servercentral®

DDoS Mitigation Techniques

Ron Winward, ServerCentral

CHI-NOG 03
06/14/14

Consistent Bottlenecks in DDoS Attacks

1. The server that is under attack
2. The firewall in front of the network
3. The internet capacity of the network

In other words, roughly 75% of the time, one of these three things will be the point of failure!

* Source: Radware ERT

Capacity

- This is your easiest way to prepare for volumetric attacks

- Have enough capacity to handle volumetric attacks
  - External capacity (transits)
  - Internal capacity (infrastructure)

- Have diverse capacity to give you options
  - If you are multihomed, you can announce your attack destination prefix out one transit and leave your other customers or services on the other provider(s)

  - If you have only one provider but run BGP over multiple uplinks, consider announcing the attack destination prefixes on only one link
    - Some providers will even accept smaller than /24 in BGP for local traffic engineering

Protect your own infrastructure

- Number your own resources from specific blocks and create policy at your border to protect your own infrastructure
  - You might block certain/all external traffic on link and loopback IPs
  - Ask your provider if they would add policy on the links facing you

- Protect your routers with a solid control plane policy
  - Limit ICMP, SSH, BGP, NTP, etc
    - Limit access but also police replies with CoPP
  - Team Cymru has a great library of examples for different devices:
    - http://www.team-cymru.org/ReadingRoom/Templates/

- If you know that certain hosts will never receive certain traffic, block it

- Don’t forget your v6 policy

Useful Tools

- Equipment
  - Routers that can easily log and manipulate traffic
    - Juniper MX are great at this
  - Appliance-based DDoS solutions
    - Radware, Juniper, Arbor, etc
  - More processing
    - More servers to handle the transactions
      - Cloud is excellent for this
    - LBs to distribute the load
- Monitoring
  - Use a tool to check your hosts for reachability and bandwidth anomalies
    - Nagios, Icinga, LogicMonitor, etc
    - You'll get an alert that something is wrong and you'll be able to react

Useful Tools

- Reporting
  - SNMP graphs to follow the attack or locate the edge port
    - Observium, Graphite, Grafana Cacti, MRTG, etc.
  - Flow data for identifying traffic
    - Exporting flow
    - A tool to interpret flow data
      - Nfdump/Nfsen, SolarWinds, PRTG, etc
- Remote Triggered Black Hole (RTBH)
  - Internal
  - External
  - Customers
- Flowspec?
  - Be careful here

Flow Examples

- Using flow to find the attack

```
Top 10 IP Addr ordered by flows:
Date first seen          Duration Proto           IP Addr    Flows(%)      Packets(%)       Bytes(%)         pps       bps   bpp
2014-06-10 16:58:12.966   359.936 any        10.93.250.92    44913(21.0)  367.9 M(17.9)    15.8 G( 1.8)     1.0 M  351.6 M    43
2014-06-10 16:58:28.611   344.084 any        172.16.14.27     3526( 1.6)   34.4 M( 1.7)    39.0 G( 4.3)   100113  905.6 M  1130
2014-06-10 16:58:15.603   357.095 any       172.24.14.166     3306( 1.5)   27.1 M( 1.3)     8.1 G( 0.9)    75887  181.1 M   298
2014-06-10 16:58:14.689   358.213 any       172.24.14.165     3302( 1.5)   27.1 M( 1.3)     7.6 G( 0.8)    75559  169.8 M   280
2014-06-10 16:58:13.424   359.272 any       10.225.225.66     2720( 1.3)   28.6 M( 1.4)    34.5 G( 3.8)    79691  768.3 M  1205
2014-06-10 17:00:05.339   247.557 any        10.94.98.133     2321( 1.1)   19.1 M( 0.9)   535.4 M( 0.1)    77235   17.3 M    28
2014-06-10 17:00:05.339   247.557 any       192.168.2.160     2321( 1.1)   19.1 M( 0.9)   535.4 M( 0.1)    77235   17.3 M    28
2014-06-10 16:58:13.416   359.282 any       172.24.14.172     2221( 1.0)   18.2 M( 0.9)     3.2 G( 0.4)    50755   71.4 M   175
2014-06-10 16:58:18.407   353.660 any       172.24.14.176     2124( 1.0)   17.4 M( 0.8)     3.0 G( 0.3)    49199   66.9 M   169
2014-06-10 16:58:13.417   359.516 any       172.24.14.192     2039( 1.0)   16.7 M( 0.8)     2.8 G( 0.3)    46483   63.3 M   170
```

- Using flow to fingerprint the attack

```
ip 10.93.250.92
Date first seen          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Packets    Bytes Flows
2014-06-10 16:58:51.846     0.000 UDP     71.107.169.232:33988 ->    10.93.250.92:53745      8192   352256     1
2014-06-10 16:58:27.735     0.000 UDP      71.80.193.232:32143 ->    10.93.250.92:46669      8192   352256     1
2014-06-10 16:58:41.964     0.000 UDP      71.24.200.232:24262 ->    10.93.250.92:38805      8192   352256     1
2014-06-10 16:58:32.800     0.000 UDP      71.53.219.232:53818 ->    10.93.250.92:21926      8192   352256     1
2014-06-10 16:58:52.652     0.000 UDP      71.11.225.232:3065  ->    10.93.250.92:32039      8192   352256     1
2014-06-10 16:58:57.901     0.000 UDP      71.25.225.232:8765  ->    10.93.250.92:48502      8192   352256     1
2014-06-10 16:58:47.847     0.000 UDP      71.11.232.232:36804 ->    10.93.250.92:45259      8192   352256     1
2014-06-10 16:59:00.664     0.000 UDP      71.39.234.232:23596 ->    10.93.250.92:53102      8192   352256     1
2014-06-10 16:58:28.426     0.000 UDP      71.246.15.233:18361 ->    10.93.250.92:57943      8192   352256     1
2014-06-10 16:58:26.195     0.000 UDP      71.79.110.232:44910 ->    10.93.250.92:28733      8192   352256     1
2014-06-10 16:58:28.235     0.000 UDP     71.161.111.232:28374 ->    10.93.250.92:57734      8192   352256     1
2014-06-10 16:58:32.419     0.000 UDP     71.136.132.232:2435  ->    10.93.250.92:9878       8192   352256     1
```

RTBH

- Allows you to discard specific routes locally in your network
  - A quick way to drop all traffic no matter where it ingresses
- IBGP internally
- EBGP externally
  - Multihop or over direct link
- You can accept RTBH routes from your customers
- You can pass RTBH routes up to your providers if they support it
- Remember that if you export RTBH routes to your transits and your customer is multihomed, you can cause more issues for them

RTBH

```
user@re0.ar1.ord6> show route 134.147.204.115

inet.0: 496477 destinations, 992257 routes (496473 active, 3 holddown, 12 hidden)
+ = Active Route, - = Last Active, * = Both

134.147.204.115/32 *[BGP/170] 14w1d 01:37:37, localpref 100, from 10.10.10.244
                      AS path: I
                    > to 10.255.255.255 via dsc.0
                    [BGP/170] 14w1d 01:37:34, localpref 100, from 10.10.10.245
                      AS path: I
                    > to 10.255.255.255 via dsc.0

user@re0.ar1.ord6>

user@re0.ar1.ord6> show route receive-protocol bgp 10.10.10.244 134.147.204.115/32 detail

inet.0: 496475 destinations, 992255 routes (496471 active, 3 holddown, 12 hidden)
* 134.147.204.115/32 (2 entries, 1 announced)
     Accepted Multipath
     Nexthop: 10.255.255.255
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  10.10.10.244
     Originator ID: 10.10.20.242
     Communities: 23352:666

user@re0.ar1.ord6>
```

Relationships

- Get to know the people in your professional network
- Ask for help when you need it
- Help your peers when you can

Handling Attacks

Local Filtering

- Log then filter the attack

```
user@re0.ar10.ord6# show | compare
[edit firewall family inet filter CUSTOMER:Customer1:OUT]
+       term TICKET-1234 {
+           from {
+               destination-address {
+                   10.61.200.153/32;
+               }
+               destination-port 80;
+               protocol udp;
+           }
+           then {
+               discard;
+           }
+       }
        term LOG { ... }

[edit]
user@re0.ar10.ord6#
```

Mitigation Services

- CDN/DNS-based providers
  - DNS Redirection
  - Anycast for distribution
  - Your content is distributed globally, so DDoS traffic is directed to the closest content site, lessening the burden of distributed attacks

- Pros
  - Less expensive
  - PoPs are overbuilt specifically to handle DDoS
  - Often easy and user friendly

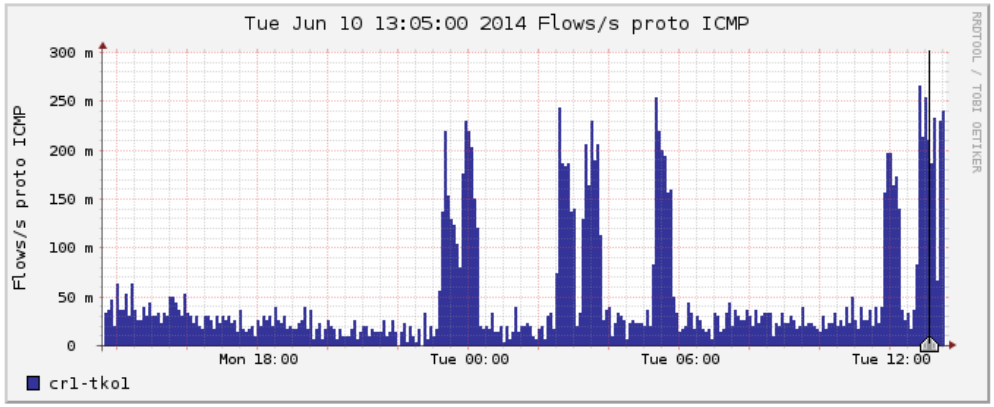
- Cons
  - More for web content
  - Reactive / longer time to setup mitigation
  - Won't protect you in volumetric floods toward your IP addresses or attacks on your other infrastructure

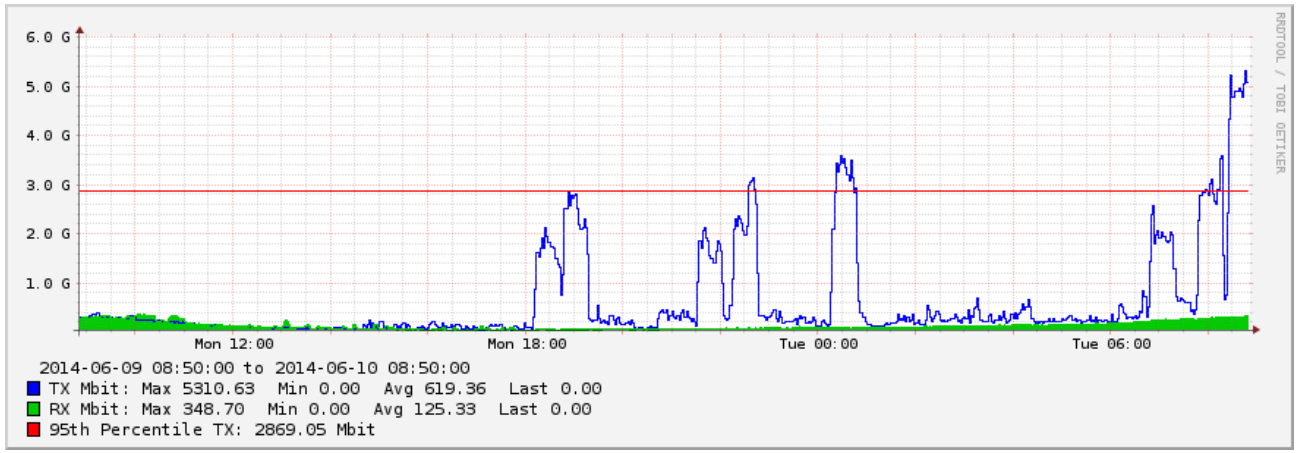
Mitigation Services

- Off-site Scrubbing
  - Your traffic is routed offsite and then clean traffic is returned to you
  - BGP can be used to advertise your prefixes at the LSC
  - GRE or cross connect can be used to send your attack traffic to the provider
  - Clean traffic can then be routed back to you via GRE or cross connect
- Pros
  - Trained security professionals with mitigation experience
  - PoPs are overbuilt specifically to handle DDoS
  - Ability to react to changes in DoS
- Cons
  - Very expensive
  - Reactive / longer time to setup mitigation
  - No detection/baseline capabilities
  - Less effective in multi-vector attacks

Attack Example

- NOC receives an automated alert to a traffic anomaly in Tokyo
- Network engineer checks flow data for anomalous traffic





Attack Example cont.

- Network engineer identifies the attack destination using flow data:

```
Top 500 Dst IP Addr ordered by flows:
Date first seen          Duration Proto       Dst IP Addr    Flows(%)      Packets(%)       Bytes(%)         pps      bps   bpp
2014-06-10 13:03:29.266   358.783 any       10.61.200.153     1441(16.5)    14.0 M(15.6)    19.0 G(30.7)     39066  423.9 M  1356
2014-06-10 13:03:29.267   358.751 any       10.93.150.151      733( 8.4)     7.4 M( 8.2)    477.0 M( 0.8)     20642   10.6 M    64
2014-06-10 13:03:41.300   345.717 any       10.199.82.244      176( 2.0)     1.7 M( 1.9)    193.9 M( 0.3)      4833    4.5 M   116
2014-06-10 13:03:48.274   336.742 any       10.199.82.246      126( 1.4)     1.1 M( 1.2)    134.9 M( 0.2)      3308    3.2 M   121
```

- Network engineer identifies the location of the attack destination:

```
user@re0.cr1.tko1> show route 10.61.200.153

inet.0: 536686 destinations, 1415944 routes (495096 active, 41447 holddown, 468 hidden)
+ = Active Route, - = Last Active, * = Both

10.61.200.0/23     *[BGP/170] 3w5d 15:47:29, MED 50, localpref 300, from 10.57.160.250
                      AS path: 65473 I
                    > to 10.21.29.110 via ae1.71
                    [BGP/170] 3w5d 15:47:26, MED 50, localpref 300, from 10.57.160.247
                      AS path: 65473 I
                    > to 10.21.29.110 via ae1.71

user@re0.cr1.tko1>
```

Attack Example cont.

- Network engineer logs the attack data:

```
user@re0.cr1.tko1# show | compare
[edit interfaces ae1 unit 71 family inet]
+       filter {
+           output DEVICE:Device2:OUT;
+       }
[edit firewall family inet]
      filter DEVICE:Device1:OUT { ... }
+     filter DEVICE:Device2:OUT {
+         term LOG {
+             then {
+                 log;
+                 accept;
+             }
+         }
+         term DEFAULT {
+             then accept;
+         }
+     }

[edit]
user@re0.cr1.tko1#
```

Attack Example cont.

- Network engineer reviews the log to identify the fingerprint:

```
user@re0.cr1.tko1> show firewall log detail | match 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 212.231.210.224, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 24.173.98.212, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 95.79.98.118, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 210.235.79.83, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 212.231.210.224, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 216.81.62.250, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 221.134.88.18, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 72.215.241.181, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 118.163.33.115, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 125.227.113.134, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 103.21.186.4, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 72.34.80.26, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 45, Source address: 105.228.65.80, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 125.213.233.82, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1492, Source address: 109.204.59.249, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 222.43.23.97:161, Destination address: 10.61.200.153:5121
Name of protocol: UDP, Packet Length: 1500, Source address: 183.203.229.66, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 103.21.186.4, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 118.163.73.103, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 118.163.33.115, Destination address: 10.61.200.153
Name of protocol: UDP, Packet Length: 1500, Source address: 118.163.33.115, Destination address: 10.61.200.153
```

Attack Example cont.

- Network engineer blocks the attack:

```
user@re0.cr1.tko1# show | compare
[edit firewall family inet filter DEVICE:Device2:OUT]
+      term Customer1 {
+          from {
+              destination-address {
+                  10.61.200.153/32;
+              }
+              packet-length 1500;
+              protocol udp;
+          }
+          then {
+              discard;
+          }
+      }
       term LOG { ... }

[edit]
user@re0.cr1.tko1#
```

Non-volumetric Attacks

Overview

- As networkers, we're used to volumetric attacks
  - They're most easily identified
  - Can be easy to mitigate

- What happens when we don't or can't see every attack?

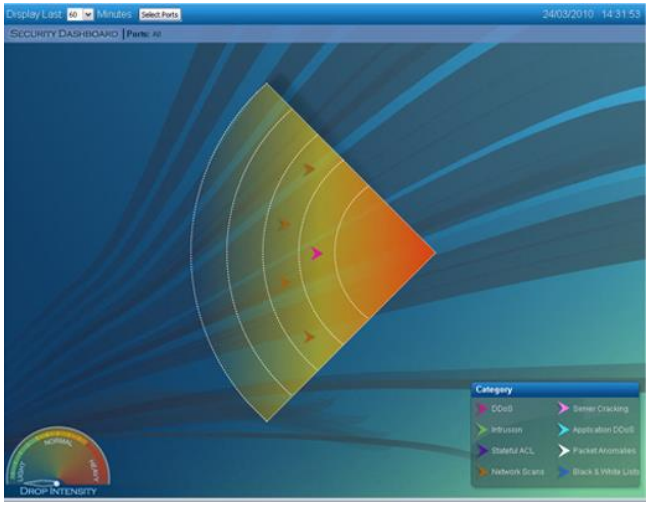
ICMP Floods
TCP Fragment Floods
IGMP Floods
ACK Floods
RFC Violation Attacks
HTTP GET Page Floods
SSL Attacks
Memory Allocation Attacks
Brute Force Attacks
SQL Attacks
TCP SYN Floods
Concurrent Connection Attacks
TCP Out-of-State Floods
DNS Query Floods
SIP Attacks
Session Attacks
TCP SYN-ACK Floods
TCP Stack Resource Attacks
HTTP POST Floods
TCP FIN Floods
TCP Reset Floods

Application Layer Attacks

- These are often the most difficult for network operators to mitigate
- It's usually difficult to distinguish between legitimate and malicious traffic
  - How can you block tcp/80 toward a web server on a router from 10,000 source IPs?
- What happens when it's SSL traffic?

Appliance Based Solutions

- We use Radware DefensePro and DefenseSSL
- Multi-vector attack protection
- Behavioral anomaly detection in both Network and Application layer
- Challenge/Response technology to determine validity of client
- Visibility into encrypted SSL attacks
- Stateful awareness to Low & Slow availability-based threats
- Signature-based Intrusion Prevention System (IPS)
- Detection and mitigation are real time, usually under 20 seconds for mitigation



What's the Best Solution?

- There isn't one single best solution!
- Being prepared is most important
- Have the ability to detect anomalous traffic and then quickly locate it
- Have the ability to filter traffic
- Consider appliance-based solutions
  - Most attacks are not volumetric!
  - You don't know what you don't know
  - You could use a smaller appliance for the layer 7 defense and your traditional tools for volumetric defense
- Stay calm and keep at it

Thank you!

Feel free to contact me at rwinward@servercentral.com.