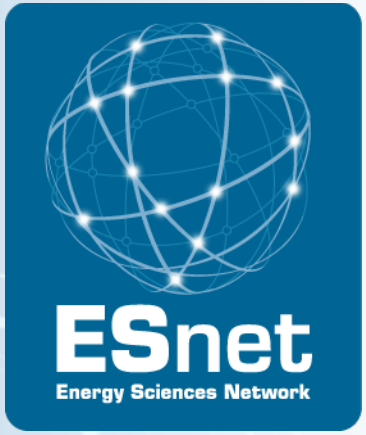

Security Requirements for Esnet Dynamic Circuit Services

Chin Guok (chin@es.net)

GLIF NSI Implementation Working Group

Atlanta, GA

Mar 20, 2014

ESnet AUP in a Nutshell

Traffic entering/leaving ESnet production network* must terminate/originate at/from an ESnet customer site

- One side of the connection is an ESnet customer
- Transit between commodity peers is not allowed (e.g. carrying traffic between Google and Yahoo)

**NB: Exceptions can be made (considered on a case-by-case basis) for ESnet testbed connections*

Connection Service Trust Relationships

User (Client) Relationships

- Each user must have a distinct account with a distinct credential*
- Users are associated with roles (e.g. end user, site administrator) and organization/project (e.g. LBNL, LHC ATLAS, etc)
- Permissions are based on roles and associated organizations/projects (e.g. site coordinator can view all circuits originating/terminating at his/her site and cancel or modify them as needed)

Peer Relationships

- Each peer must have a distinct account with a distinct credential
- Peers are associated with roles (e.g. NSA) and organizations (e.g. Internet2)
- Permissions are based on roles and associated organizations
- Follows ISP peering relationships
  - Trust only directly connected (control plane) peer domain
  - No relationships with downstream (not directly connected) domains
  - Consistent with ISP peering recharge model where charges cascade back the the user, e.g.
    - Request workflow: user -> ISP-A -> ISP-B -> ISP-C
    - Recharge workflow: ISP-C -> ISP-B -> ISP-A -> user

**NB: If user is associated with multiple organizations/projects (e.g. LHC ATLAS, LHC CMS, etc), each distinct association will have an individual account with a distinct credential*

Questions?

chin@es.net | Chin Guok