# “Science DMZ” security

Tim Chown, Duncan Rand (Jisc)

GridPP 53, Manchester, 11 April 2025

# Science DMZ

- The Science DMZ model was documented by ESnet in 2013
  - https://www.es.net/assets/pubs_presos/sc13sciDMZ-final.pdf
  - Appropriate “friction free” (zero loss) local network architecture
  - Appropriate software tools – e.g., Globus not FTP
  - Dedicated data transfer node(s) (DTNs) and (TCP) tuning
  - Efficient application of security policy (**NOT** a “firewall bypass”)
  - Persistent monitoring of network characteristics
- GridPP sites have evolved similar practices over time, just not written it up or come up with a cool name
  - But we could write up a short guide… hence this talk to solicit input…

# GridPP network architectures

- Historically GridPP sites have used different Janet links for science traffic to campus “business” traffic
  - University has 4x10G: 2x10G for GridPP, 10G campus and 10G backup
  - GridPP traffic is then filtered by stateful ACLs rather than big, stateful campus firewalls (which then don’t need to be so big and costly)
- But what are the newly 100G-connected sites doing?
  - Might use a “backup” link for GridPP? Or carve out 40G of their resilient 100G?

- LHCONE provides a “trust fabric” over which WLCG traffic is carried between T0/T1/T2 sites
  - Specific prefixes used, may be routed differently, then split out at campus edge
  - But only 2 UK sites are on LHCONE (RAL and Imperial)

# GridPP – other Science DMZ elements

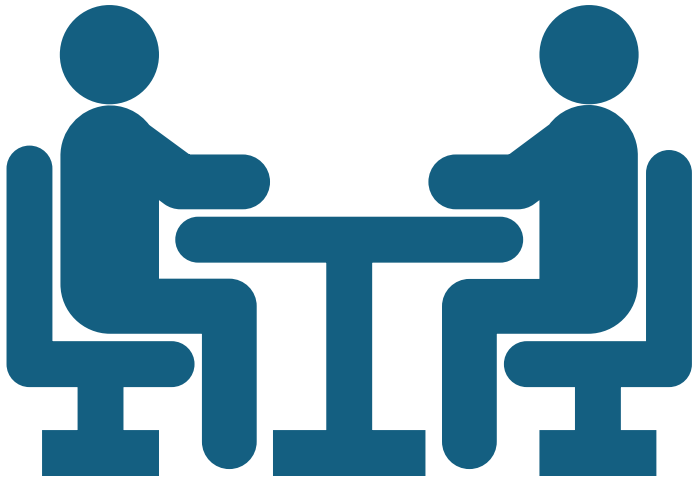
- Software tools
  - Rucio, FTS, XRootD, dCache,… GridPP seems happy with these
- Tuned DTNs
  - Interface to back-end CEPH/other
  - But is there network tuning applied – if so, what? Might it be improved?
- Efficient application of security policy
  - Stateless ACLs and host firewalls minimise exposed services/ports
  - Would use of LHCONE give greater assurance of peer trust?
- Persistent network monitoring
  - perfSONAR in use (as recommended by Science DMZ)
  - Other tooling emerging, e.g., Scitags

# Some considerations / discussion points

- **How is GridPP doing “Science DMZ” today?**
  - **What is technical state-of-the-art? Any BCP examples to share?**
- What general security practice advice should we share to ensure appropriate controls and mitigations are still followed?
- Are newer, high-performance, high-throughput firewalls changing the rationale for Science DMZ?
  - Or is the price point still too high for most sites?
- How do we take care to avoid ‘accidental’ exposure
  - Services/data appearing in a Science DMZ that shouldn’t?
- Is the GridPP compute/storage/network model changing with HL?

# And more things to think about…

- LHCONE seems useful for “static-to-static” (T0/1/2) transfers, but what about other (T3, non-LHCONE) access to GridPP resources?
  - In other disciplines, data may be downloaded for local compute
- Sites presumably run periodic security posture checks
  - How are GridPP resources included – if so, is bespoke knowledge used?
- What about zero trust architectures? (e.g., as per [1] and [2])
  - Becoming popular elsewhere – should they be explored for GridPP?
- Should we require common policies across GridPP sites?
  - Recent example: filtering practices for ICMP and UDP (they vary!)



# Discuss!

tim.chown@jisc.ac.uk

duncan.rand@jisc.ac.uk