Making your Campus Network Safe for Google IPv6 Whitelisting

David Farmer
University of Minnesota
Lighting Talk - ESCC/Internet2 Joint Techs
Columbus, Ohio
July 14th 2010

Google IPv6 Whitelisting

- Google controls which networks it will send DNS AAAA(IPv6) records to
- Why
  - Many networks have poor IPv6 connectivity
  - Performance issues with IPv6 transition technologies (especially 6to4)
  - Black holes created by networks filtering IP protocol 41 (6to4)

Campus Networks

- IPv6 Connectivity
  - We can easily get good Native IPv6 connectivity
  - Just turn it on with your GigaPOP and/or Internet2
- Transition Technology Issues
  - Need to ensure hosts are using Native IPv6
  - Need to prevent host from “helping“ each other by mitigating or preventing Rouge RAs
  - Don’t block IP Protocol 41

How to Ensure Native IPv6

- Disable Transition Technologies in Host Stack
  - Pro: No changes to Network Config
  - Pro: Can be deployed by AD or other Host configuration tools
  - Con: Requires Changes to all Hosts
  - Con: Prevents mobile Host from using Transition Technologies else where they might be useful
- Ensure only Native RAs (Router Advertisements) are used on your Network

How to Ensure Native IPv6 RAs

- Use RA-Guard Technology
  - Pro: No changes to Hosts
  - Pro: Eliminates Rouge RAs
  - Con: Not readily available at this time

- Please pressure you vendors to support RA Gaurd

How to Ensure Native IPv6 RAs

- Filter ICMPv6 Type 133 (Router Advertisement) at edge access ports
  - Pro: No changes to Hosts
  - Pro: Eliminates Rouge RAs
  - Con: Few edge switches support IPv6 ACLs

- Please pressure you vendors to support IPv6 ACLs

How to Ensure Native IPv6 RAs

- Advertise your RAs at High Priority
  - Pro: No changes to Hosts
  - Pro: No changes to Edge Switches
  - Con: Rouge RA still visible to Hosts
  - Con: Does not prevent malicious RAs

But I'm not Doing IPv6 yet

- **We'll your Wrong!!!!**
  - 6to4 is turned on by default on many OSes
  - Large numbers of clients and servers are probably doing IPv6
  - Go look at the logs on your AD servers
- **BUT DON'T FILTER** IP Protocol 41
  - In the long run you will only make IPv6 and your Network less reliable

Blocking 6to4

- Don’t block Protocol 41 in IPv4
- Administratively deny packets in the IPv6 domain
  - Return ICMPv6 Type 1 Code 1 (administratively prohibited) in 6to4
- Problem: I’m not aware of Router ACL or Firewall that can do this

Disable IPv6

- Worst case
  - But it's better than Black Holes
- Filter EtherType 86DD Packets
  - Pro: No IPv6 support necessary on Equipment
  - Pro: Eliminates Rouge RAs
  - Pro: Allows IPv6 to be safely enabled on Host
  - Con: Completely disables IPv6

Disable IPv6

- Filter IPv6 Global Unicast at the Router
  - Enable IPv6 on router
  - Advertise High Priority RA
  - Allow Link Local traffic only
  - Filter all other traffic
  - Pro: Allows IPv6 to be safely enabled on Host
  - Con: Rouge RA still visible to Hosts
  - Con: Essentially disables IPv6

What is U of MN doing?

- Just finished year long test of IPv6 on Wireless
  - Enabled dual stack on separate 802.1x SSID
  - Allowed for user controlled testing of IPv6 over the entire campus
  - Over 5000 unique users in final 6 month
  - Moving to production will be disabled by fall

What is U of MN doing?

- Wired
  - Filtering ICMPv6 Type 133 on all access ports
  - Enabling IPv6 on VLANs upon request with High Priority RA
- 802.1x Wireless
  - Enabling IPv6 with High Priority RA

What is U of MN doing?

- Web Portal Wireless
  - Web portal only supports IPv4
  - Filtering EtherType 86DD to disable IPv6
- Something we tried
  - Filtering EtherType 86DD until Authenticated
  - Didn't work because of Periodic RAs couldn't be blocked

What is U of MN doing?

- A New Option
  - The web portal proxies DNS until Authenticated
  - Point web portal at a BIND 9.7 DNS server with "filter-aaaa-on-v4" option turned on
  - Will filter AAAA Records until Authenticated
  - Also filter EtherType 86DD until Authenticated
  - Forces Authentication via IPv4
  - Allows IPv6 after Authentication

See Me for any Questions

David Farmer
University of Minnesota
farmer@umn.edu