Internet2 DDoS Mitigation Service Pilot

Internet2 is pleased to offer a cloud-based volumetric Distributed Denial of Service (DDoS) Mitigation Service procured on behalf of the community from a commercial service provider.

Each Subscriber/Tenant will have:

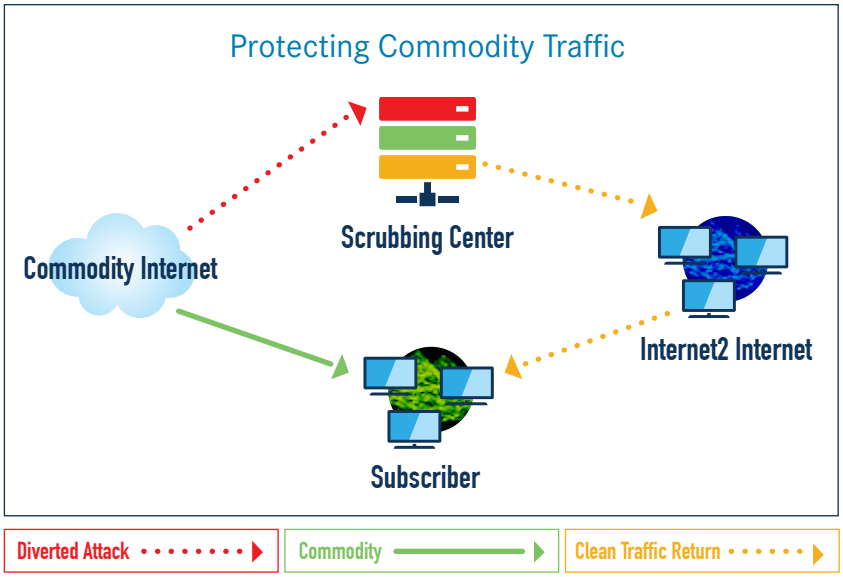
- **Direct access to the Security Operations Center (SOC) of the provider to initiate mitigation**
- **Access to a portal to review mitigation efforts and subsequent reports**
- **Clean traffic carried to the Subscriber's routers across the Internet2 network**

Community Effort

After the community encouraged Internet2 to obtain the service, we worked with members of the Security Working Group and developed requirements for a cloud-based DDoS service to be used in an RFP for the service. The RFP responses were reviewed and rated by a community technical team and then Internet2 negotiated with three high ranking providers. When creating the business model for the service, Internet2 consulted with the Network Architecture, Operations and Policy Program Advisory Group (NAOPpag) and convened a group of regional representatives. A group of technical leaders from the pilot group has met with Internet2 and the service provider to delve into the technical details.

How Does the Service Work?

DDoS Mitigation Service Subscribers procure 1G of clean pipe capacity while being allowed to burst into the available capacity provided by Internet2 on the clean pipe (up to 10G initially). The Subscriber will direct attack traffic to the DDoS Mitigation Service provider, and the clean traffic will be carried back on the Subscriber's existing Internet2 connection. To activate the service, a Subscriber detects the attack and requests that the service provider begin scrubbing a specified prefix. The service provider then draws all traffic for the prefix to their scrubbing center where the traffic is scrubbed and the clean traffic is returned to the Subscriber on the Subscriber's existing Internet2 connection.



A Subscriber will be allowed to offer the service to its downstream members (e.g., a regional could offer the service to a university or a K-12 district). Downstream members (e.g., a university or a K-12 district) have the option to obtain the same direct access services from the provider by choosing the Tenant option, with an associated fee structure.

For an additional fee, the provider also offers a Monitoring service for those Subscribers or Tenants without on-premise appliances for attack detection. With the Monitoring service, netflow records are sent to the service provider's analytics appliance and the provider is able to notify the Subscriber or Tenant of the need for mitigation.

For more information, please contact: DDoSService@internet2.edu or go to the FAQ page at:
www.internet2.edu/products-services/advanced- networking/ddos-mitigation-service/#service-faq