

Network Defenses to Denial of Service Attacks

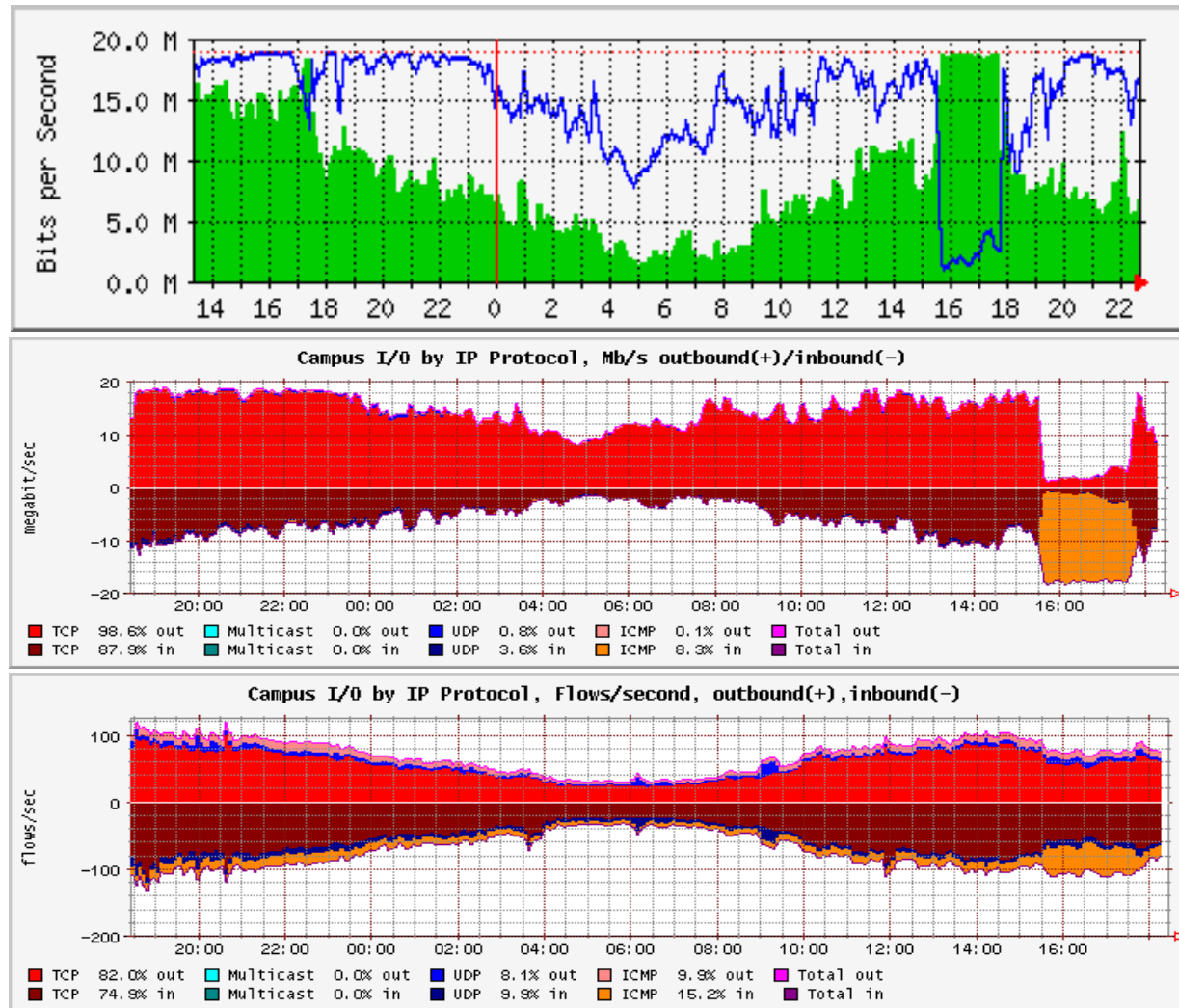
John Kristoff
jtk@depaul.edu
+01 312 362-5878

DoS attack prevention is difficult

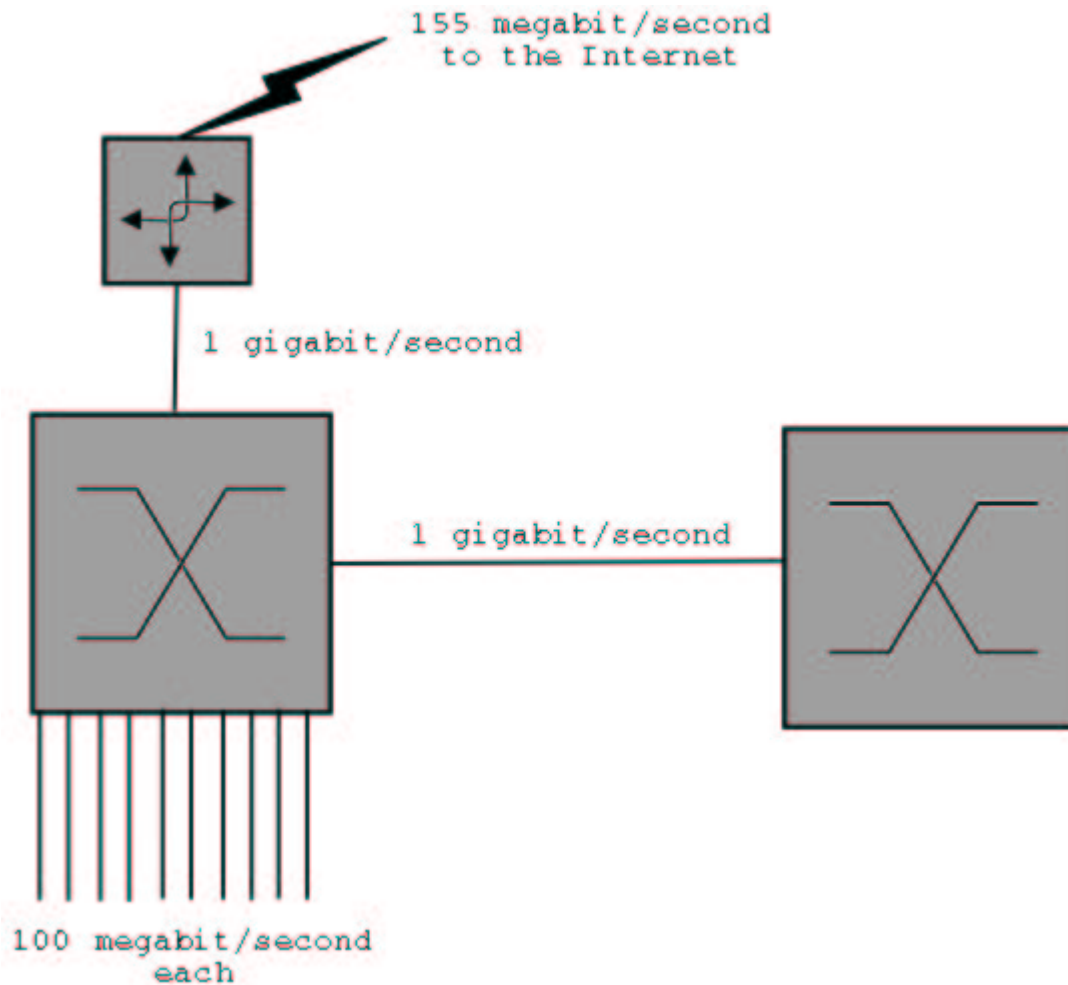
- Applications, hosts and networks are often significantly oversubscribed.
- Internet (data) traffic is naturally bursty on all time scales, thus
- discerning bad traffic from good can be hard.
- There is no one, easy thing to fix that will make the problem go away.

Its been proposed that re-architecting the Internet is a solution, but no one wants to go through that pain.

Visualizing DoS Attack Data



Visualizing Bottlenecks



What are the popular defenses?

- Block bogon, invalid and attack packets.
- Monitor traffic thresholds, patterns and trends.
- Rate limit traffic to help prevent oversubscription.
- Prevent end hosts from becoming DoS agents.
- Black hole victim hosts/networks.
- Maintain good incident response and support staff.

As you might guess, no one defense solves it all.*

In depth look at packet blocking

- Blocking invalid/bogon packets from reaching the net is generally considered a best practice.
- However, it may severely impact forwarding performance and be difficult to manage.
- Blocking on general attack characteristics may also block and break legitimate applications.

Many ISPs mitigated the recent Slammer/Sapphire worm by temporarily blocking UDP port 1434 traffic.

Traceback

- Enabled routers generate or encode trace information to the traced destination.
- Victims can use trace information to discover the real path back to the original source.
- Authentication, deployment and practical issues exist.

Source path isolation engine

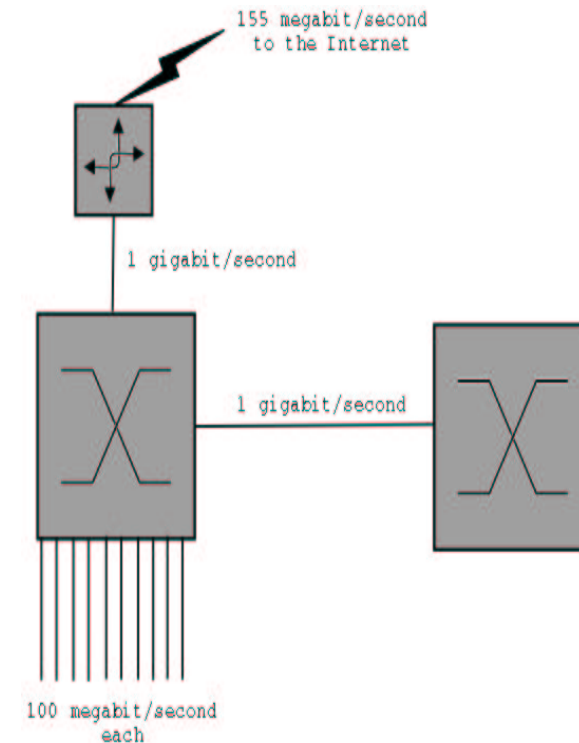
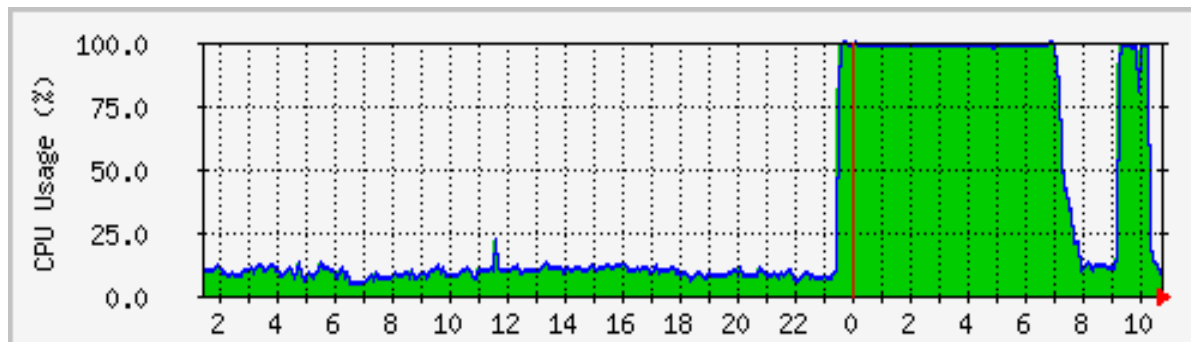
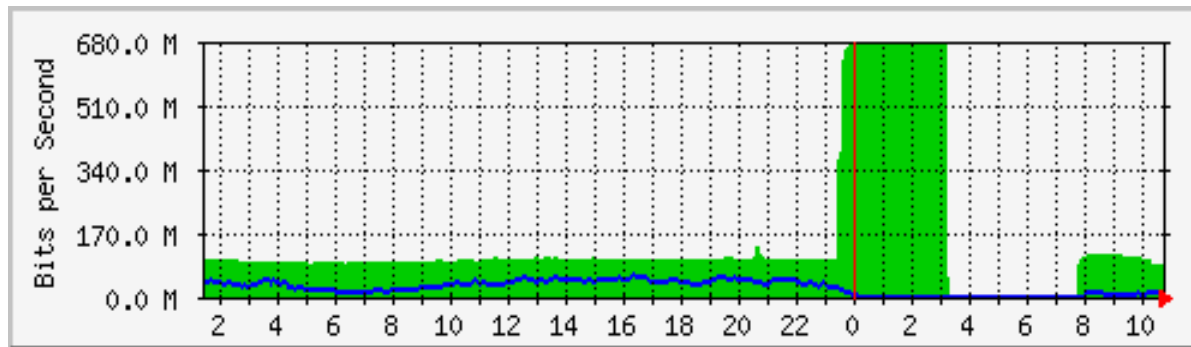
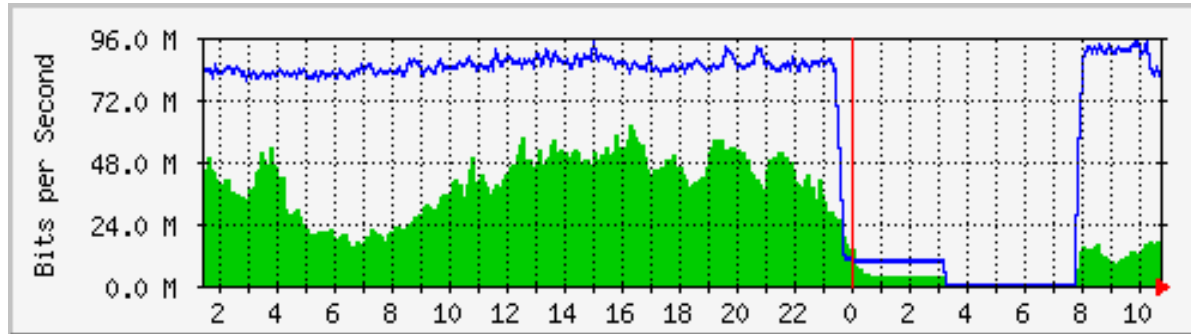
- Routers keep a hash of all packets passing through and send to a collector.
- To trace a packet, query the collector based on packet characteristics.
- SPIE can potentially trace a single packet.
- Significant scaling and deployment issues.

Pushback

- A mechanism to signal downstream routers to aggressively drop/limit attack traffic.
- Routers must detect attack traffic. A similar problem shared by signature based filters.
- If attack traffic is widely distributed, pushback may be ineffective.

IMHO, pushback and related techniques are the most interesting and elegant network-based solutions.

Slammer/Sapphire the DoS attack



Other defenses

- Legal action. Costly (in more ways than one) and problematic when crossing legislative borders.
- Mirror and distribute victims. Costly and management intensive.
- User education? Security Forum 2003!

Thanks! Stop by for a visit at <http://ntg.depaul.edu/rd/>