

Router Security, Just Add Peers!

or, No one likes to say “ouch” at 3 AM!

Rob Thomas robt@cymru.com

6 November 2003

Thrill as Rob Babbles About...

- The security problem.
- The template approach.
- Resources.

The Security Problem

“I try to say ‘Internet Security’ with a straight face!”

- Internet Security is all about the other guy.
 - 1.2Gbps from 1.3.3.7
- “heh ill trade 4 ccs for 1 cisco”
 - 17683 and 31920 in 2002.
- “Oh, please, they’re not smart enough to do that.”

The Security Problem

BGP as collateral damage

- bang.c and friends.
 - Attacks from TCP 179
 - 346719
- Attacks on routers.
 - <A> wat did u hit
 - his router
 - if u hit his router and not him
 - he stays down longer

The Security Problem

And in the ether bind them...

- Three things run the Internet:
 - BGP
 - DNS
 - Caffeine

Protect them all!

The Template Approach

One size never fits all!

- First, know your topology and business requirements.
- Second, know how to validate that your topology *exists* and is meeting your business requirements.
- Modify to suit.
- Wash, rinse, repeat.

The Template Approach

Global configuration.

- service timestamps debug datetime msec
show-timezone localtime
- service timestamps log datetime msec
show-timezone localtime
 - Timestamp all log entries.
 - Don't forget to configure NTP!

The Template Approach

Global configuration.

- service password-encryption
 - Clear text passwords are always a bad idea.
- enable-secret <BLAH>
- No enable password
 - Use the more robust MD5 encrypted enable password.
- If you can use TACACS+ or RADIUS, all the better!

The Template Approach

Global configuration.

- username <USER> password 5 <PASSWORD>
 - Use MD5 for login accounts.
- no ip http server
- no ip http server-secure
 - Routers are *NOT* web servers!
 - Commonly abused by the miscreants.

The Template Approach

Global configuration.

- no ip source-route
 - Don't let just anyone map your network.
- no ip finger
- no ip bootp server
- no cdp run
 - Disable noxious services.

The Template Approach

Interface configuration.

- ip verify unicast reverse-path
 - Is our data path symmetric?
- no ip redirects
- no ip unreachable
- no ip directed-broadcast
- no ip proxy-arp
- no ip mask-reply

The Template Approach

Interface configuration.

- ACLs to protect at least the router, of not the networks.
- ip route-cache flow
 - Export the flows if you can.
 - Use `sh ip cac flo` to view the statistics.
 - No one can lie to the flows. ☺
 - Flows are what your peers and upstreams need to help you block and track DDoS.

Brief Interlude – NetFlow

Packet distribution.

```
router#sh ip cac flo
```

```
IP packet size distribution (7735165 total packets):
```

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.000	.415	.360	.033	.038	.007	.006	.001	.001	.005	.001	.002	.005	.005	.001
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.007	.002	.000	.006	.094	.000	.000	.000	.000	.000	.000				

Brief Interlude – NetFlow

Protocol distribution.

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	1	0.0	1	60	0.0	0.0	15.0
TCP-FTP	44	0.0	2	53	0.0	6.5	15.0
TCP-WWW	460	0.0	1	478	0.0	4.9	5.7
TCP-SMTP	39	0.0	1	339	0.0	11.0	3.8
TCP-BGP	21672	0.0	1	40	0.0	0.0	0.9
TCP-other	22234	0.0	2	50	0.0	6.8	14.9
UDP-DNS	9987	0.0	1	74	0.0	1.6	15.0
UDP-other	1245	0.0	1	190	0.0	0.0	15.0
ICMP	11884	0.0	1	91	0.0	0.0	15.0
Total:	67566	0.0	1	60	0.1	2.5	10.4

Brief Interlude – NetFlow

Flow distribution.

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi0/0	68.22.187.16	Local	68.22.187.7	06	E274	0050	51
Gi0/1	68.22.187.15	Local	216.90.108.3	01	0000	0800	1
Gi0/1	68.22.187.15	Local	216.90.108.1	01	0000	0800	1

The Template Approach

BGP global configuration.

- no bgp fast-external-fallover
 - Tolerance is a virtue.
- bgp log-neighbor-changes
 - Because it's always the other guy's fault! ;)

The Template Approach

BGP neighbor configuration, part one.

- neighbor 1.1.1.1 soft-reconfiguration inbound
 - Do you have memory to burn?
- neighbor 1.1.1.1 description ...
 - NOC numbers.
 - Circuit IDs or interface labels.
 - Documentation hurts, but in a good way.
- neighbor 1.1.1.1 password ...
 - The simple things work, folks.

The Template Approach

BGP neighbor configuration, part two.

- neighbor 1.1.1.1 prefix-list bogons in
 - Don't accept garbage.
 - Don't accept unauthorized prefixes (edge).
- neighbor 1.1.1.1 prefix-list announce out
 - Announce only what has been allocated to you.
 - “Wow, both pipes are full!”

The Template Approach

BGP neighbor configuration, part three.

- neighbor 1.1.1.1 maximum-prefix ...
 - Currently running at about 131K prefixes based on my five peers.
 - Can run this in advisory mode:
 - neighbor 1.1.1.1 maximum-prefix 200000 warning-only

The Template Approach

The BGP config looks like this:

```
neighbor 1.1.1.1 remote-as 222
neighbor 1.1.1.1 description eBGP with ISP222
neighbor 1.1.1.1 soft-reconfiguration inbound
neighbor 1.1.1.1 password bgpwith222
neighbor 1.1.1.1 version 4
neighbor 1.1.1.1 prefix-list bogons in
neighbor 1.1.1.1 prefix-list announce out
neighbor 1.1.1.1 maximum-prefix 200000
```

The Template Approach

Filtering with prefix-lists.

- At a minimum, inbound filtering should be configured to block all of the obvious bogons, e.g. RFC1918 netblocks, IANA Reserved, and special use.
- I filter all unallocated and bogon netblocks.
Change log:
 - June 2001, October 2001, December 2001.
- If you are at the edge, announce only what you have been allocated! Be wary of providers that accept anything.

The Template Approach

Filtering BGP.

- Only your peers should be able to reach TCP 179. Remember bang.c!
- “I had to set them straight, ayup.”

```
access-list 185 permit tcp host 1.1.1.1 host 1.1.1.2 eq bgp
access-list 185 permit tcp host 1.1.1.1 eq bgp host 1.1.1.2
access-list 185 deny tcp any any eq bgp log-input
```

Resources

- **RANCID (Really Awesome New Cisco confIg Differ)**
 - <http://www.shrubbery.net/rancid/>
- **RAT (Router Audit Tool)**
 - http://www.cisecurity.org/bench_cisco.html

Resources

- “Cisco ISP Essentials,” Cisco Systems,
 - <http://www.cisco.com/public/cons/isp/essentials/>
- NANOG
 - <http://www.nanog.org>
- Philip Smith’s Routing Table Report
 - bgp-stats-request@lists.apnic.net

Resources

(and shameless self promotion)

- <http://www.cymru.com/Documents/>
 - [secure-ios-template.html](#)
 - [secure-bgp-template.html](#)
- <http://www.cymru.com/Bogons/>
- <http://www.cymru.com/BGP/>
- <http://www.cymru.com/DNS/>

*IOS and BGP templates have been ported to Juniper
by Steve Gill, also of Team Cymru.*

Resources

- *You and the persons next to you!*
- I'm always questing for ideas and feedback. Be the first in your ASN to join my Credits section. 😊

Thank you for your time!