RTBH-plus

or more fun with BGP communities

Chris Chaundy

APNIC 36, 29-Aug-2013

RTBH – REMOTE TRIGGERED BLACK HOLE

RTBH was documented in RFC 3882 and expanded on in RFC 5635. Using these as foundations, RTBH can be further enhanced as shown in this presentation:

- Trigger router and customer initiated options
  - Minimum requirements
  - Other possibilities
  - Customer filters and limitations
- RTBH scope of operation
  - Internal
  - General
  - Selective
- Source-based RTBH
  - Limitations and associated risks

nextgen GROUP

TRIGGER ROUTER AND CUSTOMER INITIATED OPTIONS

- This can be a very small router - it just has to be part of your iBGP mesh but it does not need to carry any BGP routes – just the capability to advertise a prefix with minimal routing for connectivity.
- Alternatively, software should be able to be used such as quagga (not tested) or other popular DDoS detection appliances.
- Static customers are dependent on the provider-applied options above, but BGP Customers may initiate destination-based RTBH with restrictions:
  - Limited to prefixes which they are permitted to announce to the provider
  - Recommendation that only host routes (IPv4 /32 or IPv6 /128) be accepted with the RTBH community set to prevent accidents
  - Depending on customer skill level, limit the range of RTBH options
  - Enforce commercial controls over RTBH such as duration, etc.
  - Do NOT give customers access to source-based RTBH

nextgen GROUP

RTBH SCOPE OF OPERATION

Basic RTBH is only deployed within your network but if peers or providers have RTBH capabilities, you can manage the impact of RTBH on the target system(s). Here are some examples:

- You can have one RTBH community for 'internal only' but this may not help you (or the target customer) with the size of attacks that are now common if your links to peers or providers are melting!
- Pick providers who support RTBH and choose a community that not only applies RTBH within your network but at the borders is replaced by the appropriate community for each provider (this is the best 'default' protection scenario).
- Choose and group your providers (or peers) into categories such as 'domestic' and 'international'. Often, the major attack volume is from overseas sources. Have a community which will trigger a selection of RTBH advertisements as above but specify the customer's real next-hop in the announcement instead of the 192.0.2.1 or IPv6 equivalent static route to null (see RFC 6666 ☺).

nextgen GROUP

SOURCE-BASED RTBH

Do NOT give customers access to source-based RTBH. This could be accidentally or maliciously be used against you or other customers!

- Only applies where interfaces have uRPF configured - loose uRPF should be sufficient and is a LOT safer, but check with your router vendor documentation.
- Again, use routing policy to restrict this to host routes.
- Use source-based RTBH for external attack sources and only apply loose uRPF to external interfaces on your border routers (if the source is internal to your network, use a filter or pull the plug).
- You must carry a full Internet routing table on your border routers as the uRPF 'drop when the next-hop is invalid' rule will not work with a default route (again, check with router vendor documentation – I can only speak for the vendor that I have deployed this on).
- Do not advertise the black hole route externally.

nextgen GROUP

RTBH-PLUS

This talk does not prescribe what you must do, so use your imagination to work with what you have available, but also to provide a framework on which to base future decisions. See the RFC's for configurations.

RTBH is cannot be a total DDoS solution but it can provide a cheap and easy approach to managing simple attacks limiting customer impact.

Questions?

nextgen GROUP