Some slides on Dynamic Connectivity Service.

John White, Helsinki Institute of Physics.
EGEE JRA1 Deputy Middleware Manager.

www.eu-egee.org

Information Society

The problem

- **The problem.**
  - Connectivity of site worker nodes (WNs).
    - Grid “clients” would prefer more connectivity.
    - Site operators would prefer less (none!).
- **Current situation.**
  - WNs have outbound but no inbound connectivity.
- **A generic solution.**
  - Default configuration: connectivity blocked.
  - Connection request → port opened.
  - **Dynamic connectivity service.**
- **The problem with the solution.**
  - Site operators will probably not like this.
  - It potentially interferes with their firewalls.

DCS with PDP

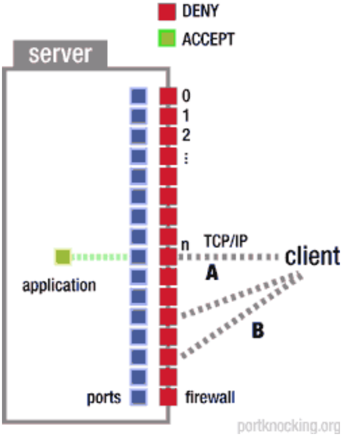
- **What gLite components could be used to form a DCS?**
  - Currently: None.
- Could we write an XACML security policy?
- Evaluate with PDP...
  - WN from subnet xxx.yyy authenticates.
  - Requests connection to host aaa.bbb.ccc.ddd.
  - Reply: Yes/No. Some instruction on port etc
  - Send instruction to gateway to open explicit connection.
- Questions:
  - PEP on WN.
  - Process on gateway machine (obvious).
  - How to close afterwards.
  - Rates expected?
- Sorry, no diagrams.

Port Knocking

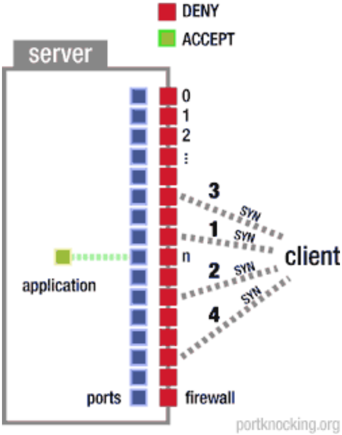
Host-to-host communication where information flows across closed ports.

- Server presents no open ports to the public and monitors all connections.
- Client initiates connection attempts by sending SYN packets to the ports specified in the knock.
- The server offers no response to the client during the knocking phase:”silently” processes the port sequence.
- Server decodes a valid knock, it triggers a server-side process.
- Opens a specified port for connection.
- Closes once connection established.
- Variants of the port knocking method: port sequence or a packet-payload.

Port Knocking

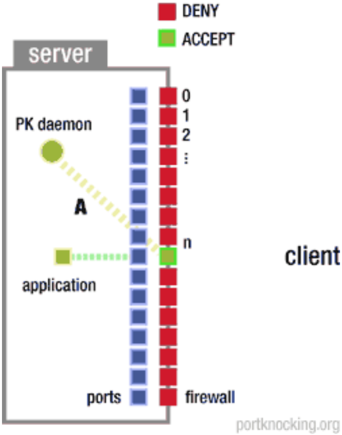


Port Knocking

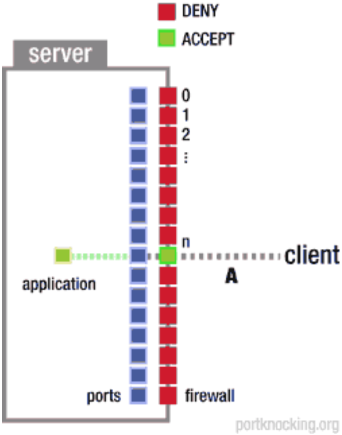


portknocking.org

Port Knocking



Port Knocking



Port Knocking

Is this practical?

- Knock sequence would be entirely internal to site.
- Many WNs accessing the gateway machine... rate?
- Still need a daemon process able to modify “iptables”.

Summary

- (This) scheme would certianly improve the WN connectivity security.
- DCS should be possible.
- Has there been any explicit request?
- Do we have the developers available in EGEE-III?
  - Design PEP/PDP with this in mind.
  - Support external development of DCS.
- Sites need to be polled early.
  - Not much opinion from “users”.

The End

Lightweight Middleware for Grid Computing