Review skalierbarer Netzwerkdesign-Prinzipien zur Optimierung des Campus-Edge für BigData Forschung

Die ScienceDMZ mit Data Transfer Nodes (DTN)

Jakob Tendel [1] [2]

Abstract: Für bandbreitenstarke Datenübertragung ist es erforderlich, dass die Netzwerksysteme bis zu den Endpunkten der Übertragung hin für gute Performance geeignet und konfiguriert sind. Die per TCP Protokoll praktisch zu erreichende Datenrate hat einige Abhängigkeiten mit in Standortnetzwerken auftretenden Faktoren. Dazu gehören Spezifikation und Konfiguration der Endsysteme und Netzwerkkomponenten auf dem Pfad, sowie Quellen von Paketverlust. Der negative Einfluss dieser Faktoren auf den zu erreichenden Durchsatz skaliert nichtlinear mit der Paketlaufzeit, also der Entfernung zwischen den Endpunkten der Verbindung, sodass bei Weitverkehrsverbindungen mitunter gravierende Einbrüche der Datenrate auftreten können. Die koordinierte und konsequente Anwendung einiger gängiger Best-Practices, wie im Folgenden vorgestellt, kann bereits eine erhebliche Durchsatzoptimierung bringen. Im Wesentlichen wird die Entflechtung auf Netzarchitektur-Ebene von bandbreitenstarken BigData Anwendungen und der alltäglichen Nutzung des Campus-Netzwerks empfohlen, damit eingesetzte Komponenten und Architekturen auf die jeweiligen Bedürfnisse optimiert werden können und störende Wechselwirkungen vermieden werden. Die Maßnahmen umschließen die Schaffung eines Hochleistung-Netzsegments mit möglichst direktem Anschluss an den Campusrouter zum Forschungsnetz (der ScienceDMZ) und den Einsatz von optimierten Host-Systemen (Data Transfer Nodes - DTN) in der DMZ. Diese Architektur ist ebenfalls bereits bestens geeignet für den Einsatz zusammen mit software-gesteuerten Forschungsdaten-Portalen oder Research-Gateways mit systematisch automatisiertem Datenaustausch in ortsunabhängigen Forschungsvorhaben.

Keywords: Forschungsnetz, BigData, Paketverlust, ScienceDMZ, DTN.

1 Einleitung

Die Übertragung großer Forschungsdatensätze über große Entfernungen wird für die zunehmend internationalen Forschungsvorhaben immer wichtiger. Beispiele für Datenmengen in Petabyte-Größenordnung sind Klimadaten, Genomdaten, Satellitenbilder, oder Physik-Experimente, welche Forschungsgruppen mitunter über Kontinente hinweg miteinander austauschen. Für praktikabel zeitnahe Anwendungen sind hier dauerhafte Datenraten im Gigabit bzw. multi-10Gigabit Bereich für einzelne Verbindungen („Flows“) notwendig, ein im regulären LAN und Internet-Bereich

[1] DFN-Verein e.V., Alexanderplatz 1, 10178 Berlin, tendel@dfn.de
[2] GÉANT Association

unübliches und daher nicht standardmäßig optimal unterstütztes Verkehrsmuster. Die erreichbaren Datenübertragungsraten solcher Flows sind trotz der hierfür speziell optimierten Forschungsnetze abhängig von Netz-Architekturen und Systemen in Einrichtungen an beiden Enden. Dieser Review-Artikel stellt die grundlegende Problematik des Performanceverlusts vor, geht auf Lösungsansätze wie die ScienceDMZ ein, und stellt einige praktische Umsetzungen vor. Es wird eine Sammlung von Design-Prinzipien und Technologie-Bausteinen vorgestellt, wie Systeme und Netz am Campus-Edge zum Forschungsnetz optimal gestaltet werden können. Ziel ist es, BigData Spitzenforschung und alltägliche Nutzung des Campus-Netzes bei Wahrung der notwendigen IT-Sicherheit in Einklang zu bringen.

2 Problemstellung

Ein möglich auftretender Effekt bei der Übertragung von Daten über große Entfernungen ist eine mit steigender Entfernung stark nachlassende Übertragungsrate, während im lokalen Netzwerk die theoretisch zu erreichende Datenrate meist zufriedenstellend approximiert werden kann. Selbstverständlich liegen diverse mögliche Fehlerquellen und Flaschenhälse auf der Strecke zwischen den Endpunkten, z.B. Überlast oder asymmetrisches Routing, die allesamt die Datenrate stark beeinträchtigen können. Forschungsnetze sind jedoch gezielt optimiert und überwacht, um solche Fehlerquellen zu minimieren.

An dieser Stelle wird konkret auf Störfaktoren rund um die Endpunkte von Flows, also von Verbindungen über das TCP-Protokoll, eingegangen. Die Literatur z.B. [Da13] beschreibt mehrere Fehlerquellen und Einflussgrößen, welche in Kombination die zu beobachtenden Leistungsverluste ergeben. Diese gliedern sich grob in nicht-optimierte Software und Hardware sowie Paketverlust.

2.1 Das TCP Protokoll

Den meisten Verfahren zur Übertragung von Datensätzen über Computer-Netzwerke liegt das TCP Protokoll (engl. "Transmission Control Protocol") zugrunde, essentieller Bestandteil der Familie der Internet-Protokolle zur paketvermittelten Kommunikation. Es stellt mittels automatischer Mechanismen zur Synchronisierung und Bestätigung (Three-Way-Handshake) zwischen zwei Endpunkt-Systemen eine Verbindung für den zuverlässigen Austausch von Datenpaketen her.

2.2 TCP Einstellungen für lange Strecken

TCP hat Mechanismen zur Flusssteuerung und Überlaststeuerung, um möglichst zuverlässigen Datendurchsatz zu ermöglichen. Diese benötigen jedoch für den jeweiligen

Anwendungsbereich adäquate Einstellungen, um nicht selbst zur Durchsatzbremse zu werden. In einer Situation mit langen Umlaufzeiten („Round-Trip-Time“; RTT) ab ca.10-20ms kann eine fehlerfreie Übertragung unter Umständen trotzdem ein timeout und damit eine unnötige wiederholte Übertragung („Retransmission“) veranlassen. Bei bandbreitenstarken Flows mit großen RTT kann das „Bandwidth- Delay- Product“ in Größenordnungen wachsen, die das vereinbarte TCP Window übersteigen und zur Drosselung der Übertragung führen. Mit der TCP Window Size wird von einem Empfänger die maximale Datenmenge angegeben, die ohne Empfangsbestätigung (TCP ACK) verarbeitet wird. Nicht optimal konfigurierte Systeme sind in der Folge selbst bei null Fehlern nicht in der Lage, die volle Leistung des Netzwerks auszunutzen. Trotz der Verbreitung von Jumbo-Frames zur Steigerung der Datenmenge pro Paket, oder der Verfügbarkeit neuerer Steueralgorithmen und Autotuning, erfordert Performance-Tuning eines TCP-Stacks nach wie vor die bewusste Betrachtung des beabsichtigten Einsatzbereichs, um die TCP Parameter mit ihren zahlreichen teils gegensätzlichen Effekten optimal abzustimmen.

2.3 Anforderungen an Router

Um ideale Bedingungen für große Datenraten herzustellen, muss neben den TCP Einstellungen der Hosts an den Endpunkten auch die Netzwerkinfrastruktur auf dem Übertragungspfad den Anforderungen an verlustfreie Übertragung starker Flows gewachsen sein. Das erfordert die Fähigkeit, den Inhalt großer TCP Sende-Puffer mit der vollen Line-Rate eines Host Systems zu verarbeiten. Idealerweise enthält der Pfad durch das Netzwerk lediglich performante Switches und Router, und davon so wenige wie möglich. Jede Netzwerkkomponente stellt eine potentielle Fehlerquelle oder einen Engpass dar. Ganz besonderes Augenmerk gilt der Dimensionierung der Router-Puffer, die selbst bei Konfluenz mehrerer starker Flows auf einem Sende-Interface den Datenfluss bewältigen können müssen. Dies ist häufig bei „kleinen“ LAN Routern und Switches nicht ausreichend gegeben.

2.4 TCP und Paketverlust

Da in der Praxis jedoch keine idealen Bedingungen vorausgesetzt werden können, muss man die Situation inklusive Übertragungsfehler betrachten. Übertragungsfehler an dieser Stelle bedeutet, dass eines der Pakete der TCP Verbindung nicht die Gegenstelle erreicht hat, ein sogenannter Paketverlust. Ein Paketverlust wird durch die ausbleibende Bestätigung schnell erkannt und kann üblicherweise durch eine schnelle Wiederholung der Übertragung (fast retransmit) kompensiert werden. Dies funktioniert jedoch nur bis zu einer gewissen Paketverlustrate, ab der dann der TCP Algorithmus die gesamte Übertragungsrate herunter regelt. Je nach eingestelltem Algorithmus fallen diese Drosselungen teils drastisch aus und halten die Übertragungsrate lange Zeit unterhalb des Idealwertes. Die Abhängigkeit dieser Prozesse von der RTT bedeuten, dass die kritische Paketverlustrate für eine optimale Übertragungsgeschwindigkeit also mit steigender RTT

sinkt, bzw. bei konstanter Paketverlustrate sinkt die mögliche Übertragungsgeschwindigkeit mit der RTT (Abb. 1). Im Zusammenspiel mit suboptimal konfigurierten Systemen verursacht Paketverlust je nach RTT der Verbindung massive Einbrüche in der Übertragungsrate. Durch die physikalischen Gegebenheiten steigt die Signallaufzeit und damit auch die RTT linear mit der Entfernung (z.B. Glasfaser addiert ca. 2x1ms pro 100km zusätzlich zur RTT, hin/rück).

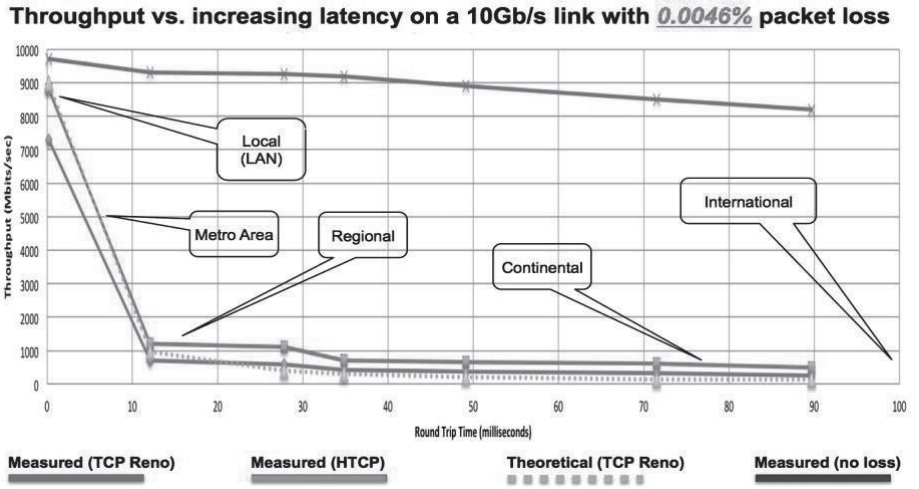

Abb. 1: Datendurchsatz vs RTT [fasterdata.es.net]

2.5 Ursachen für Paketverlust

Mit der Digitalisierung aller Facetten des Betriebs an Einrichtungen bauen zahllose andere Anwendungen nun ebenfalls auf die Infrastruktur. Viele dieser Anwendungen, wie für Personalangelegenheiten oder Finanzen mit erhöhtem Schutzbedarf, und der Einsatz von Standard-PC Systemen für Mitarbeiter und Studenten, haben die Anwendung diverser Komponenten und Praktiken für IT-Sicherheit und -Management im Campusnetz notwendig gemacht, die in der reinen Forschungsdaten-Verarbeitung unnötig oder gar hinderlich sind. Dazu gehören Firewalls, Intrusion Detection Systeme, VPN Gateways, Limiter, Proxys, NAT-Gateways, etc. Alle zusätzlichen aktiven Netz-Komponenten, besonders solche die Deep-Packet-Inspection (DPI) durchführen, können stark limitierende Flaschenhälse für Flows von Wissenschaftsdaten sein. Sie können in vielen Fällen auch den so schädlichen Paketverlust verursachen, da sie einzelne extrem starke Flows nicht in voller Geschwindigkeit verarbeiten können. Dazu kommt, dass DPI auf Wissenschaftsdaten in den meisten Fällen wenig sinnvoll ist, da es sich hier um große Sätze Binärdaten handelt und nicht um Webinhalte mit potentiellen Schadskripten oder persönlichen Daten.

3 Lösungsansatz

Die vorgestellten Ansätze verfolgen allesamt das Ziel, eine dynamische Forschungstätigkeit mit großen Datenmengen über verteilte Standorte zu ermöglichen, und dabei gegenseitig schädliche Wechselwirkungen mit der alltäglichen Netz/Internet-Nutzung auf einem Campus zu vermeiden. Dies geschieht im Wesentlichen durch eine infrastrukturelle Trennung der Datenpfade vom allgemeinen Campusnetz. Zur Vermeidung multipler hops durch ein hoch ausgelastetes Campusnetz voll heterogener Anwendungen und Infrastruktur, sehen diese Ansätze, analog einer Webserver-DMZ, die Einrichtung einer spezialisierten Netz-Enklave neben dem Übergang zum Forschungsnetz vor. Dort befinden sich dedizierte und optimierte Übertragungs-Server, welche dann ungestört die Fernübertragung der Forschungsdaten übernehmen. Dabei wird der Sicherheit im erforderlichen Umfang Rechnung getragen, jedoch mit anderen Methoden und Metriken als in der Unternehmens-IT Praxis.

3.1 Die Science DMZ

Entwickelt am „Energy Sciences Network“ ESnet des US Energieministeriums DoE steht ScienceDMZ für ein bereits mehrfach bewährtes Design-Muster für Campus-Infrastruktur an Einrichtungen mit Bedarf an schnellem Austausch von Forschungsdaten. Dazu gehören die dem DoE unterstehenden und von ESnet betreuten nationalen Forschungslabore der USA, mit Physik-, Material-, und HPC-Forschung an weit verteilten Standorten, aber auch die Universitäten und andere Einrichtungen, an denen mit solchen Daten geforscht wird. Umfassend beschrieben in [Da13] und seither vielfältig zitiert und implementiert [Ma14], [Pe17], stellt die ScienceDMZ einen Baukasten von Best Practices zur Mitigation der eingangs beschriebenen Problemstellung dar. Die ScienceDMZ ist ein generalisierter Satz von Design-Mustern, der flexibel und skalierbar je nach den lokalen Gegebenheiten und Bedarfen eine passende Lösung ermöglicht.

Die Science DMZ bietet:

- Eine skalierbare und erweiterbare Netzwerkplattform ohne Paketverlust, speziell optimiert für die Übertragung umfangreicher Wissenschaftsdaten
- Dem tatsächlich notwendigen Sicherheitsniveau angemessene Nutzungsrichtlinien, damit performante Anwendungen nicht unnötig eingeschränkt werden
- Eine effektive Anbindung lokaler Ressourcen an die Weitverkehrsnetze
- Mechanismen zur laufenden Messung der Netzperformance

Die einfachste Ausführung der ScienceDMZ (Abb. 2) besteht aus einem separaten Netzbereich außerhalb der Campus Firewall, angeschlossen an den Border-Router durch einen dedizierten DMZ Router. In der DMZ befindet sich ein spezialisierter Server (Data

Transfer Node – DTN) zur Datenübertragung, sowie eine perfSONAR[3] Box zur Messung der Netzperformance. Die DTN kann direkt über nur zwei Router mit dem WAN kommunizieren, ohne den Einfluss des weiteren Campus-LAN. Die Forscher im Campus LAN haben über den kurzen Pfad zur DTN wegen der niedrigen Latenz kaum Performance Einbußen zu befürchten.

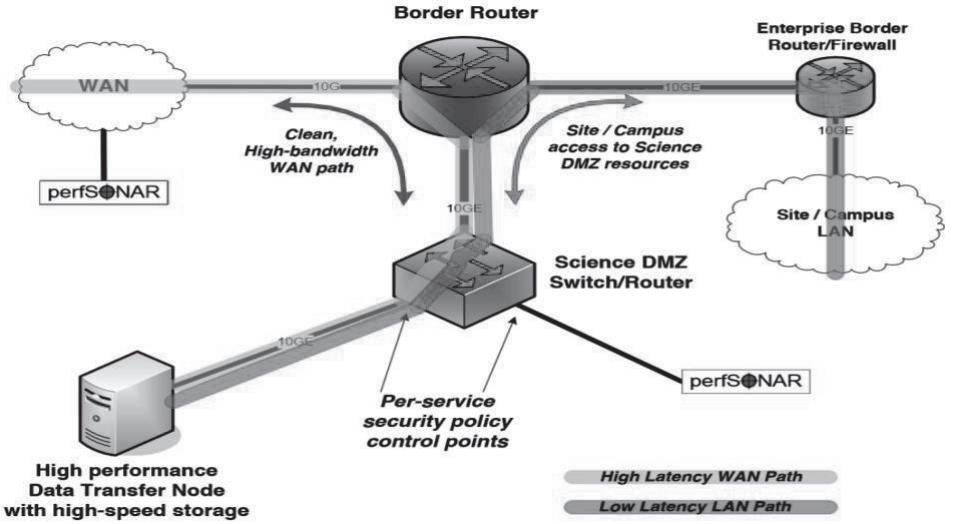

Abb. 2: Eine einfache ScienceDMZ [Da13]

Traditionelle Werkzeuge der Netzwerksicherheit, wie Firewalls und andere Middleboxen, erzielen ihre Wirkung größtenteils durch die Analyse von Web-Traffic auf aktive Schad-Inhalte. In diesem Kontext werden aber lediglich große Datensätze ohne aktive Inhalte und über sehr wenige Anwendungen und Ports bewegt. Aktive Analyse bringt hier also wenig tatsächlichen Sicherheits-Mehrwert und kann wie beschrieben darüber hinaus schädlich auf die Datenrate wirken. Deswegen wird die Sicherheit der DMZ ohne Einsatz aktiver Analyse mit mehreren ineinandergreifenden Maßnahmen realisiert. Zum einen bedarf es geeigneter Security Policies auf dem DMZ Router, welcher unter Anderem als statische Paketfilter-Firewall mit voller Leitungsgeschwindigkeit fungiert und über Access Control Lists (ACL) zur Begrenzung der Dienste auf spezifisch benannte Gegenstellen verfügt. Zum anderen sind die DTN Systeme gehärtet und nicht zur interaktiven Bedienung durch Anwender konfiguriert. So arbeiten sie als „headless“ Systeme mit stark eingeschränktem Funktions-Umfang an nach außen hin offenen Schnittstellen und Protokollen.

[3] https://www.perfsonar.net/

Durch diese Entflechtung der Netzinfrastruktur profitiert auch der Rest des Campusnetzwerks von der reduzierten Beanspruchung. Die IT-Sicherheit im restlichen Campus kann erhöht werden, weil Sonderregeln und Löcher in der Firewall zurückgenommen werden können und sich insgesamt die Angriffsfläche reduziert. So wird dem Bedarf der wissenschaftlichen Anwendungen an Performance gerecht, ohne die Sicherheit zu vernachlässigen.

Eine Eigenschaft der ScienceDMZ ist, dass sie fast beliebig skaliert werden kann. Am Beispiel einer HPC Einrichtung zeigt [Da13] die Möglichkeit der Parallelisierung vieler Netzkomponenten und Pfade, um Lastverteilung und Ausfallsicherheit zu gewährleisten. Mehrere DTN übernehmen die Datenübertragung und können dabei auf ein mit dem Cluster gemeinsames Dateisystem zugreifen. So werden gar keine großen Datenströme ins Campusnetz geführt, sondern verbleiben gleich im Kontext der HPC Anlage. Ebenfalls werden so die Login Knoten des HPC Systems von der Datenübertragung entlastet.

Je komplexer die Auslegung der DMZ wird, desto wichtiger ist die Überwachung der Netzperformance auch in Teilsegmenten. Man hat in diesem Fall also mehrere perfSONAR Boxen an strategischen Punkten auf dem Datenpfad, um die kritischen Teilsegmente DTN-Router und Router-WAN separat ausmessen zu können.

3.2 Die Data Transfer Node

Um unter den beschriebenen Bedingungen dauerhaft performante TCP Verbindungen aufrecht zu erhalten, hat sich der Einsatz dedizierter und optimierter Host Hardware bewährt. Unter dem Begriff Data Transfer Node – DTN[4] wird eine Refenrenz-Konfiguration mit Hardware der Server-Klasse und einer speziell zusammengestellten Software-Konfiguration auf Linux-Basis vorgestellt. Eine Priorität sind selbstverständlich Netzwerk-Interfaces höchster Qualität. Zugang zu schnellem Massenspeicher ist ebenso notwendig, um die Übertragung nicht durch I/O Limits auszubremsen. Software-seitig kommen gängige Datentransfer-Tools wie GridFTP, GLOBUS online, oder SSH/SCP mit high-performance patches sowie ein getunter TCP Stack zum Einsatz. Die Konfiguration ist im Hinblick auf laufende Services und offene Ports stark eingeschränkt und gehärtet, um die Stabilität und Angriffsfläche zu optimieren. Die Empfehlungen gehen bis hin zu Treiber-Versionen und Zuweisung einzelner Prozesse zu CPU Kernen, was nachweislich Einfluss auf Stabilität und Durchsatz hat.

[4] http://fasterdata.es.net/science-dmz/DTN/

3.3 Research Data Portal

Es werden zunehmend integrierte und effiziente Umgebungen und IT Infrastrukturen für datenintensive Forschung an verteilten Standorten nachgefragt. Diese Forderung nach Integration beinhaltet zunehmend auch geeignete Softwaresysteme zur Datenlogistik und Bearbeitung. Diese "Research Data Portal" genannten Dienste basieren traditionell auf Webservern, was jedoch an Grenzen der Skalierbarkeit und Flexibilität stößt. Aufbauend auf der ScienceDMZ haben [Ch18] eine moderne Fassung entworfen, welche die vormals im Server vereinten Funktionen der Anfragesteuerung, Datenübertragung, und Autorisation/Koordination aufteilen. Der Server im Campusnetz bleibt erhalten, übernimmt aber nur noch die klassischen Webserver-Aufgaben wie z.B. Das Benutzer-Interface und die Suchfunktion. Die Datenübertragung erfolgt durch DTNs und die Koordination und Zugangssteuerung des ganzen kann mit einem externen Data Manager wie Globus [Ch14] durchgeführt werden. Mit einer ScienceDMZ ist eine Einrichtung also bestens auf die Unterstützung moderner Forschungsdaten-Portale vorbereitet.

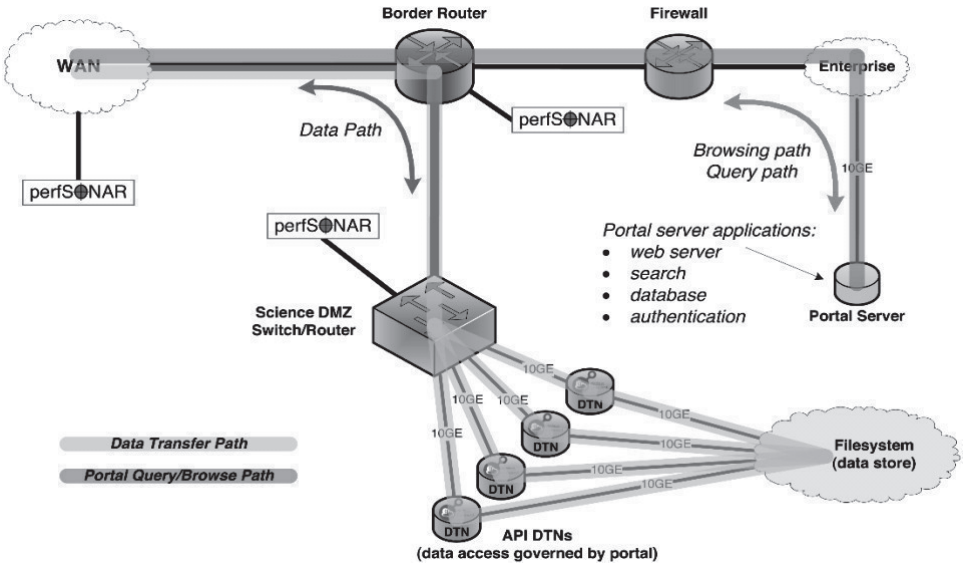

Abb. 3: Modern Research Data Portal [Ch18]

3.4 Fallbeispiel University Otago, Neuseeland

Die University of Otago in Neuseeland, steht vor der Herausforderung, dass alle internationalen Verbindungen automatisch über sehr große Entfernungen gehen. Eine optimale Ausnutzung der Dateninfrastruktur ist also essentiell.

Forscher stellten eine ernüchternd niedrige maximale Datenrate im Bereich weniger 100Mbps aus dem Campus-Netz zum nationalen Forschungsdatenspeicher und zu internationalen Partnern fest. In Zusammenarbeit mit Ihrem Forschungsnetz REANNZ richtete die Universität Otago eine ScienceDMZ ein[5] und konnte so eine dramatische Optimierung der maximalen Datenübertragungsrate erzielen [Abb. 4].

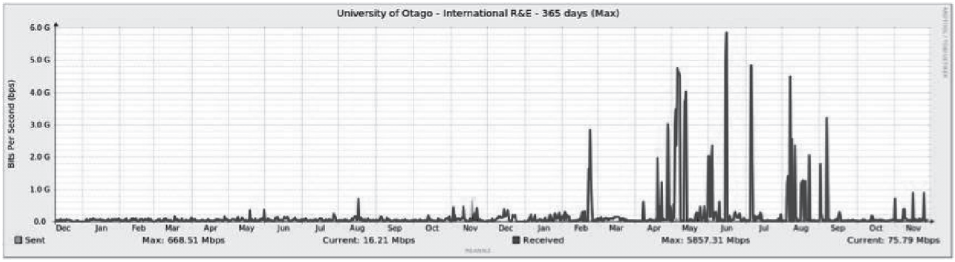

Abb. 4: Erreichbare Lastspitzen vor und nach Einrichtung der ScienceDMZ [REANNZ]

4 Zusammenfassung

In der heutigen Zeit der BigData Forschung ist eine effektive Ausnutzung der vorhandenen Infrastruktur mindestens genau so wichtig wie ständige Leistungssteigerungen. Das Ziel muss sein, die optimale Leistungsfähigkeit der Infrastruktur für die anspruchsvollsten Anwendungen aus der Wissenschaft spürbar und praktisch nutzbar zu machen, ohne dadurch den täglichen Betrieb der Brot-und-Butter Anwendungen im Campus zu beeinträchtigen. Der Trend geht klar in Richtung Entflechtung dieser zwei unterschiedlichen Anwendungsbereiche sowohl bei der Netzarchitektur, als auch der Benutzer-Interfaces und Softwareschnittstellen. So kann die intensive Optimierung für Übertragungsleistung auf einen überschaubaren und schützbaren Netzbereich beschränkt werden. Die vorgestellten Best Practices beschreiben eine moderne Basis für zukünftige Forschungsdaten-Infrastruktur.

Die ScienceDMZ ist natürlich nicht für alle Anwendungen das perfekte Werkzeug. Kritisch zu betrachten ist sicherlich die Umgehung der traditionellen IT Sicherheit. Ein Anschluss von Netzwerkinfrastruktur an Forschungsnetz/Internet ohne Einsatz einer Firewall bedarf einer genaueren Untersuchung der Wirksamkeit der alternativen

[5] https://reannz.co.nz/case-studies/getting-up-to-speed/

Sicherheitsmaßnahmen und der zu übertragenden Datentypen in Bezug auf Schutzklassen. Eine differenzierte Abwägung des Risiko-Nutzen-Verhältnisses ist in jedem Fall durchzuführen.

Die größere Herausforderung bei der Umsetzung ist meist nicht technischer, sondern organisatorischer Natur. Die Notwendigkeit für neue Sicherheitskonzepte und Metriken erfordert die konstruktive und lösungsorientierte Zusammenarbeit unterschiedlicher Funktionsrollen wie Netz-Architektur, IT-Sicherheit und Datenschutz in ungewohnten Konstellationen. Die Erfahrung vieler Einrichtungen zeigt jedoch auch, dass dieser Aufwand die Dienstqualität sowohl für die Wissenschaft als auch für die alltäglichen Nutzer des Campusnetzes spürbar verbessert und neue Möglichkeiten schafft.

5 Literaturverzeichnis

[Ch14] Chard, K. , Tuecke, S., Foster, I.: Efficient and Secure Transfer, Synchronization, and Sharing of Big Data In IEEE Cloud Computing, vol. 1, no. 3, pp. 46-55, Sept. 2014., doi: 10.1109/MCC.2014.52

[Ch18] Chard K, et al.: The Modern Research Data Portal: a design pattern for networked, data-intensive science., 2018, PeerJ Computer Science 4:e144 doi: 10.7717/peerj-cs.144

[Da13] Dart, E., et al: The Science DMZ: A network design pattern for data-intensive science, 2013 SC - International Conference for High Performance Computing, Networking, Storage and Analysis (SC), Denver, CO, 2013, pp. 1-10. doi: 10.1145/2503210.2503245

[Ma14] Magri, D. R. C, et al.: Science DMZ: Support for e-Science in Brazil, 2014 IEEE 10th International Conference on e-Science, Sao Paulo, 2014, pp. 75-78., doi: 10.1109/eScience.2014.53

[Mi15] Miteff, S., Hazelhurst, S.: NFShunt: A Linux firewall with OpenFlow-enabled hardware bypass, 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, 2015, pp. 100-106. doi: 10.1109/NFV-SDN.2015.7387413

[Pe17] Peisert,S., et al: The medical science DMZ: a network design pattern for data-intensive medical science, Journal of the American Medical Informatics Association, , ocx104, doi: 10.1093/jamia/ocx104

ESnet Fasterdata Knowledge Base http://fasterdata.es.net/, 12.2.2018

Petascale DTN Project, https://cs.lbl.gov/news-media/news/2017/esnets-petascale-dtn-project-speeds-up-data-transfers-between-leading-hpc-centers/, 12.2.2018

SWITCH Stories: Wissen verwalten im Zeitalter von Big Data, https://www.switch.ch/de/stories/big_science_data/, 13.2.2018