Firewall on Demand

Evangelos Spatharas

TF-CSIRT/FIRST Meeting
Las Palmas 26 January 2015
INDEX

● Common network security threats
  ● DDoS – statistics, illustration and ramifications

● DDoS Countermeasures
  ● Traditional - ACLs
  ● Modern BGP Approaches – RTBH/Flowspec

● BGP Flowspec
  ● What it is

● From RFC to FoD
  ● How it works
  ● Security concerns & best practices

● What next

● Q & A
Network Security Threats

- DNS, NTP, SMPT and other amplification attacks..
DDoS – High level network view

- DDoS attack launched from compromised systems (bots)
- DDoS attack traffic consumes network capacity
- DDoS attack targets applications and services
DDoS – Ramifications

- **Network**
  - Performance degradation
  - Services malfunction
  - Outages
- **Staff & Company**
  - Productivity reduction
  - Wasted resources
  - Reputation
  - Profit reduction
- **Clients**
  - Dissatisfaction
  - Change upstream?
DDoS - Countermeasures

- ACLs (2004)
  - Doesn’t scale
  - Time consuming
  - Granular
  - Less coarse

- RTBH

- BGP Flowspec (2009)
  - Scalable
  - Fast implementation
  - No granularity
  - Too much coarse
  - Scalable
  - Fast implementation
  - Granular
  - Less coarse
ACL vs RTBH vs Flowspec

<table>
<thead>
<tr>
<th>Method</th>
<th>ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency</td>
<td>High</td>
</tr>
<tr>
<td>Steps</td>
<td>Many</td>
</tr>
<tr>
<td>Legitimate Traffic</td>
<td>Flow</td>
</tr>
<tr>
<td>Attacking Traffic</td>
<td>Block</td>
</tr>
<tr>
<td>Time</td>
<td>Plenty</td>
</tr>
</tbody>
</table>

DDoS attack launched from compromised systems (bots)

DDoS attack traffic consumes network capacity

DDoS attack targets applications and services

Legitimate traffic

Attack traffic
ACL vs RTBH vs Flowspec

<table>
<thead>
<tr>
<th>Method</th>
<th>ACL</th>
<th>RTBH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency</td>
<td>High</td>
<td>Poor</td>
</tr>
<tr>
<td>Steps</td>
<td>Many</td>
<td>3</td>
</tr>
<tr>
<td>Legitimate Traffic</td>
<td>Flow</td>
<td>Block</td>
</tr>
<tr>
<td>Attacking Traffic</td>
<td>Block</td>
<td>Block</td>
</tr>
<tr>
<td>Time</td>
<td>Plenty</td>
<td>No</td>
</tr>
</tbody>
</table>

- **DDoS attack launched from compromised systems (bots)**
- **DDoS attack traffic consumes network capacity**
- **DDoS attack targets applications and services**
- **UPSTREAM**
- **IX**
- **Victim**
- **NREN**

**Legend**
- Green: *Legitimate traffic*
- Red: *Attack traffic*
ACL vs RTBH vs Flowspec

<table>
<thead>
<tr>
<th>Method</th>
<th>ACL</th>
<th>RTBH</th>
<th>Flowspec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency</td>
<td>High</td>
<td>Poor</td>
<td>High</td>
</tr>
<tr>
<td>Steps</td>
<td>Many</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Legitimate Traffic</td>
<td>Flow</td>
<td>Block</td>
<td>Flow</td>
</tr>
<tr>
<td>Attacking Traffic</td>
<td>Block</td>
<td>Block</td>
<td>Block</td>
</tr>
<tr>
<td>Time</td>
<td>Plenty</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

DDoS attack launched from compromised systems (bots)
DDoS attack traffic consumes network capacity
DDoS attack targets applications and services

Legitimate traffic
Attack traffic
BGP Flowspec

- RFC 5575
- Layer 3 and 4 filters are distributed via BGP using a dedicated NLRI
- Currently supported by CISCO, Juniper (only IPv4) and others..

**Match**
- Src/dst prefix
- Src/dst port
- ICMP type/code
- Packet size
- TCP/UDP protocols
- TCP flags
- Others

**Actions**
- Discard
- Rate-limit
- Redirect
- Accept
- Others
From RFC to a WEB based tool

• GOOD! Till now all work perfect! …

Not anymore! GRNET has already provided a solution!

fod.geant.net

Developed and designed by

Networking • Services • People | www.geant.org
FoD Web GUI
How does it work behind the scenes

In less than 10 seconds!!!
Security Concerns – A hypothetical scenario

DDoS attack launched from compromised systems (bots)

Possible mitigation with RTBH, ACL

!! Security Tool == Hacking tool !!

Initiate BGP Flowspec announcement

Non-flowspec capable/enabled NREN

Legitimate traffic

Attack traffic

eBGP

iBGP

Web

Netconf

www.geant.org
Security Best Practices

• **Application level**
  ✓ NRENs can only block traffic that destined towards their IP space
  ✓ A user can only filter up to /29 subnet blocks
  ✓ Only explicitly defined NOC admins have access rights to FoD application
  ✓ Flowspec rules are automatically deactivated after one week unless explicitly specified
  ✓ Logging

• **Network level**
  ✓ Before a flow route installed on the table, is checked against subnet length
  ✓ Even an admin user cannot block traffic destined to GEANT routers (via policy)
  ✓ Reachable only from GEANT/NREN IP space
Okay! I want to use it!!!

Status

Currently: Installing/configuring the platform

Next: Running final pilot – February 2015 onwards

In production: Before end of March 2015
Any issues?

- **BGP Flowspec**
  - eBGP flaps on 12.3R6.6 JunOS – currently running 13.2R4-S2 (but haven’t tested eBGP)

- **FoD Application - RHEL**
  - Easier to install on Debian Wheezy
  - Some applications not natively supported – e.g gunicorn & celeryd
I definitely like it!! But I want some more!!

- DDoS attack launched from compromised systems (bots)
- Possible mitigation with RTBH, ACL
- Initiate BGP Flowspec announcement
- Non-flowspec capable/enabled NREN

Colors:
- **Legitimate traffic**
- **Attack traffic**
- **eBGP**
- **iBGP**
- **Web**
- **Netconf/SSH**
The BIG question

Do **YOU** want to keep out the bad guys?
Thank you!

Security@dante.net
Evangelos.Spatharas@dante.net