Volumetric DDoS Mitigation Service

George K. Loftus
AVP Network Services, Internet2
Internet2 DDoS Mitigation Service

- Internet2 plans to provide a cloud-based Distributed Denial of Service (DDoS) Mitigation Service procured from a commercial service provider.

- Subscribers to the service will be able to direct attack traffic to the DDoS Mitigation Service provider, and carry the clean traffic back to them via a vlan on their existing Internet2 connection.
Internet2 DDoS Mitigation Service

• The Subscriber will have access to an aggregated amount of ‘clean pipe” service (10G) to which the community has subscribed.

• Subscriber will get 1G of clean pipe capacity (commit rate) but will be allowed to burst into the available capacity on the clean pipe (up to 10G initially)
  • Currently this bursting will have no additional cost, unless it becomes a regular occurrence for a subscriber, or Internet2 incurs additional costs.
Internet2 DDoS Mitigation Service

Provider Selection Process

• Working with our technical community, Internet2 developed requirements for a cloud-based DDoS service.

• We issued an RFP and solicited responses from six providers.

• A review of responses by a community technical team yielded ratings and Internet2 negotiated with three high ranking providers.

• We then convened a group of regional representatives to review the proposed business models.
Internet2 DDoS Mitigation Service

- Provides coverage for commodity traffic and R&E traffic
  - IPv4 and IPv6
  - Coverage of unlimited assets/IP addresses
- Traffic is returned via a vlan provisioned during service onboarding
- Scrubbing is signaled via eBGP peering with provider SOC
  - Provider will announce /24 (IPv4) subnet globally to draw traffic to the scrubbing center and returned to connector/campus
Internet2 DDoS Mitigation Service

- Plan to have connections to Internet2 in Chicago & Sunnyvale

- Each Subscriber will have access to Security Operations Center (SOC), a services portal and a direct vlan back to its edge.

- There is an option for those downstream of a Subscriber to become a Tenant and have access to the SOC, the services portal and a direct vlan back to its edge routers for an additional fee.
Protecting commodity traffic

Commodity Internet

Scrubbing Center

Diverted attack traffic
Commodity traffic
Clean traffic return path

Internet2 Network

Subscriber

Tenant
Protecting Research and Education traffic

- Diverted attack traffic
- Research and Education traffic
- Clean traffic return path

- Scrubbing Center
- Internet2 Network
- Regional/Member Network
- Subscriber
- Tenant
Internet2 DDoS Mitigation Service

- This service will be offered to R&E Network members and connectors, and like all Internet2 services it will also be made available to any Internet2 member who wishes to procure the service directly.

- Pricing model will favor R&E Network Members/Connectors procuring the service and then sharing costs among its members.
Internet2 DDoS Mitigation Service

Optional Services

- Tenant, provides those downstream from Subscriber with:
  - Direct access to SOC personnel to initiate mitigation
  - Access to SOC portal for status and reporting
  - A direct VLAN across Internet2 to the Tenant’s edge router

- MRC - $750
- Set Up Fee $500
Optional Services

- Monitoring of Edge Routers for auto-detection
  - Allows DDoS Provider to notify Subscriber or Tenant of attack
  - Uses Netflow data to create a more specific attack template for mitigation
  - Could lead to faster mitigation of the attack

- MRC - $750 per monitored router
Internet2 DDoS Mitigation Service

What will it cost?

Up to 16 Subscribers - $6K MRC
16-20 Subscribers $5K MRC

$500 NRC Setup Fee
Method for Setting Fees Annually

• We will use a sliding scale with the fees being reduced as more subscribers join.

• Fee will be reviewed annually, and amount will be adjusted according to the number of subscribers on July 1 of each year.
Thank you.

DDOS MITIGATION SERVICE

George K. Loftus
AVP, Network Services, Internet2
GKLoftus@Internet2.edu