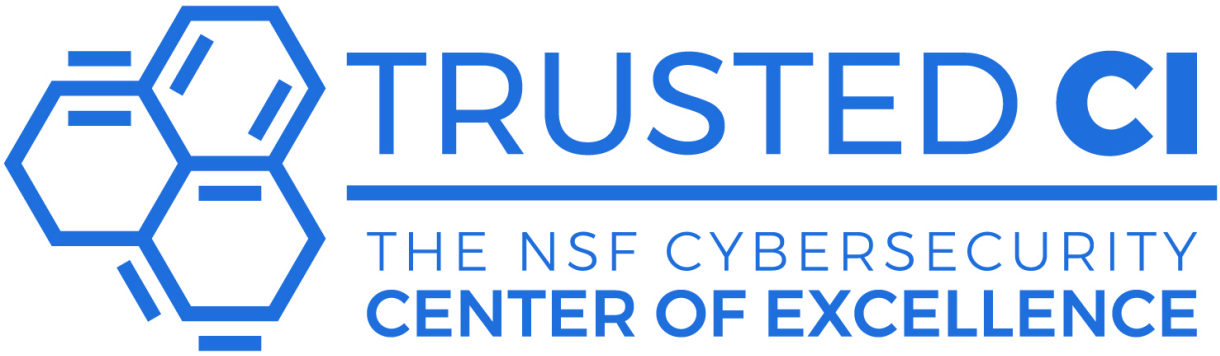

Science DMZ

Secure High Performance Data Transfer

January 6th, 2022

Status: V1

Distribution: Public

Ishan Abhinit, Hans Addleman, Kathy Benninger, Don DuRousseau, Mark Krenz, Brenna Meade

About Trusted CI

The mission of Trusted CI is to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and what is needed to achieve and maintain an appropriate cybersecurity program.

About EPOC

The Engagement and Performance Operations Center (EPOC) was established in 2018 as a collaborative focal point for operational expertise and analysis and is 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.

About DART

The Arkansas NSF EPSCoR Data Analytics that are Robust and Trusted (DART) program[1] was awarded July 1, 2020 and will fund cutting-edge data science research and education around the state. DART is a multi-institutional, interdisciplinary, statewide grant program leveraging $24 million over 5 years to expand research, workforce development, and science, technology, engineering, and mathematics (STEM) educational outreach in Arkansas. The program is administered by the Arkansas Economic Development Commission (AEDC) Division of Science and Technology to maximize resources available to support the advancement of STEM in Arkansas.

The DART project engaged with Trusted CI and EPOC in the 2nd half of 2021 to seek assistance with the networking design and security of their Science DMZ implementation.

[1] https://www.arkansasedc.com/science-technology/division/data-analytics-that-are-robust-trusted-(dart)

Acknowledgments

We would like to thank the following non-author collaborators who have helped us to create this document. Trusted CI's engagements are inherently collaborative; the authors would like to thank the DART project staff at University of Arkansas, UAMS, and ARE-ON for the collaborative effort that made this document possible.

This document is a product of Trusted CI. Trusted CI is supported by the National Science Foundation under Grant #1920430. For more information about Trusted CI, please visit: http://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

Cite this work using the following information:
Ishan Abhinit, Hans Addleman, Kathy Benninger, Don DuRousseau, Mark Krenz, Brenna Meade
"Science DMZ: Secure High Performance Data Transfer," December 2021
https://hdl.handle.net/2022/27007

Executive Summary 5

The Science DMZ 5

The Need 6

The Challenge 7

The Concern 7

Benefits of the Science DMZ model 7

Addressing the Security Concerns 8

Cybersecurity Program/Framework/Control Set and the Science DMZ 8

Security without the Traditional Firewall Box 8

The Role of ACLs 9

The Role of Network Monitoring and Intrusion Detection 10

Securing the Servers 11

Designing and Building Your Science DMZ 13

Testing Your Science DMZ 14

Additional Security Techniques 14

Conclusion 15

References and Resources 16

Footnotes in this document 16

Additional information 18

Executive Summary

This whitepaper addresses three Science DMZ documentation needs of the cyberinfrastructure and cybersecurity communities:

1. Provide an introduction to the Science DMZ concept and purpose for CISOs and other managers with cybersecurity responsibility.
2. Provide an overview and technical information of security best-practices and techniques for networking, systems, and security personnel responsible for implementing a Science DMZ.
3. Provide references to more in depth reading and implementation guidance.

The Science DMZ

From the Energy Sciences Network (ESnet) Science DMZ homepage[2]:

Science DMZ - A Scalable Network Design Pattern for Optimizing Science Data Transfers
The Science DMZ is a portion of the network, built at or near the campus or laboratory's local network perimeter that is designed such that the equipment, configuration, and security policies are optimized for high-performance scientific applications rather than for general-purpose business systems or "enterprise" computing.

Developed by ESnet engineers, the Science DMZ model addresses common network performance problems encountered at research institutions by creating an environment that is tailored to the needs of high performance science applications, including high-volume bulk data transfer, remote experiment control, and data visualization.

The Science DMZ is scalable, incrementally deployable, and easily adaptable to incorporate high performance and advanced technologies such as 100 Gigabit Ethernet services, virtual circuits, and software-defined networking capabilities.

Key Components

[2] https://fasterdata.es.net/science-dmz/

A Science DMZ integrates four key concepts into a unified whole that together serve as a foundation for this model. These include:

- *A network architecture explicitly designed for high-performance applications, where the science network is distinct from the general-purpose network*
- *The use of dedicated systems for data transfer*
- *Performance measurement and network testing systems that are regularly used to characterize the network and are available for troubleshooting*
- *Security policies and enforcement mechanisms that are tailored for high performance science environments*

The Need[3]

High performance data transfer capability has become integral to scientific and data-intensive research. Workflows often comprise data acquisition/creation, transfer, storage, and processing. Data transfer becomes increasingly important as the data creation/acquisition is done at a resource location (e.g., a scientific simulation, an electron microscopy lab, an optical or radio telescope, a geologic sensor array) and the resulting data sets need to be transferred to another site for storage and/or processing. With research data set size now terabytes, and even petabytes, acceptable workflow performance requires efficient, rapid data transfer. For example, a reasonable expected throughput rate for a well-tuned, 10Gbit/sec-based Science DMZ is 1TB/hour (2.22 Gbits/sec)[4].

NSF, NIH, DoE, and DoD require conformity of the nation's research cyberinfrastructure (CI) to provide a comprehensive, integrated, sustainable, and secure platform to accelerate research and education in computational and data-intensive science and engineering.[5]

[3] https://fasterdata.es.net/science-dmz/motivation/

[4] https://fasterdata.es.net/performance-testing/2019-2020-data-mobility-workshop-and-exhibition/

[5] NIST Cyberinfrastructure Framework for 21st Century Science and Engineering (CIF21) https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504730

NSF proposals must be prepared in the context of a coherent campus-wide strategy and approach to CI that is integrated horizontally intra-campus and vertically with regional and national CI investments and best practices.

The Challenge

Sustained, high speed data exchange with external collaborators, or even between departments within the same institution, is often not among the design priorities of a campus network. Research data flows typically share the same network paths, and are subject to the same firewall overhead, as business process and personal productivity software. All applications compete for the available bandwidth. As a result, the bursty nature of relatively short user application traffic (e.g., document editing, browser requests, email, database lookup), along with the overhead imposed by firewall packet inspection, disrupts and impedes the flow of research datasets.

The Concern

The Science DMZ architecture[6] explicitly states that security is implemented by policies and techniques that DO NOT include the traditional firewall that is often viewed as the fundamental component for providing network security. Upon reviewing this design, the concern often expressed by management and senior leadership about Science DMZ deployment is, "How can I be sure this design is secure?"

Benefits of the Science DMZ model

The Science DMZ is explicitly designed for high-performance large dataset transfer, comprising infrastructure that is separate and distinct from the general-purpose network. Rather than relying on a single device, i.e., a firewall, to address all security needs, servers in the Science DMZ are protected by several straightforward cybersecurity concepts and mechanisms that can be tailored to fit the institution's needs. Placing these high bandwidth transfers outside the general-purpose network also has the benefit of reducing the load on enterprise network devices. The

[6] https://fasterdata.es.net/science-dmz/science-dmz-architecture/

configuration choices for securing a Science DMZ can support a range of security postures.

Addressing the Security Concerns

As stated in the previous section, Science DMZ services are targeted toward high performance data transfer. Thus, the security controls and cyberinfrastructure that are recommended for this type of environment must work in concert toward achieving that goal.

Cybersecurity Program/Framework/Control Set and the Science DMZ

The implementation choices for the Science DMZ will be made based on the organization's cybersecurity program and its underlying cybersecurity framework and control set. The framework and control set will guide the cybersecurity team through decisions regarding identification of the assets to be protected, access control, and network and server security management. The security of the Science DMZ network depends on cooperation between an organization's cybersecurity, network, and systems teams, so it is recommended that they meet regularly to raise and discuss issues.[7]

Security without the Traditional Firewall Box

One of the aims of this whitepaper is to clarify the role of a "firewall" with respect to a Science DMZ. Unfortunately, this topic has generated a great deal of confusion and skepticism between cyberinfrastructure (CI) engineers and their information security office (ISO, and particularly CISO) colleagues. A significant complicating factor is that traditional firewall devices, with stateful deep packet inspection and other sophisticated capabilities, which can truly support the high performance bandwidth needs of a Science DMZ are prohibitively expensive for most research budgets. Beware of vendors who claim otherwise! While the perception of the Science DMZ architecture is "no firewall, period", basic ***firewall functionality*** is, in fact, strongly recommended through the use of a multi-pronged security

[7] https://www.youtube.com/watch?v=IPh3aZ18IuY, Best practices for Securing the Science DMZ by Nick Buraglio

approach[8] including access control lists (ACLs)[9] and intrusion detection systems (IDSs). In combination these network security mechanisms implement key functions of a firewall device without the performance penalty and cost imposed by such a firewall. Each of these security techniques is commonly used and well-understood within the networking and security communities.

The Role of ACLs

ACLs provide light-weight, stateless, firewall functionality when configured on the network routers/switches in the Science DMZ path. Router and switch ACLs are implemented at network Layer 2 or Layer 3. ACL rules are most commonly configured based on source and/or destination IP addresses or address ranges, VLANs, protocol port numbers, or network protocol and can filter incoming as well as outgoing packets. The allowed IP addresses will include your collaborators' servers and clients. VLAN numbers might be used to separate traffic within your site. Permitted port numbers and network protocols will likely be determined by the application requirements, for example the Globus server TCP listening ports[10]. Following the equipment manufacturer's instructions for creating ACLs and which types of ACLs are supported and can coexist is key to a successful implementation.

Access control can similarly be implemented on the hosts residing in the Science DMZ. These hosts, which are typically Linux platforms, support nftables[11], firewalld[12], and the older iptables[13] tools to create and manage host ACLs. The packet filtering offered by these tools is also based on IP address, VLAN, port numbers, or network protocol. See RedHat's "Getting Started with nftables"[14] for a succinct comparison and suggestions on when to use nftables, firewalld, or iptables. Nftables may be the better option in the case of a ScienceDMZ, because it is higher performance than iptables. Firewalld is a frontend that can manage either iptables or nftables rulesets at the lower level interface.

---

[8] https://fasterdata.es.net/science-dmz/science-dmz-security/best-practices-for-science-dmz-security/
[9] https://fasterdata.es.net/science-dmz/science-dmz-security/
[10] https://docs.globus.org/globus-connect-server/v5/#open-tcp-ports_section
[11] https://www.netfilter.org/projects/nftables/index.html
[12] https://firewalld.org/
[13] https://www.netfilter.org/projects/iptables/index.html
[14] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/getting-started-with-nftables_configuring-and-managing-networking

Wherever ACLs are configured, on routers, switches, or hosts, they secure the Science DMZ by dropping traffic between the Science DMZ hosts/services and any disallowed sources/destinations.

The Role of Network Monitoring and Intrusion Detection

A Science DMZ network is usually not intended to allow general access from arbitrary hosts on the Internet, thus it is important to monitor the network for unexpected traffic. At a minimum, it is recommended that network flow information be logged from the router or switch so that you have a record of what hosts are communicating over the network. To meet this need, Science DMZ security best practices recommend deployment of network-based and host-based intrusion detection systems (NIDS[15] and HIDS[16]). IDSs monitor network traffic, system access, and usage patterns in real-time and generate flow log entries and alarms when an anomaly is detected.

Router and switch network flow information (e.g., Cisco's NetFlow, Juniper's Jflow/cflowd, IEEE standard IPFIX, sFlow, etc.; the specific format is based on equipment vendor or open standards) is exported to a flow collector for analysis. On a regular basis the network flow log should be reviewed and ACLs can be adjusted if something unexpected and unauthorized is happening on the network. Toolsets such as the open source nfdump[17], along with its web based companion front end NfSen[18], can be used to collect, process, and display flow data and the results of flow data queries. Example output might be a list of 'top talkers' or a focused view of traffic during a specific time period.

A more advanced form of network monitoring and response is available through the use of an IDS such as Snort[19] or a Network Security Monitor (NSM) such as Zeek[20], both of which are commonly used in network cybersecurity infrastructure. Like network flow analysis, these network monitors can passively listen on the network

[15] https://fasterdata.es.net/science-dmz/science-dmz-security/network-ids/
[16] https://fasterdata.es.net/science-dmz/science-dmz-security/host-ids/
[17] https://github.com/phaag/nfdump
[18] http://nfsen.sourceforge.net/
[19] https://www.snort.org/
[20] https://zeek.org/

and alert on unexpected traffic. Zeek's protocol decoding functionality, while requiring specialized expertise to install and manage, offers a much broader range of packet analysis capability and customization as compared to the nfdump network flow analysis described above. Adding a Zeek NSM requires staff expertise and investment by the organization. There are also third party support providers who specialize in Zeek setup and support. One such company is Corelight[21].

Automated threat response other than sending an alert by routers/switches must be carefully designed and implemented because of the wide-ranging impact a false alarm could have.

Host IDSs can actively respond by installing traffic filters to block unauthorized access attempts. This automated functionality augments traffic blocking by the ACLs that have been set by the Science DMZ administrators. Fail2ban[22] is a commonly used host IDS utility that scans log files and bans IP addresses that show, for example, too many password failures or probing for exploits. The standard fail2ban response is to update the host ACL to reject the suspect IP address for some period, however, other actions may be configured. This type of host automated response is often used and has impact localized to the specific host.

Securing the Servers

Approaches for securing the Science DMZ are grounded in server cybersecurity best-practices as well as the standard network security techniques described above. End hosts and services that reside in the Science DMZ rely on Data Transfer Node (DTN) and perfSONAR cybersecurity best-practices. First is using a secure operating system. Linux offers many of the tools that are frequently used by the Science DMZ community and has a long tradition of being used on the open Internet. DTNs typically run on Linux[23] and it is the only operating system for installing native perfSONAR nodes[24]. Limiting offered services to data transfer application(s) and performance measurement improves security of the Science DMZ by employing the principle of minimization[25]. For example, running Globus Online

[21] https://corelight.com/
[22] https://www.fail2ban.org/
[23] https://fasterdata.es.net/science-dmz/DTN/
[24] http://docs.perfsonar.net/install_options.html
[25] https://cacr.iu.edu/principles/index.html

and/or Aspera as the only major service(s) on the DTN eliminates the vulnerability of access via unnecessary services. Globus offers several options for authentication/authorization including federated identity management[26,27] that can be implemented for secure user access and management. See the Globus Security FAQ[28] for additional configuration guidance. Creating an inventory of only the services that are needed is useful for consistent server management. It is also recommended that the DTN does not run a desktop graphical environment such as X Windows and that other services that may be enabled by default, such as print services, are disabled. The SSH service is usually needed to provide administrator access to the host.

Running a security assessment tool such as 'lynis'[29] can help determine the secure posture of the host and will provide recommendations for improvement. In order to help detect rootkits and other malware that have been placed on a host, system administrators should regularly run a tool like 'rkhunter'[30] on the DTN and other hosts in the Science DMZ.

Outside vulnerability scanning can provide you with notification of exposed services that may be vulnerable to attack. In a more exposed environment such as a Science DMZ, it is important to routinely scan the hosts inside the Science DMZ for vulnerabilities that attackers may be able to exploit. If you are utilizing black hole routing, IDS or intrusion prevention system (IPS), it is important to allow-list the sanctioned scanners' source addresses so that you do not inadvertently block them from scanning. In dual stacked environments such as those implementing both IPv4 and IPv6, it is important to ensure that security controls are enabled for both protocol stacks.[31]

The Science DMZ's perfSONAR[32] network performance measurement nodes are installed using a complete perfSONAR open source, Linux-based, "Toolkit" package.

---

[26] https://docs.globus.org/security/authorization-authentication-v54/
[27] https://docs.globus.org/security/high-assurance-overview/
[28] https://docs.globus.org/faq/security/
[29] https://cisofy.com/lynis/
[30] http://rkhunter.sourceforge.net/
[31] Best practices for Securing the Science DMZ by Nick Buraglio, Youtube
[32] https://www.perfsonar.net/

The software distribution includes a default set of iptables/firewalld rules[33] and fail2ban intrusion detection to secure the system[34]. perfSONAR development and support are active so following standard best-practices of keeping the server up to date and watching the perfSONAR email list[35] for security announcements will help ensure the ongoing security of the platform. A site may also want to limit access to test requests from perfSONARs on Research and Education (R&E) networks[36].

There are additional recommended best-practices that can improve system security, but their implementation will depend on the operational and system management model at your site. These include management of the hosts in the Science DMZ through a configuration management system such as Ansible, Puppet, or Chef and the collection of syslog data in a centralized log aggregator.

Another resource that can be useful for servers in general is documented in Recommendations for Improving the Security of a Science Gateway. These are a few other IU specific resources that can be used as a template for other universities:
https://policies.iu.edu/policies/it-12-security-it-resources/index.html
https://policies.iu.edu/policies/it-28-cyber-risk-mitigation/index.html

Designing and Building Your Science DMZ

A key point to keep in mind is that the Science DMZ network is deployed as separate, dedicated cyberinfrastructure, isolated from the institution's production network. To help meet the costs of this additional infrastructure, universities and colleges, as well as other non-profit, non-academic organizations, are encouraged to investigate the availability of funding through NSF's Campus Cyberinfrastructure (CC*)[37] program. A second key point to consider when planning a Science DMZ is choosing modern equipment with specifications that meet, or exceed, the minimum throughput criteria. NSF's Engagement and Performance Operations Center (EPOC)[38] is available to evaluate an institution's Science DMZ requirements and

[33] https://www.perfsonar.net/deployment_security.html#default-firewall-rules-and-requirements
Note that site-specific rules can be added to the default set for more specific access control.
[34] https://www.perfsonar.net/deployment_security.html
[35] https://www.perfsonar.net/about_contact.html
[36] http://docs.perfsonar.net/manage_limits.html
[37] https://beta.nsf.gov/funding/opportunities/campus-cyberinfrastructure-cc
[38] https://epoc.global/

offer design recommendations and advice on equipment selection. EPOC also offers a resources webpage for institutions planning to submit a CC* proposal for funding[39]. NSF's Cybersecurity Center of Excellence (Trusted CI)[40] is available to advise on cybersecurity control set[41] questions with regard to securing a Science DMZ, as well as broader questions an organization may have about how their cybersecurity program and framework related to these issues.

Testing Your Science DMZ

Sites that have deployed a new Science DMZ may want to take advantage of performance testing resources[42] offered by ESnet. These include both data movement testing, such as the the Data Mobility Exhibition program[43] (N.B. The DME is ongoing, despite the 2019-2021 end date on the web page) and performance troubleshooting guidance with recommended tools and techniques. EPOC engineers are available for consultation on performance measurement and debugging.

Additional Security Techniques

In addition to the recommendations made in this document, there are other security controls and techniques that have been implemented by institutions that have reached a level of maturity where they are looking at additional controls to reduce security risk.

Black hole routing[44], or null routing, can be implemented within a regional or campus network to further the overall cybersecurity of the institution by preventing malicious traffic from reaching the destination network. Black hole routing is often implemented by a regional network operator in cooperation with the affected institution, or by the institution itself, to redirect malicious or otherwise unwanted

[39] https://epoc.global/cc/
[40] https://www.trustedci.org/
[41] https://www.trustedci.org/framework
[42] https://fasterdata.es.net/performance-testing/
[43] https://fasterdata.es.net/performance-testing/2019-2020-data-mobility-workshop-and-exhibition/2019-2020-data-mobility-exhibition/
[44] https://fasterdata.es.net/science-dmz/science-dmz-security/black-hole-routing/

network traffic to a “black hole”, or null route. Any such traffic is then lost, so care must be taken when deploying black hole routing.

Honeypots, which are decoy hosts used to detect malicious scanning and attacks, can identify new threats to the Science DMZ network. This information may be used to help determine what remote addresses may be of interest for black hole routing or to help determine the techniques being used by attackers and if they are specifically targeting the assets of the Science DMZ.

Conclusion

In this paper we have introduced the concept of the Science DMZ, the need for them in the science research community, and how to reduce the security risk to assets within a Science DMZ network using well understood security controls. For further information on Science DMZs, please see the references below and/or contact Trusted CI at https://trustedci.org/ or EPOC at https://epoc.global/ for more resources and consultation.

References and Resources

Footnotes in this document

1. University of Arkansa Data Analytics that are Robust & Trusted (DART) project https://www.arkansasedc.com/science-technology/division/data-analytics-that-are-robust-trusted-(dart)
2. Introduction to the Science DMZ https://fasterdata.es.net/science-dmz/
3. Motivation for the Science DMZ design https://fasterdata.es.net/science-dmz/motivation/
4. 2019-2021 Data Mobility Workshop & Exhibition - data transfer performance expectations and https://fasterdata.es.net/performance-testing/2019-2020-data-mobility-workshop-and-exhibition/
5. NIST Cyberinfrastructure Framework for 21st Century Science and Engineering (CIF21) https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504730
6. Examples with diagrams and descriptions of a Simple Science DMZ, a Supercomputing Center Network, a Big Data Site, and a Regional Science DMZ "Interchange". https://fasterdata.es.net/science-dmz/science-dmz-architecture/
7. Best practices for Securing the Science DMZ by Nick Buraglio https://www.youtube.com/watch?v=IPh3aZ18IuY
8. Best practices for securing a Science DMZ describes a multiple-pronged approach to implementing security without using a "traditional" firewall box https://fasterdata.es.net/science-dmz/science-dmz-security/best-practices-for-science-dmz-security/
9. Discussion of Firewalls vs. Router ACLs for implementing Science DMZ security https://fasterdata.es.net/science-dmz/science-dmz-security/
10. Globus Connect Server v5 Installation Guide - Open TCP Ports https://docs.globus.org/globus-connect-server/v5/#open-tcp-ports_section
11. netfilter/iptables project homepage - The netfilter.org "nftables" project https://www.netfilter.org/projects/nftables/index.html
12. Firewalld - A service daemon with D-Bus interface https://firewalld.org/
13. The netfilter.org "iptables" project https://www.netfilter.org/projects/iptables/index.html

14. From RedHat: Getting started with nftables
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/getting-started-with-nftables_configuring-and-managing-networking
15. Links to network intrusion detection system resources
https://fasterdata.es.net/science-dmz/science-dmz-security/network-ids/
16. Links to host intrusion detection system resources
https://fasterdata.es.net/science-dmz/science-dmz-security/host-ids/
17. Nfdump network flow data collection, analysis, and visualization toolset
https://github.com/phaag/nfdump
18. NfSen - Netflow Sensor
http://nfsen.sourceforge.net/
19. Snort intrusion detection system
https://www.snort.org/
20. Zeek Network Security Monitor
https://zeek.org/
21. Corelight
https://corelight.com/
22. Fail2ban host intrusion detection tool
https://www.fail2ban.org/
23. Science DMZ: Data Transfer Nodes
https://fasterdata.es.net/science-dmz/DTN/
24. perfSONAR Installation Options and links to downloads
http://docs.perfsonar.net/install_options.html
25. The Information Security Practice Principles (ISPPs) Whitepaper from the Indiana University Center for Applied Cybersecurity Research (CACR, cacr.iu.edu) seeks to provide a foundational mental model for information security problem-solving.
https://cacr.iu.edu/principles/index.html
26. Globus Connect Server v5 Authorization and Authentication
https://docs.globus.org/security/authorization-authentication-v54/
27. Globus High Assurance Security Overview
https://docs.globus.org/security/high-assurance-overview/
28. Globus Security FAQ
https://docs.globus.org/faq/security/
29. Lynis - Security auditing tool for Linux, macOS, and Unix-based systems - CISOfy
https://cisofy.com/lynis/
30. The Rootkit Hunter project
http://rkhunter.sourceforge.net/
31. Best practices for Securing the Science DMZ by Nick Buraglio

https://www.youtube.com/watch?v=IPh3aZ18IuY

32. Homepage for the perfSONAR network performance measurement platform that is part of the Science DMZ design
https://www.perfsonar.net/
33. Adding rules to perfSONAR firewalld
https://www.perfsonar.net/deployment_security.html#default-firewall-rules-and-requirements
34. Overall guide to securing perfSONAR (links to the top of the same page as 13.) including host firewall, fail2ban, and limiting test access.
https://www.perfsonar.net/deployment_security.html
35. Contact information to sign up for perfSONAR email lists and request help
https://www.perfsonar.net/about_contact.html
36. Information for limiting perfSONAR testing to R&E networks
http://docs.perfsonar.net/manage_limits.html
37. NSF Campus Cyberinfrastructure (CC*). Potential funding for building a Science DMZ
https://beta.nsf.gov/funding/opportunities/campus-cyberinfrastructure-cc
38. Engagement and Performance Operations Center (EPOC) homepage
https://epoc.global/
39. EPOC's guide to preparing a proposal for an NSF CC* grant
https://epoc.global/cc/
40. Trusted CI (NSF's Cybersecurity Center of Excellence) homepage
https://www.trustedci.org/
41. Trusted CI Cybersecurity Framework, a tool to help organizations establish and refine their cybersecurity programs
https://www.trustedci.org/framework
42. ESnet reference for network performance tools, testing, and troubleshooting
https://fasterdata.es.net/performance-testing/
43. ESnet's Data Mobility Exhibition homepage
https://fasterdata.es.net/performance-testing/2019-2020-data-mobility-workshop-and-exhibition/
44. Black Hole Routing information. Note that Black Hole Routing is used to enhance the overall regional or site network cybersecurity and is not necessarily implemented within the Science DMZ.
https://fasterdata.es.net/science-dmz/science-dmz-security/black-hole-routing/

Additional information

1. Science DMZ considerations in meeting sensitive data environments (HIPAA, PHI, FISMA)

https://fasterdata.es.net/science-dmz/sensitive-data-environments/

2. Eli Dart's (ESnet) 2016 Science DMZ slide presentation, "The Science DMZ Design Pattern" provides an overview / accessible introduction https://science.nasa.gov/science-pink/s3fs-public/atoms/files/3-2-Science%20DMZ%20Design%20Pattern%20-%20ESNet%20-%20Eli%20Dart_TAGGED.pdf
3. Science DMZ "Deep Dive":
   J. Crichigno, E Bou-Harb, N. Ghani, "A Comprehensive Tutorial on Science DMZ", IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 2041-2078, 2Q2019.
   DOI: 10.1109/COMST.2018.2876086
   https://par.nsf.gov/servlets/purl/10119181
4. High-level description of why the Science DMZ architecture is secure http://www.linuxclustersinstitute.org/workshops/archive/interm19/pdfs/14-Network_Security.pdf
5. Data transfer performance reference material https://fasterdata.es.net/performance-testing/performance-expectations/
6. Reference tables showing how long it takes to move Y bytes in X time (e.g., transferring 1TB of data across a 20Gbps network takes 20 minutes). https://fasterdata.es.net/home/requirements-and-expectations/