Security at the TierX

Washington DC, 14th of June 2011

edoardo.martelli@cern.ch

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

LHCONE policy

"**Security** on the aggregation networks and the Tier1/2/3s **is the responsibility of the aggregation networks and the Tier1/2/3s** and is not the responsibility of LHCONE".

Connection to the LHCONE

Tier1/2 expressed the need to bypass expensive/slow statefull firewalls: similar to LHCOPN

Similar to the LHCOPN, the traffic must be symmteric (or a statefull firewal may drop the traffic)

Contrary to the LHCOPN, the number of announced prefixes is large and change more frequently.

Filtering by applications

Stateless ACLs: need to be open for all high number ports and be symmetric:

```
permit tcp any 8443 any range 1024-65335
permit tcp any range 1024-65535 any 8443
```

Any application not allowed will not work (no fall back to default connectivity)

A strict ACL is complicated; a loose one is useless.

Filtering by applications

Voms-proxy-init: TCP 8443, TCP 15000-15020
GRIDFTP/Globus: TCP 2811, TCP 20000-25000, UDP 20000-25000
Xrootd: TCP 1094-1095
CMSGLIDEINWMS: TCP 4080
ALICE CAF: TCP 1090-1099
ALIENDB: 8050, 8080-8081, 8093-8084, 8088-8089, 8095, 8097-8099
VOMS-PROCY-INIT: TCP 8443, TCP 15000-15020
Griddbdii: TCP 2170, 2180
…

What about port 80, 8000, 8090, 22?

Difficult to make exhaustive list.

Filtering by prefixes

- Needs to open at IP level

- List of prefix may be long and change very often

- Do you trust all the LHCONE connected sites? All at the same level? Do you know which they will be?

Filtering by servers

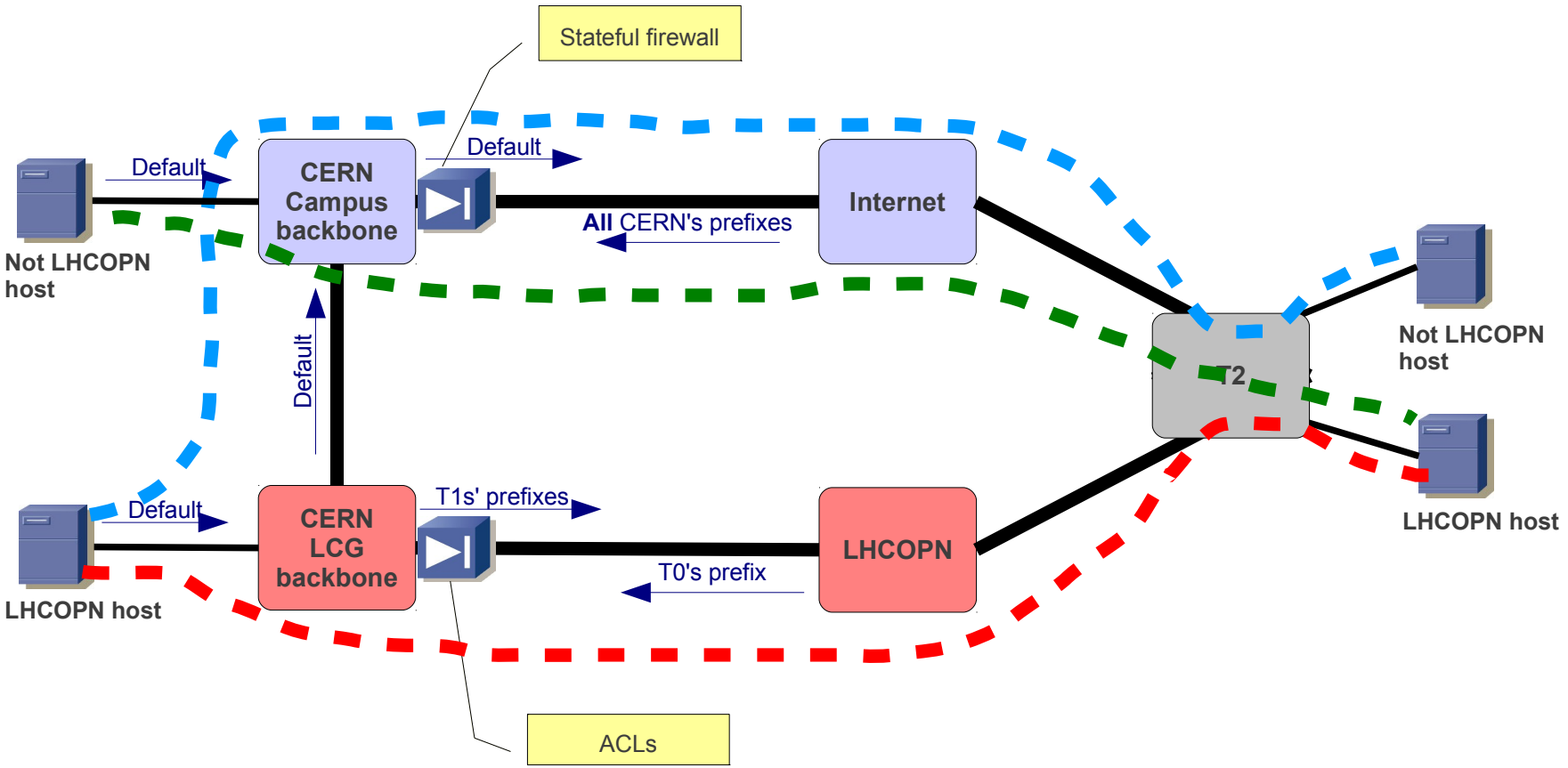
- Permit each server with only its allowed ports

- Needs lot of maintenance

- ACLs may be very long => more expensive routers

How will you do it?

Routing must be symmetric



LHCOPN host to LHCOPN host

T0's LHCOPN host to T1's not LHCOPN host

T0's not LHCOPN host to T1's LHCOPN host

Are you ready for this?

It was painful with the LHCOPN.

Opinions?

Needs to standardize

Those were only recommendations; any site can use different port settings.

Needs to standardize: list of LHCONE allowed applications (i.e. open ports)