Telco and SCADA working together

SEBASTIAN PITEI

ENEVO GROUP

Agenda

Who are we and what we do?

The Challenge

The Solution

The Ongoing Challenge

Some numbers

25 sites

75 devices

30 mobile power users

…in only 6 months

Who are we and what we do?

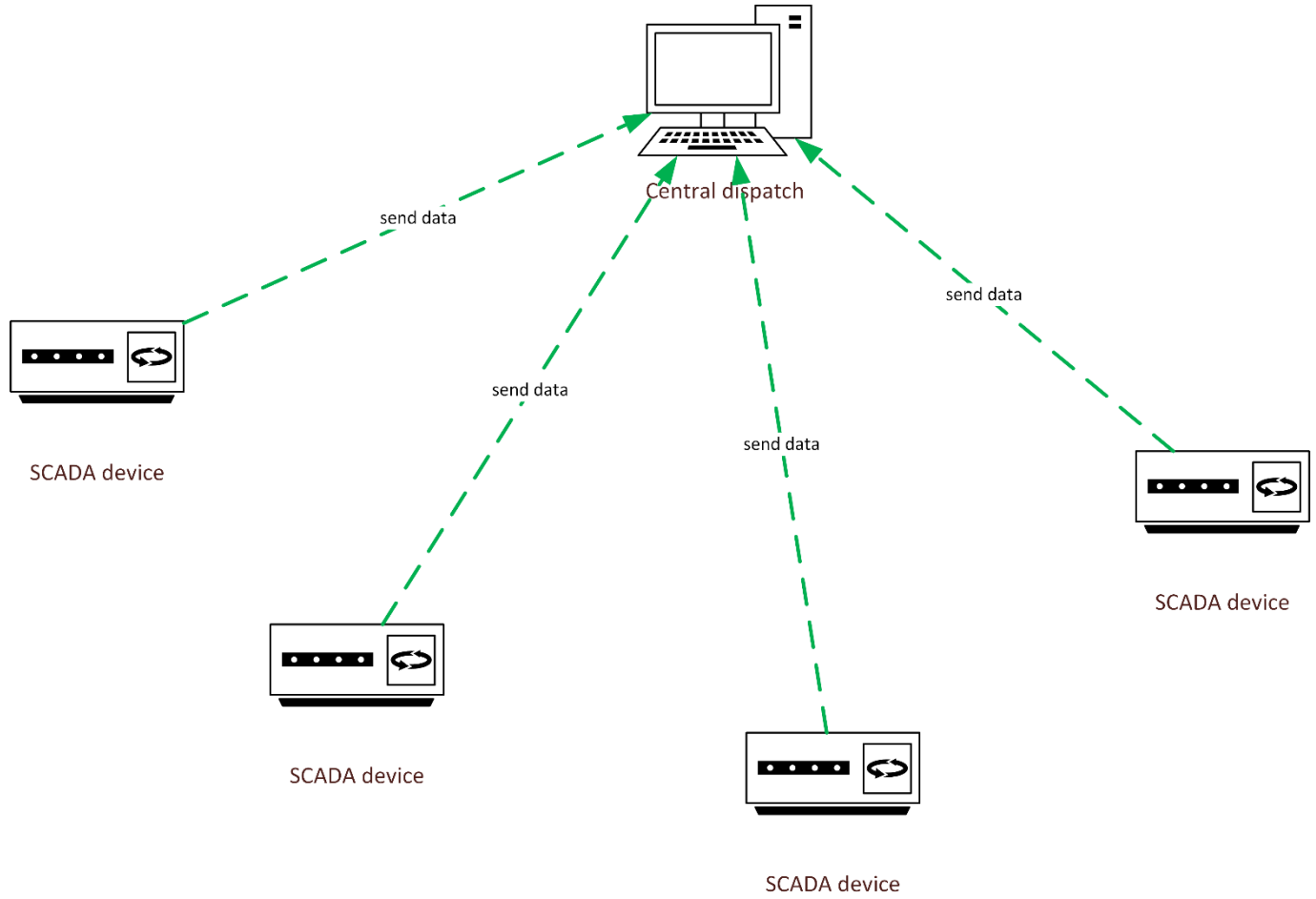
Company name: Enevo Group

Main focus: SCADA solutions

(that’s it?!?!? ☺)

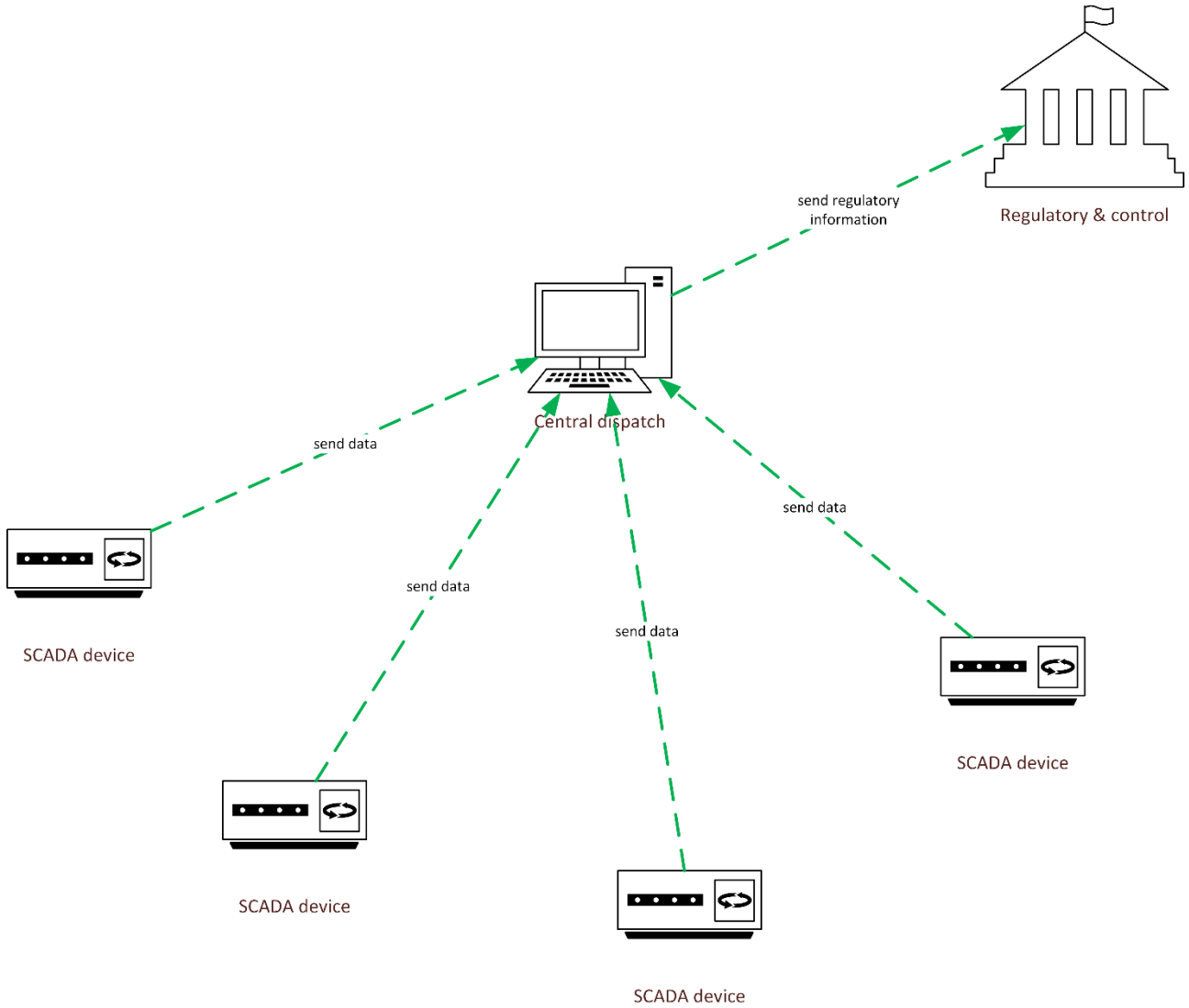
Simplified data flow

SCADA devices send information to customer’s central dispatch



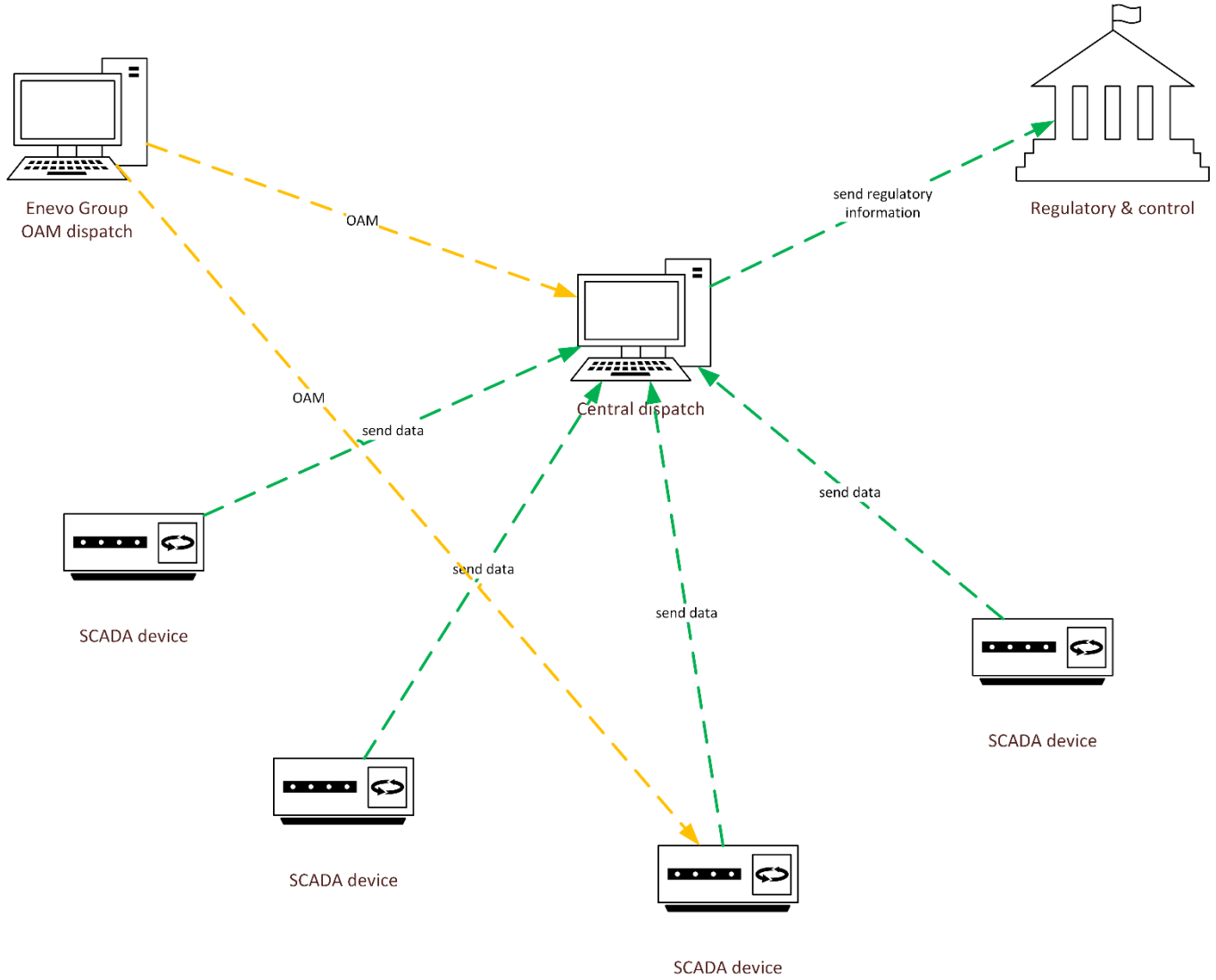
Simplified data flow (cont'ed)

customer's central dispatch sends regulatory information to relevant



Simplified data flow (cont'ed)

all SCADA equipment needs to be accessible for Operations, Administration and Management (i.e. OAM)



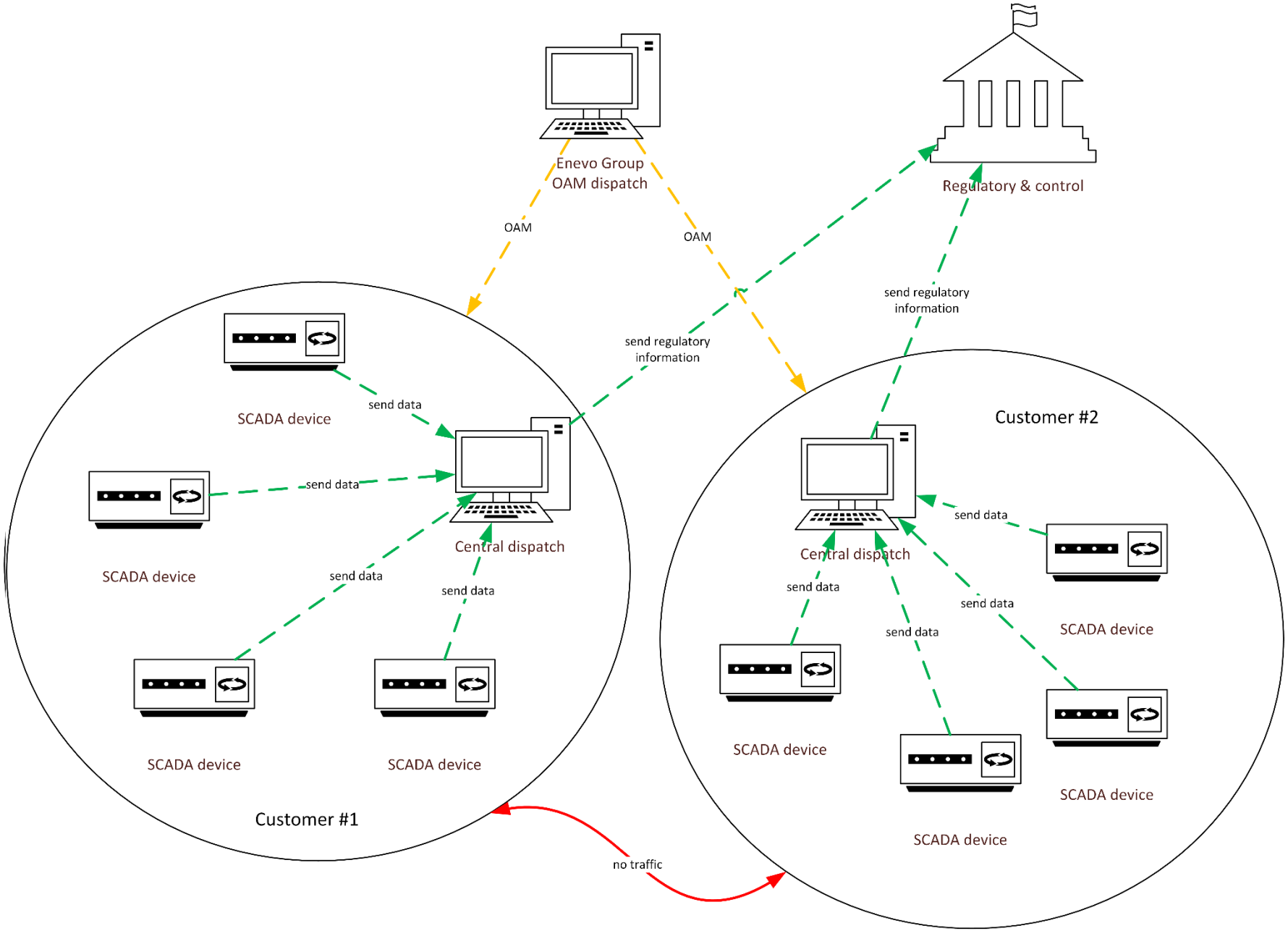
However…

each customer has multiple, geographically diverse locations

we have multiple customers

customer’s should access only their own infrastructure

all data transfers should as secure as possible


Enevo Group
OAM dispatch
OAM
OAM
Regulatory & control
send regulatory
information
send regulatory
information
SCADA device
send data
send data
SCADA device
Central dispatch
send data
send data
SCADA device
SCADA device
Customer #1
Customer #2
Central dispatch
send data
send data
send data
send data
SCADA device
SCADA device
SCADA device
SCADA device
no traffic

The Challenge

build the infrastructure presented so far

work with on-site customer assets

expect anything to be present (or not) at the customer site

no matter what limitation or challenges, the connectivity solution must work!

Connectivity, the big issue

only Internet present at customer site

customers present in remote locations with only DSL or radio Internet

certain locations are reachable only via 3G connections

public IP not always accessible

mixing VPN traffic with customer LAN traffic

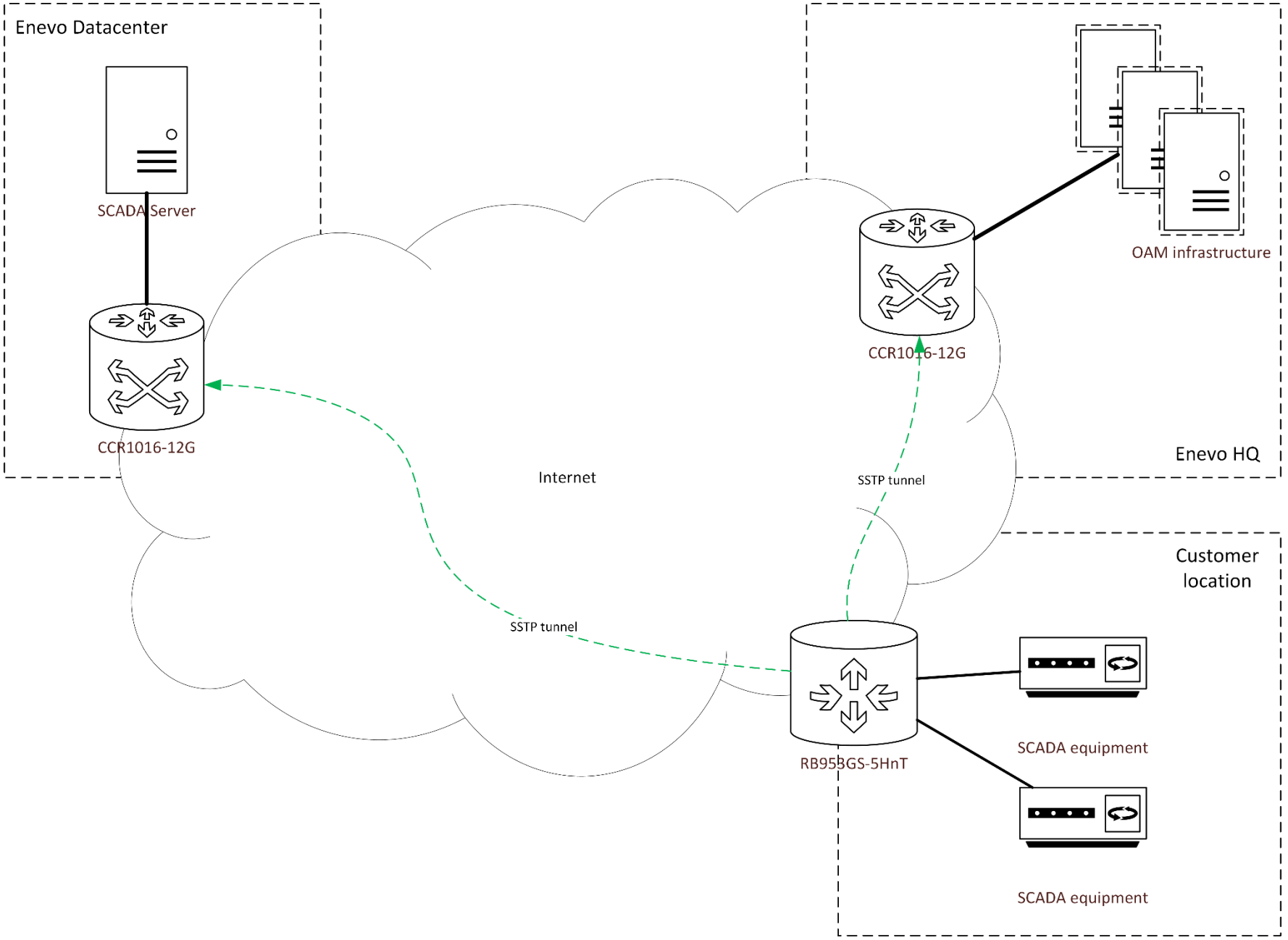
certain protocols and/or ports could be discarded, especially on 3G connections

Possible solutions

L2TP & PPTP are “heavy”, requiring multiple ports (e.g. UDP 500, UDP 4500, UDP 1701) and protocols (e.g. ESP, GRE)

OpenVPN is secure, but certificate generation leads to increased time to deploy

SSTP doesn’t required certificates (in Mikrotik RouterOS implementation), uses TCP 443 and is initiated from the customer side


Enevo Datacenter
SCADA Server
CCR1016-12G
Internet
SSTP tunnel
SSTP tunnel
CCR1016-12G
OAM infrastructure
Enevo HQ
Customer location
RB953GS-5HnT
SCADA equipment
SCADA equipment

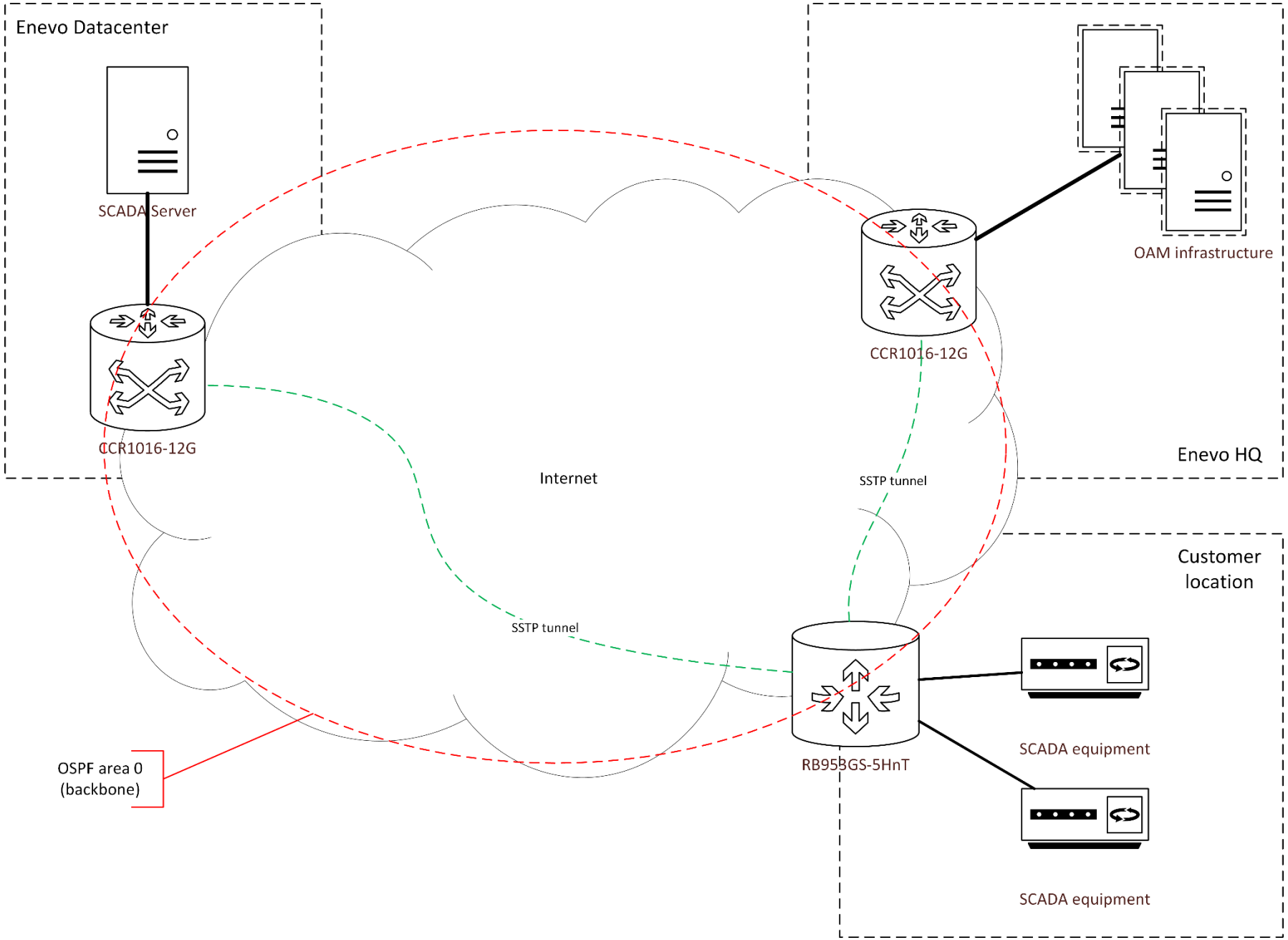
Routing

OSPF as the only possible solution

loopback interfaces are a must, not only for OSPF itself!

one big area 0 (i.e. backbone) across all devices

passive interfaces for all other


Enevo Datacenter
SCADA Server
CCR1016-12G
Internet
SSTP tunnel
SSTP tunnel
CCR1016-12G
OAM infrastructure
Enevo HQ
Customer location
RB953GS-5HnT
SCADA equipment
SCADA equipment
OSPF area 0
(backbone)

OAM

Names vs IP addresses: internal DNS

Work from anywhere: OpenVPN dial-in server

IP address management: phpipam

Central authentication: OpenLDAP & FreeRADIUS

Monitoring: Observium

Security

routing filter to limit routes installed in the routing table

firewall filters combined with dial-in VPN

restricting OAM access from defined IP ranges & jump-server

dial-in VPN needed even for in-office connection

Hardware used

RB953GS-5HnT

- 3 x 1Gbps ports
- SFP ports
- miniPCI-e ports
- additional Huawei MU609 3G card

CCR1016-12G

- powerful for medium applications
- good port density

The Ongoing Challenge

VPN MPLS deployment for customers with route leaking for common infrastructure

SSTP vs OpenVPN speed testing

DR site

Video surveillance

http://www.enevogroup.ro