A large, abstract blue ink splash or watercolor blotch on the left side of the slide, with various shades of blue and some white speckling.

# Deploy a Globus Endpoint in a NZ Institution

- Jose Higinio ([jose.higinio@nesi.org.nz](mailto:jose.higinio@nesi.org.nz))  
NeSI (NIWA)
- Dan Sun ([dan.sun@agresearch.co.nz](mailto:dan.sun@agresearch.co.nz))  
AgResearch Ltd



# What is Globus

It is a secure and reliable **research data management** service:

- ***Move, share*** and discover data
- A platform for developers to build applications and gateways

It moves data between Globus endpoints in *high performance* via a simple to use Web interface

- GridFTP made easy
- Share data without moving data

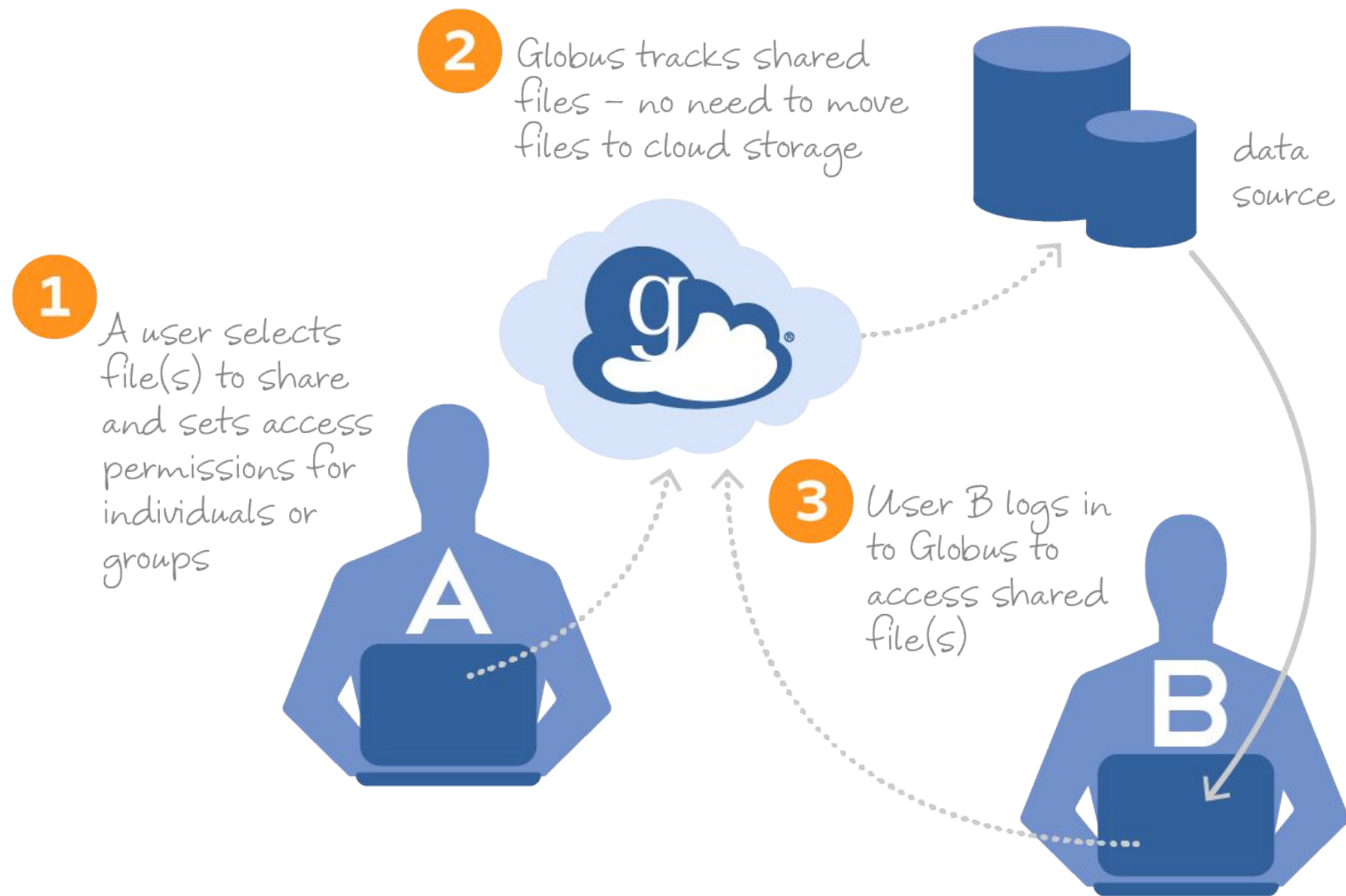


## Globus Data Transfer





# Globus Data Share





# Globus Endpoints

## Globus Connect Personal – turning a user device into a Globus endpoint

- macOS, Windows and Linux clients are available
- Firewall may get in the way

## Globus Connect Server – a dedicated server shared by all users in an institution

- Only runs on a number of Linux distributions
- Needs to be deployed and configured by a system administrator with support from a network administrator



# Considerations when deploying a Globus Connect Server

01

*Engage with institution's IT infrastructure and get their support before you start.*

02

## Security

- Authentication and authorisation, data access etc...

03

## Network security

- Edge firewall, VLAN, Science DMZ etc...

04

## Performance requirements

- Single service deployment or a clustered deployment, OS tuning and network tuning etc...



# Authorisation and Authentication Options

## MyProxy

- Short-lived certificate is generated by a public accessible MyProxy server;
- Username and password are forwarded to a MyProxy by Globus;
- Endpoint maps user certificate to local user accounts;

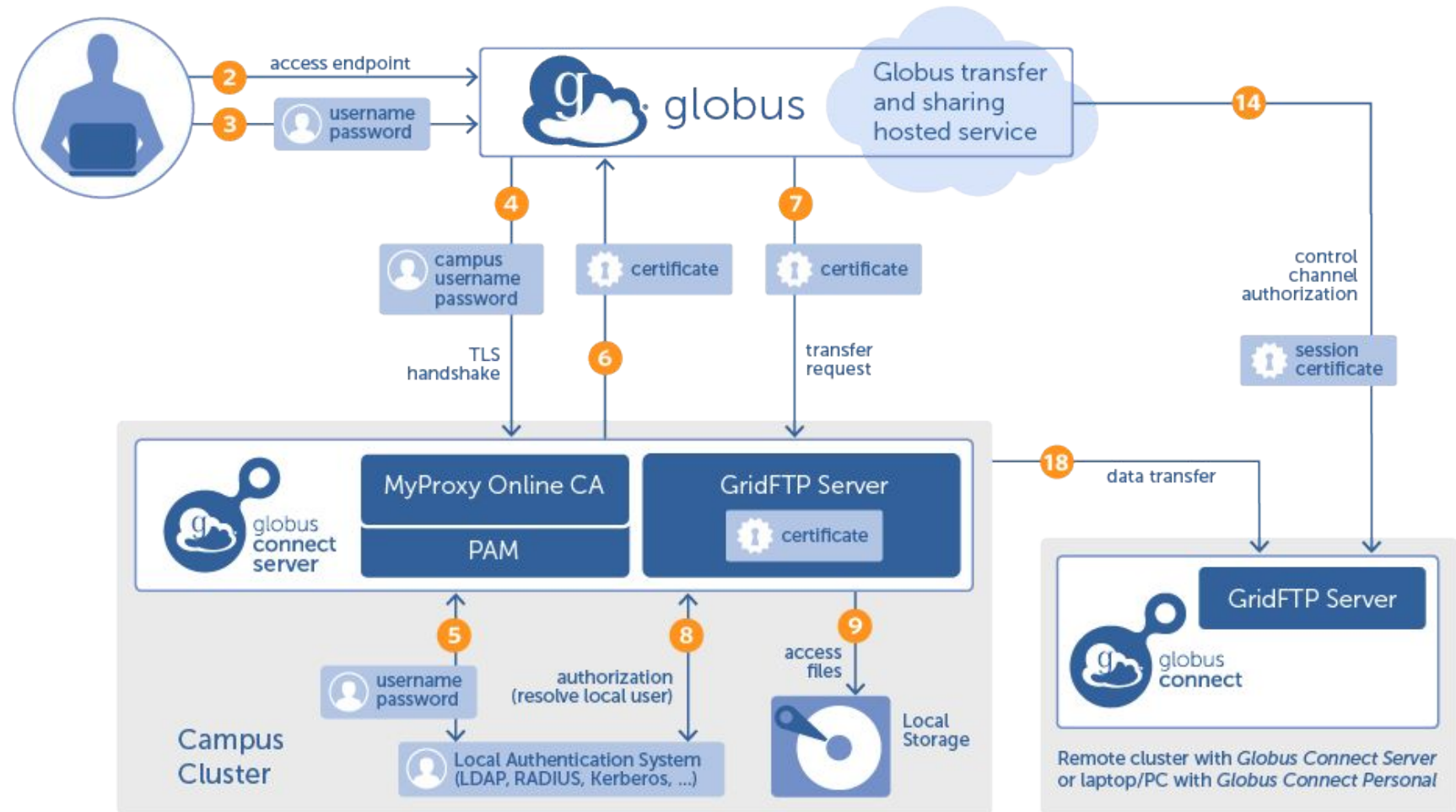
## MyProxy OAuth

- Short-lived certificate is generated by a MyProxy server that is only accessible by a MyProxy OAuth server;
- Globus redirects a user to a MyProxy OAuth server for authentication;
- Endpoint maps user certificates to local user accounts;

## CILogon (not applicable in NZ at present)

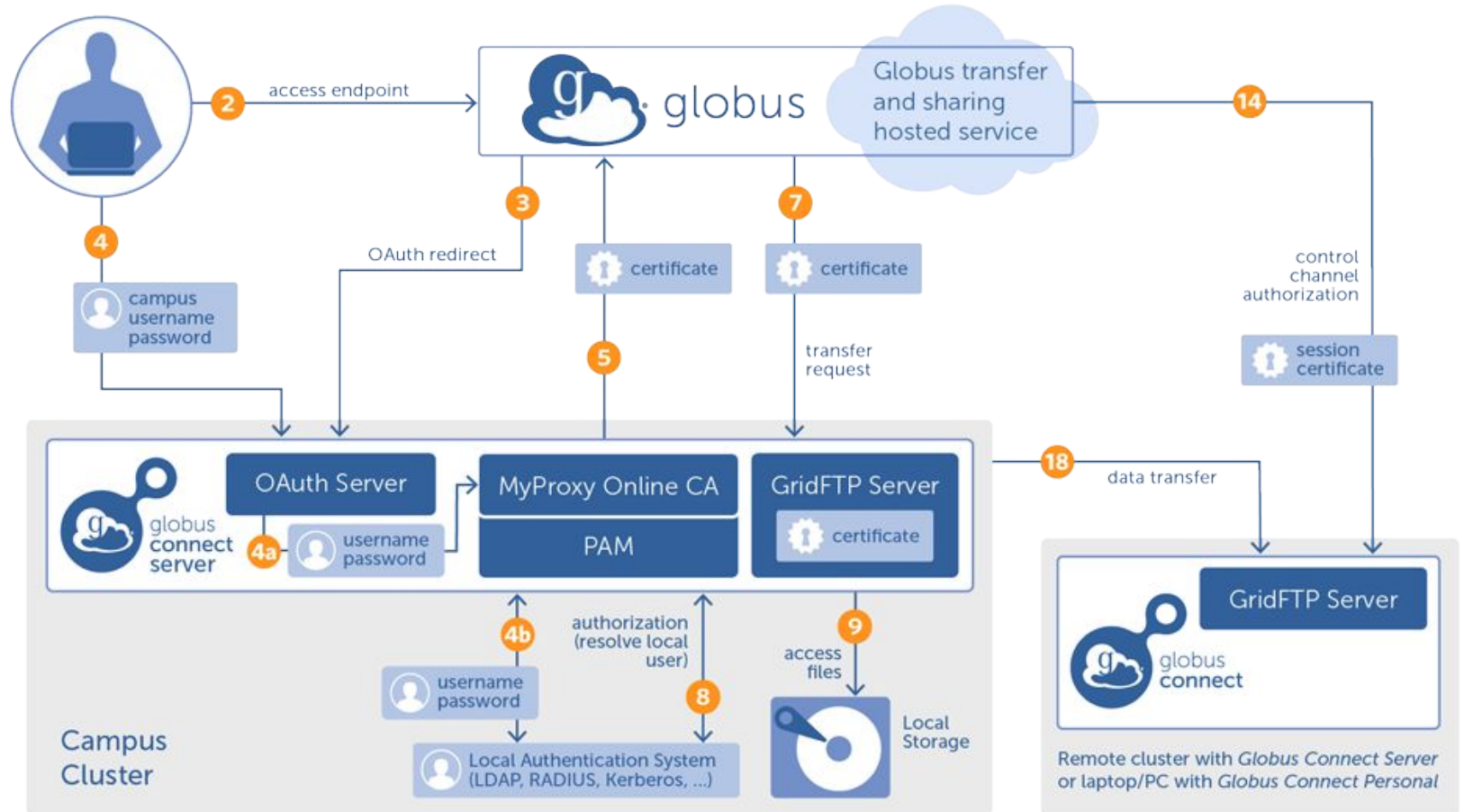


# MyProxy





# MyProxy OAuth



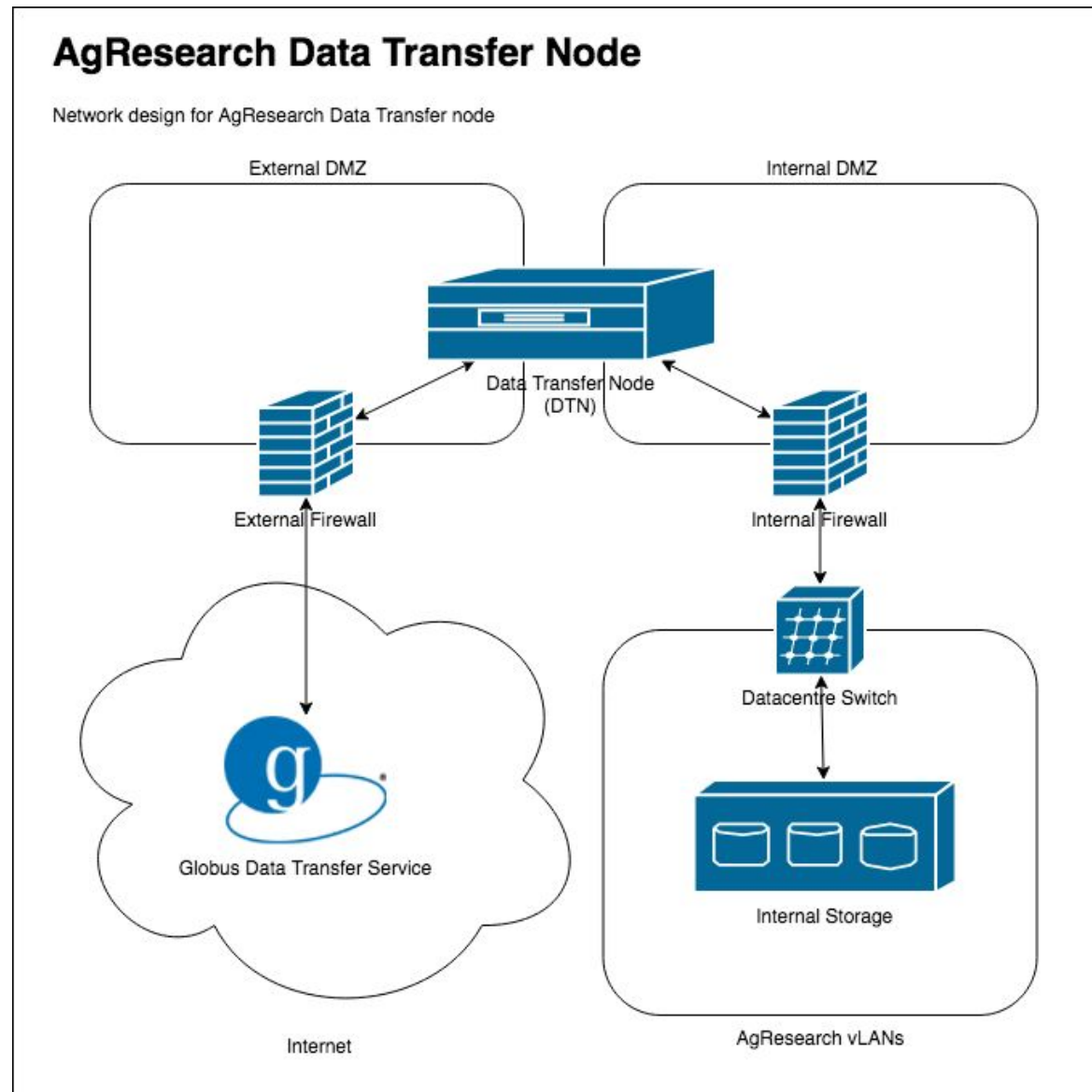


Source	Destination	Type	Port(s)	Application
ANY (Internet)	EndPoint	TCP	2811	GridFTP control channel
ANY (Internet)	EndPoint	TCP	50000-51000	GridFTP data channel
EndPoint	ANY (Internet)	TCP	50000-51000	GridFTP data channel
EndPoint	ANY (Internet)	HTTPS	443	Globus REST API
ANY (Internet)	EndPoint	HTTPS	443	MyProxy Oauth (optional)
ANY (Internet)	EndPoint	TCP	7512	MyProxy (optional)

# Firewall Rules



# Globus Endpoint Design in AgResearch





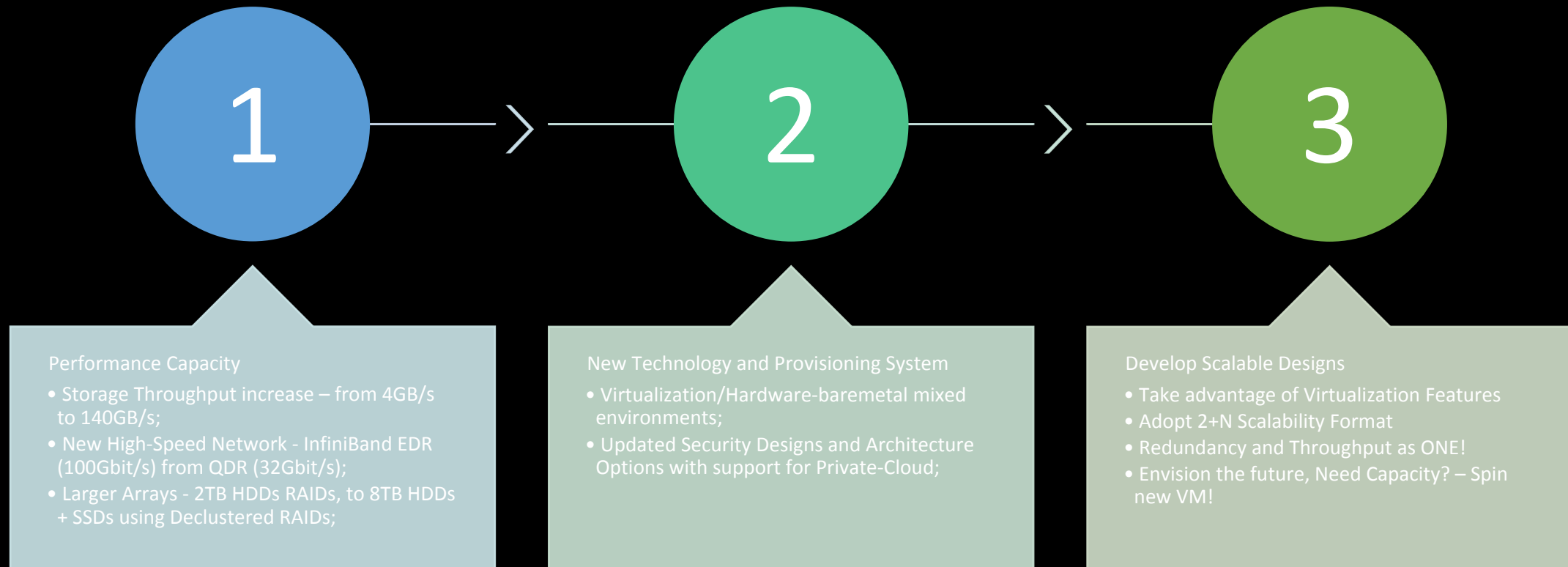
# AgResearch's Considerations

- Our security policy dictates that user credentials can only be used on resources managed by AgResearch;
- Servers in the DMZ must be multi-homed if they need to access corporate resources;
- High performance is not achievable due to current infrastructure constraints; therefore a single node deployment is adequate for our needs.



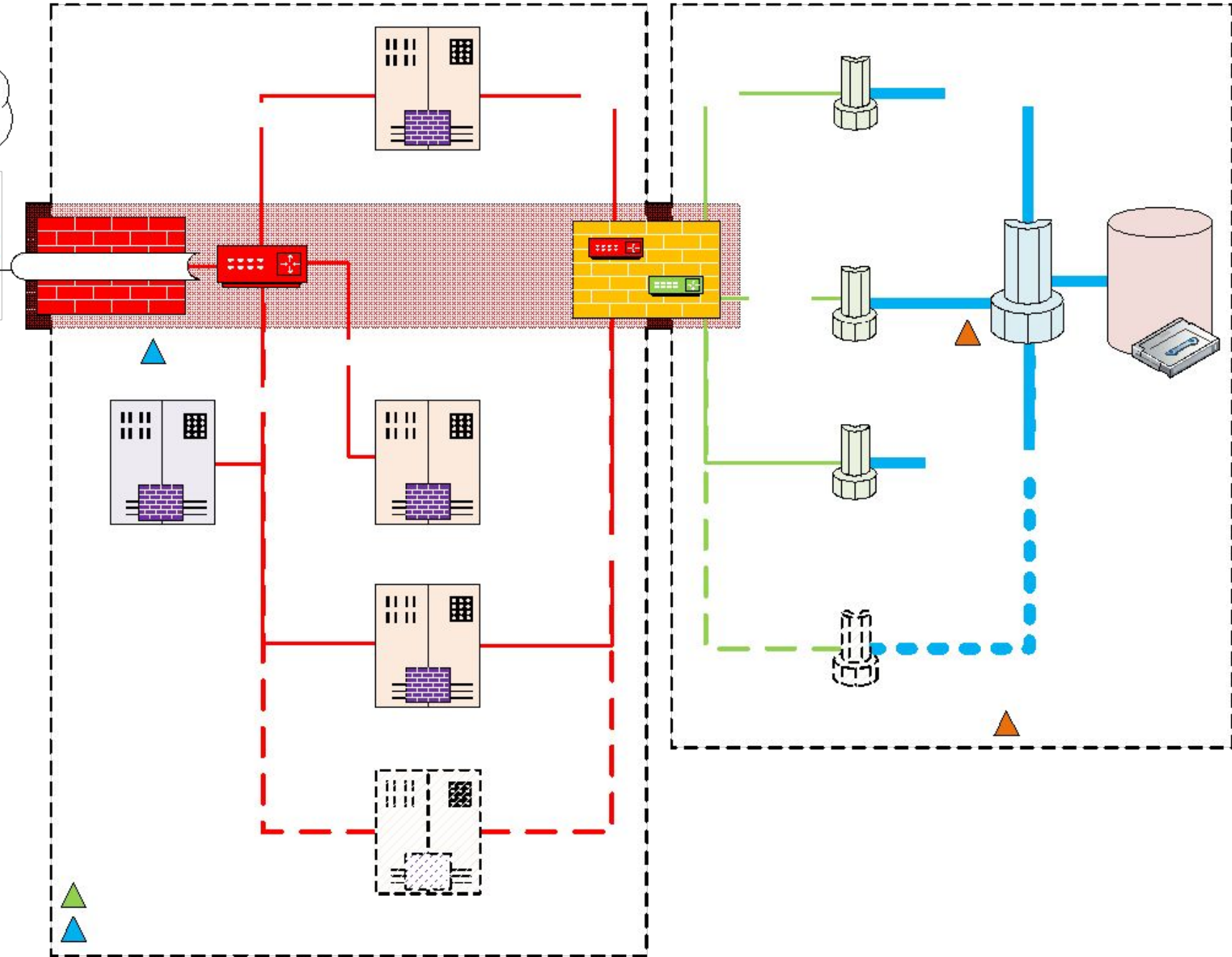


# Progression of the Data Transfer Node





NeSI  
New SDTN  
Design





# Advantages Computing Next to Data

## Energy and Performance

- Easier to find the right balance between the resource needs and the workflow requirements;
- Moving less data when possible represents less need for transmission and data validation;

## Less Complexity

- Codes and workflows will likely become easier to programme, deploy and manage;
- Simpler troubleshooting environments;

## Scalability

- No need to rebuild the entire solution;
- Data access and bandwidth are easier to share.





REANVZ

NeSI  
HPC Service

