



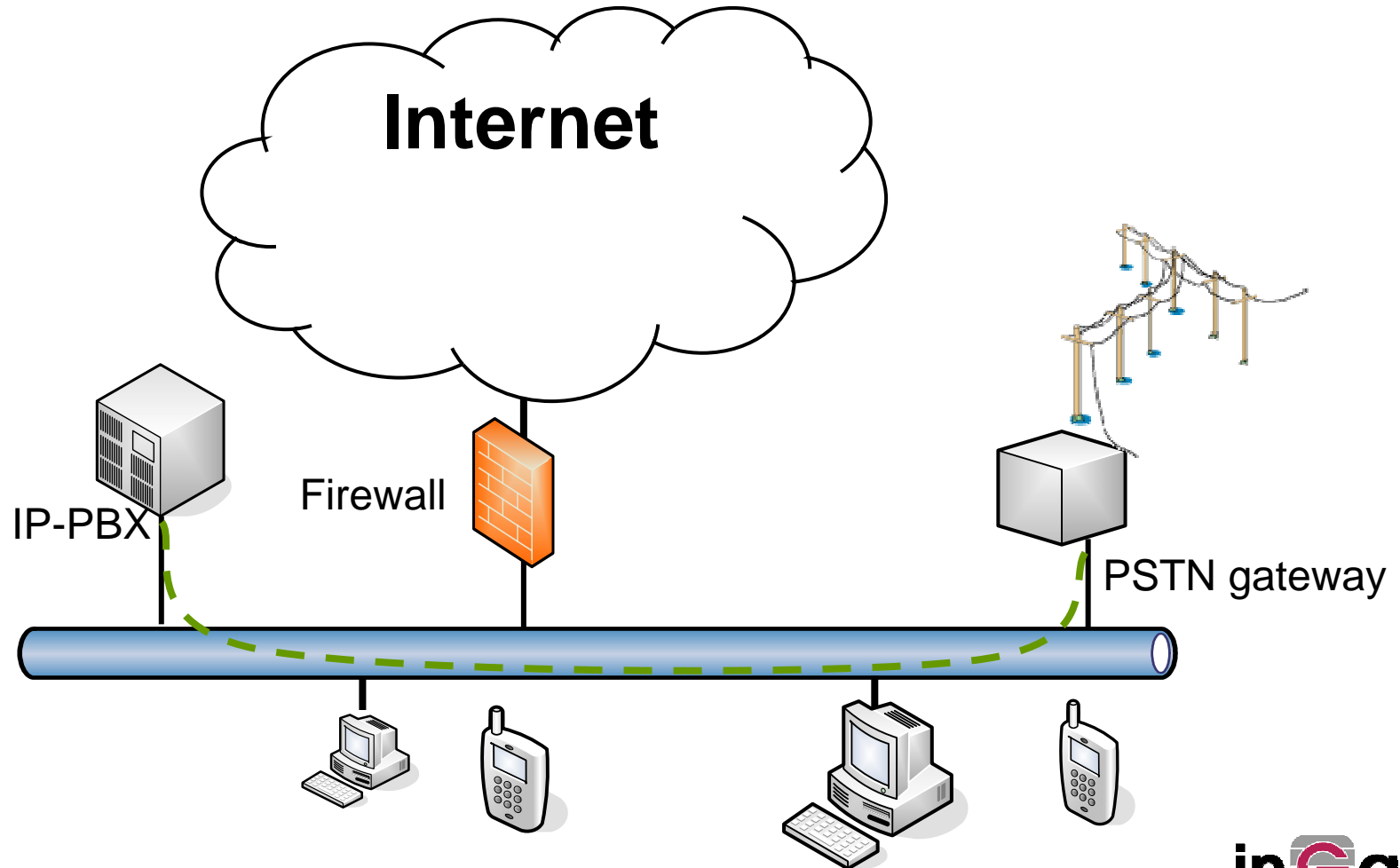
# **Enterprise Infrastructure Solutions for SIP Trunking**

Janne Magnusson, Ingate Systems

# Steps to SIP Trunking

- Connection to PSTN gateway
- Solving firewall/NAT traversal
- Addressing interoperability issues
- Security
- QoS

# Connection to PSTN-gateway

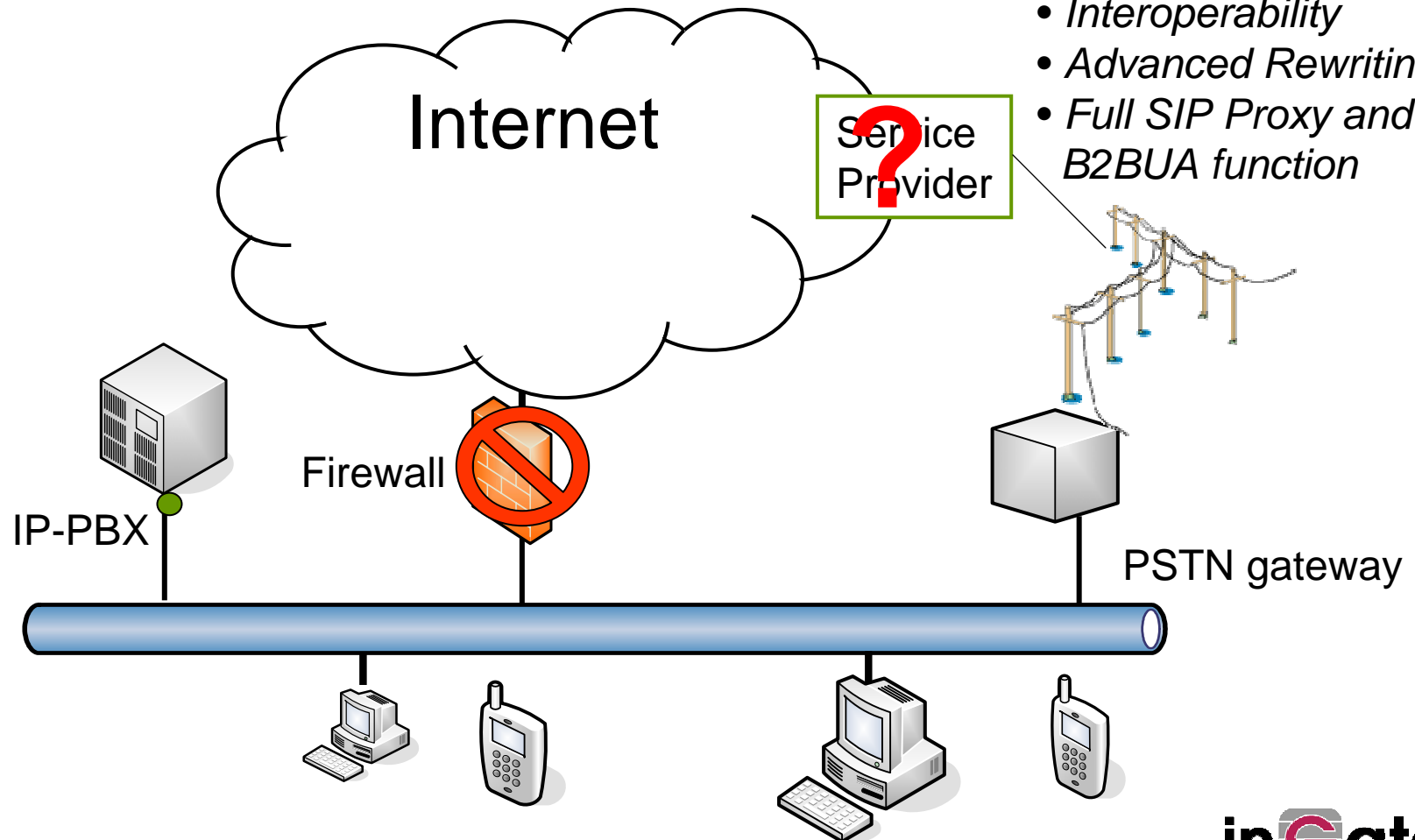


# The Network Edge Firewall problem !

- The firewall may stop the signaling

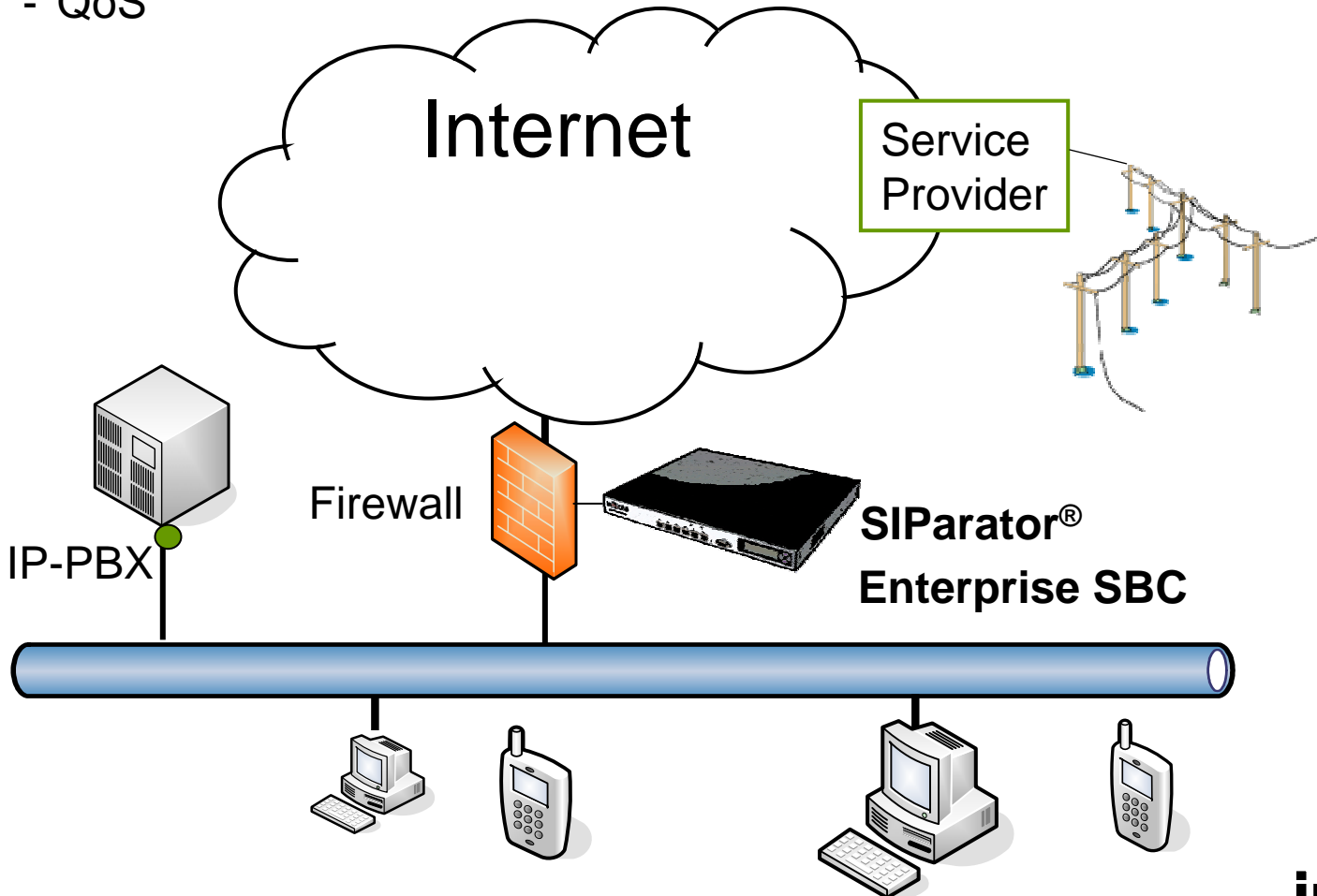
• Even if traffic is allowed signaling will be corrupt due to **lack of:**

- *Interoperability*
- *Advanced Rewriting*
- *Full SIP Proxy and B2BUA function*

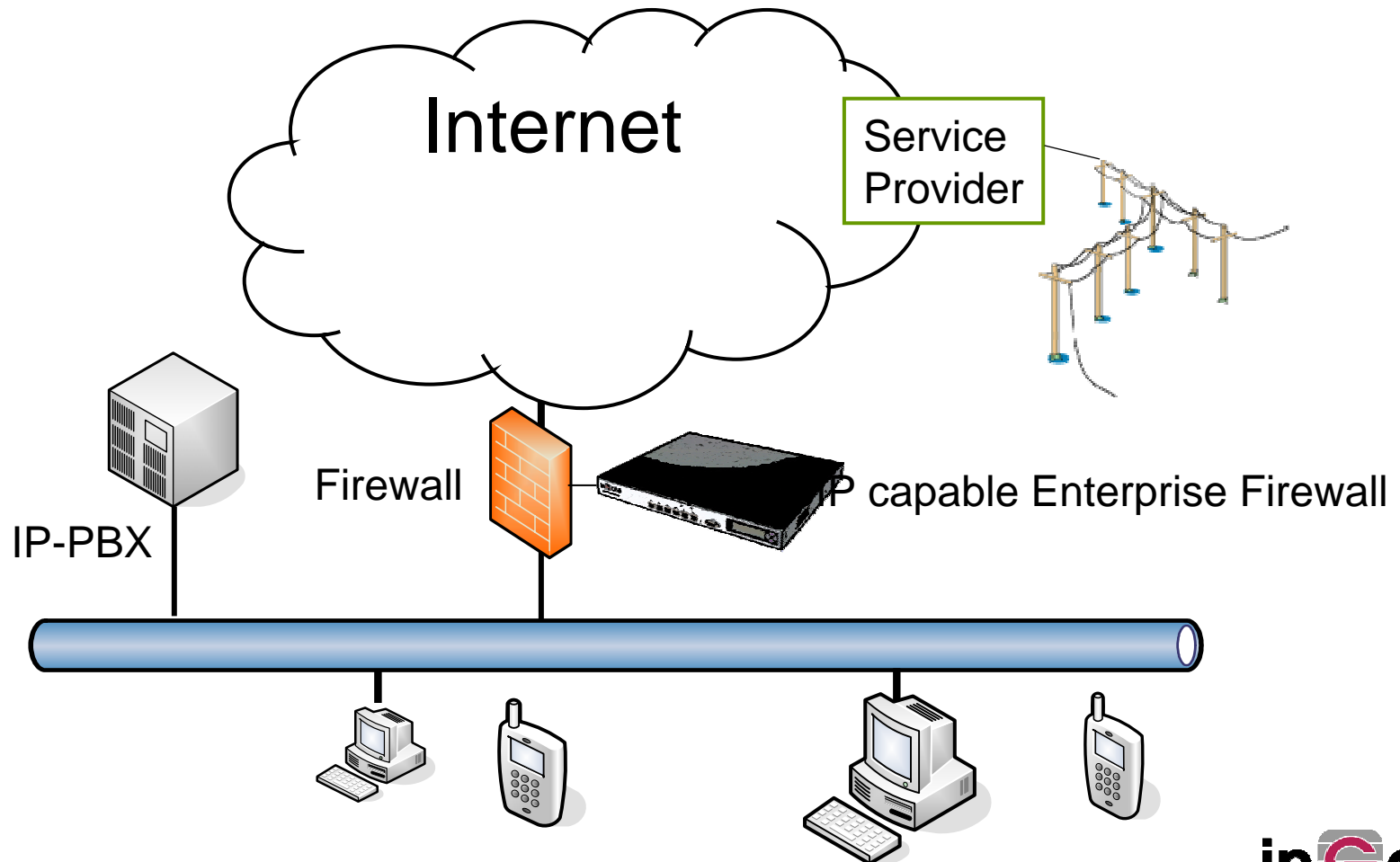


# A Enterprise edge device solves the problem

- Solves interop issues
- Designed for security
- QoS



# The SIP capability can be integrated into the corporate Firewall



# Who Shall be in Charge of the Firewall?

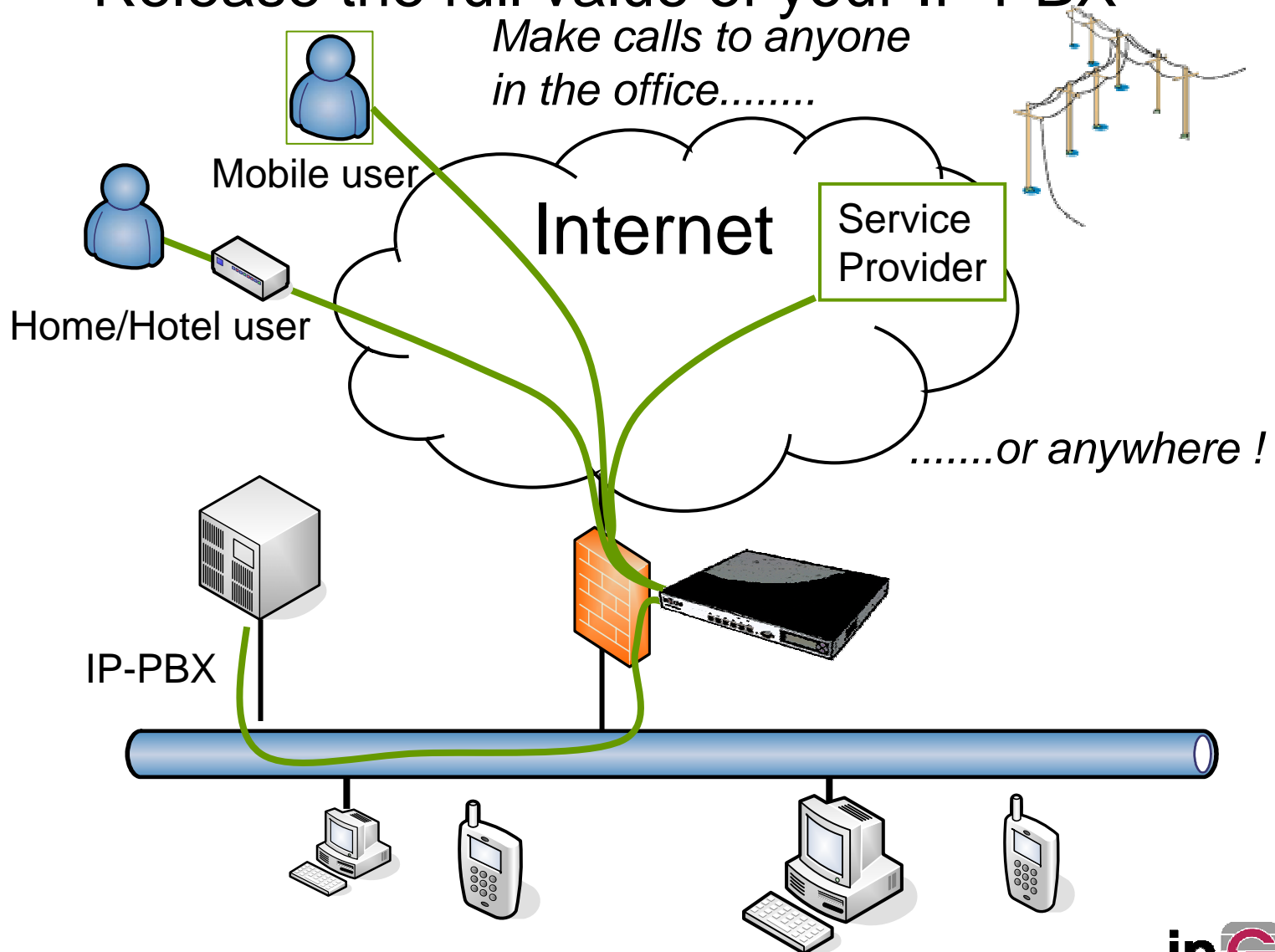
***The firewall manager, the users or some service provider?***

- STUN, TURN, ICE:
  - The users are in control, for SIP and ANY OTHER USAGE
  - The firewall has to be sufficiently open to allow this
  - Still cannot handle when the SIP Server is on the inside
  - Still interoperability problem and under development
- Session Border Controllers with Far end NAT traversal:
  - The service provider is in control
  - The firewall has to be sufficiently open to allow this
- SIP capable firewall
  - The firewall manager has a possibility to be in charge

# Increase mobility of the workforce

## Release the full value of your IP PBX

*Make calls to anyone  
in the office.....*



# Thanks

# Questions?

# The Function of a SIP Capable Firewall

- Check the SIP signaling
- Rewrite for the different address spaces
- Forward the signaling to the correct SIP proxy or client
  - For inbound calls – need to know location of each SIP user (unless registrar is on the inside)
- Open pinholes in the firewall for the media
  - Only for the duration of the call
  - Only between the exact endpoints
- Media flows through the pinhole (UDP/TCP)
- Close pinholes after the call

