Aalto University
School of Electrical
Engineering

Future Internet and 5G Using Customer Edge Switching and Ubiquitous Trust Processing + what is it and what are the benefits

Raimo Kantola
raimo.kantola@aalto.fi

www.re2ee.org

August 21st, 2015

What is Customer Edge Switching

Extension of Network Address Translator

Extension of Stateful Firewall to Cooperative Firewall

Manages all flow admission based on receiver/sender policy

Promotes cooperative security among administrations

Can eliminate spoofing and DDoS

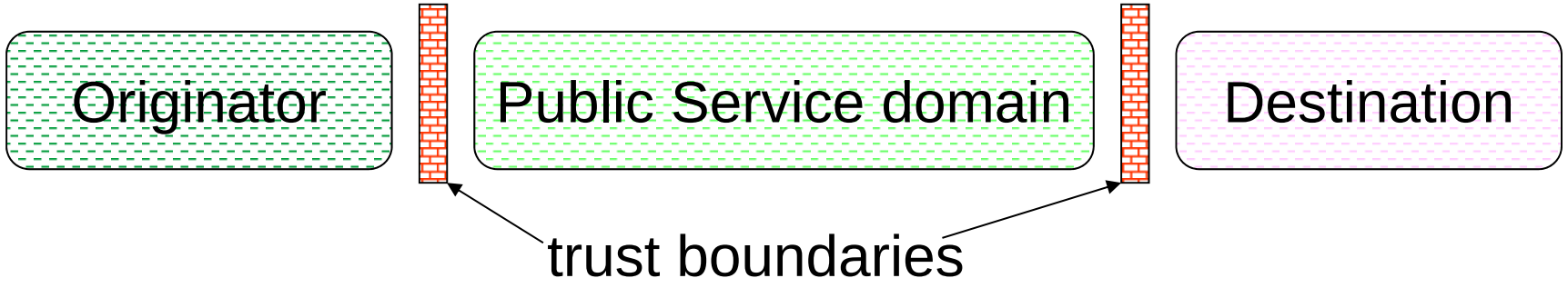
Can be deployed one network at a time

Trust Model for the Internet

Why: Prerequisites for cooperative behaviour are not in place directly between all hosts. Must be un-ending/frequent communication between actors, who understand reputation, have long memory and gossip effectively → hold for ISPs, mobile operators etc.

- The customer network will accept responsibility for good behaviour and misbehaviour of the hosts that it is serving
- ISP networks form federated trust domains
- Evidence of (host, application, customer network) behaviour is collected by each entity and aggregated by an **Internet wide trust management system** (can be many)
- Each entity (host, customer network etc.) has an ID; due to variability of needs of applications, many types of IDs should be supported.

Communication over Trust Domains

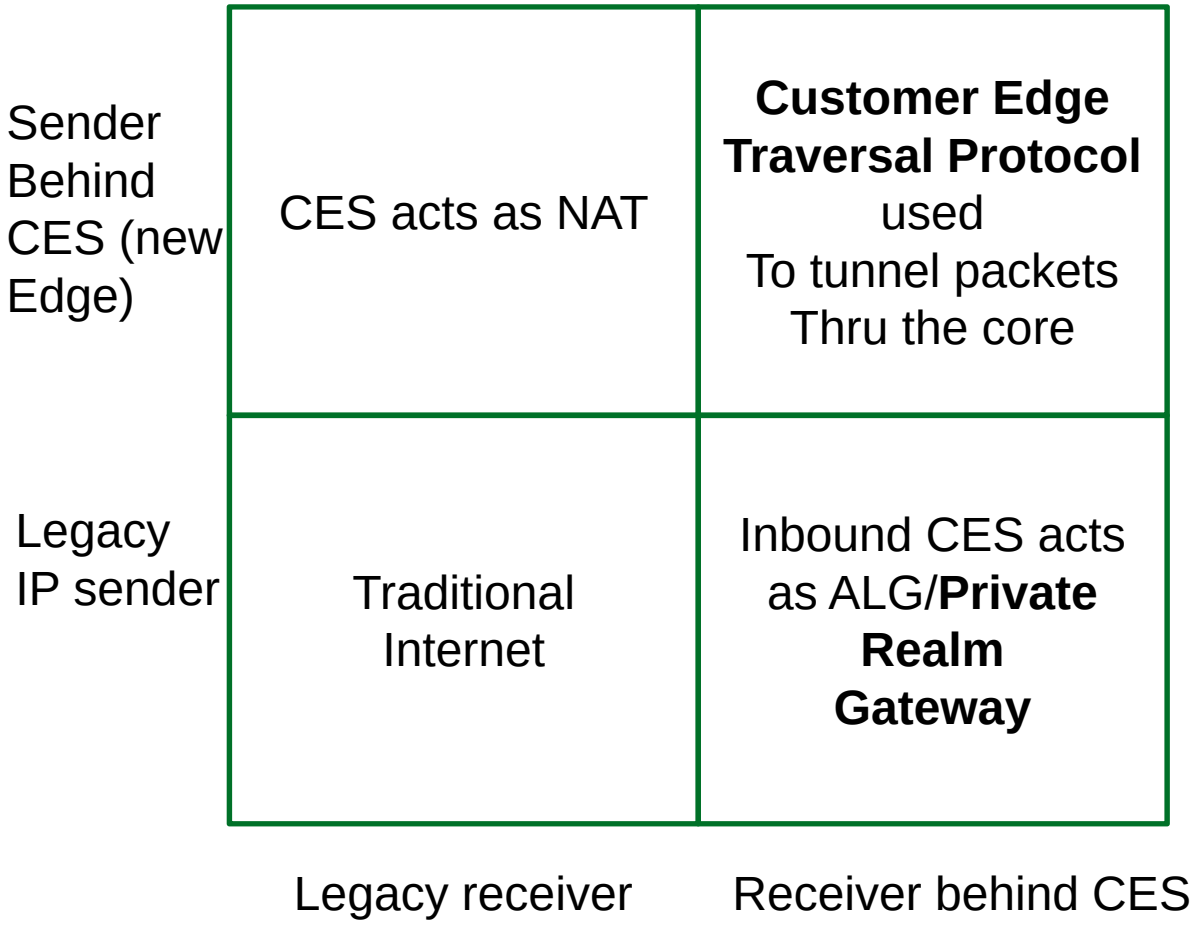


Originator and Destination are customer networks (stub networks in terms of IP routing)
+ each of them may have one or many private address spaces;
+ extreme case: mobile network addressing model: each user device is in its own address space and all communication takes place through the gateway or edge node connecting the user devices to the Internet

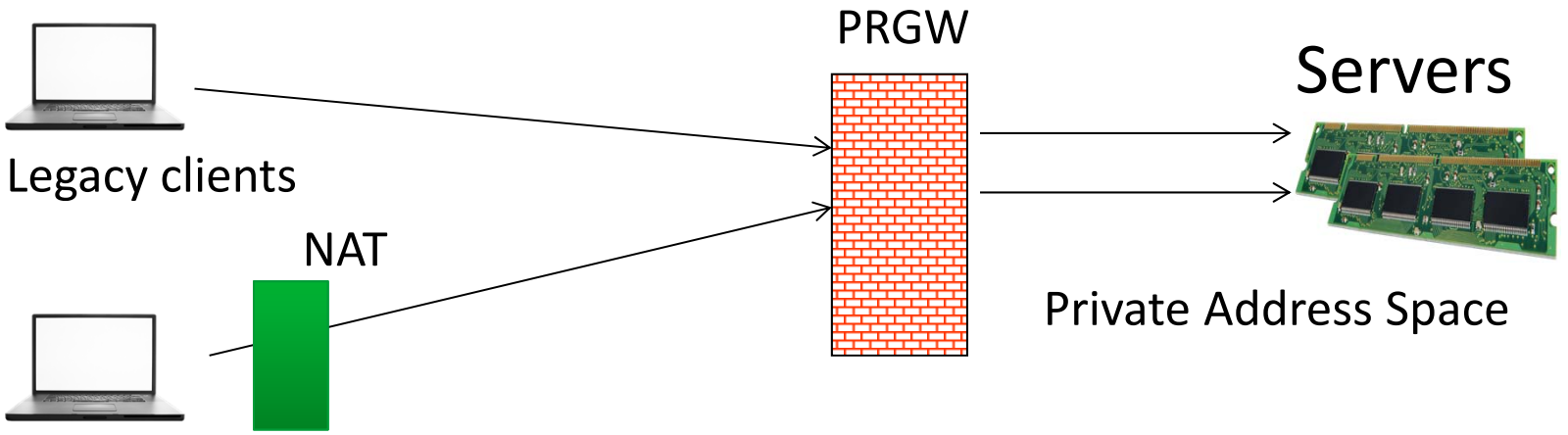
Trust Boundary == Customer Edge Switch == Co-operative firewall

A CES has one or several RLOCs (routing locators) that make it reachable in the public service domain

Signaling Cases



Private Realm Gateway



IDEA: Generalize NAT to server side

- Allow connections from any legacy client
- Admit flows by local policy (can use shared reputation info)
- no static configuration, NAT binding created dynamically
- use 3 approaches: Circular pool of addresses, Primary service and Reverse Proxy for http.

Deployment Constraints on the solution

- Because we can not solve the problems of unwanted traffic and NAT traversal in hosts for battery powered wireless devices
  - → MUST change a network node
  - → MUST not require changes in hosts at all
- Changes only in one place at a time: must bring benefit to the adopter irrespective what other players are doing

CES Product Use Cases

- CES for mobile broadband
  - CES hosts trust services for mobiles
  - Resides in the Mobile ”Core” network (PDN-GW) or Policy Enforcement next to BS.
  - Address allocation: each mobile in its own address space
- CES for fixed broadband
  - Hierarchical: partly implemented in xDSL modem, partly in the fixed access network gateway → also carrier grade realm gateway
  - The Access Network CES may have several IP addresses at the customer network side
  - If the Access network CES has many RLOCs, multi-interface access to the Internet can be supported
- CES for hosting trust services for corporate networks
  - Speeds up CES adoption
  - MUST have many IP addresses at the customer side and MAY have many RLOCs
- A Corporate network CES
  - Large corporations only, because CES must have an RLOC and ISPs may want to adopt a conservative RLOC allocation policy: SOHO – use CG hierarchical model

RGW use cases

- Standalone or Integrated with CES
- Single protocol vs. multiprotocol (IPv4 and IPv6)
- Customer Premises small (P)RGW and large Carrier Grade RGW with multiple connections
- CG RGW
  - Better robustness under attack (more options what to do under attack → more fine-grained response to attack)
  - Better scalability (less globally unique addresses needed)
  - Should have multiple interfaces towards the Internet
  - Can help to implement ISP level policies e.g. for cooperation with other ISPs against attacks

Related work on Future Internet

- Proposals can be classified by where changes are required:
  - Hosts; network nodes; if network nodes, which?
  - It is critical for adoption that the investor gets his money back
- IPNL, TRIAD, MILSA, Pub/Sub, Shim6, HIP, PBS (permission based sending), Information Centric Networks
- Typical weaknesses
  - Most popular motivation: scalability of the core → where is the new revenue?
  - Have to make changes in many places
  - Investments and benefits are not perfectly aligned or for some proposals: start Melcalfe's law from zero!

Conclusions on CES

- CES adapts Internet to the needs of mobile/wireless devices
  - NAT traversal →fast session setup, no NAT-traversal code in apps, less traffic over air interface, no polling→ saves the device battery
  - No source address spoofing based (DDoS) attacks over Air-interface
- CES improves scalability of the core: host addresses do not appear in core RT, renumbering of core has no impact on customer nets, renumbering or multi-homing of customer nets has no impact on core
- Trust: CES makes it practical to collect and attribute evidence of any misbehaviour
  - Internet trust system can calculate and assign trust/reputation values for each host, customer network and each application (white-, grey- and black-listing)
  - Policies can be dynamic: under attack apply stricter policy
  - Every aspect of CETP is policy controlled
- Isolation of technology choices due to tunnelling over the core: each network can choose its technology: IPv4, IPv6, versions of MPLS and Ethernet

What can we achieve for SECURITY by CES and Internet wide trust management?

- CES
  - Eliminate Source Address spoofing
  - Tackle DDoS attacks efficiently
  - Dissolve boundary between closed and open networks
  - Leverage Mobile network style IDs for data communications
- Trust:
  - Fast location of bots → “useful” lifetime of a bot is reduced → bot renting business becomes less profitable
- Together: improved robustness of critical infra → national security
- **BUT: most vulnerabilities are on application layer → security should be based on multiple layers of defense + proactive trust mgt**

Benefits to Mobile Operators (1)

- Technical benefits:
  - No spoofing over Air interface, no polling for NAT traversal over air interface, no cluttering of mobile Apps, DDoS resistance; saving of device battery; less useless/non-chargeable traffic over mobile networks; more robust service (malicious actors can not disrupt service); ease of renumbering; isolation of technology choices; multi-homing with no impact on non-default core network routing tables…
- MO can become a trust broker among customers: mediate customer to customer trust
  - Leverage mobile IDs (USIM+HSS) to datacoms
- Makes sense to build an alternative non-default core for the Internet with entry points in every major eyeball ISP using CES nodes → spoofing and DDoS mitigation for all traffic
  - When under attack makes sense to prefer traffic sourced through this new trusted non-default core
  - Still need to verify this use case!

Benefits to Mobile Operators (2)

- MO can sell Trust as a cloud service (e.g. Firewall in the cloud) – (Silver Service)
  - Fast trace back of attacks
  - FW rules can be per subscriber and follow the sub while the sub is roaming
  - Business customers and Families
  - Dissolving the closed/open network boundary: implementing “Family and Friends” or “me and my gadgets” –like service by defining a suitable policy.
  - Help in cleanup after infection; may be security can be sold as insurance? Clean-up fee for opt-out customers?
- MO can sell Security as a cloud service (Gold Service)
  - Cloud knows exactly what Apps mobile device is running and automatically takes care of updates; admits exactly this traffic.
  - Probably together with security software companies and App Stores
  - Trust processing must know that such customers are not careless!

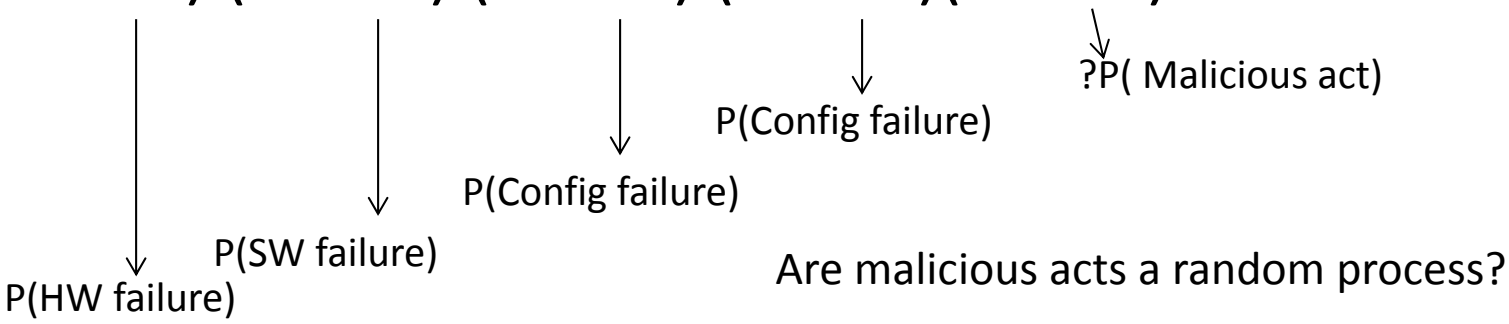
Benefits to Mobile Users

- Battery saving when using communications apps
- Fast session setup for VOIP, (even P2PSIP) for all communications apps → VOIP matures to Quality of experience where it is a real alternative to circuit telephony (ITU-T requirement for session setup: 2s)
- Better protection against all attacks
- Other
  - Non-repudiation of Transactions such as sw or even file download, commercial operations?
  - Parental control using FW in the cloud (like Internet is closed 2200-0500 for teens)
  - Tailored to corporations: security as a cloud service

5G – ultra reliable communications

- Is it a very secure network over which malicious actors can effectively conduct fraud?
- Or will the MOs do their best to prevent fraud and protect their customers using whatever means are technically feasible?

$$R = (1 - F1)\,(1 - F2)\,(1 - F3)\,(1 - F4)(\,1 - F5)$$



Extra1: What about scalability and IPv6?

- Most hosts (80%) should have only private IPv4 address
  - Each host may be in its own private address space or a private address space may be shared by e.g. corporate hosts.
- Network nodes and Heavy duty servers may have globally unique IPv4 addresses
- Core routing table: host addresses are gradually removed from the RT → less power hungry, fast memory in routers.
- Technically, it becomes easier to deploy IPv6 but the urgency to do so will be relieved.

Extra 2: What about UNSAF style NAT traversal

- From deployment point of view, CES can be seen as an optimization of UNSAF (ICE etc)
- Apps that use NAT-unfriendly protocols and do have an ALG in every CES, can continue to traverse NATs (and CES) using e.g. ICE
- It is important for CES to be compatible without ICE/UNSAF with most communications apps used by mobile devices – from Nokia/Ericsson point of view, the rest can keep using ICE etc.