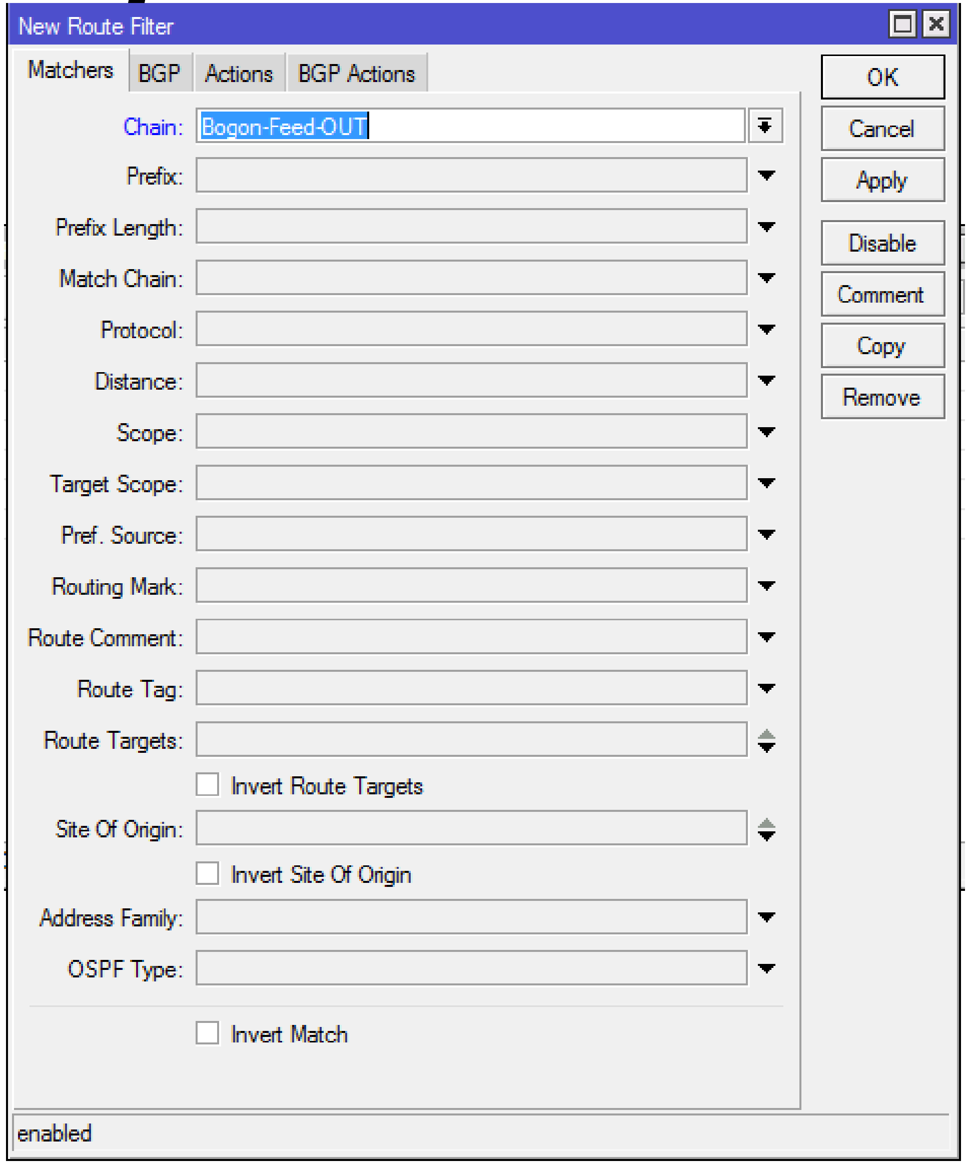
Append Route Targets

Set Site Of Origin

enabled

Discard all route advertisements from us to our bogon peer

- ✓Create a Bogon-Feed-Out Chain
- ✓And Configure a rule to drop everything
- ✓To drop everything all matcher fields must be greyed out!



New Route Filter

Matchers | BGP | Actions | BGP Actions

Chain: Bogon-Feed-OUT

Prefix:

Prefix Length:

Match Chain:

Protocol:

Distance:

Scope:

Target Scope:

Pref. Source:

Routing Mark:

Route Comment:

Route Tag:

Route Targets:

□ Invert Route Targets

Site Of Origin:

□ Invert Site Of Origin

Address Family:

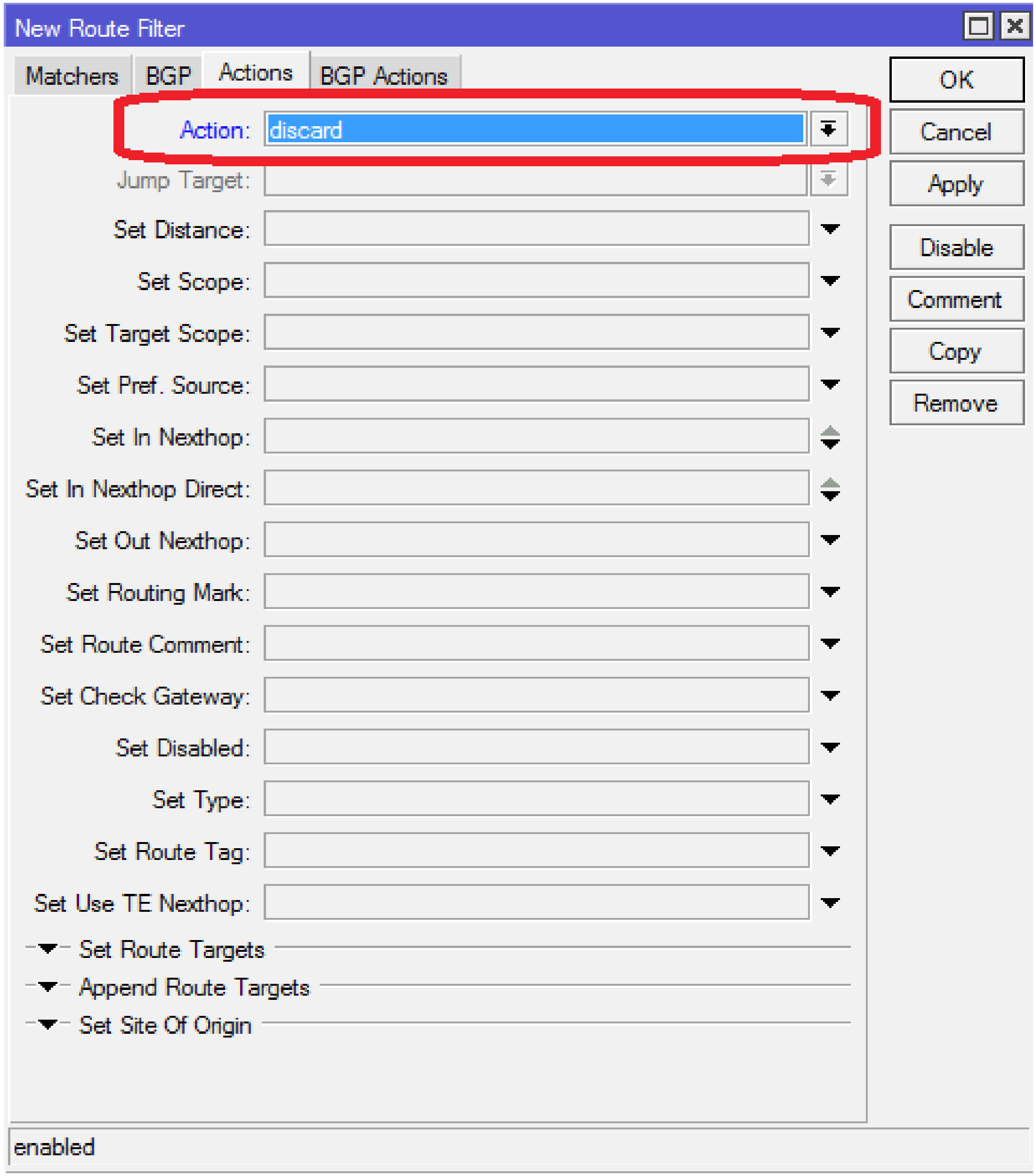
OSPF Type:

□ Invert Match

enabled

Drop All Route Advertisements

- ✓Discard Routes using the Discard Action in Route Filter Action Tab



Action: discard

Jump Target:

Set Distance:

Set Scope:

Set Target Scope:

Set Pref. Source:

Set In Nexthop:

Set In Nexthop Direct:

Set Out Nexthop:

Set Routing Mark:

Set Route Comment:

Set Check Gateway:

Set Disabled:

Set Type:

Set Route Tag:

Set Use TE Nexthop:

Set Route Targets

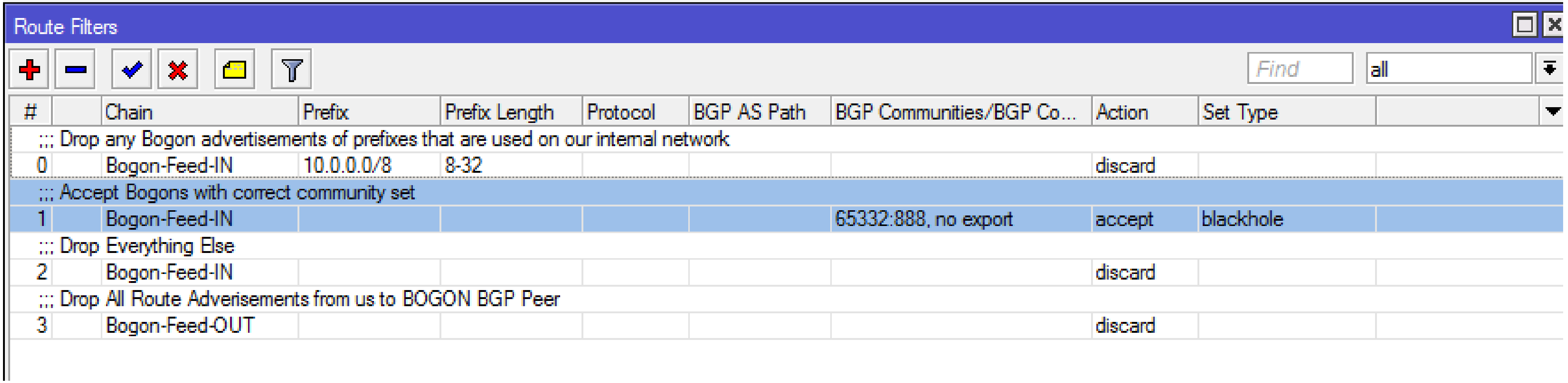
Append Route Targets

Set Site Of Origin

enabled

Route Filters Completed

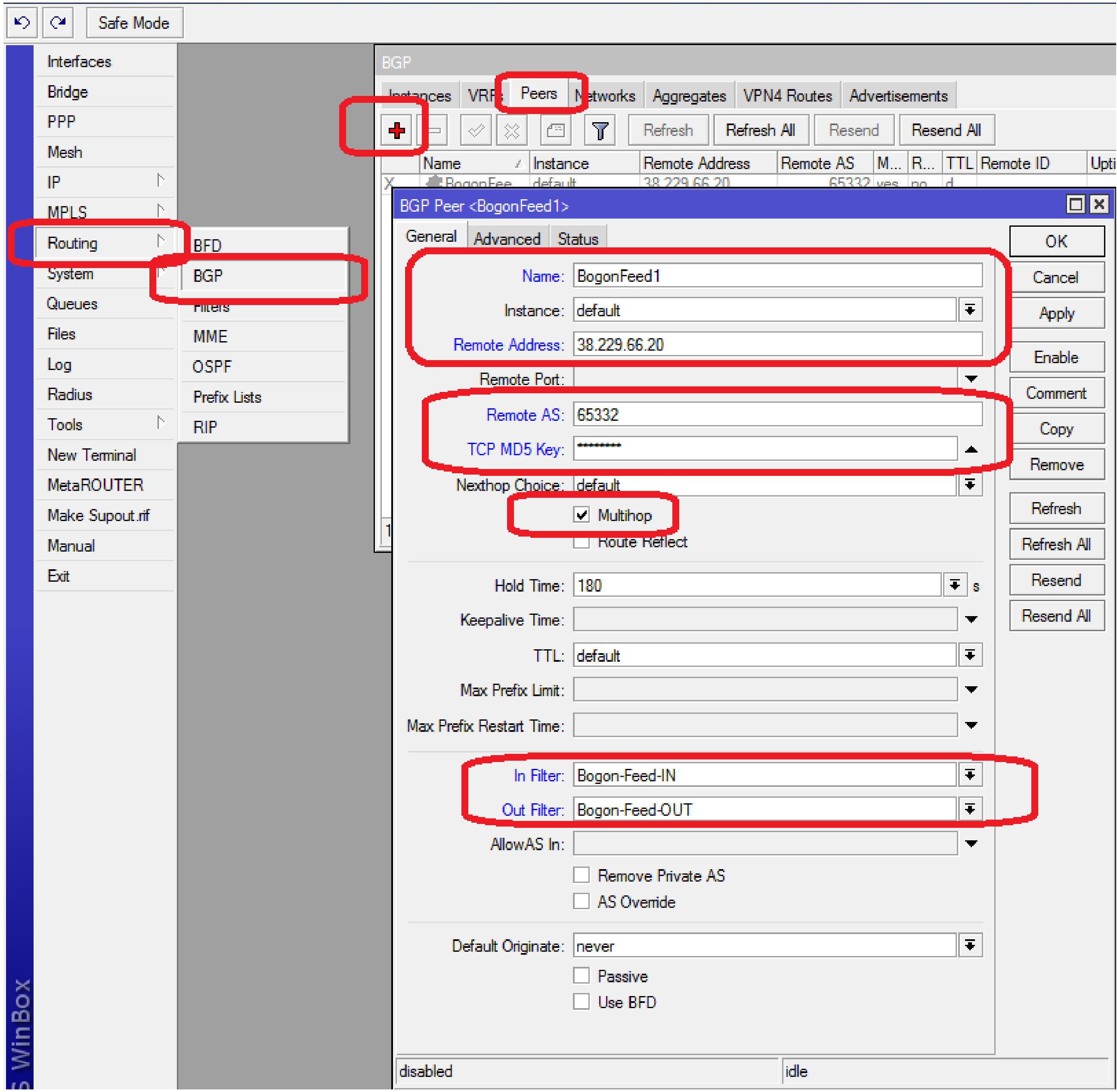
- ✓Order of the Rules are important
- ✓Filter all what you definitely dont want to happen first,
- ✓Allow only what you know you need
- ✓Drop Everything else
- ✓Similar to the Firewall Specific Rules towards the top General Rules towards the bottom



#		Chain	Prefix	Prefix Length	Protocol	BGP AS Path	BGP Communities/BGP Co...	Action	Set Type
;;; Drop any Bogon advertisements of prefixes that are used on our internal network									
0		Bogon-Feed-IN	10.0.0.0/8	8-32				discard	
;;; Accept Bogons with correct community set									
1		Bogon-Feed-IN					65332:888, no export	accept	blackhole
;;; Drop Everything Else									
2		Bogon-Feed-IN						discard	
;;; Drop All Route Adverisements from us to BOGON BGP Peer									
3		Bogon-Feed-OUT						discard	

Configure the Bogon Feed as a BGP Peer

- ✓Configure your Bogon BGP Feed by inserting the values given to you by Team Cymru
- ✓Essential Values include
- ✓Remote Address
- ✓Remote AS Number
- ✓TCP MD5 Key
- ✓Enabling Multi-hop (peer is not directly connected)
- ✓Using the In and Out Route Filters that we created earlier



Name: BogonFeed1

Instance: default

Remote Address: 38.229.66.20

Remote Port:

Remote AS: 65332

TCP MD5 Key: ********

Nexthop Choice: default

☑ Multihop

□ Route Reflect

Hold Time: 180 s

Keepalive Time:

TTL: default

Max Prefix Limit:

Max Prefix Restart Time:

In Filter: Bogon-Feed-IN

Out Filter: Bogon-Feed-OUT

AllowAS In:

□ Remove Private AS

□ AS Override

Default Originate: never

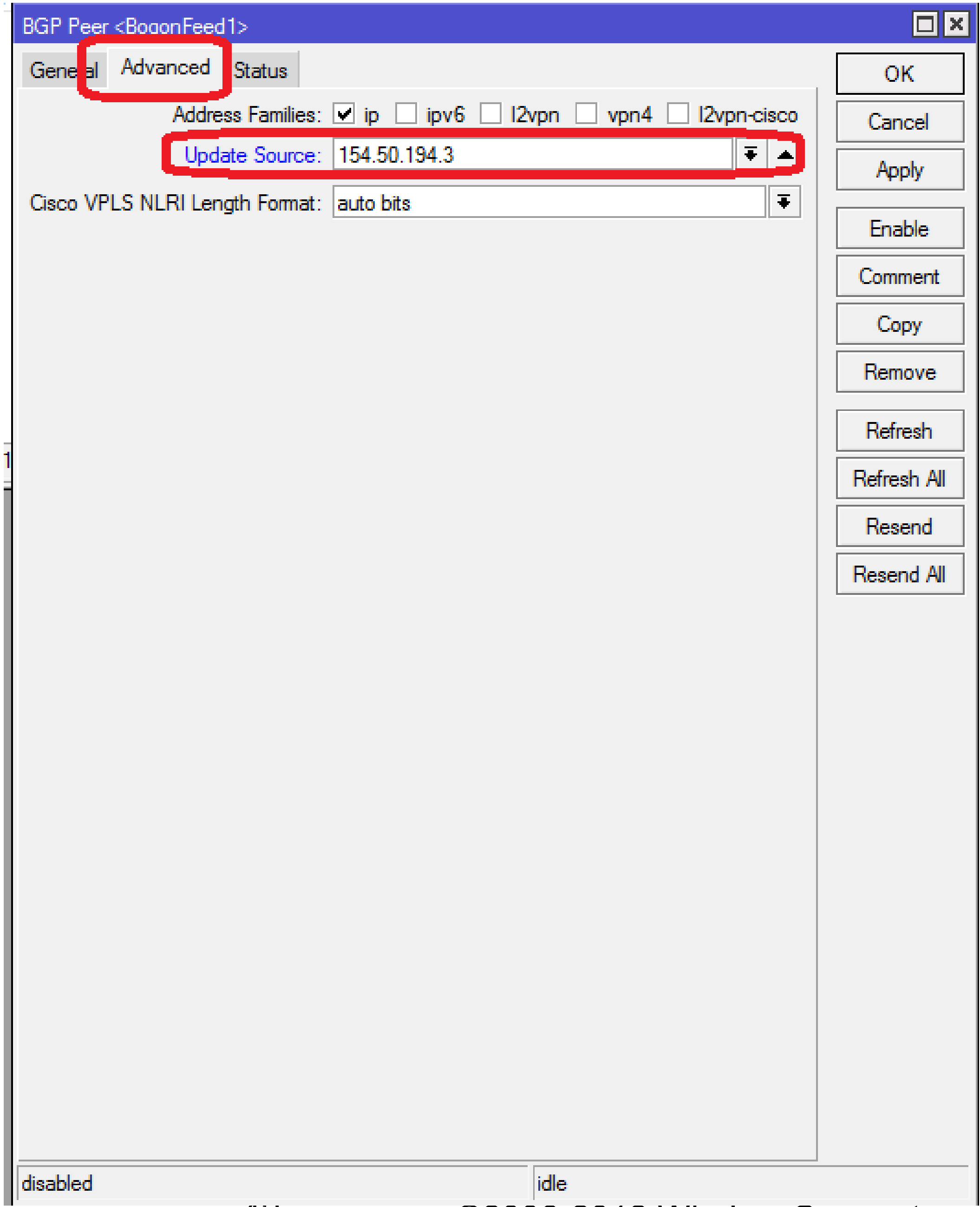
□ Passive

□ Use BFD

disabled idle

Configuring your Routers Update source IP

- ✓Set the Update source to be the same as the public IP you submitted to TeamCymru
- ✓Set the Address Families to IP


BGP Peer <BogonFeed1>

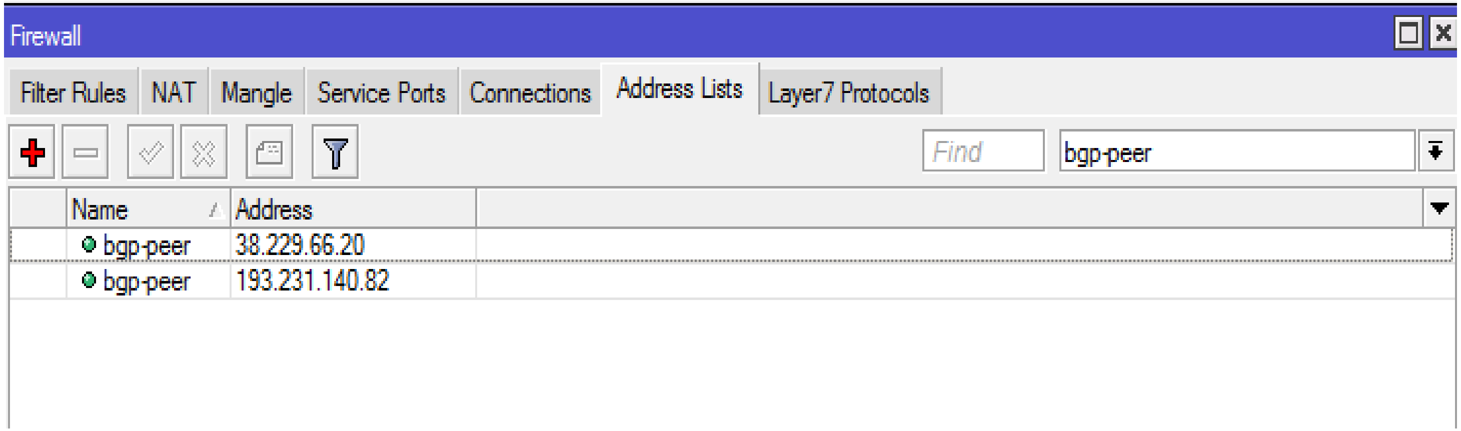
Address Families: ☑ ip ☐ ipv6 ☐ l2vpn ☐ vpn4 ☐ l2vpn-cisco

Update Source: 154.50.194.3

Cisco VPLS NLRI Length Format: auto bits

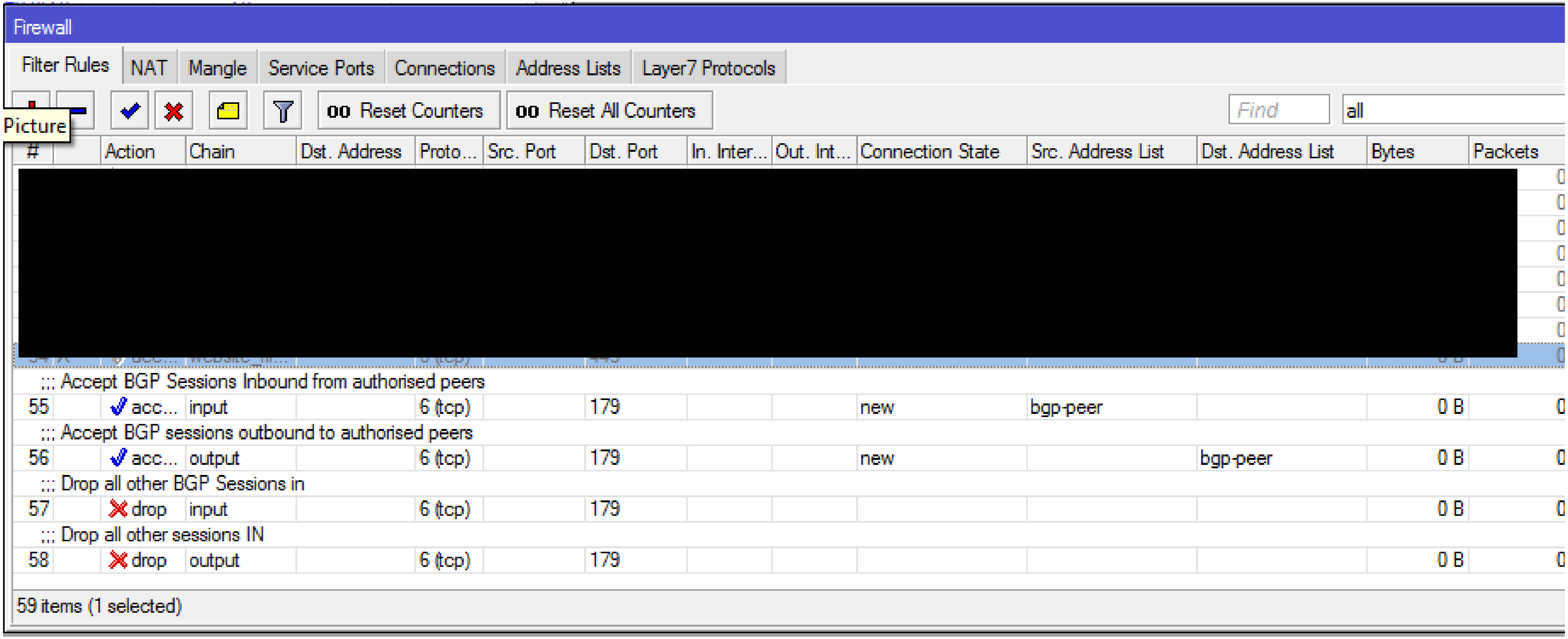
disabled idle

Securing your BGP Sessions with Firewall



bgp-peer

Name	Address
● bgp-peer	38.229.66.20
● bgp-peer	193.231.140.82



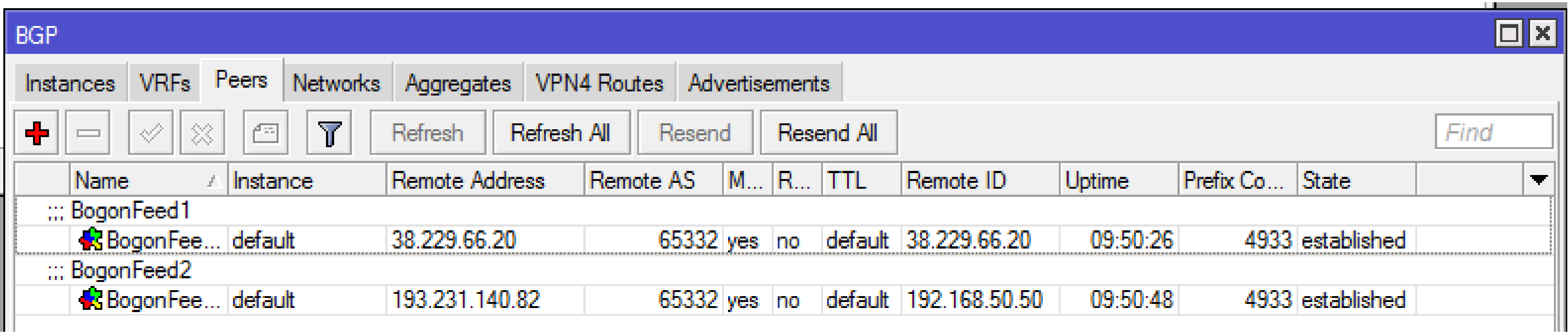
all

#		Action	Chain	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Bytes	Packets
[redacted]														
;;; Accept BGP Sessions Inbound from authorised peers														
55		✓ acc...	input		6 (tcp)		179			new	bgp-peer		0 B	0
;;; Accept BGP sessions outbound to authorised peers														
56		✓ acc...	output		6 (tcp)		179			new		bgp-peer	0 B	0
;;; Drop all other BGP Sessions in														
57		✗ drop	input		6 (tcp)		179						0 B	0
;;; Drop all other sessions IN														
58		✗ drop	output		6 (tcp)		179						0 B	0

59 items (1 selected)

Bogon Feeds from Team Cymru

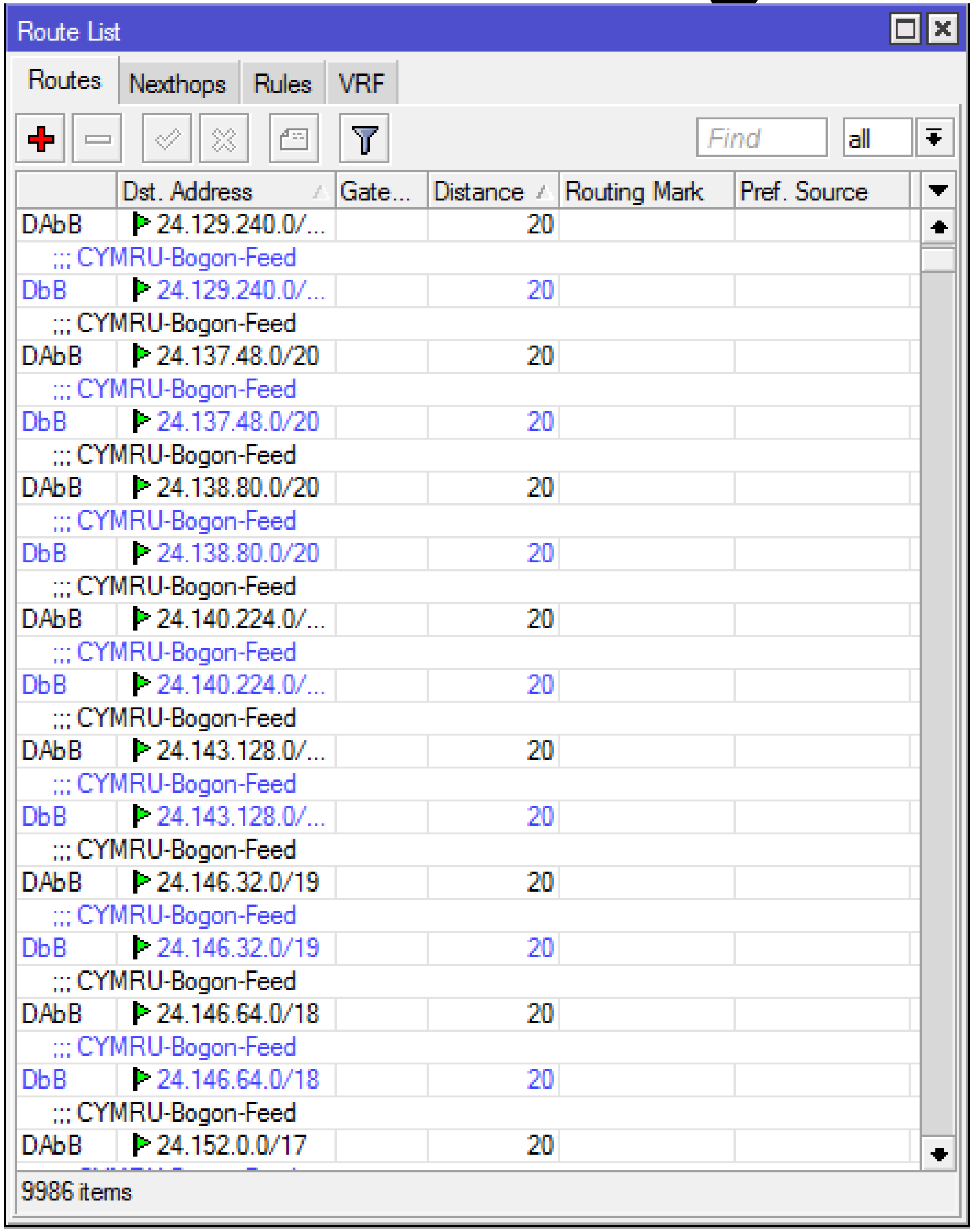
- ✓Configure the Second Peer in a similar manner to the first peer
- ✓Once the peers are enabled they take a few seconds to converge, and download all the prefixes.
- ✓Over 4933 routes are sent down to your Router through the Bogon BGP Feed



Name	Instance	Remote Address	Remote AS	M...	R...	TTL	Remote ID	Uptime	Prefix Co...	State
;;; BogonFeed1										
BogonFee...	default	38.229.66.20	65332	yes	no	default	38.229.66.20	09:50:26	4933	established
;;; BogonFeed2										
BogonFee...	default	193.231.140.82	65332	yes	no	default	192.168.50.50	09:50:48	4933	established

Black Hole Routes in the Routing Table

- Routes are populated into the Routing table with DabB / DbB Status
  - Dynamic
  - Active
  - bGP
  - BlackHole
- Comments are automatically added as per our Peer configuration
- 4933 active blackhole routes
- 4933 standby blackholeroutes

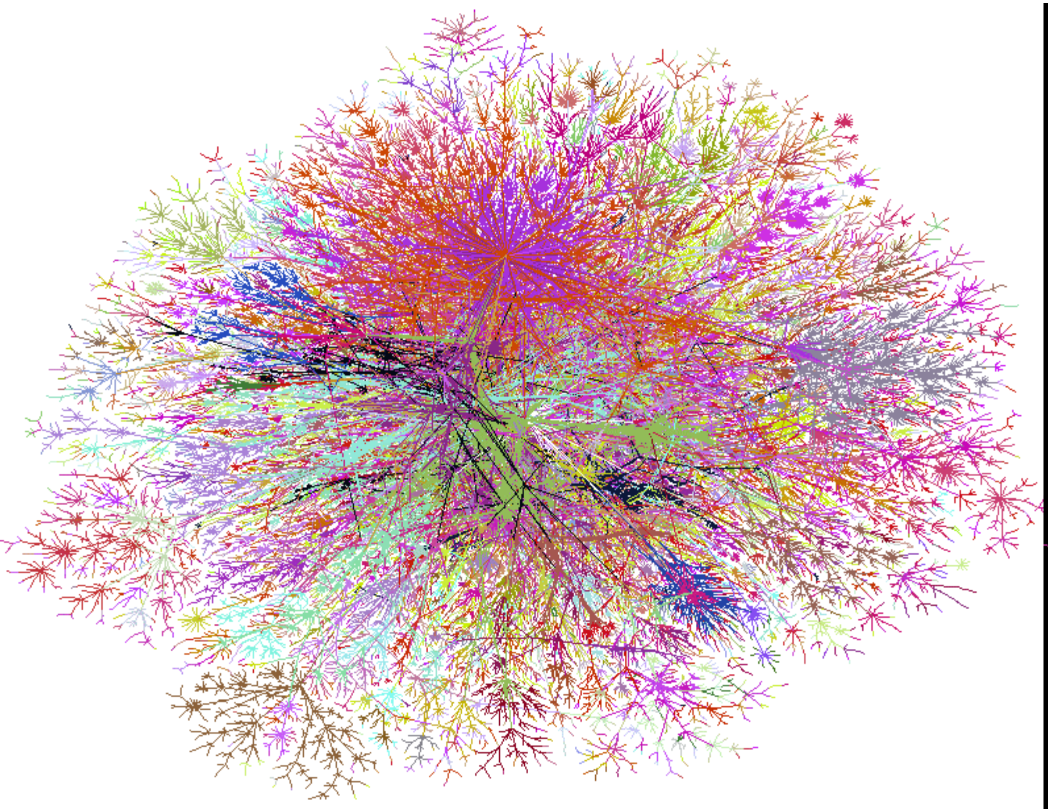


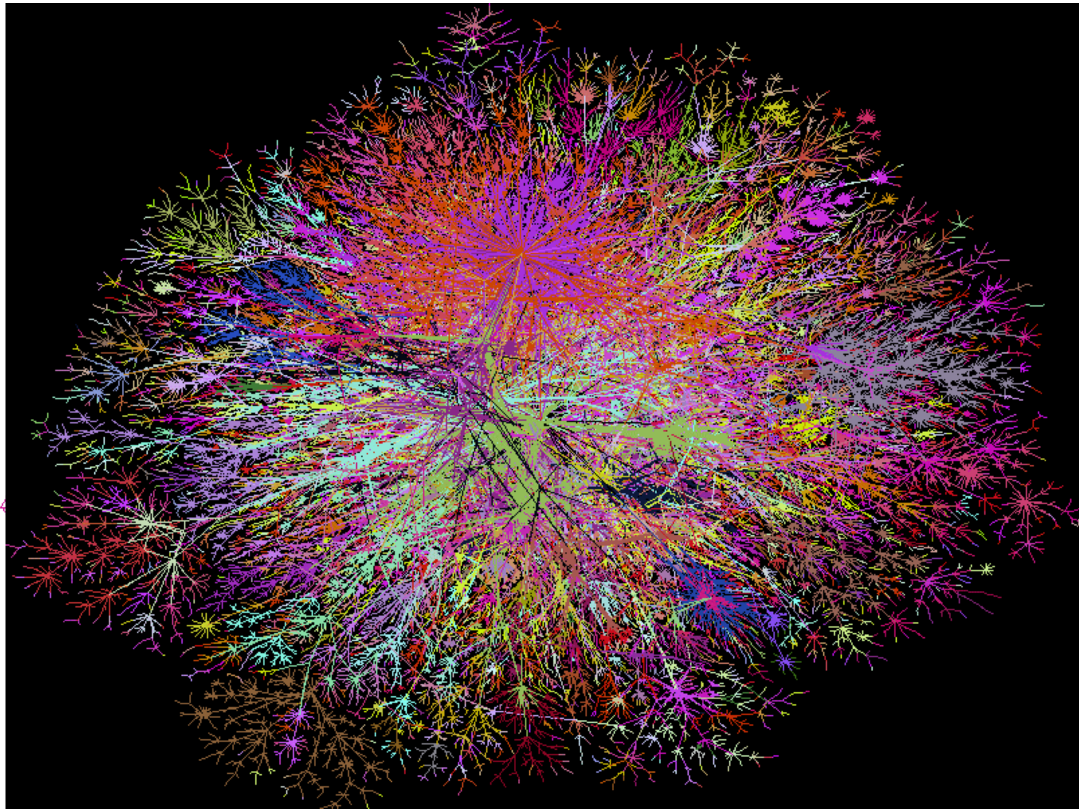
	Dst. Address	Gate...	Distance	Routing Mark	Pref. Source
DAbB	24.129.240.0/...		20		
;;; CYMRU-Bogon-Feed					
DbB	24.129.240.0/...		20		
;;; CYMRU-Bogon-Feed					
DAbB	24.137.48.0/20		20		
;;; CYMRU-Bogon-Feed					
DbB	24.137.48.0/20		20		
;;; CYMRU-Bogon-Feed					
DAbB	24.138.80.0/20		20		
;;; CYMRU-Bogon-Feed					
DbB	24.138.80.0/20		20		
;;; CYMRU-Bogon-Feed					
DAbB	24.140.224.0/...		20		
;;; CYMRU-Bogon-Feed					
DbB	24.140.224.0/...		20		
;;; CYMRU-Bogon-Feed					
DAbB	24.143.128.0/...		20		
;;; CYMRU-Bogon-Feed					
DbB	24.143.128.0/...		20		
;;; CYMRU-Bogon-Feed					
DAbB	24.146.32.0/19		20		
;;; CYMRU-Bogon-Feed					
DbB	24.146.32.0/19		20		
;;; CYMRU-Bogon-Feed					
DAbB	24.146.64.0/18		20		
;;; CYMRU-Bogon-Feed					
DbB	24.146.64.0/18		20		
;;; CYMRU-Bogon-Feed					
DAbB	24.152.0.0/17		20		

9986 items

BGP-- Bogon filtering illustrated

- ✓All unallocated areas of IPv4 spaces are masked off with blackhole Routes
- ✓Communication with illegally advertised addresses will not be possible



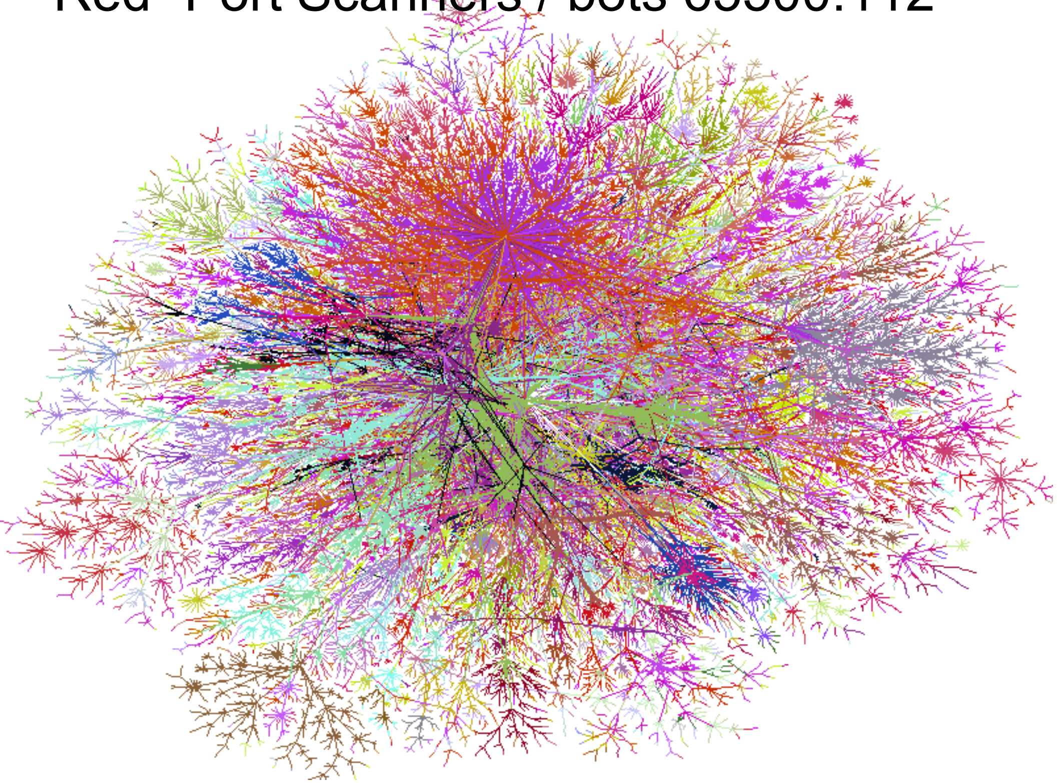


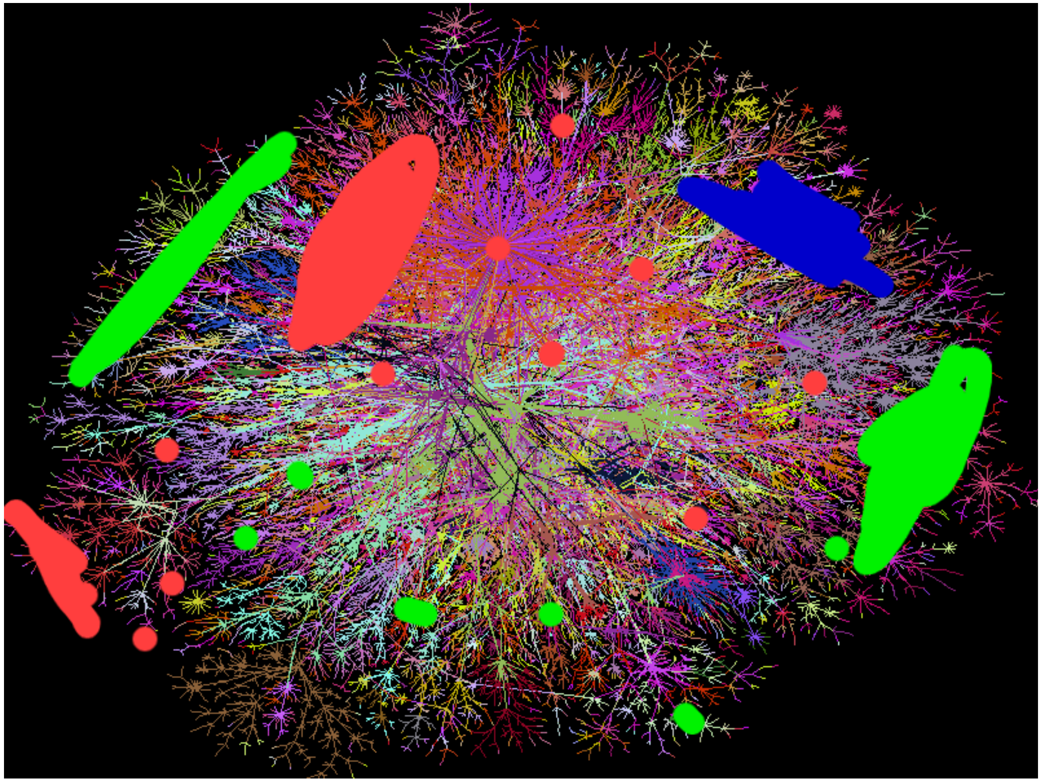
Taking BGP Filtering to next Level

- ✓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
- ✓IBGP routes would overlay blackhole routes on your network in addition to other routes propogated by your IGP such as OSPF

BGP Granular Filtering

- ✓One could use communities to differentiate between different kinds of threats
- ✓Green- Virus Infected machines community 65500:999
- ✓Blue- Spammers community 65500:666
- ✓Red- Port Scanners / bots 65500:112





BGP Filtering – protection vs censorship

- ✓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
- ✓Censorship –Implementing at ISP level
- ✓Protection – allowing a consumer or a business to opt into the protection model

Making Router OS even More Secure

Shakespeare on Perfection

Those who Strive for Perfection soon Find it is a moving Target

Kernel Hardening Parameters (Proxies) non Routers

- ✓Allow users to set the following parameters on Router OS Devices that are not Gateway devices (NSA/ CIS)
  - Usermanager
  - Proxy
  - NTP
  - DNS Servers
- ✓net.ipv4.ip forward = 0
  - Disable the ability of the router to route packets from one interface to another based on IP
- ✓net.ipv4.conf.all.send redirects = 0
- ✓net.ipv4.conf.default.send redirects = 0

Kernel Hardening for All Routers

- Allow to harden Router to NSA / CIS Standards
- net.ipv4.conf.all.accept_source_route = 0
- net.ipv4.conf.all.accept_redirects = 0
- net.ipv4.conf.all.secure_redirects = 0
- net.ipv4.conf.all.log_martians = 1
- net.ipv4.conf.default.accept_source_route = 0
- net.ipv4.conf.default.accept_redirects = 0
- net.ipv4.conf.default.secure_redirects = 0

Kernel Hardening all routers

- ✓net.ipv4.icmp_echo_ignore_broadcasts = 1
- ✓net.ipv4.icmp_ignore_bogus_error_messages = 1
- ✓net.ipv4.tcp_syncookies = 1
- ✓net.ipv4.conf.all.rp_filter = 1
- ✓net.ipv4.conf.default.rp_filter = 1

Default Drop Firewall Checkbox

- ✓Option to have firewall load initially with all traffic drop until rules are fully loaded

Configurable SSL Parameters

- ✓Supported Ciphers should be configurable
- ✓NSA/ CIS Standards... Ciphers >>128bits
- ✓Supported Cipher bit Length should be configurable
- ✓Client Side Authentication should be supported

Use SSL for Winbox

- ✓Use SSL so that a user is automatically warned if the SSL certificate on the server is in valid
- ✓Client automatically informed if encryption on the session is not enabled or at a required level
- ✓Use SSL to enforce Client Side Certification phase in with winboxs or swinbox (running in parallel)
- ✓In windows 7 / Windows Server 2008 RDP encryption was supplemented with TLS / SSL encryption.

Password Protected KeyRing in Winbox Loader

- ✔Passwords stored on the computer should be encrypted with a username and password using AES-256 or better encryption
- ✔

SAPI / APIS

- ✓Secure API Traffic with SSL
- ✓Client and server Authenticated

Disable insecure services by default

- ✓API
- ✓Winbox
- ✓Telnet
- ✓Ftp
- ✓Bandwidth Test Server

Buffer Overflow protection

- ✓kernel.exec-shield = 1
- ✓kernel.randomize_va_space = 1
- ✓As Mikrotiks Popularity grows so too will desire for people to attempt compromising MikroTik Router OS
- ✓Fuzzing etc

Stunnel Feature

- ✓SSL Wrapper for generic TCP Services running on servers etc
- ✓SSL Accelerator Reverse Proxy etc
- ✓Turn a standard imap server into an Imaps server
- ✓Allow a CCR 1036 to terminate SSL for webservers behind it
- ✓CCR1036 RB1000, RB1100AH & Rb1200 all have Hardware acceleration for SSL
- ✓X86 have SSE Extensions for increased SSL Performance

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.