Admin Tools for Blackhole Administration

Ingvar Mattsson

RIPE 61 — May 2nd – 6th, 2011

Outline

Blackholing Is Tedious

- Blackholing involves configuring static routes
- Router configurations have poor-to-no support for comments
- This sums up to an administrative burden

Blackholing is useful

- Blackholing uses routes, not ACLs
- Routing is relatively cheap
- With SYN cookies, there's no server overhead

So, What Do We Need?

- We want to track:
  - Reason for blackholing
  - When we blackholed
  - Who decided it was needed
  - When the blackhole should be removed
- We also want a web interface
- And a command-line interface

Outline

Blackhole Administration Tool

To facilitate this, I decided to write a proof-of-concept implementation of a system that has the properties we want.

It uses an SQL database for state information and operator information (essentially just a username and a password). It has both a command-line and a web-based interface.

It also has a "reaper" that should be run periodically, to clean up existing blackhole routes that have aged to the point they should be deleted.

Intended architecture

- One machine with the web front-end
- One machine with the database (possibly the same as the web server)
- One ruter dedicated as the blackhole router, injecting routes via BGP.

One of the reasons for a separate router is to allow for the possibility of having a statically configured admin password, so as to separate admin privileges on the blackhole router from admin privileges in the rest of the network.

Tagging

To allow for various administrative and functional separation of blackholed routes, the Blackhole Administration Tool has the concept of tagging. This is simply a number, that will need supporting cnfiguration on the router(s) in the network.

The example code contains configuration for three scenarios, simply blackholing traffic, forwarding the packets to the blackhole router and forwarding to a dedicated packet capturing machine.

Tagging, continued

cont'd.

It would also be possible to allow for blocking using RPF (ideally relaxed RPF), propagating blackhole information to BGP peers or other route manipulation, as long as the router architecture allows route-manipulation based on a tag-like criterion.

Back-ends

The tool is written so that multiple different back-ends can be used. Provided with the source code package is a back-end that can communicate with a Cisco router, one that can inject routes locally on a linux box using the `ip route` command and one that is a no-op back-end.

Writing a new back-end should be relatively easy, as all that is needed is to provide one Python function to inject a given prefix with a tag and one function to remove a given prefix.

Outline

The web interface

- The web interface is a single page
- This page is split into:
  - A form for new blackhole routes
  - A table for existing blackholes
- This leads to a single, convenient URL

Operator: download
Password:
Reason: Blackholed
Prefix: / 32
Duration: 1 week Tag: 666 - Blackhole on all routers
Submit

Prefix	Blackholed	Expires	Reason	Tag	Who
172.31.255.252/30	2009-04-06 20:07:30	2010-04-07 01:56:42	Blackholed, larger range	666	ingvar
172.31.255.248/30	2009-04-15 08:11:09	2009-04-22 08:11:09	Blackholed	666	ingvar

The command-line interface

- Common options
  - -u *operator*
  - -c *comment*
  - -l *lifetime*
- Add blackholes
  - blackhole add *prefix . . .*
- Delete blackholes
  - blackhole del *prefix . . .*
- List blackholes
  - blackhole list

Outline

The reaper

The reaper process (reaper.py in the proof-of-concept implementation) is intended to be run fron cron (or similar), on a regular basis. In past production experience, running the reaper a few times per day provides timely enough deletion of blackhole routes. Once in the morning, once roughly mid-day and once in the late afternoon. The exact freequency would depend on how timely routes should be removed, and may require a bit of experimentation

Last slide

- Test implementation and a short article about the admin tool are available at http://src.hexapodia.net/blackhole/
- With proper automation in place, blackholing is a useful tool
- Questions?