Ohio State University Science DMZ Policy Portal

Alex Berryman
OARnet
berryman@oar.net

Paul Schopis
OARnet
pschopis@oar.net

ABSTRACT

The OSU Science DMZ utilizes a number of emerging network protocols and services to support a diverse set of network intensive science applications. Many of the research workflows in the OSU Science DMZ involve multiple applications executing in parallel. This demo will show how applications in a researcher's workflow can be prioritized by a Science DMZ Policy Portal which uses intelligent network monitoring to control the software-defined networking paths. The researcher's workflow consists of a real-time remote instrument steering application that allows for setup and monitoring of experiments at a remote site. These instruments create large datasets that need to be transferred for analysis. Both of these flows require high throughput, but the remote steering application is highly sensitive to jitter and latency while the large data flow is mainly sensitive to packet loss. In order to support this particular workflow it is imperative to have an accurate view of the current path characteristics and a historical baseline of its typical performance. The Science DMZ Policy Portal is able to combine both the passive and active monitoring data to determine when action is required to prevent the remote steering application from being impeded by the data transfer. In practice the researcher only uses the remote-steering application for a short time to setup the experiment while the large data flow will run for hours. Using OpenFlow we are able to redirect large data flow traffic from the AL2S path to a traditional Internet2 path to optimize the remote steering user experience.

Keywords

Software defined networking, Network monitoring and management and control, Scheduling and reservation.

1. Overview

This demo will showcase the adaptive control that researchers have in the Ohio State University Science DMZ. This control is orchestrated by the Science DMZ Policy Portal which allows researchers and Science DMZ operators to define and prioritize flows. The researcher is able to classify the multiple types of data and flows in the workflow so instrument control traffic can be prioritized or handled differently than the private research or restricted patient imaging data that instrument produces. These classifications are used to make decisions that can improve performance and aid the Information Risk Management process.

Performance matters can be addressed by defining high-level logic to make network path choices. A single endpoint produces multiple types of traffic during an experiment such as high speed RoCE transfers that require layer 2 connections that are provided through AL2S. While RoCE traffic requires a layer 2 connection, other types of traffic like instrument control traffic prefer AL2S paths due to the lower latency. Other types of traffic like SSH sessions have no major performance requirements. Using software defined networking these flexible types of traffic can be dynamically switched between the ideal path. Both active and passive network measurements are used to influence these decisions.

Security aspects are improved by giving fine grained control to Security Engineers to selectively send subsets of an experiments traffic to monitoring tools like a Bro Cluster. As the network cumulative speeds Science DMZs increase it is becoming critical to identify which flows are worthwhile to inspect versus those that contain content that poses little risk.

2. Problem Statement

In large organizations with decentralize IT groups, like the Ohio State University, the Science DMZ penetrates from the regional level, through Central IT, and into each department. This cross-boundary nature requires transparent chain of ownership which the centralized Science DMZ Policy Portal provides.

3. Relevance

The first round of NSF CC-NIE Science DMZ projects are approaching the two year mark. This means the organizations need to develop the tools needed to integrate Science DMZ operations into the overall IT infrastructure from helpdesk operation, network security, and billing processes. The Science DMZ Policy Portal is essential to making the transfer from a research project into sustainable service.

4. SCinet and Network Requirements

Nothing special is required from SCinet. This experiment operates between the Ohio State University's, and University of Missouri's respective Science DMZs. Web access, and SSH traffic to the public IPs of these nodes is the only requirement.