Trusted CI Webinar Series

Title: The Science DMZ at Arizona State University

Presenters: Douglas Jennewein and Chris Kurtz

Host: Jeannette Dopheide  Slides: https://tinyurl.com/44p2xtaf

The meeting will begin shortly.

Participants are muted. Click the chat button to ask a question.

This meeting will be recorded.

The Trusted CI Webinar Series is supported by National Science Foundation grant #1920430.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.
The Science DMZ at ASU

TrustedCI Webinar Series
April 26, 2021

Douglas M. Jennewein, Senior Director, ASU Research Computing
Chris Kurtz, Senior Systems Architect, ASU Research Technology Office
Overview

The Science DMZ Architecture
• Motivation
• Design Principles

The Science DMZ at ASU
• NSF Proposal
• Current State
• Technical Summary
Motivation

(when in doubt, blame TCP…)

ASU
TCP, The Fragile Workhorse

- TCP is (for very good reasons) timid
- Packet loss is interpreted as congestion
- Packet loss in conjunction with latency is a performance killer
- Dropped packets can destroy throughput on high latency (e.g. WAN) connections
- Packet loss is still the number one performance killer in long distance high performance environments
- Stateful packet inspection (read: firewall) can be a huge source of these dropped packets
Origins of the Science DMZ

• Effective support for TCP-based data transfer
  – Design for correct, consistent, high-performance operation
  – Design for ease of troubleshooting

• Easy adoption is critical
  – Large laboratories and universities have extensive IT deployments
  – Drastic change is prohibitively difficult
Origins of the Science DMZ

- Cybersecurity – defensible without compromising performance
- Borrow ideas from traditional network security
  - Traditional DMZ
    - Separate enclave at network perimeter ("Demilitarized Zone")
    - Specific location for external-facing services
    - Clean separation from internal network
  - Do the same thing for science – Science DMZ
Design Principles

A Trifecta in Four Parts
The Science DMZ* in 1 Slide

Consists of **four key components**, all required:

- “Friction free” network path
  - Highly capable network devices (wire-speed, deep queues)
  - Virtual circuit connectivity option
  - Security policy and enforcement specific to science workflows
  - Located at or near site perimeter if possible
- Dedicated, high-performance Data Transfer Nodes (DTNs)
  - Hardware, operating system, libraries all optimized for transfer
  - Includes optimized data transfer tools such as Globus and GridFTP
- Performance measurement/test node
  - perfSONAR
- Engagement with end users

Details at [http://fasterdata.es.net/science-dmz/](http://fasterdata.es.net/science-dmz/)

*Science DMZ* is a trademark of The Energy Sciences Network (ESnet)
Friction Free Network Path: Local And Wide Area Data Flows
PerfSONAR: Wide Area Network Performance Measurement

perfSONAR is:

• A widely-deployed test and measurement infrastructure used by ESnet, Internet2, US regional networks, international networks, Laboratories, supercomputer centers, universities

• A suite of test and measurement tools

• A collaboration that builds and maintains the toolkit

By installing perfSONAR, a site can leverage over 1100 test servers deployed around the world
TCP was intentionally designed to hide all transmission errors from the user: “As long as the TCPs continue to function properly and the internet system does not become completely partitioned, no transmission errors will affect the users.” (From RFC793, 1981)

perfSONAR is ideal for finding soft failures
• Alert to existence of problems
• Fault isolation
• Verification of correct operation
ESnet - ESnet Packet Loss Testing

- Loss rate is <= 0.001
- Loss rate is > 0.001 and <= 0.1
- Loss rate is > 0.1
- Unable to retrieve data
- Check has not yet run

Services

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>STATUS</th>
<th>VERSION</th>
<th>PORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>esmond</td>
<td>Running</td>
<td>4.2.4-1.et7</td>
<td></td>
</tr>
<tr>
<td>lsregistration</td>
<td>Running</td>
<td>4.2.4-1.et7</td>
<td></td>
</tr>
<tr>
<td>owamp</td>
<td>Running</td>
<td>4.2.4-1.et7</td>
<td>861</td>
</tr>
<tr>
<td>pscheduler</td>
<td>Running</td>
<td>4.2.4-1.et7</td>
<td></td>
</tr>
<tr>
<td>pconfig</td>
<td>Running</td>
<td>4.2.4-1.et7</td>
<td></td>
</tr>
<tr>
<td>twamp</td>
<td>Running</td>
<td>4.2.4-1.et7</td>
<td>862</td>
</tr>
</tbody>
</table>

Test Results (22 Results)

Search: 

Results for the last... 1 week
Data Transfer Node

• The DTN is dedicated to data transfer
• Set up specifically for high-performance data movement
  – System internals (BIOS, firmware, interrupts, etc.)
  – Network stack
  – Storage (global filesystem, Fibrechannel, local RAID, etc.)
  – High performance tools
  – No extraneous software
• Limitation of scope and function is powerful
  – No conflicts with configuration for other tasks
  – Small application set makes cybersecurity easier

Data transfer test from Berkeley, CA to Argonne, IL (near Chicago). RTT = 53 ms, network capacity = 10Gbps.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>scp</td>
<td>140 Mbps</td>
</tr>
<tr>
<td>HPN patched scp</td>
<td>1.2 Gbps</td>
</tr>
<tr>
<td>ftp</td>
<td>1.4 Gbps</td>
</tr>
<tr>
<td>GridFTP, 4 streams</td>
<td>5.4 Gbps</td>
</tr>
<tr>
<td>GridFTP, 8 streams</td>
<td>6.6 Gbps</td>
</tr>
</tbody>
</table>

Note that to get more than 1 Gbps (125 MB/s) disk to disk requires properly engineered storage (RAID, parallel filesystem, etc.)
Globus: Parallel High Speed Data Movement

- GridFTP Protocol
- Suspend-Resume Transfers
- Federated Authentication
It Does Other Things too
Science DMZ Superfecta: Engagement

Data Transfer Node
- High performance
- Configured for data transfer
- Proper tools

Science DMZ
- Dedicated location for DTN
- Proper security
- Easy to deploy - no need to redesign the whole network

Engagement with Network Users

Performance Testing & Measurement

Network Architecture

Dedicated Systems for Data Transfer

perfSONAR
- Enables fault isolation
- Verify correct operation
- Widely deployed in ESnet and other networks, as well as sites and facilities

Engagement
- Partnerships
- Education & Consulting
- Resources & Knowledgebase

© 2015, The Regents of the University of California, through Lawrence Berkeley National Laboratory and is licensed under CC BY-NC-ND 4.0
Engagement As A Service… Sort Of

- One-on-one engagement with researchers and labs
- End-to-end performance measurement
- Guidance setting up globus
- Coordination with other campuses and regional networks

The Engagement and Performance Operations Center is a collaborative focal point for operational expertise and analysis jointly led by Indiana University (IU) and the Energy Sciences Network (ESnet). EPOC provides researchers with a holistic set of tools and services needed to debug performance issues and enable reliable and robust data transfers. By considering the full end-to-end data movement pipeline, EPOC is uniquely able to support collaborative science, allowing researchers to make the most effective use of shared data, computing, and storage resources to accelerate the discovery process.
The Wizard Gap

Ratio of effective network performance attained by an average user to that attainable by a network *wizard*...
Security Considerations: What to do in the absence of a perimeter firewall

Enable **high performance** data transfer while maintaining adequate **security**.

- Reduce the network visible attack surface: Don’t run anything else on the DTN, minimize exposed ports
- Host level firewalls on DTNs
- Patch aggressively
- User training on e.g. phishing
- Few user accounts on DTNs
- 2-factor authentication, strong passphrase requirements
- Employ Intrusion Detection System to monitor a copy of all traffic
- Encrypt data in flight
ASU Science DMZ
### NSF CC* Proposal

**CC* Networking Infrastructure: Science DMZ for Data-enabled Science, Engineering, and Health**

**NSF Org:** Office of Advanced Cyberinfrastructure (OAC)

<table>
<thead>
<tr>
<th>Driver</th>
<th>Project</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.1 Spence</td>
<td>X-ray Free-e-laser</td>
<td>20-80TB weekly</td>
</tr>
<tr>
<td>C.2 Williams</td>
<td>Cryo-EM biomolecule</td>
<td>10TB / 3.5 days</td>
</tr>
<tr>
<td>C.3 Liang</td>
<td>Medical imaging</td>
<td>5 TB / day</td>
</tr>
<tr>
<td>C.4 Krajmalnik-Brown</td>
<td>Microbes/health</td>
<td>10 TB / 2 weeks</td>
</tr>
<tr>
<td>C.5 Georgescu</td>
<td>Urban climate</td>
<td>100 TB / experiment</td>
</tr>
<tr>
<td>C.6 Vivoni</td>
<td>Water supply</td>
<td>76 TB / project</td>
</tr>
<tr>
<td>C.7 Salamanca</td>
<td>Ag/Urban modeling</td>
<td>.5 TB weekly</td>
</tr>
<tr>
<td>C.8 Jacobs/Bowman</td>
<td>Early universe</td>
<td>5TB / day</td>
</tr>
<tr>
<td>C.9 Wahal</td>
<td>Financial trading</td>
<td>524 TB / year</td>
</tr>
<tr>
<td>C.10 Sankar</td>
<td>Power grid</td>
<td>100GB / month</td>
</tr>
<tr>
<td>C.11 Munk</td>
<td>Biochem course</td>
<td>Real-time viz</td>
</tr>
</tbody>
</table>

**Initial Amendment Date:** June 29, 2020

**Latest Amendment Date:** June 29, 2020

**Award Number:** 2018886

**Award Instrument:** Standard Grant

**Program Manager:**
- Kevin Thompson
  - OAC Office of Advanced Cyberinfrastructure (OAC)
  - CSE Direct For Computer & Info Scie & Engnr

**Start Date:** July 15, 2020

**End Date:** June 30, 2022 (Estimated)

**Awarded Amount to Date:** $494,273.00

**Investigator(s):**
- Douglas Jennewein douglas.jennewein@asu.edu (Principal Investigator)
- Lalitha Sankar (Co-Principal Investigator)
- James McCabe (Co-Principal Investigator)
- Chris Kurtz (Co-Principal Investigator)
- Barbara Munk (Co-Principal Investigator)

**Sponsor:**
- Arizona State University
- ORSPA
- TEMPE, AZ 85281-6011 (480)965-5479

**NSF Program(s):** Campus Cyberinfrastructure

[Link to NSF proposal](https://www.nsf.gov/awardsearch/showAward?AWD_ID=2018886)
Current State

• Deployed amid an existing WAN overhaul
  o Moving to fiber ring topology across points of presence
  o Central IT Deploying SDN

• All Campus Equipment Installed, Brought online December 2020

• Additional pair of border routers en route for off-campus data center at Iron Mountain Phoenix
Current State

- Deployed VM environment to run:
  - ARTEMIS – BGP Hijacking protection
  - ZEEK IDS
  - Spoofer

- Bare metal FIONA DTN to run
  - Globus
  - Containerized(?) PerfSONAR

- Piloting new HPC access node for interactive sessions via OpenOnDemand, specific use cases
Current State

Working with IU on NetSAGE deployment at the Sun Corridor Network, AZ’s state R&E network

Working with EPOC for on-campus deep dives with faculty and research computing staff
Equipment

Arista 7280R3 pair at Tempe campus data center

- Maintained by ASU Central IT
- Additional pair for Iron Mountain data center coming soon
- 32x100GbE ports, 4x400GbE
- 100 GbE feeds from both campus network cores
- MPLS/BGP/VXLAN
- Feeds to:
  - Research Computing, HPC, VMs
  - Science DMZ use cases
  - Servers in campus data center
Equipment

Servers at Campus Data Center

• Globus DTN / PerfSONAR (100GbE+)
• “Infrastructure” HCI VMs (40GbE+)
  o ARTEMIS (BGP Monitoring)
  o SPOOFER (anti IP spoofing)
  o Honeypots / Blackholes
  o Other FOSS Security Tools
  o Science DMZ User VMs
  o HPC login node testing (Science DMZ-style firewall avoidance)
Figure 1: Existing ASU Border, Research Computing, and Researcher Access
Figure 2: Next Generation Network (NgN) and Research Networks
Questions?

Click on the chat icon to type a question
Community Updates

- Trusted CI Webinar: **Mon May 24th** at 11am Eastern
  Topic: Identifying Vulnerable GitHub Repositories
  Presenters: Sagar Samtani, Indiana University

- ResearchSOC webinar: "Building a vulnerability management workflow that works, and getting the buy-in to implement it," Thursday, May 27th, 3pm Eastern.
  [researchsoc.iu.edu/training/webinars.html](researchsoc.iu.edu/training/webinars.html)

- Trusted CI Framework, previously recorded webinar
  [https://www.youtube.com/watch?v=G9V2nbZ-1hQ](https://www.youtube.com/watch?v=G9V2nbZ-1hQ)

- Trusted CI podcast version of webinars coming soon!
About the Trusted CI Webinar series

To view presentations, join the announcements mailing list, or submit requests to present, visit: trustedci.org/webinars or email webinars@trustedci.org

Next Webinar: Mon May 24th at 11am Eastern
Topic: Identifying Vulnerable GitHub Repositories
Presenters: Sagar Samtani, Indiana University