FLR Science DMZ

Ryan Vaughn

ryan.vaughn@flrnet.org

Senior Network Engineer

Florida LambdaRail NOC

FLR Science DMZ Overview

FLR Overview

- FLR operates a 1540 mile optical backbone utilizing multiple 100G waves.
- The FLR transport network utilizes MPLS to provide multiple VRFs. Each VRF provides a different service: FLR Internet Service, FLR Commodity Peering Service, FLR Research and Education Peering, and L2 and L3 VPNs.
- This enables FLR members to configure their own routing and security profile for each service.
- FLR Members access FLR at 1G, 10G, or 100G.

FLR Science DMZ

- A new VRF on the FLR transport network.
- Designed to support Intensive Science Applications and High Performance Computing.
- Offers L3 peering and L2 circuits.
- Provides a method for FLR members to separate research and science applications from the Campus enterprise and commodity traffic.
- This allows for a smaller routing domain and security perimeter.

FLR Science DMZ: Member Connections

- The FLR NOC will work with FLR Members to design and/or validate a Campus's Science DMZ for connectivity to FLR.
- FLR Engineering is using the Esnet Science DMZ model as the standard for recommended best practices. It can be found at http://fasterdata.es.net/science-dmz/
- The Campus should have created a Campus Science DMZ that is physically or virtually separated from the enterprise network and should only be used for research, science applications, or HPC type traffic. The size of the Campus Science DMZ network will vary based on the needs and applications of that campus. It could be as large as a fully distributed backbone with many endpoints or as small as a single Data Transfer Node. No general purpose workstations should exist on the Campus Science DMZ.
- The Campus Science DMZ network should be a limited and specific subset of the Campus's IP space. IPv4 and IPv6 is supported.

FLR Science DMZ: Member Connections

- The security architecture of the Campus Science DMZ network should not include firewalls in the data path. The state engine in firewalls will negatively effect the performance and optimization of intensive science applications and large data transfers.
- The Campus Science DMZ network will have a separate physical or virtual connection to the FLR Regional Science DMZ.
- The Campus Science DMZ network should be able to BGP peer with the FLR Regional Science DMZ.
- The Campus Science DMZ may peer with the Campus Enterprise network or have other additional peering connections (FLR R&Enet, Internet, private peers, etc), but should not transit other traffic to the FLR Regional Science DMZ.
- The Campus Science DMZ should implement a least one PerfSonar monitoring system within their Science DMZ.