Approaches for DDoS — an ISP Perspective

barry@null0.net

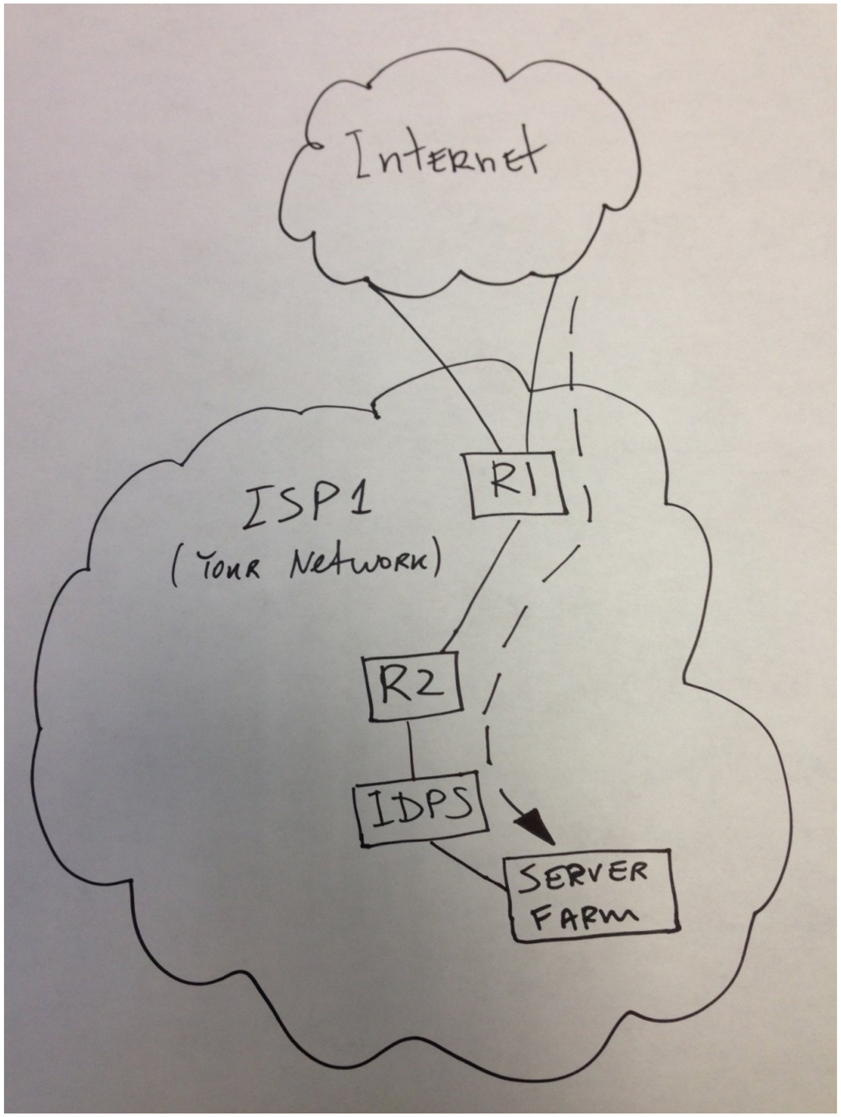
ognian.mitev@viawest.com

Home School

- How everyone starts
- It’s all up to you
- It’s inexpensive (compared to other forms of education)
- Quality may not be the highest attribute here

DDoS Mitigation (Phase IDPS)

- When things are small you can deploy an IDPS
- It is ideal for small attacks
- You can deploy it in-line or at a remote location for shared/occasional needs
- The IDPS box will
  - Identify malicious activity
  - Log information
  - Attempt to block/stop
  - Report



Our Happy Little School

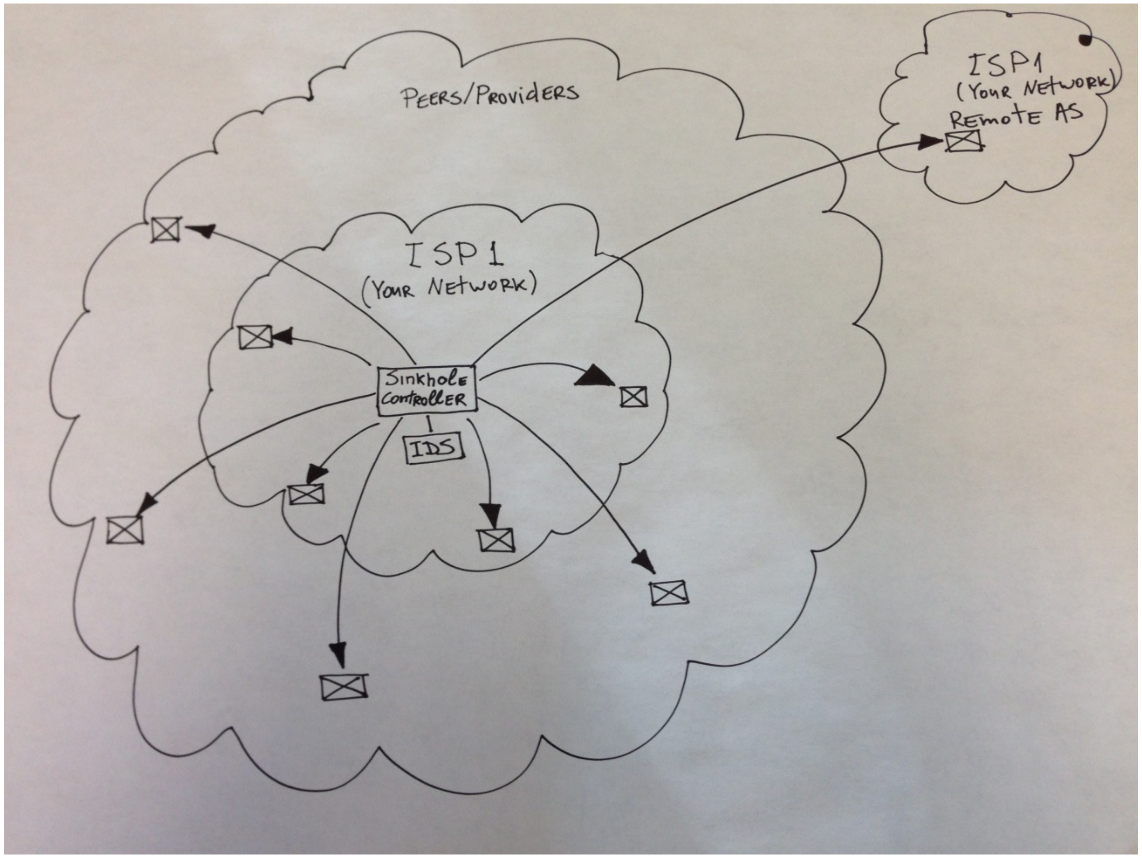
- Single Room School
- Everyone travels far distances back and forth
- Everything is handled locally
- The neighborhood is responsible for curriculum selection (no outside integration)
- It's just large enough to do the job

Disruption of our Neighborhood

- Street Gangs
- Nobody is safe
- They are strain on local resources (systems are disrupted)
- They are organized
- Smaller neighborhoods often require outside help

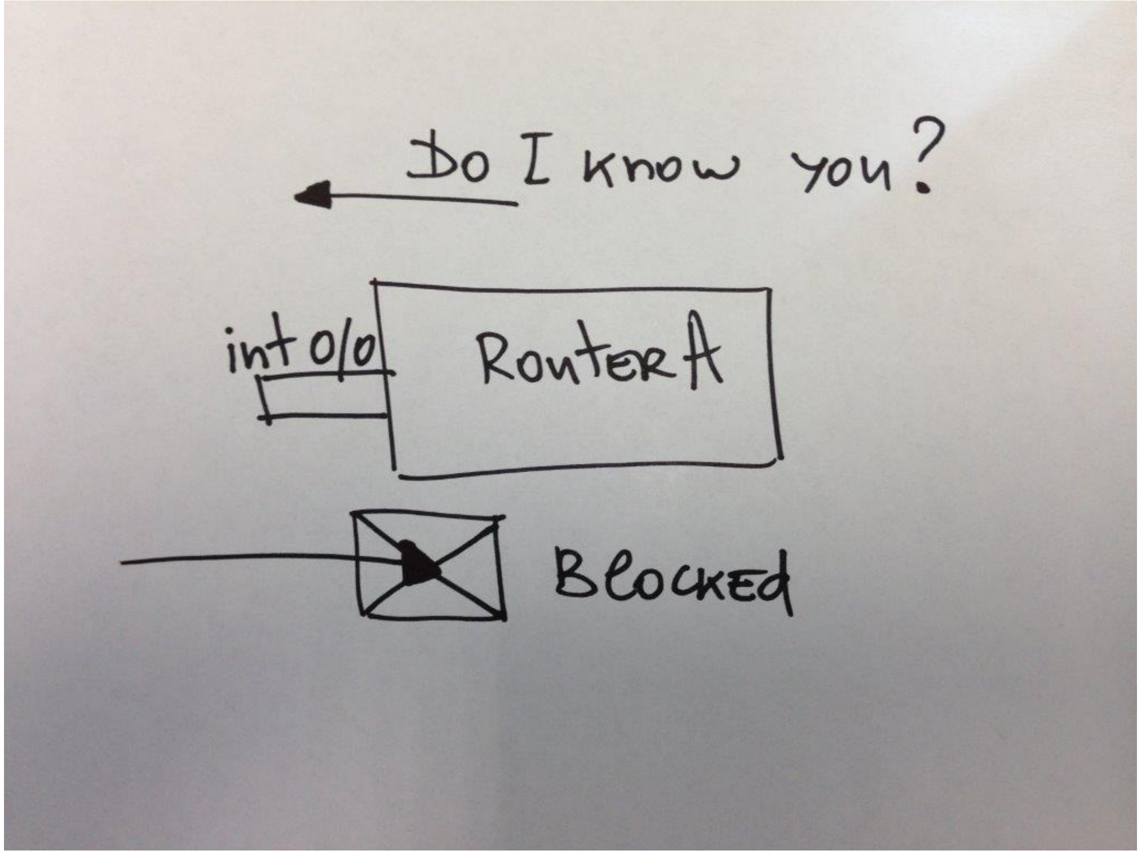
Sinkhole Controller Approach (Phase 1)

- Sinkhole on Destination IP
  - Deploy a sinkhole (trigger) server on your network
  - Establish iBGP sessions with routers inside your network and eBGP sessions with routers outside your network
  - Implement two ways of tagging routes: “internal” and “external”
  - The “internal” tag sets an “internal” BGP community
  - The “external” tag sets an “external” BGP community
  - Add static routes for 192.0.2.1/32 to Null0 to your routers on your network
  - Advertise routes with a next-hop of 192.0.2.1 which creates the mapping to Null0



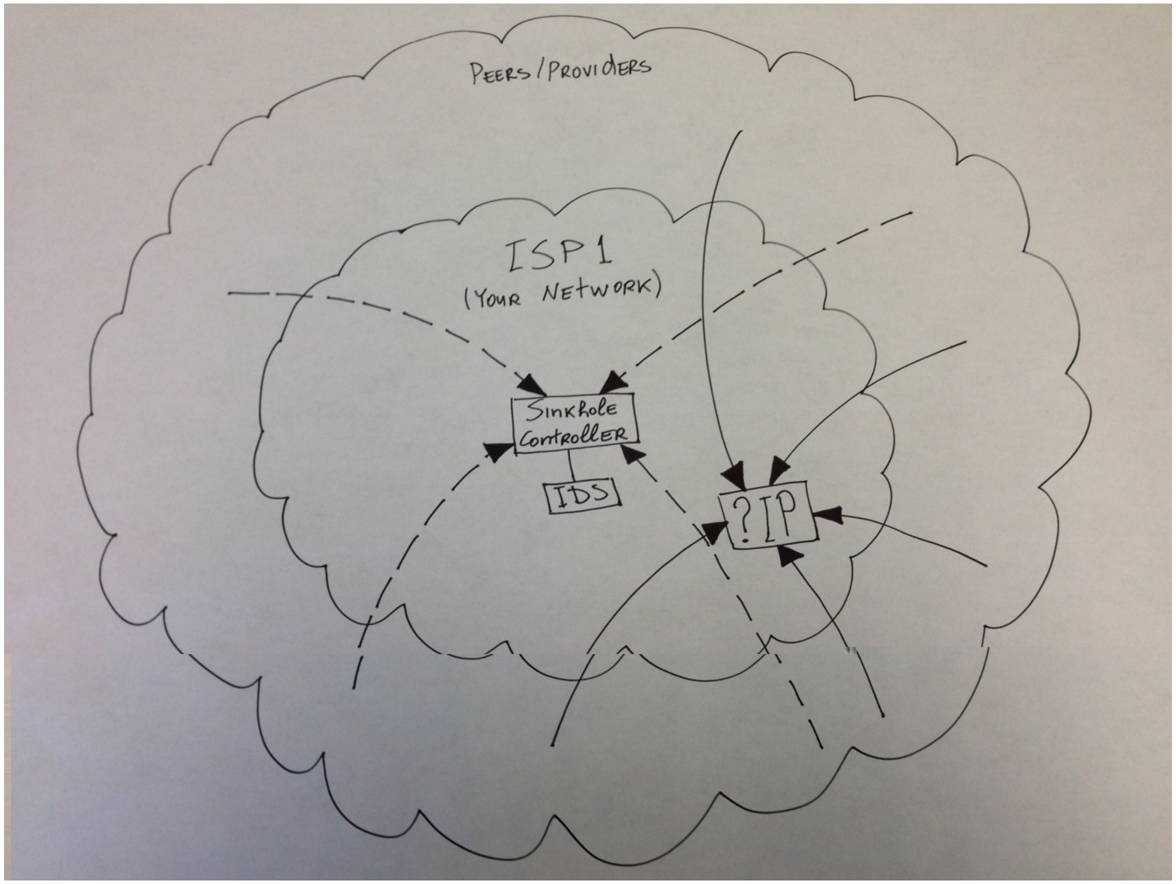
Sinkhole Controller Approach (Phase 1)

- Sinkhole on Source IP
  - Take advantage of Unicast Reverse Path Forwarding (uRPF) available on certain network platforms
  - Implement loose uRPF and add a default route
  - Routers on your network will verify the reachability of the source address of packets being forwarded
  - Your sinkhole server will advertise routes with a next-hop of 192.0.2.1
  - 192.0.2.1 is statically routed to Null0
  - All traffic passing through an interface with the source verification command will be dropped if it can't be forwarded back to the source
  - The traffic from and to the IP address under attack will be dropped



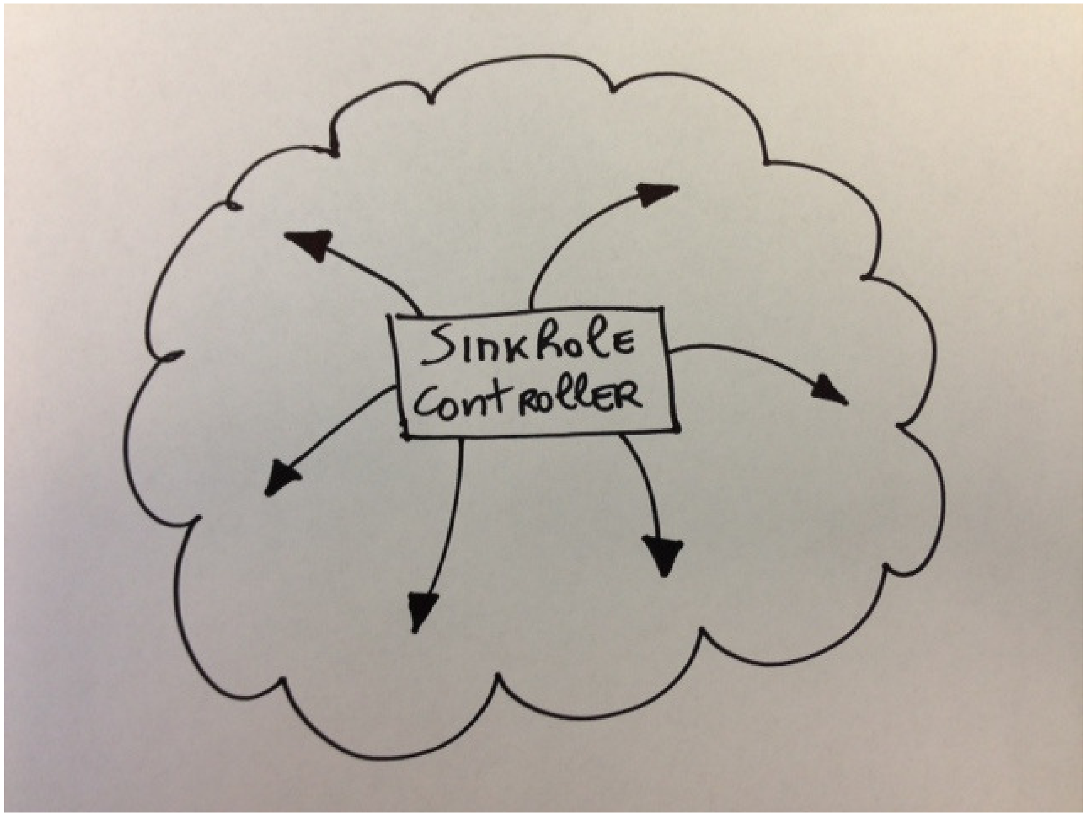
Sinkhole Controller Approach (Phase 1)

- Re-route and capture an attack
    - Announce the IP under attack from your sinkhole environment
    - Review netflow/jflow information on your sinkhole server
    - Look at the traffic with a basic interface ACL (icmp, udp, tcp and ip), just look at which line gets most matches
    - You can use an "IDS" box to capture the attack traffic for additional analysis
    - Create a management web interface to add routes
    - Routes will be automatically removed after a certain period of time



Sinkhole Controller Approach (Phase 1)

- Pros
  - Inexpensive solution to implement (you can start with a router that you are not using, it only takes few hours to configure)
  - Works great for small attacks
- Cons
  - You complete the attack,
  - Slow process (you see a lot of traffic, you start looking at netflow/jflow, you manually add tagged routers on your sinkhole server)
  - Not all peers/providers support blackhole BGP communities
  - Not easy to understand if the attack has stopped especially if you are using the “external” BGP communities
  - Performance issues to the remote AS

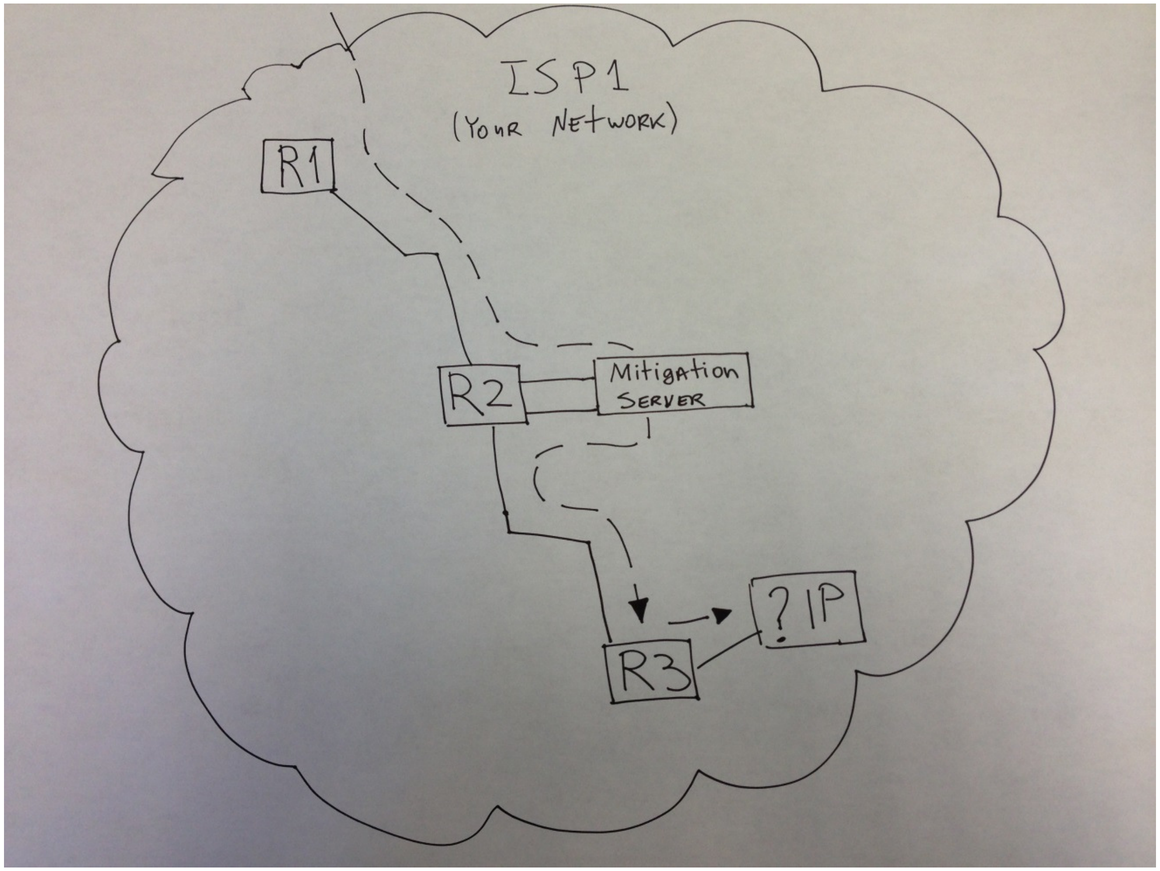


Our Happy Little School Grows

- Single location School
- Everyone travels far distances back and forth
    - It’s now getting very expensive
    - The transportation system must grow to compensate
        - Roads (along with more complicated design, maintenance, resurfacing
- Some of the same properties that the original solution was designed to solve

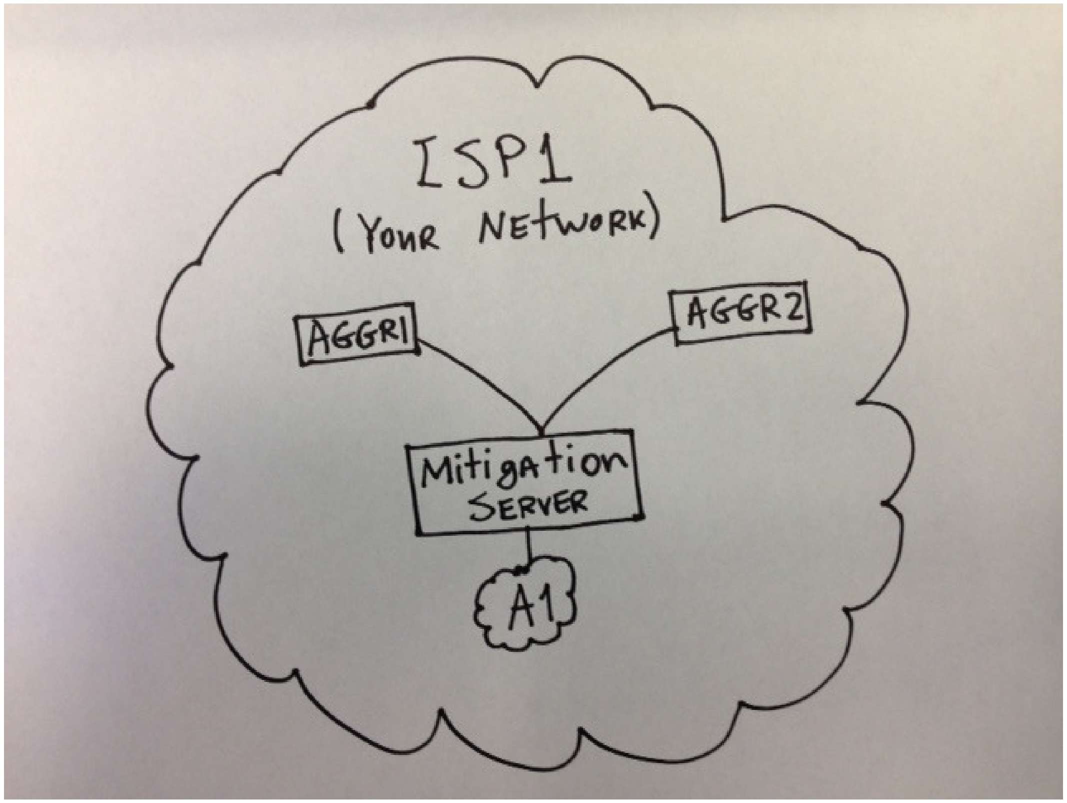
DDoS Mitigation Server Approach (Phase 2)

- Start with a single piece of scrubbing hardware that is just large enough to do the job - much like a single room schoolhouse
- Everything is pulled to the scrubber, improved, and returned to the proper destination
- This has a level of complication of moving traffic where it doesn’t naturally want to go within the network
- The rest of the network and devices must scale with the solution



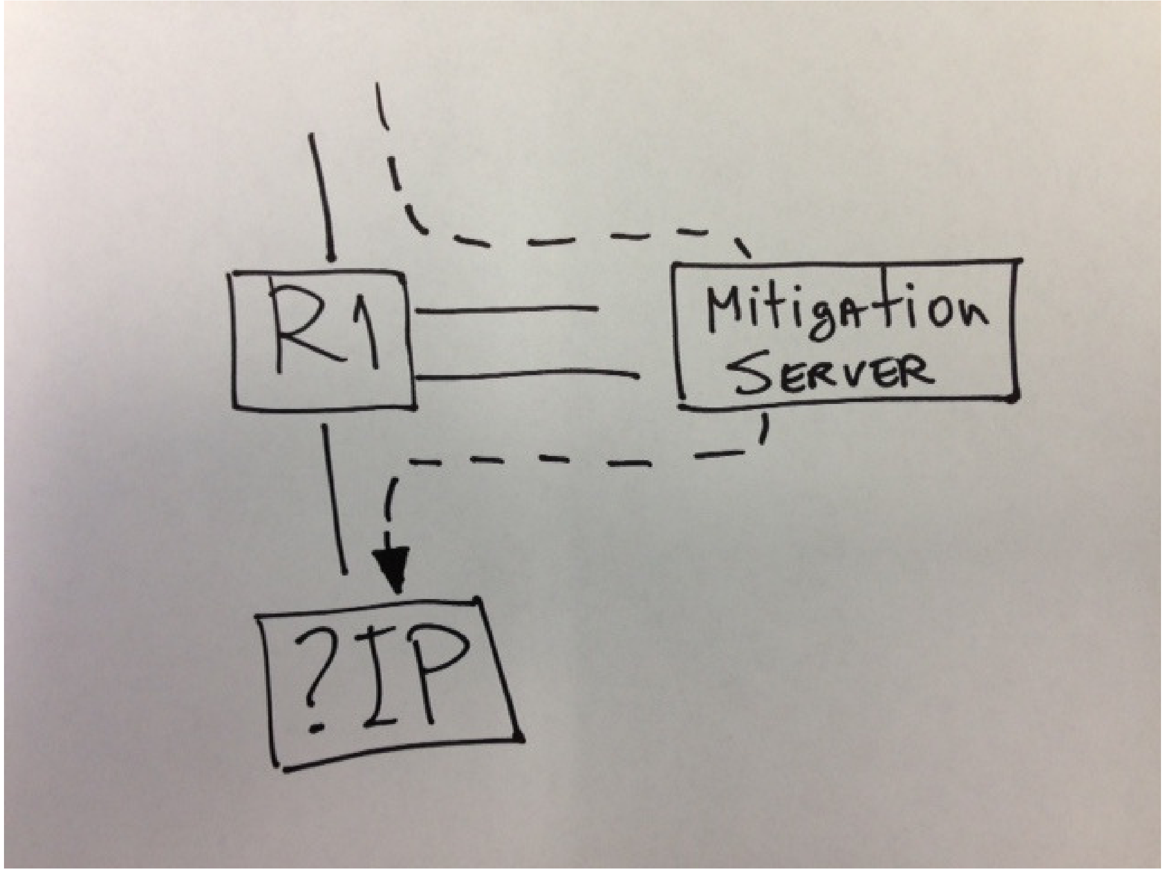
DDoS Mitigation Server Approach (Phase 2)

- In-line mitigation for an environment running a low traffic application



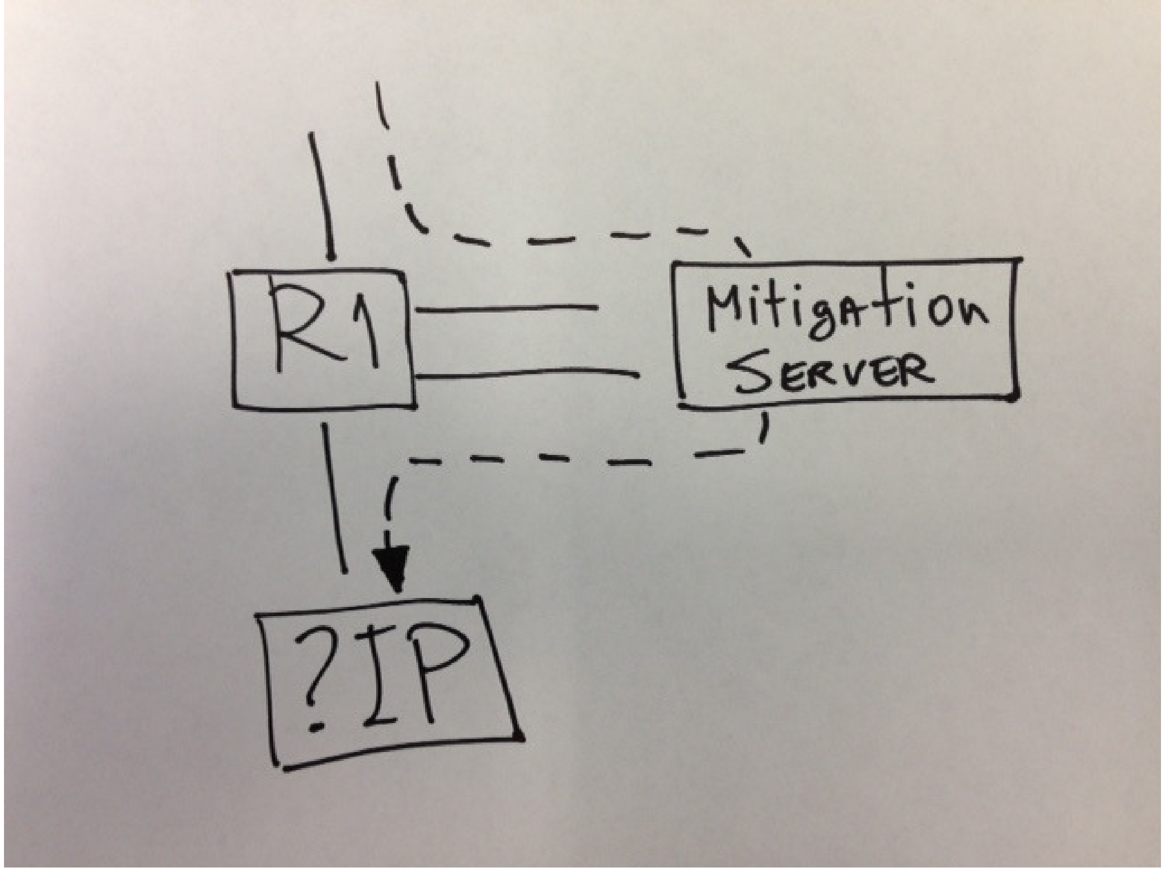
DDoS Mitigation Server Approach (Phase 2)

- Pros
  - Tunable to requirements
    - Many have lots of knobs to turn
  - Local mitigation available
    - No routing outside of network to "make it happen"
  - Has self-identifying traffic monitoring
    - Doesn't need direct access to routers and switches
  - Can be integrated with local tools easier
    - Monitoring for instance
  - Participate in a global anti-threat monitoring environment



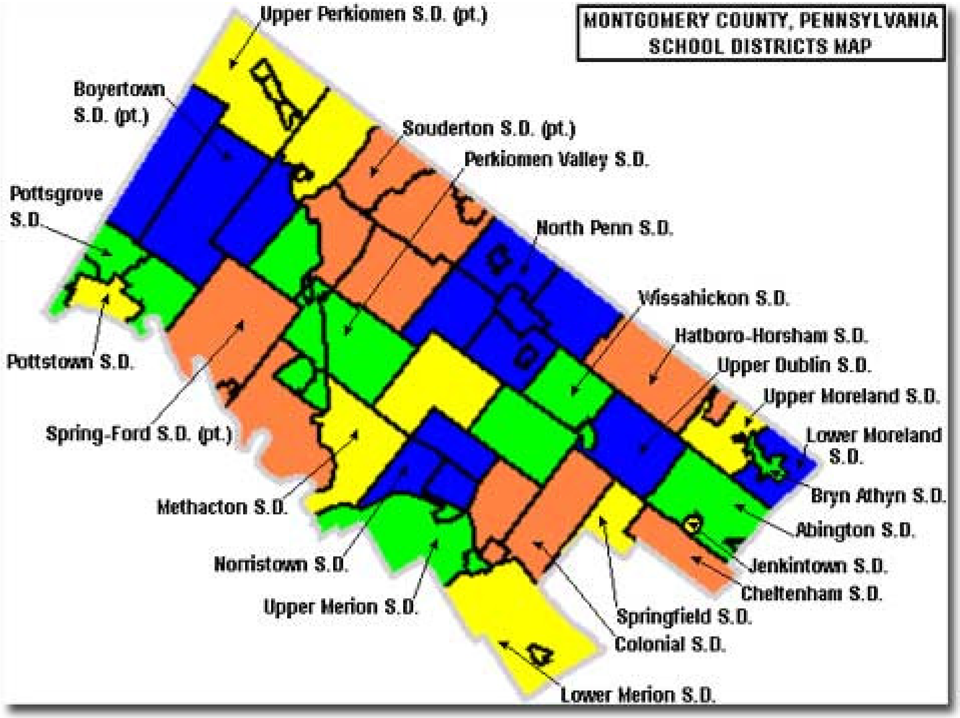
DDoS Mitigation Server Approach (Phase 2)

- Cons
  - Requires internal expertise
    - Available 24/7 or on-call
  - Burden of scale falls to Provider
    - Many hardware solutions seemed PPS limited
    - Answer is usually “Just buy bigger”
  - Expensive
    - CSO wants clear ROI
    - Multiple locations can easily cost multiple millions of dollars
  - Still increases OpEx
    - Doesn’t solve Transit capacity issues (you will pay for both good and bad traffic)
      - Increase Transit capacity to absorb large attacks
    - Requires additional license and support costs
      - 15% - 20%



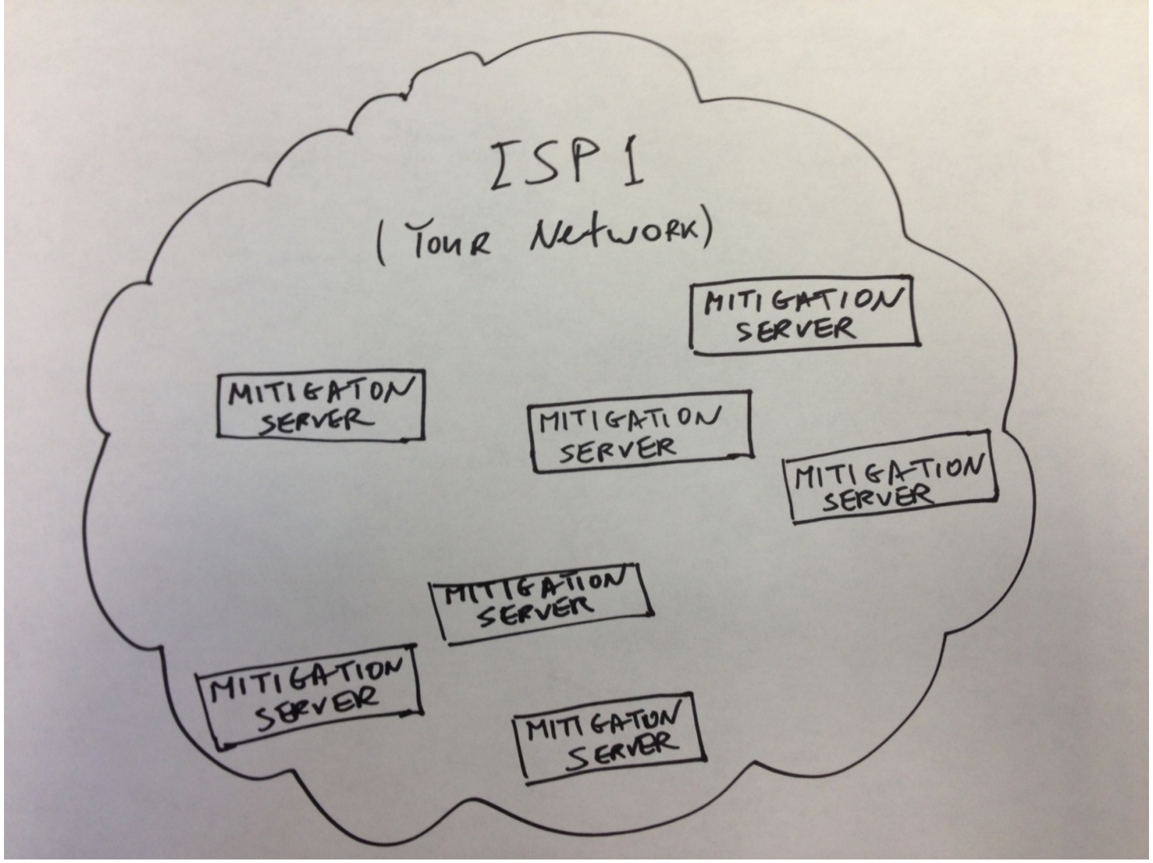
Our Happy Little School (System) Grows

- Multiple location County School System
- Really a method for controlling transportation cost
  - The transportation system doesn't grow to compensate
  - It's now getting very expensive (for the school system directly)
  - Cost is pushed to properties, building maintenance, and administrative staff
- Some of the same properties that the original solution was designed to solve



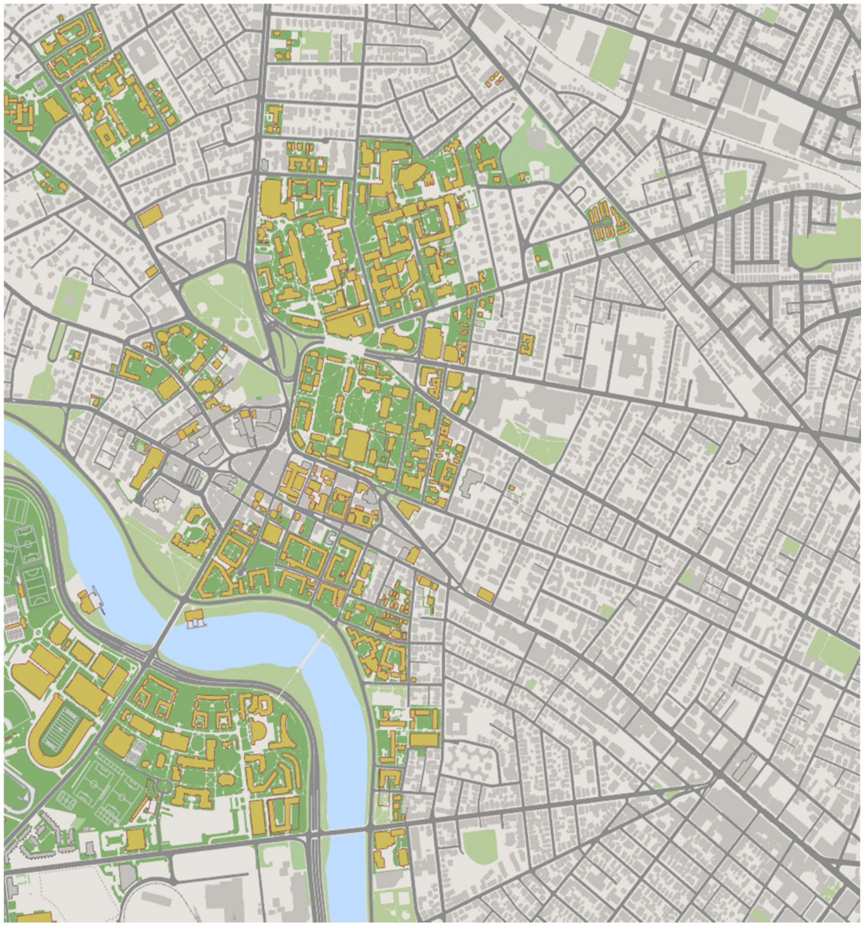
DDoS Mitigation Server Approach (Phase 2a)

- Multiply the hardware to control the scaling network and equipment cost
- All of the issues of a single device, but multiplied
- More equipment means more personnel



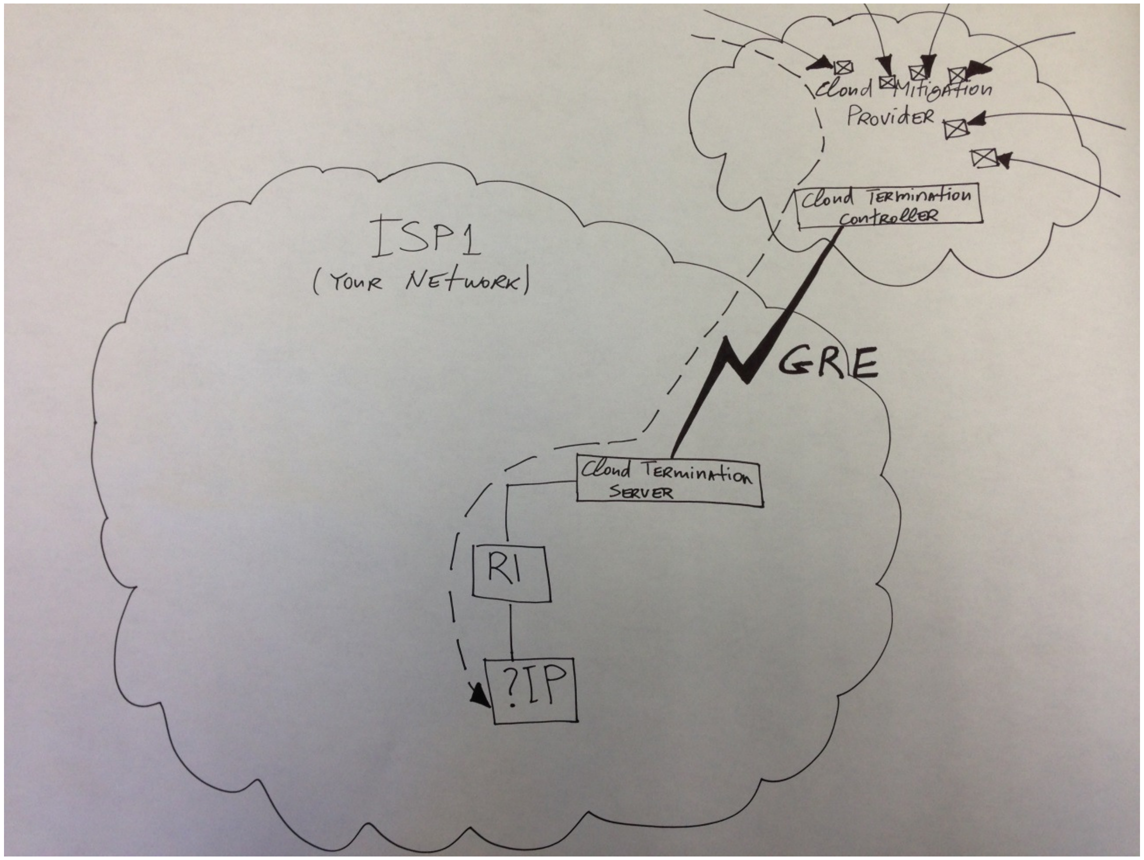
Outsourcing our Education (College)

- Let someone else deal with the scale and growth of the problem
- Instead of single location issues:
  - It’s now getting very expensive
  - The transportation system must grow to compensate
    - Roads (along with more complicated design, maintenance, resurfacing
- We send our students off to remote colleges:
  - Expense is no longer local – but is higher than our original school house by a lot
  - We are no longer able to reach our students when we desire
  - There is travel cost involved to send students back and forth
  - Living expenses are now added to the burden of education



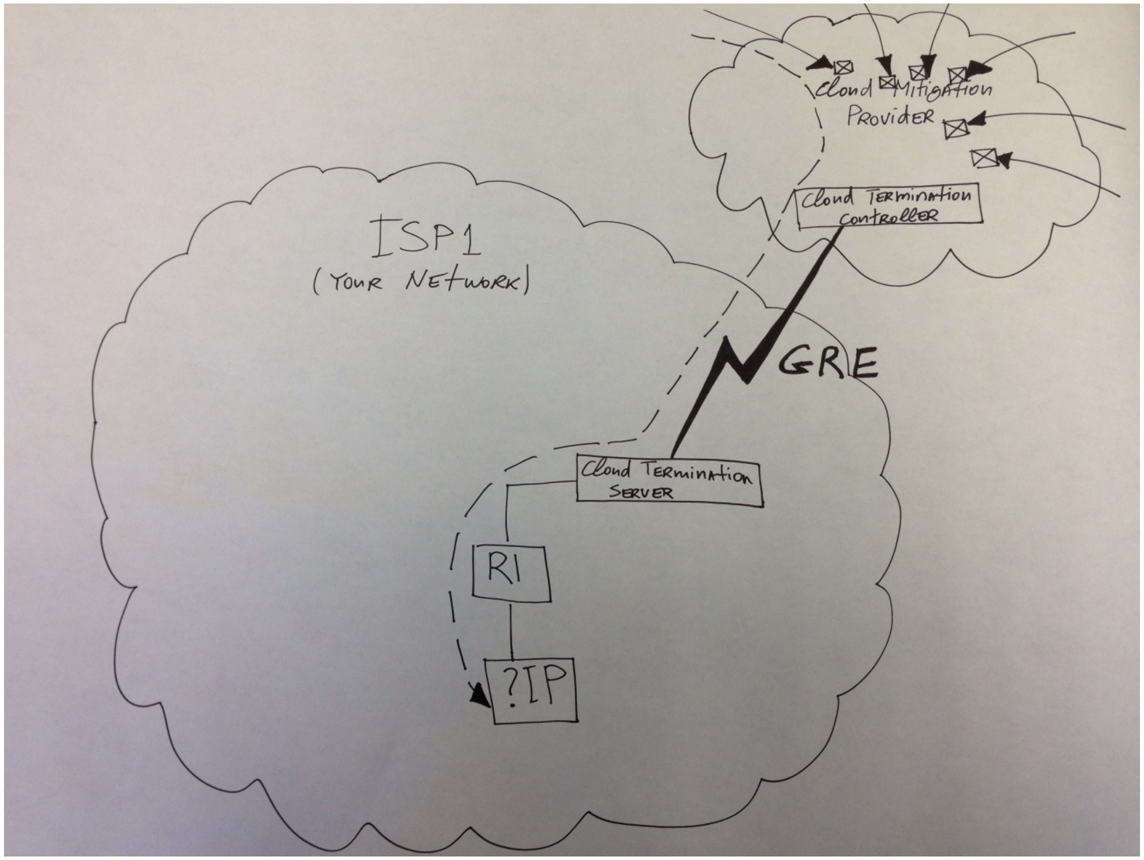
DDoS Cloud Mitigation Approach (Phase 3)

- Begin to utilize Cloud based services much like sending our students away
- Everything is pulled to the cloud, improved, and returned to the proper destination
- This is has a level of complication of moving traffic where it doesn't naturally want to go in the Internet



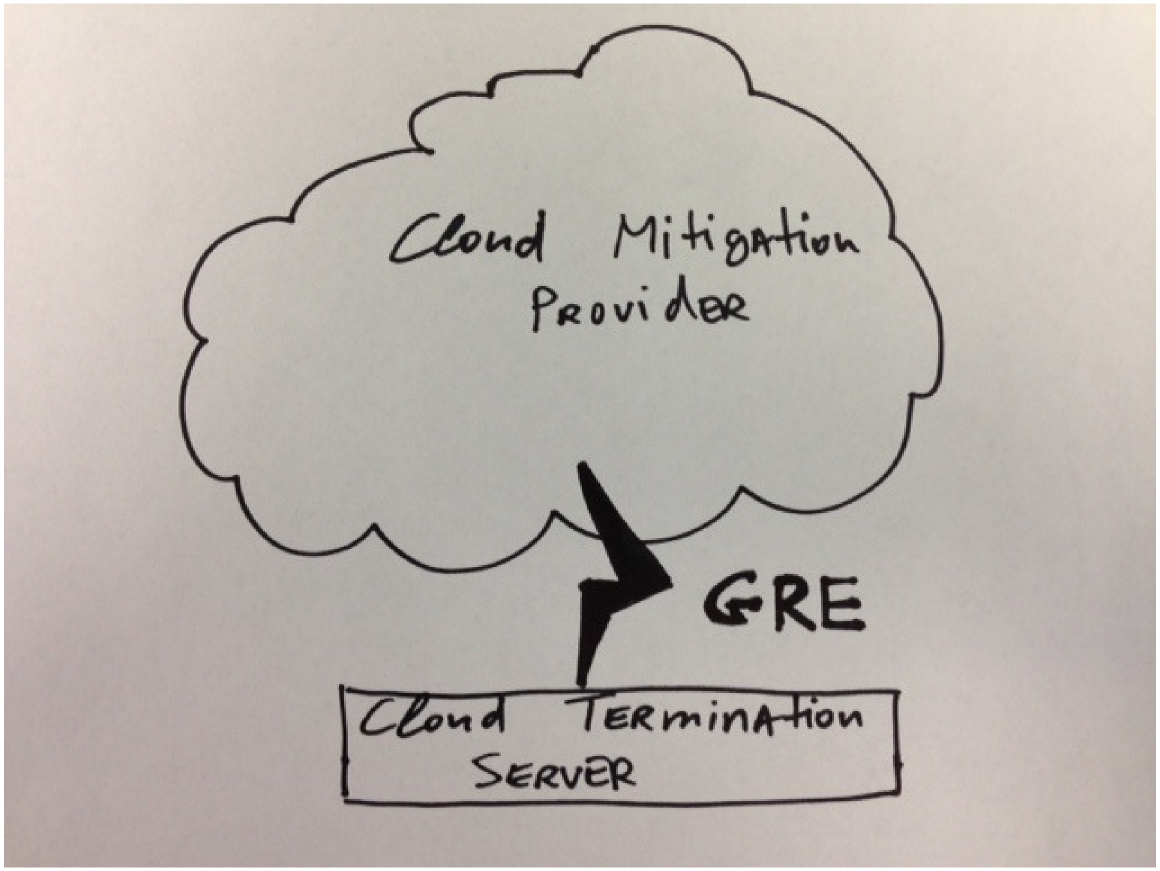
DDoS Cloud Mitigation Approach (Phase 3)

- Deploy Cloud Termination Server on your network
- Build a GRE tunnel to your Cloud Mitigation provider
- Establish eBGP session over the GRE tunnel
- Announce a dedicated IP prefix (minimum /24) part of an aggregate, only to the Cloud Mitigation provider (most specific routing)
- Lower the MTU on the tunnel interface
- Lower the maximum segment size (MSS) on your servers. This limits the maximum TCP datagram size which will fit inside the GRE tunnel without fragmentation.
- Clean traffic will be passed over the GRE tunnel
- 1 way latency will be added for incoming traffic, outbound traffic will go directly to the Internet



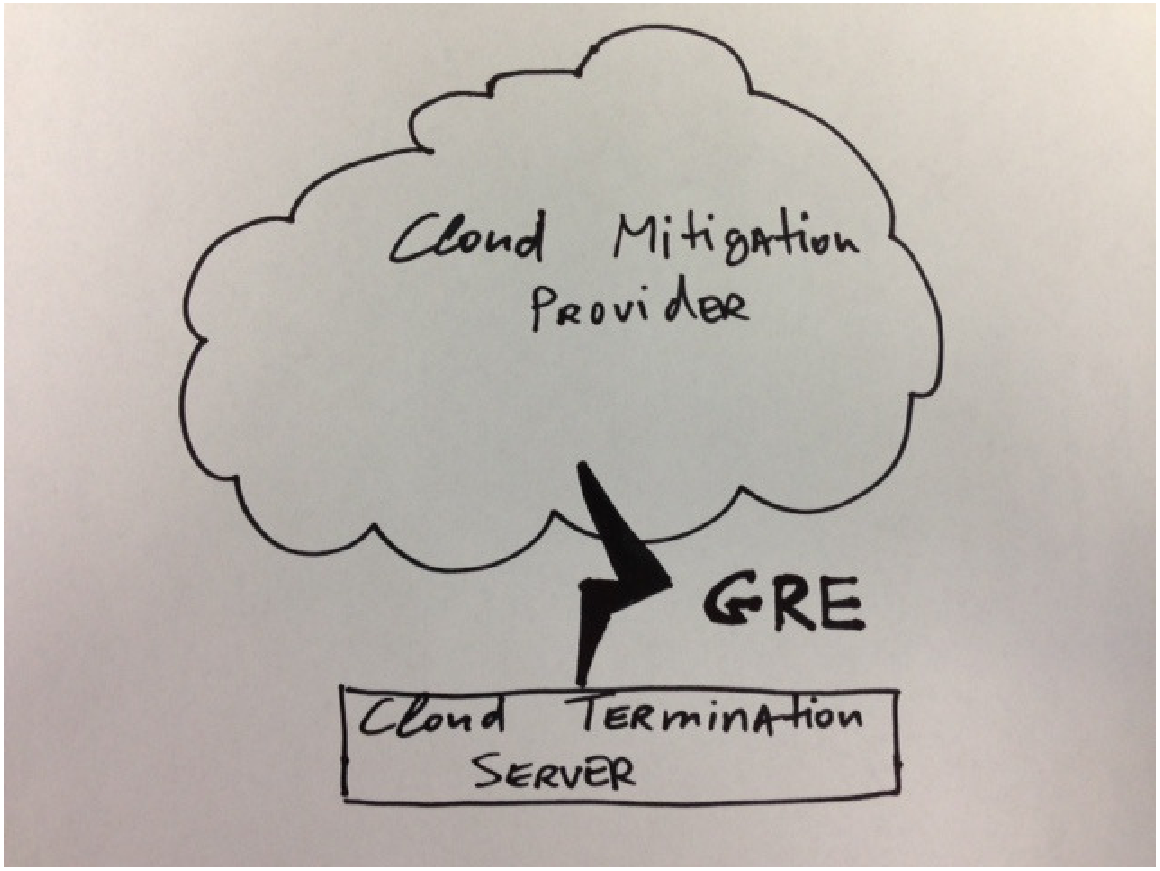
DDoS Cloud Mitigation Approach (Phase 3)

- Pros
  - Mitigation service carries burden of scale
  - Mitigation service has 24/7 support for attack and portal to understand what is occurring
  - Mitigation service must maintain expertise
  - Mitigation service must maintain hardware and support
  - Two Methods -
    - Always on
      - No routing updates involved during mitigation
      - Tunneling issues immediately obvious
      - Performed independently of local network
        - They don't need router/SNMP/Flow access
    - As Needed
      - Controls transit and mitigation costs



DDoS Cloud Mitigation Approach (Phase 3)

- Cons
  - Increases latency
  - Return traffic delivery concerns
    - MTU and Path concerns
  - GRE performance issues over the Internet
  - No mitigation inside your network
  - Two Methods -
    - Always on
      - Always feel Mitigation's issues (packed loss…)
      - Difficult to scale (especially return path)
      - Always paying for traffic (even though no attack)
      - IP range complexity (customer renumbers into /24)
    - As Needed
      - Needs Attack Identification mechanism (many wanted router access and use Flow data)



Our Hybrid School System

- Partner with someone else to deal with the scale and growth of the problem
- Don't neglect the value of higher educational systems
  - Use of remote video conferencing and networked computer systems
- Take advantage of local representation
  - Smaller staff needs because of technology
- Use the best attributes of all current solutions
  - We are able to reach our students when we desire
  - There is no travel cost involved to send students back and forth
  - Living expenses are now removed from the burden of education

A Hybrid Approach to DDoS Mitigation (Phase 4)

Hardware Attributes to Obtain …

- Local mitigation available
  - No routing outside of network to “make it happen”
- Has self-identifying traffic monitoring
  - Doesn’t need direct access to routers and switches
- Can be integrated with local tools easier
  - Monitoring for instance

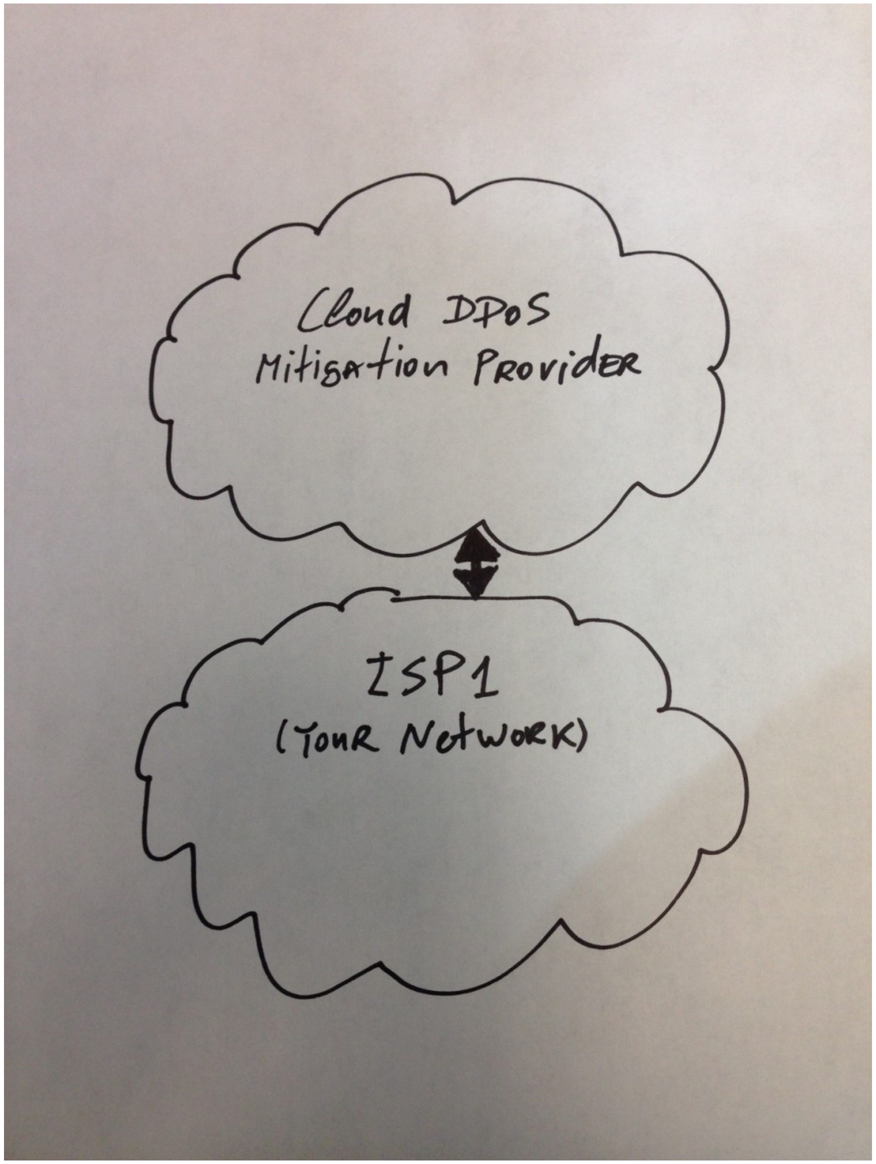
Cloud Attributes to Obtain …

- Mitigation service carries burden of scale
- Mitigation service has 24/7 support for attacks
  - And portal to understand what is occurring
- Mitigation service must maintain expertise
- Mitigation service must maintain hardware and support
- As Needed
  - Controls transit and mitigation costs

A Hybrid Approach to DDoS Mitigation(Phase 4)

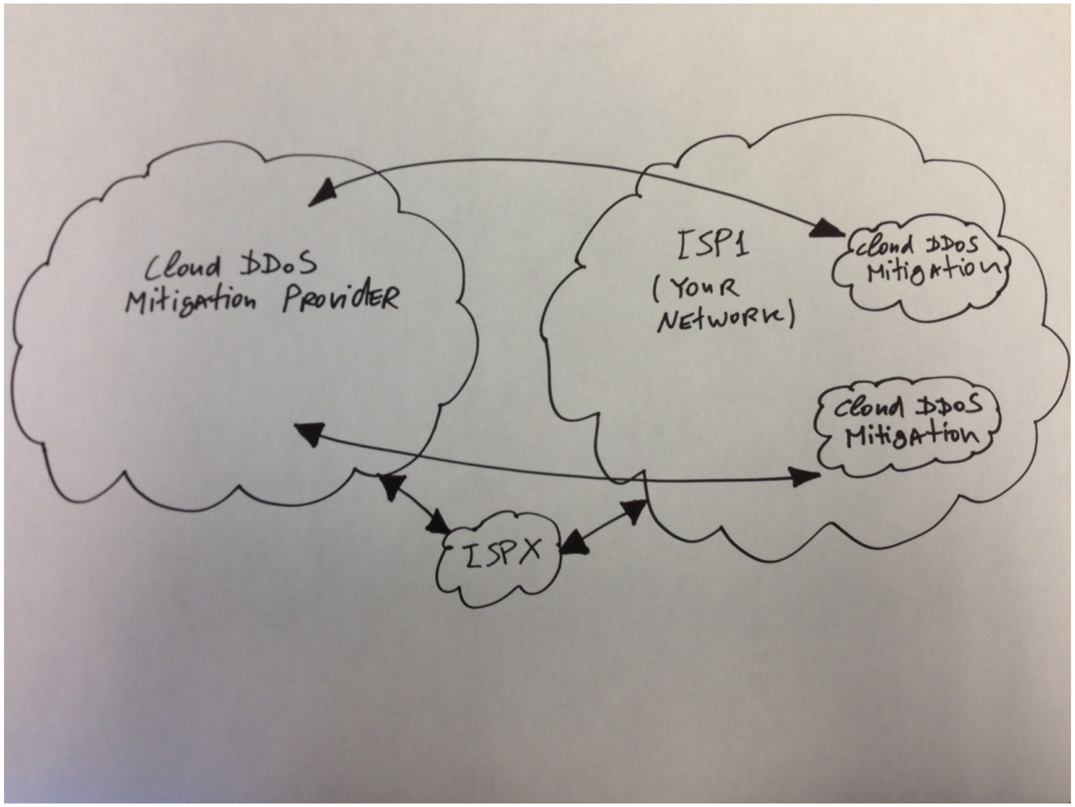
Neither of the usual methods were appealing
But attributes of them were!

- Attributes to Avoid
  - Large CapEx cost
    - A medium sized network could easily cost several millions!
  - Adding large OpEx cost
    - Adding headcount
    - Adding transit capacity
  - Carrying burden of scale



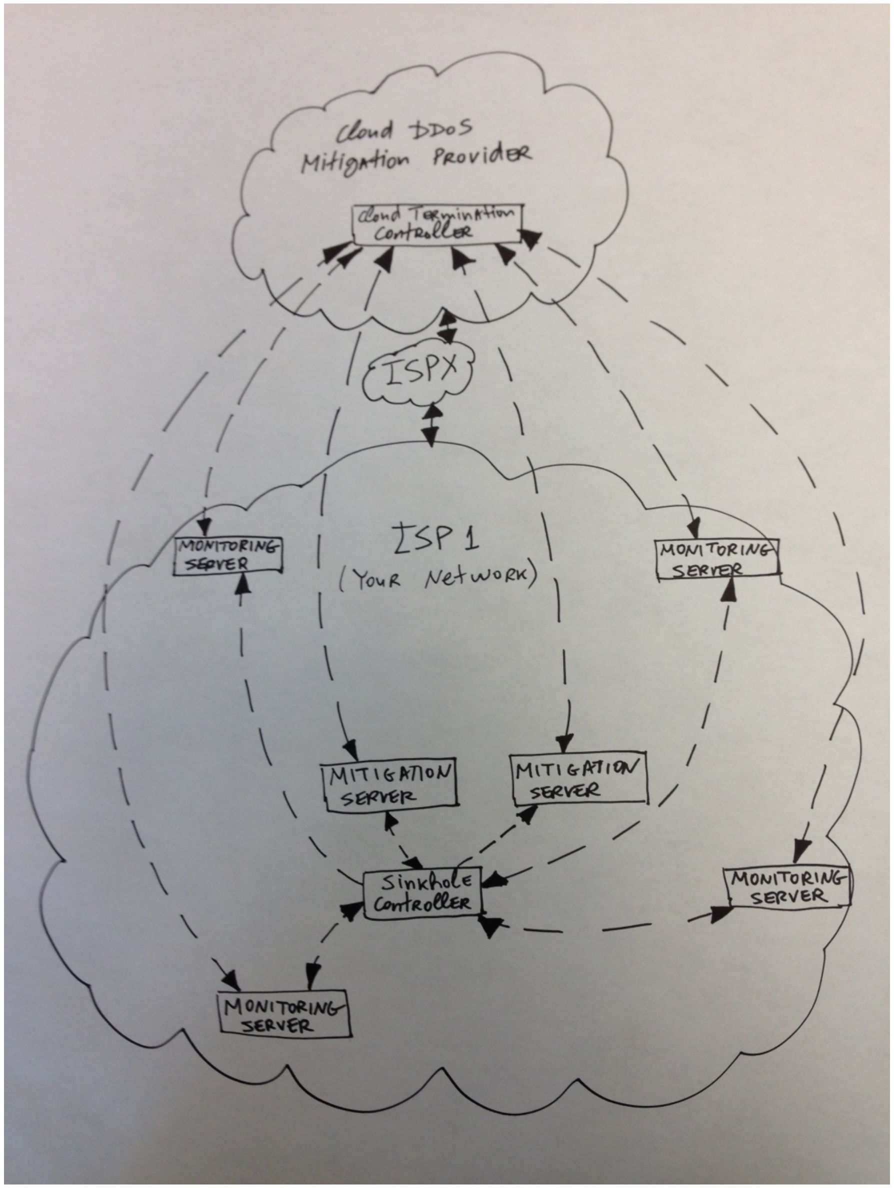
A Hybrid Approach to DDoS Mitigation (Phase 4)

- We wanted a hybrid of local and cloud!
  - Something to handle the smaller issues locally
  - Let the cloud handle the big things
  - A Hybrid approach!
- A Cloud Mitigation Service satellite
  - Some local capabilities
  - Operated by Cloud Provider
    - They have expertise
  - Cloud Provider hardware
    - Their support
    - No large capital outlay
    - Scaling is outsourced
  - Independent monitoring
- Must aggregate the data before implementing mitigation (must have centralized DB to work properly)
- Automation is key



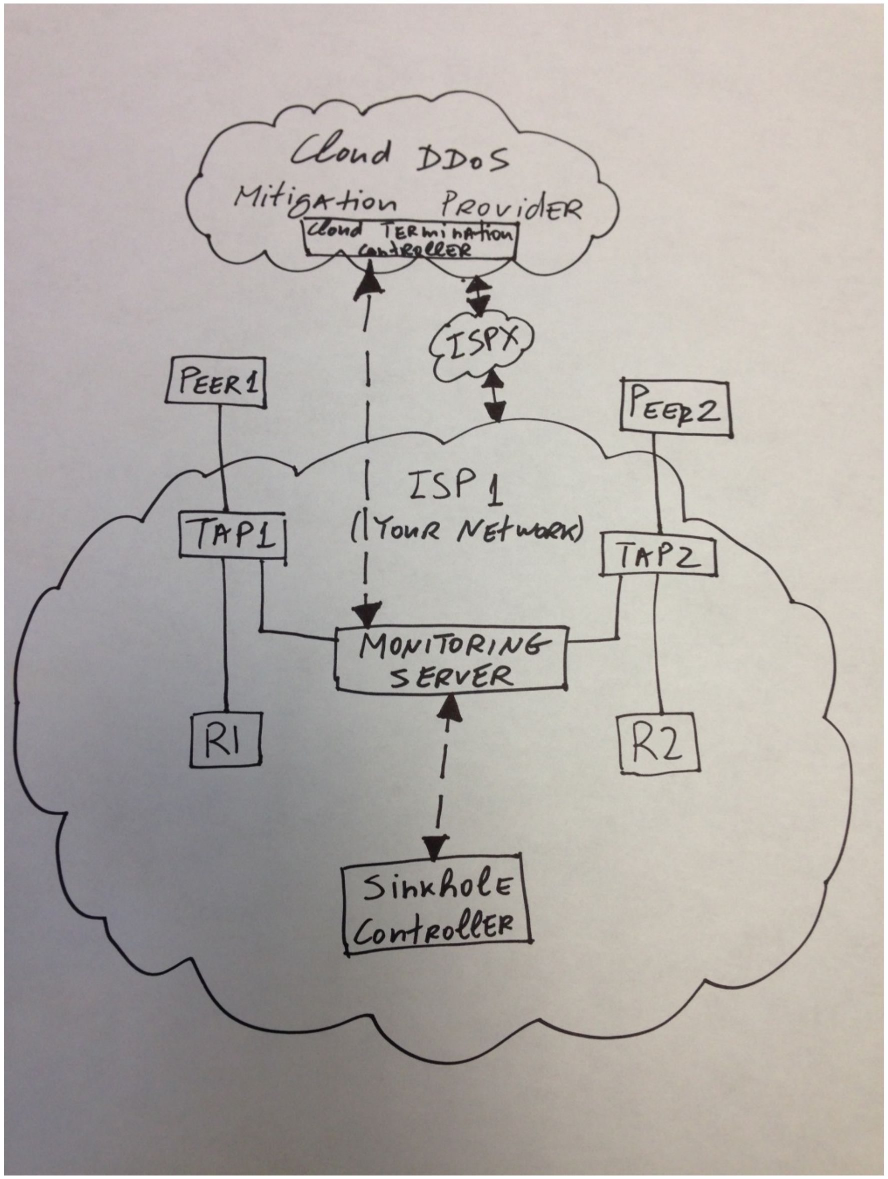
A Hybrid Approach to DDoS Mitigation(Phase 4)

- Integration of systems
    - Deploy edge termination, monitoring and mitigation servers on your network
    - Connect to the Cloud DDoS Mitigation provider over a common ISP
    - Establish eBGP session over the dedicated connection
    - Configure the ability to announce any IP prefix from your network



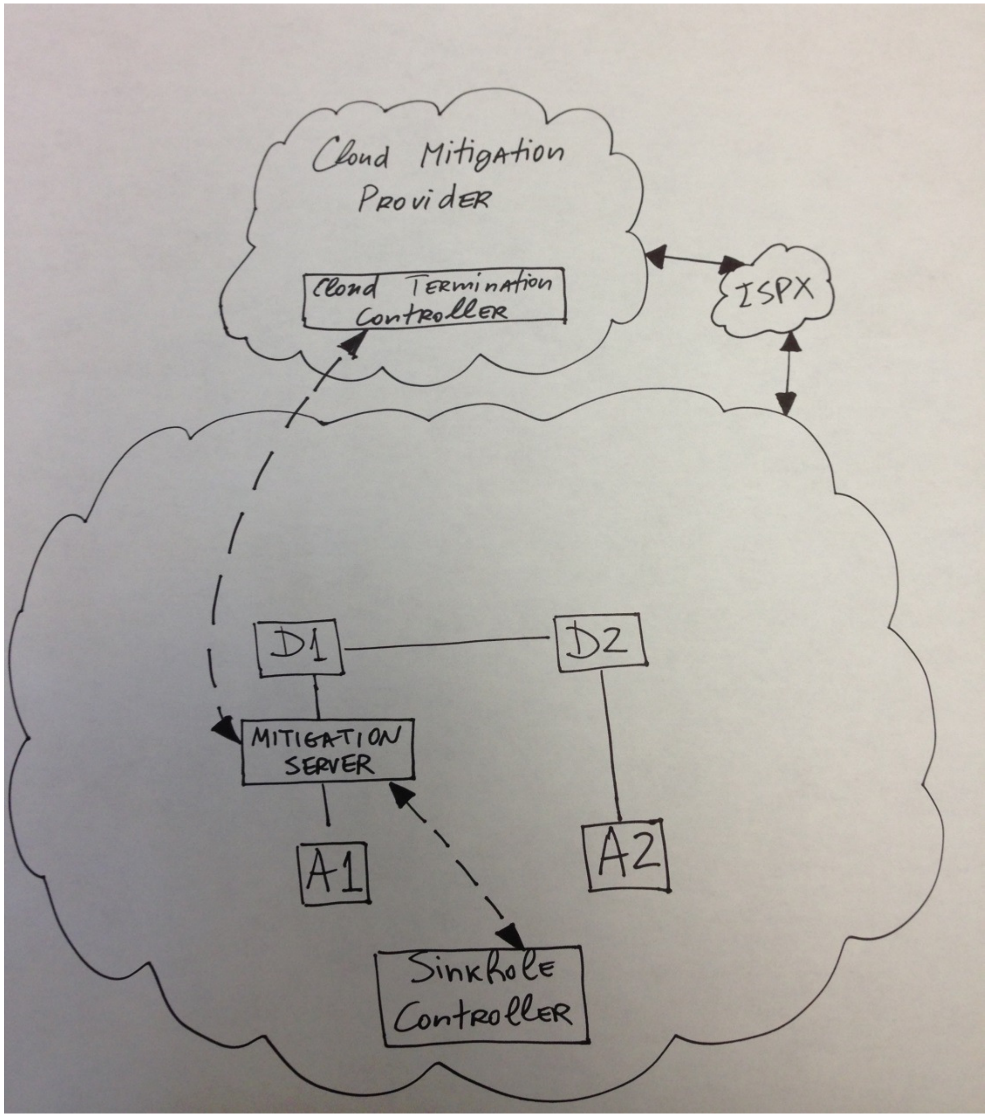
A Hybrid Approach to DDoS Mitigation(Phase 4)

- Utilize passive fiber-optic taps duplicating every packet to the monitoring server.
- The server provides continuous monitoring of traffic entering your network
- Enables automated Sinkhole capabilities with “internal” and “external” tagging
- Adds the automatic “Swing to Cloud” capability
- Controls failure domains
  - Not in data path
- Allows multiple monitoring points per monitoring server



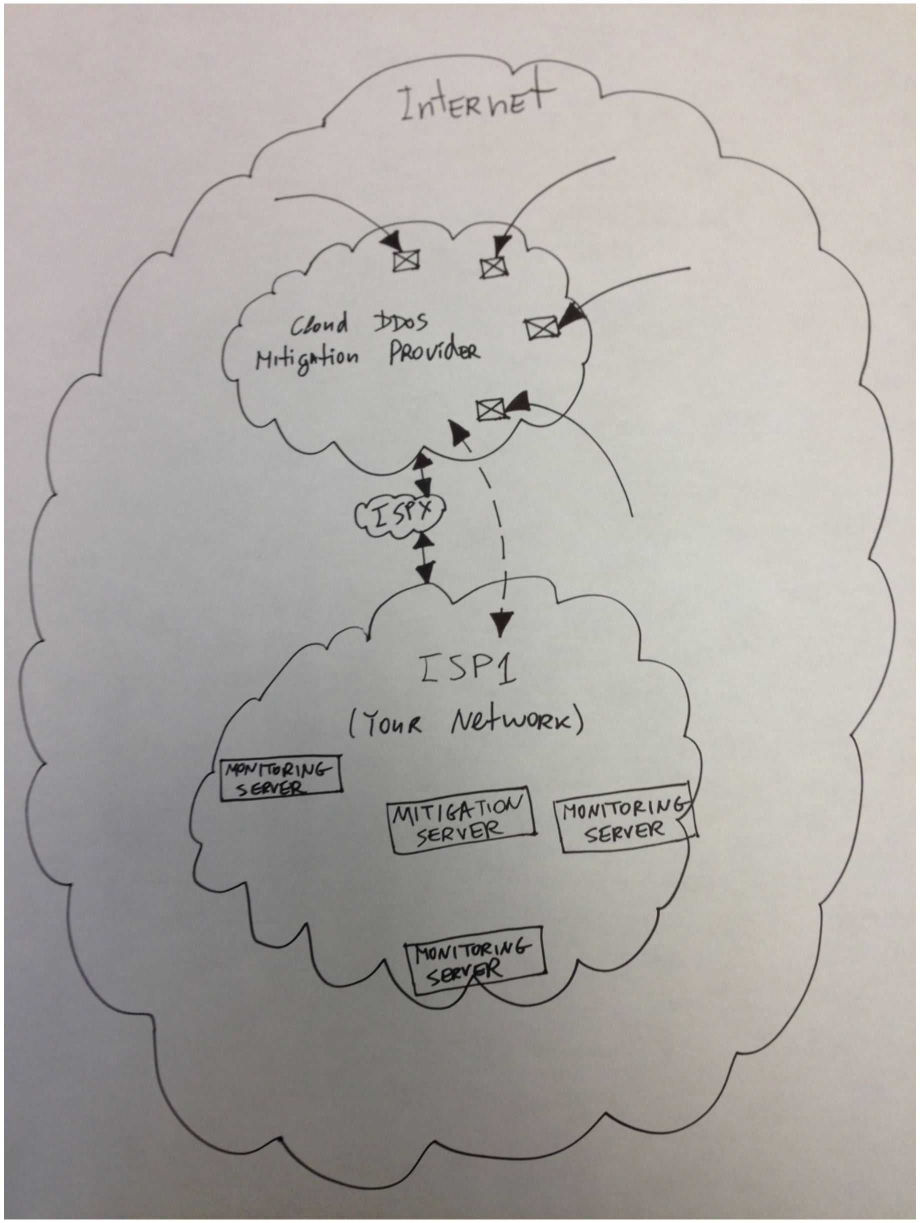
A Hybrid Approach to DDoS Mitigation(Phase 4)

- The mitigation server sits in front of a local environment in your network
- The mitigation server is an in-line device that acts just like an IDPS system
- Dirty traffic enters one interface, attack traffic is dropped, and cleaned traffic leaves the other interface



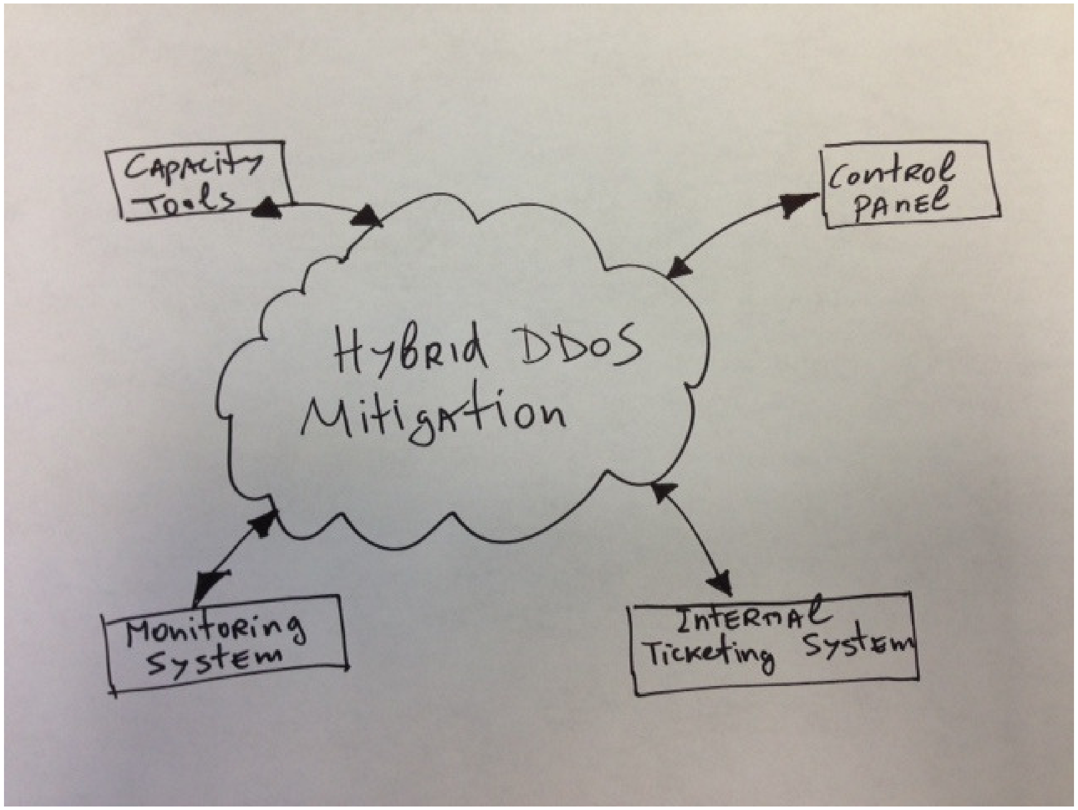
A Hybrid Approach to DDoS Mitigation(Phase 4)

- When DDoS attack is too big perform the “Swing to Cloud” function
  - The /24 subnet the targeted IP space resides in will be re-routed to the Cloud DDoS Mitigation Provider
  - The individual host address(es) under attack will be mitigated
  - The clean traffic including the traffic for the remaining addresses in the /24 subnet will be routed back to ISP1 with an increased latency
  - Hosts on the entire /24 subnet will experience packet loss as the re-routing occurs between the Cloud DDoS Mitigation Provider and the ISP1



A Hybrid Approach to DDoS Mitigation(Phase 4)

- Management and Alerting
  - You can create profiles that are used to set thresholds for determining when an attack occurs
  - Detects attacks based on a combination of packet analysis and throughput (bits per second or packets per second), but not deep packet inspection.
  - Alerting with e-mail notifications, SNMP checks, and API calls



Schools Out (for now)

- Education is never really "done" and neither is DDoS mitigation technology

Approaches for DDoS — an ISP Perspective

barry@null0.net

ognian.mitev@viawest.com