multiONE - introduction

17th of July 2019

edoardo.martelli@cern.ch

LHCONE

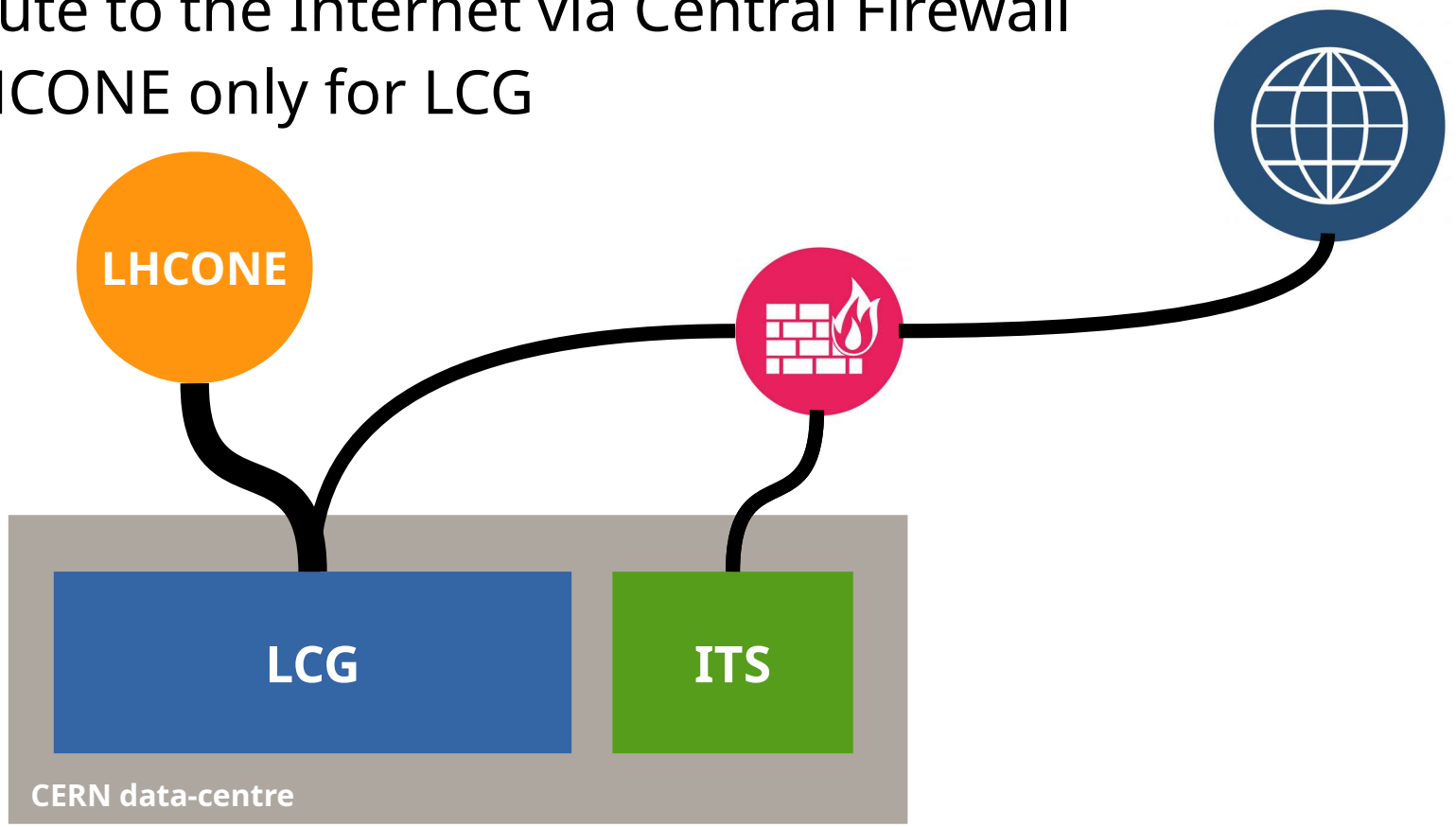
LHCONE is a Virtual Private Network (VPN) implemented by Research and Education Network providers (RENs)

Original AUP:
- Only WLCG Tier1/2/3 can connect to LHCONE
- Only servers dedicated to WLCG can use LHCONE

Thus: sites can trust LHCONE to be safe and connect it directly to the datacentre, bypassing expensive security equipment 

LHCONE access at CERN

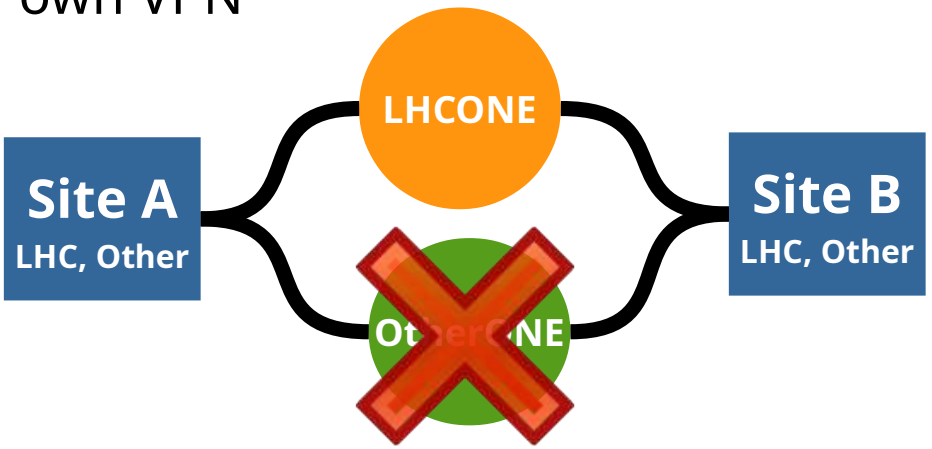
- Servers assigned statically to two domains: LCG and ITS
- Default route to the Internet via Central Firewall
- Path to LHCONE only for LCG



Participating collaborations

- Defining a new VPN is simple for RENs.
- But it's difficult for sites participating in multiple collaborations to put the traffic in the right VPN, if resources are not grouped and segregated

- Thus, over the years, few small HEP collaborations (Pierre Auger, XENON, BelleII, protoDUNE…) have simply joined LHCONE instead of building their own VPN



Problems with participating collaborations

- The more sites join LHCONE, the less trustable it becomes

- Funding agencies prefers to have a clear distinction of who is using the resources they found

=> VPNs dedicated to every collaboration would help

Problems with multiple VPNs

- Difficult to identify what VPN to use if a site serves multiple collaborations

- Collaborations may share same servers and applications

- It’s ineffective to segregate resources

multiONE

Issue discussed several time at LHCONE meeting

Agreed to start a project to verify if it is possible to use multiple VPNs for sites that participate to several science collaborations

Discussion on going to check if DUNE could be a possible use-case

Contacts established with GNA-G to define a possible collaboration using their virtual testbed

Some possible solutions

Use different data-centre domains (VRF or VXLAN domains):

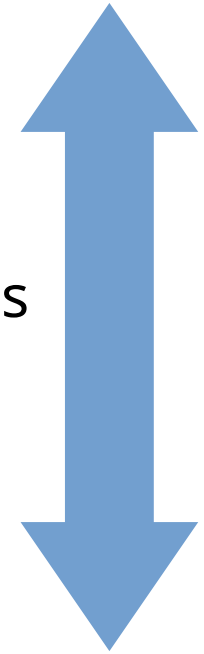
- resource association must be software defined and agile

Assign different IP(v6) addresses to each collaboration:

- servers must use the correct source and destination addresses

Packet tagging:

- applications tags the packet with owner information
- the network put the tags in the corresponding VRF



Next steps

- Brain-storm for possible solutions

- Discuss at next GDB in Fermilab

- Define action plan

Questions?

edoardo.martelli@cern.ch