DDoS Mitigation

Using BGP Flowspec

Justin Ryburn
Senior System Engineer
jryburn@juniper.net
Is DDoS Really an Issue?

“…taking down a site or preventing transactions is only the tip of the iceberg. A DDoS attack can lead to reputational losses or legal claims over undelivered services.”

Kaspersky Lab [1]

Verisign [2]

“Attacks in the 10 Gbps and above category grew by 38% from Q2 … Q3.”

NBC News [3]

“…more than 40 percent estimated DDoS losses at more than $1 million per day.”

Tech Times [4]

“DDoS attack cripples Sony PSN while Microsoft deals with Xbox Live woes”
Blocking DDoS in the “Old” Days

- Ease of implementation and uses well understood constructs
- Requires high degree of co-ordination between customer and provider
- Cumbersome to scale in a large network perimeter
- Mis-configuration possible and expensive
Destination Remotely Triggered Black Hole (D/RTBH)

- RFC 3882 circa 2004
- Requires pre-configuration of discard route on all edge routers
- Victim’s destination address is completely unreachable but attack (and collateral damage) is stopped.
Source Remotely Triggered Black Hole (S/RTBH)

- RFC 5635 circa 2009
- Requires pre-configuration of discard route and uRPF on all edge routers
- Victim’s destination address is still useable
- Only works for single (or small number) source.
BGP Flow Specification

• Specific information about a flow can now be distributed using a BGP NLRI defined in RFC 5575 [5] circa 2009
  • AFI/SAFI = 1/133: Unicast Traffic Filtering Applications
  • AFI/SAFI = 1/134: VPN Traffic Filtering Applications

• Flow routes are automatically validated against unicast routing information or via routing policy framework.
  • Must belong to the longest match unicast prefix.

• Once validated, firewall filter is created based on match and action criteria.
BGP Flow Specification

- BGP Flowspec can include the following information:
  - Type 1 - Destination Prefix
  - Type 2 - Source Prefix
  - Type 3 - IP Protocol
  - Type 4 – Source or Destination Port
  - Type 5 – Destination Port
  - Type 6 - Source Port
  - Type 7 – ICMP Type
  - Type 8 – ICMP Code
  - Type 9 - TCP flags
  - Type 10 - Packet length
  - Type 11 – DSCP
  - Type 12 - Fragment Encoding
BGP Flow Specification

- Actions are defined using BGP Extended Communities:
  - 0x8006 – traffic-rate (set to 0 to drop all traffic)
  - 0x8007 – traffic-action (sampling)
  - 0x8008 – redirect to VRF (route target)
  - 0x8009 – traffic-marking (DSCP value)
Vendor Support

- DDoS Detection Vendors:
  - Arbor Peakflow SP 3.5
  - Juniper DDoS Secure 5.14.2-0

- Router Vendors:
  - Alcatel-Lucent SR OS 9.0R1
  - Juniper JUNOS 7.3
  - Cisco 5.2.0 for ASR and CRS [6]
What Makes BGP Flowspec Better?

• Same granularity as ACLs
  • Based on n-tuple matching
• Same automation as RTBH
  • Much easier to propagate filters to all edge routers in large networks
• Leverages BGP best practices and policy controls
  • Same filtering and best practices used for RTBH can be applied to BGP Flowspec
Inter-domain DDoS Mitigation Using Flowspec

- Allows ISP customer to initiate the filter.
- Requires sane filtering at customer edge.
Edge Router Configuration

|----------------|--------------------|-----------------------------------|

```
router
  autonomous-system 64496
bgp
  group "CUST-FLOWSPEC"
  neighbor 192.0.2.1
    family ipv4 flow-ipv4
    peer-as 64511
    no flowspec-validate
  exit
exit
no shutdown
Exit

router bgp 64496
  ! Initializes the global address family
  address-family ipv4 flowspec
  !
  neighbor 192.0.2.1
    remote-as 64511
    ! Ties it to a neighbor configuration
    address-family ipv4 flowspec

protocols {
  bgp {
    group CUST-FLOWSPEC {
      peer-as 64511;
      neighbor 192.0.2.1 {
        family inet {
          flow;
        }
      }
    }
  }
}
routing-options {
  flow {
    term-order standard;
  }
}
```
Intra-domain DDoS Mitigation Using Flowspec

• Could be initiated by phone call, detection in SP network, or a web portal for the customer.
• Requires co-ordination between customer and provider.
## Edge Router Configuration

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>router</td>
<td>router bgp 64496</td>
<td>protocols {</td>
</tr>
<tr>
<td>autonomous-system 64496</td>
<td>! Initializes the global address family</td>
<td>bgp {</td>
</tr>
<tr>
<td>bgp</td>
<td>address-family ipv4 flowspec</td>
<td>group RR-CLIENT-FLOWSPEC {</td>
</tr>
<tr>
<td></td>
<td>!</td>
<td>type internal;</td>
</tr>
<tr>
<td></td>
<td>neighbor 198.51.100.1</td>
<td>neighbor 198.51.100.1 {</td>
</tr>
<tr>
<td></td>
<td>family ipv4 flow-ipv4</td>
<td>family inet {</td>
</tr>
<tr>
<td></td>
<td>peer-as 64496</td>
<td>flow;</td>
</tr>
<tr>
<td>exit</td>
<td>exit</td>
<td>}</td>
</tr>
<tr>
<td>exit</td>
<td>no shutdown</td>
<td>}</td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>routing-options {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>flow {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>term-order standard;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

**Juniper**

```perl
protocols {
    bgp {
        group RR-CLIENT-FLOWSPEC {
            type internal;
            neighbor 198.51.100.1 {
                family inet {
                    flow;
                }
            }
        }
    }
}
```
## Route Server Configuration

|---------------|-----------|---------|
| router        | router bgp 64496 | protocols {
| autonomous-system 64496 |   ! Initializes the global address family |
| bgp           | address-family ipv4 flowspec |    bgp {
|               | ! |    group RR-CLIENT-FLOWSPEC {
| group "RR-CLIENT-FLOWSPEC" | neighbor 198.51.100.2 |    type internal;
|    neighbor 198.51.100.2 |   remote-as 64496 |    neighbor 198.51.100.2 {
|    family ipv4 flow-ipv4  | ! Ties it to a neighbor configuration |
|    peer-as 64496 | address-family ipv4 flowspec |    family inet {
| exit          | |    flow;
| exit          | |    export FLOWROUTES_OUT;
| exit          | | }
| exit          | exit no shutdown |


Route Server Configuration

### Cisco [7]

```plaintext
class-map type traffic match-all attack_fs
match destination-address ipv4 203.0.113.1/32
match protocol 17
match destination-port 53
end-class-map
!
policy-map type pbr attack_pbr
class_type traffic attack_fs
drop
class class-default
end-policy-map
!
flowspec
address-family ipv4
  service-policy type pbr attack_pbr
exit
```

### Juniper

```plaintext
routing-options {
  flow {
    term-order standard;
    route attack_fs {
      match {
        destination 203.0.113.1/32
        protocol udp;
        destination-port 53;
      }
      then discard;
    }
  }
}
policy-options {
  policy-statement FLOWROUTES_OUT {
    from {
      rib inetflow.0;
    }
    then accept;
  }
}
```
DDoS Mitigation Using Scrubbing Center

- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Allows for mitigating application layer attacks without completing the attack.
Edge Router Configuration

Alcatel-Lucent

```
router
  autonomous-system 64496
  bgp
    group "RR-CLIENT-FLOWSPEC"
    neighbor 198.51.100.1
      family ipv4 flow-ipv4
      peer-as 64496
      exit
      exit
      no shutdown
    exit
    exit
```

Cisco [7]

```
router bgp 64496
  ! Initializes the global address family
  address-family ipv4 flowspec
  !
  neighbor 198.51.100.1
    remote-as 64496
    ! Ties it to a neighbor configuration
    address-family ipv4 flowspec
```

Juniper

```
protocols {
  bgp {
    group RR-CLIENT-FLOWSPEC {
      type internal;
      neighbor 198.51.100.1 {
        family inet {
          flow;
        }
      }
    }
  }
}
routing-options {
  flow {
    term-order standard;
  }
}
```
**Route Server Configuration**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>router</td>
<td>router bgp 64496</td>
<td>protocols {</td>
</tr>
<tr>
<td>autonomous-system 64496</td>
<td>! Initializes the global address family</td>
<td></td>
</tr>
<tr>
<td>bgp</td>
<td>address-family ipv4 flowspec</td>
<td>bgp {</td>
</tr>
<tr>
<td></td>
<td>!</td>
<td></td>
</tr>
<tr>
<td></td>
<td>neighbor 198.51.100.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remote-as 64496</td>
<td></td>
</tr>
<tr>
<td></td>
<td>! Ties it to a neighbor configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address-family ipv4 flowspec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2014 Juniper Networks, Inc.
## Route Server Configuration

<table>
<thead>
<tr>
<th><strong>Cisco [7]</strong></th>
<th><strong>Juniper</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type traffic match-all attack_fs</td>
<td>routing-options {</td>
</tr>
<tr>
<td>match destination-address ipv4 203.0.113.1/32</td>
<td>flow {</td>
</tr>
<tr>
<td>match protocol 17</td>
<td>term-order standard;</td>
</tr>
<tr>
<td>match destination-port 53</td>
<td>route attack_fs {</td>
</tr>
<tr>
<td>end-class-map</td>
<td>match {</td>
</tr>
<tr>
<td>!</td>
<td>destination 203.0.113.1/32</td>
</tr>
<tr>
<td>policy-map type pbr attack_pbr</td>
<td>protocol udp;</td>
</tr>
<tr>
<td>class type traffic attack_fs</td>
<td>destination-port 53;</td>
</tr>
<tr>
<td>redirect nexthop 192.0.2.7</td>
<td>then discard;</td>
</tr>
<tr>
<td>class class-default</td>
<td>}</td>
</tr>
<tr>
<td>end-policy-map</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td>}</td>
</tr>
<tr>
<td>flowspec</td>
<td>}</td>
</tr>
<tr>
<td>address-family ipv4</td>
<td>policy-options {</td>
</tr>
<tr>
<td>service-policy type pbr attack_pbr</td>
<td>policy-statement FLOWROUTES_OUT {</td>
</tr>
<tr>
<td>exit</td>
<td>from {</td>
</tr>
<tr>
<td></td>
<td>rib inetflow.0;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {</td>
</tr>
<tr>
<td></td>
<td>next-hop 192.0.2.7;</td>
</tr>
<tr>
<td></td>
<td>accept;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
## How Do I Know It Is Working?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• show router bgp routes flow-ipv4</td>
<td>• show processes flowspec_mgr location all</td>
<td>• show bgp neighbor &lt;neighbor&gt;</td>
</tr>
<tr>
<td>• show router bgp routes flow-ipv6</td>
<td>• show flowspec summary</td>
<td>• show route table inetflow.0 extensive</td>
</tr>
<tr>
<td>• show filter ip fSpec-0</td>
<td>• show flowspec vrf all</td>
<td>• show firewall filter <strong>flowspec_default_inet</strong></td>
</tr>
<tr>
<td>• show filter ip fSpec-0 associations</td>
<td>• show bgp ipv4 flowspec</td>
<td></td>
</tr>
</tbody>
</table>
Where Are We Going?

• IPv6 Support
  • http://tools.ietf.org/html/draft-ietf-idr-flow-spec-v6-06

• Relaxing Validation

• Redirect to IP Action
State of the Union
Summary of Survey

• Great idea and would love to see it take off but…
• Enterprises and Content Providers are waiting for ISPs to accept their Flowspec routes.
  • Some would even be willing to switch to an ISP that did this.
• ISPs are waiting for vendors to support it.
  • More vendors supporting it
  • Specific features they need for their environment
  • Better scale or stability
References

• [3] NBC News – Internet Speeds are Rising Sharply, But So Are Hack Attacks [http://tinyurl.com/q4u2b7m]
• [6] Cisco - Implementing BGP Flowspec [http://tinyurl.com/mm5w7mo]
Thank You!