Effective and TIMELY Bogon Filtering

Dave Deitrich

Team Cymru Inc.
team-cymru@cymru.com

ARIN XVII - 09 April 2006

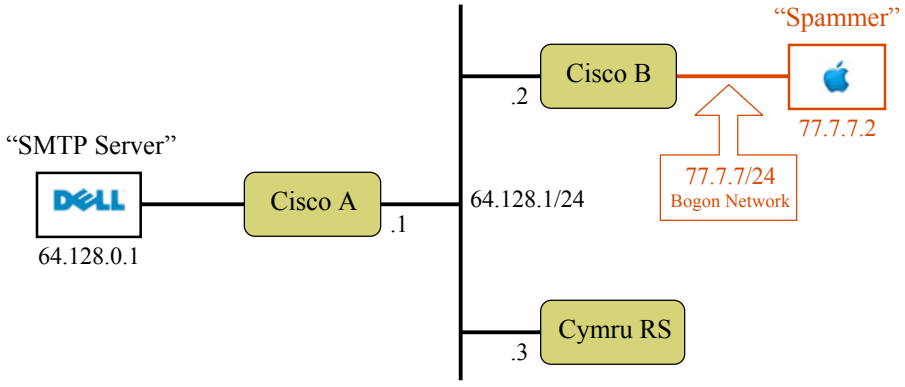
What's a Bogon?

- A BOGON is a prefix that should never appear in the Internet routing table
  - Occasionally used as sources for Spam and DDoS attacks
- Filtering bogons can sometimes be helpful
- **Problem**: bogon filters must occasionally be updated

Automated Bogon Filtering

- Can use BGP to filter bogons on routers
  - Team Cymru runs Bogon Route Servers
  - Can also set up your own Bogon RS
- "Remote Triggered Black Hole Filtering"
  - Can also be used to blackhole problem IP addresses and netblocks
  - Useful for DDoS response
  - Works on Cisco, Juniper, others…

Demonstration Setup



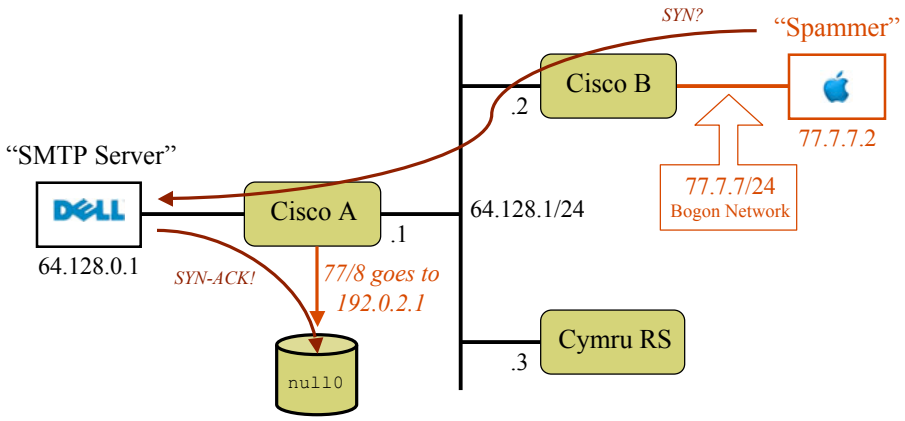
Peering with the Bogon RS

- Cisco A peers with Cymru RS
  - Define route for 192.0.2.1 pointed to **null0**
  - Use a route map to set next hop for all bogon routes to **192.0.2.1**
- **Result**: All routes learned from route server are **blackholed**

Peering with the Bogon RS

```
ip bgp-community new-format
!
ip route 192.0.2.1 255.255.255.255 null0
!
ip community-list 10 permit 65333:888
!
route-map CYMRUBOGONS permit 10
  match community 10
  set ip next-hop 192.0.2.1
```

What's Really Happening?



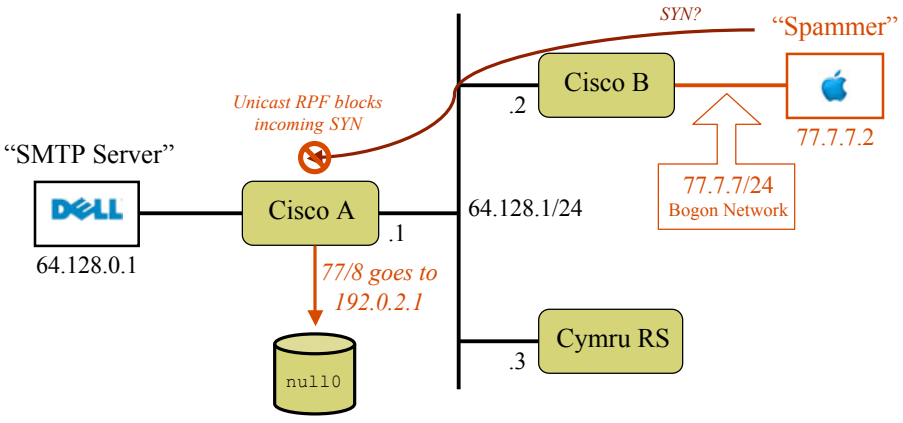
Unicast Reverse Path Forwarding

- Unicast RPF is a feature that protects against forged IP addresses
  - Compares ingress interface against routes in forwarding information base (FIB)
  - If doesn't match best path, packet is dropped
- Because of the BGP route map, best path for bogon netblocks is from **null0**

Unicast Reverse Path Forwarding

```
interface Ethernet1
 ip address 64.128.1.1 255.255.255.0
 ip verify unicast reverse-path 155
 no ip redirects
 no ip proxy-arp
 no cdp enable
!
access-list 155 deny tcp any any log-input
```


Unicast Reverse Path Forwarding



Bogon Updates

- When networks become non-bogon we immediately stop advertising them
  - Route to **null0** for bogon goes away
  - Unicast RPF stops blocking incoming traffic
- *Best of all, no changes or updates are needed on Cisco A!*

Internal Route Filtering

```
router bgp 64700
 neighbor 64.128.1.3 remote-as 65333
 neighbor 64.128.1.3 route-map cymru in
!
ip prefix-list except seq 5 deny 10/8 ge 32
ip prefix-list except seq 99 permit 0/0 ge 8
!
route-map cymru permit 10
 match ip address prefix-list except
 set ip next-hop 192.0.2.1
```

Caveats

- More specific routes take precedence
  - Limit incoming prefixes to minimum allocation size or larger
- BGP failures cause open policy
  - Can peer with multiple route servers
- uRPF requires careful network planning

Other Sources for Bogon Info

- Bogon lists are also available as:
  - Text lists (aggregated & unaggregated)
  - BIND Templates
  - Prefix lists (Juniper and Cisco)
  - RADB, RIPE NCC, DNS
  - Mailing list for changes

http://www.cymru.com/Bogons/index.html

Useful Links

ftp://ftp-eng.cisco.com/cons/isp/security/
- Remote-Triggered-Black-Hole-Filtering-02.pdf
- URPF-ISP.pdf
- Ingress-Prefix-Filter-Templates

Barry Greene, Philip Smith, *Cisco ISP Essentials*, 2002, Cisco Press; ISBN 1587050412

http://www.cymru.com/BGP/bogon-rs.html

THANK YOU!

If you have any comments or questions please feel free to contact us at:

team-cymru@cymru.com

http://www.cymru.com