Network Security and the Science DMZ

Jim Basney and John Zage

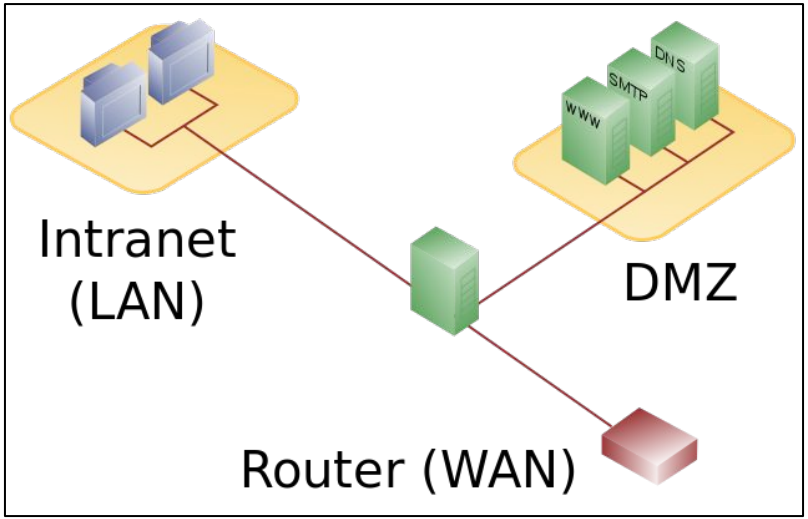
This material is based upon work supported by the National Science Foundation under grant number 1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Outline

- Intro to Science DMZ
- Network Security Challenges for Science DMZ
- Network Intelligence Sharing for Science DMZ
- Hands-on with Science DMZ security

What is a network DMZ?

- A "demilitarized zone" or perimeter network that is exposed to the internet



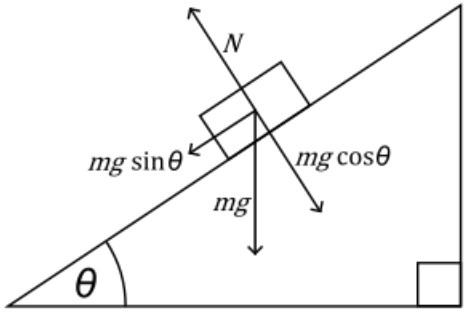
By en:User:Pbroks13 - http://en.wikipedia.org/wiki/Image:DMZ_network_diagram_1_firewall.png, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4045242

The Science DMZ* in 1 Slide

Consists of **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 Online and GridFTP
- Performance measurement/test node
  - perfSONAR
- Engagement with end users

Details at http://fasterdata.es.net/science-dmz/



globus

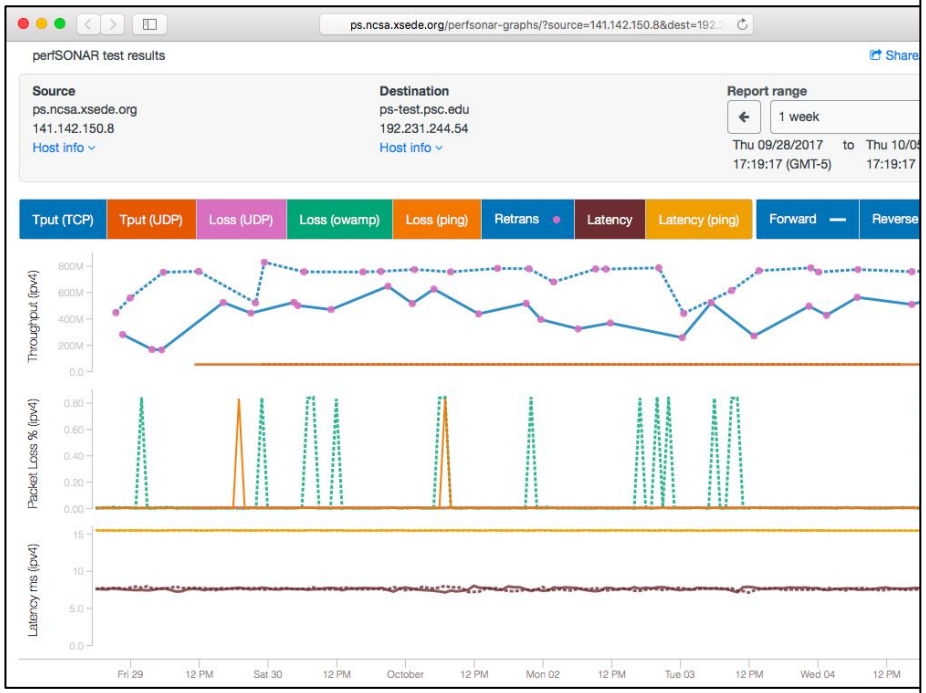
perfSONAR

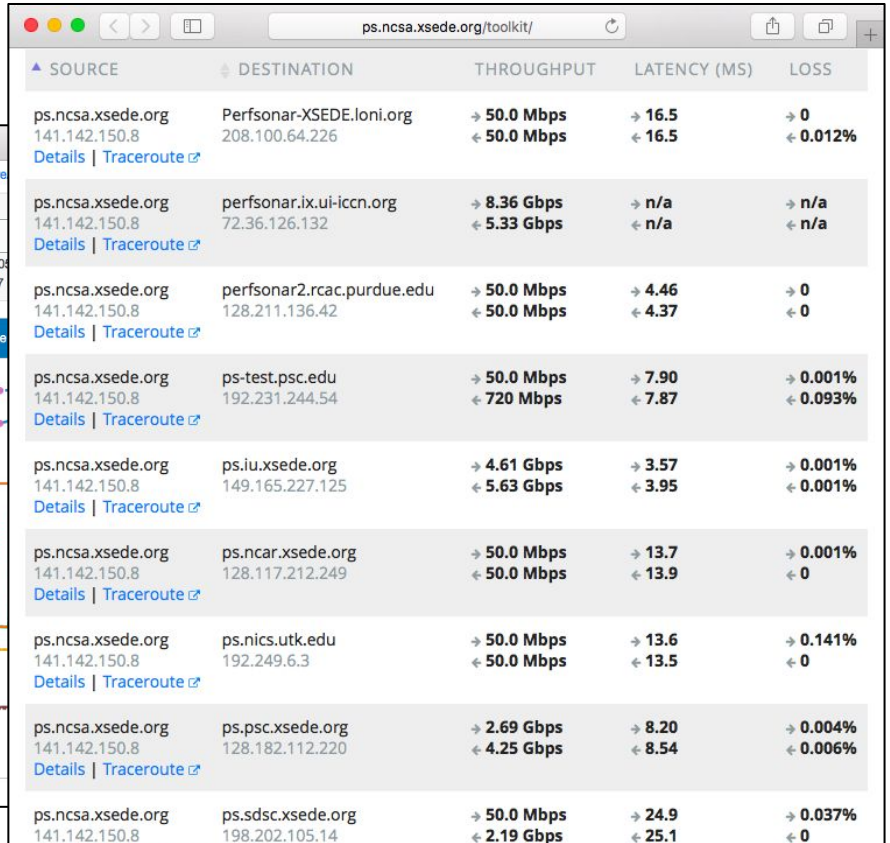
ESnet

* ***Science DMZ*** is a trademark of The Energy Sciences Network (ESnet)

Monitoring the Science DMZ - perfSONAR

- http://ps.ncsa.xsede.org/





Network Security Challenges for Science DMZ

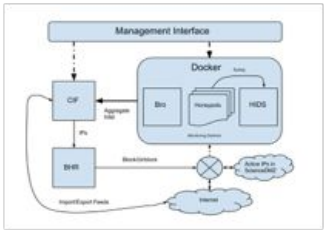
- International research collaborations = external users
- Sharing BIG DATA - legitimate network requests can look like attacks
  - striped data transfers look like DoS attack
  - data replication to/from many sites
- Need to avoid the "firewall bottleneck"
- Operating an "open network"
  - University: Science DMZ is a dedicated network area
  - Supercomputer Center: most of the LAN is the Science DMZ
- Access to powerful services: remote job submission, large data transfer

Network Intelligence Sharing for Science DMZ

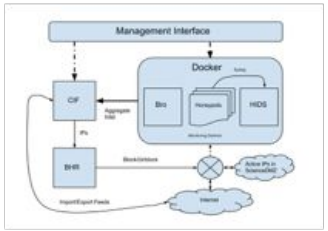
- Research collaborators use Science DMZs at multiple universities
  - Common threats to Science DMZs across many universities
- Share intelligence across Science DMZs to enhance threat detection
  - Threats seen in multiple location can provide deployments an edge
- Threat intelligence data can also be used for cyber security research
- Visibility into activity at the perimeter and provide the ability to act on it
  - Network monitoring equipment (i.e. taps, aggregators) in high throughput networks
- Result: Enhancing the security of the Science DMZ model

Intelligence Sharing Example

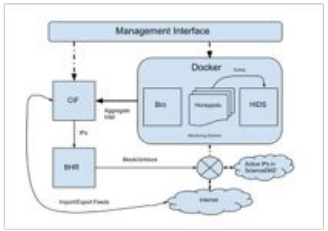
SSH brute force attempt:
srcip 1.1.1.1
<login name list>



Site A



Site B

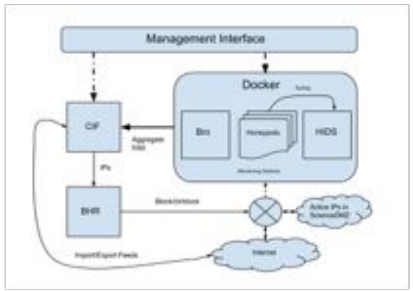


Site C

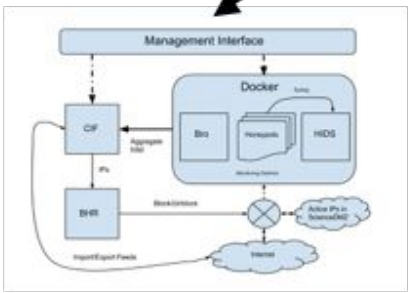
Intelligence Sharing Example

SSH brute force attempt:
srcip 1.1.1.1
<login name list>

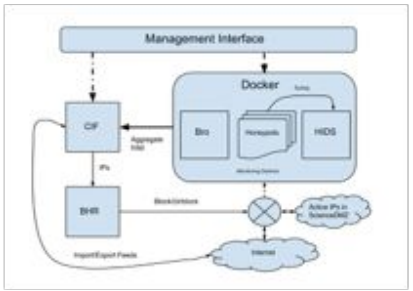
Alert other sites



Site A



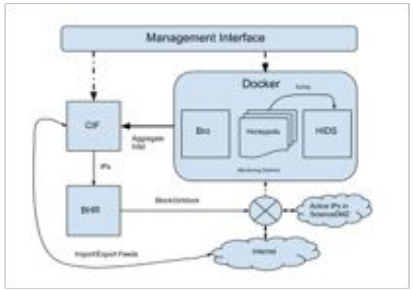
Site B



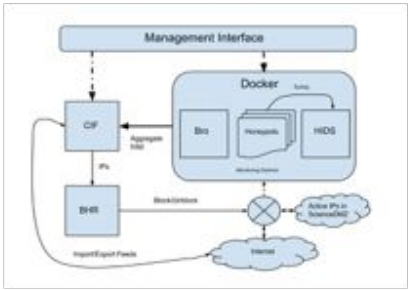
Site C

SSH brute force attempt:
srcip 2.2.2.2
<login name list>

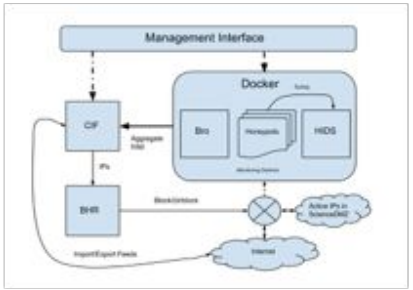
SSH brute force attempt:
srcip 1.1.1.1
<login name list>



Site A



Site B

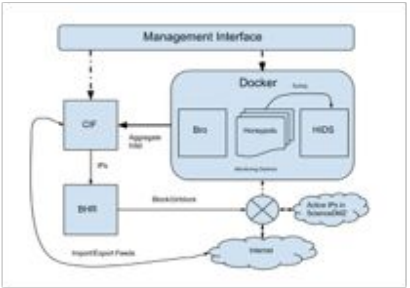


Site C

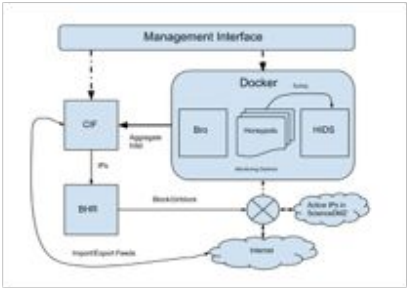
SSH brute force attempt:
srcip 2.2.2.2
<login name list>

SSH brute force attempt:
srcip 1.1.1.1
<login name list>

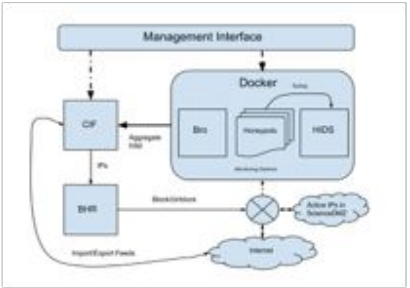
login name list identical



Site A



Site B



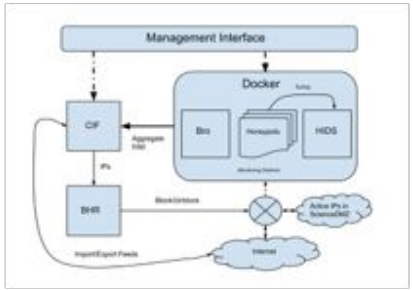
Site C

SSH brute force attempt:
srcip 2.2.2.2
<login name list>

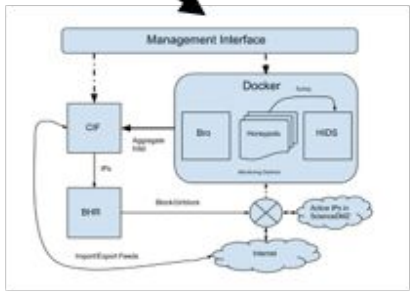
SSH brute force attempt:
srcip 1.1.1.1
<login name list>

login name list identical

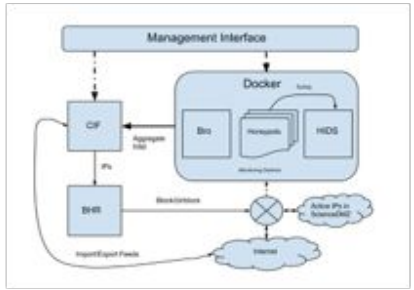
New event with increased confidence



Site A



Site B



Site C

Hands-on with Science DMZ security

More info

- Related videos on CTSC's YouTube channel (https://trustedci.org/webinars)
  - The Science DMZ as a Security Architecture
  - Demystifying Threat Intelligence
- https://fasterdata.es.net/science-dmz/