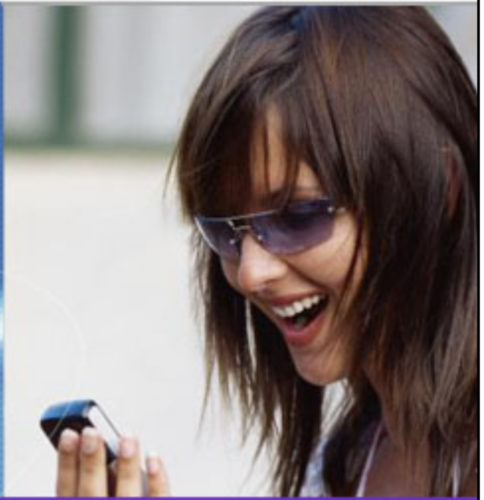
Alcatel·Lucent

Secure Cloud Computing with a Virtualized Network Infrastructure

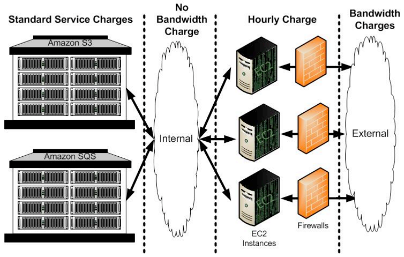


Fang Hao, T.V. Lakshman, Sarit Mukherjee, Haoyu Song

Bell Labs

Cloud Security: All or Nothing?

Amazon EC2



Shared computing,
storage, & network

Government Cloud

Dedicated infrastructure,
secured facility

"Good enough"
security
with low cost?

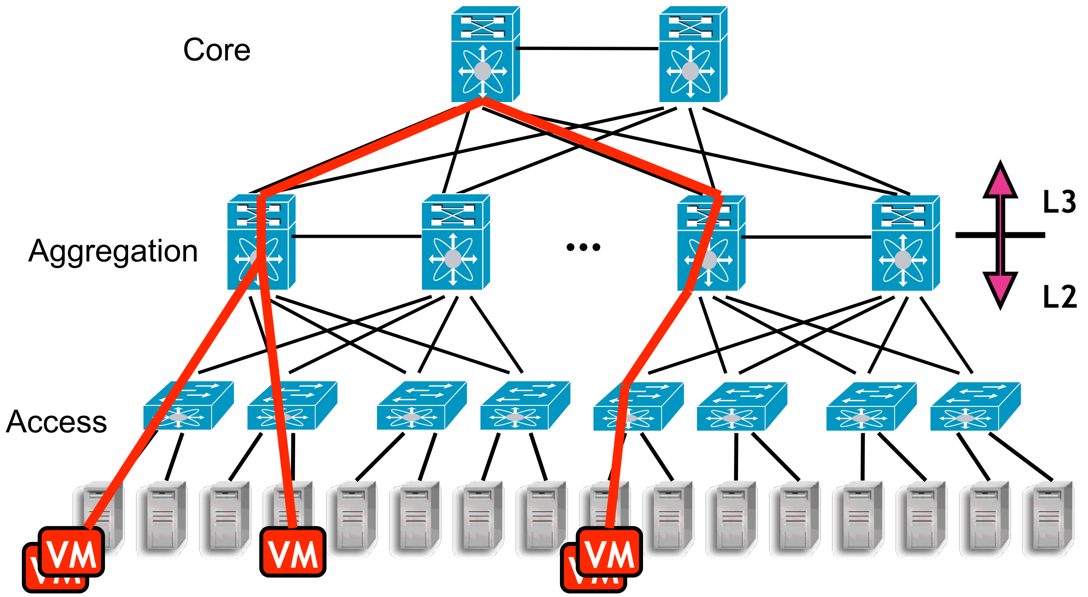
- Max sharing, low cost
- Low security

- No sharing, high cost
- Max security

Secure Elastic Cloud Computing (SEC2): Design Goals

- Isolation: private IP address space and networks, no trespassing traffic
- Transparency: users don't see underlying data center infrastructure; they only see their own (logical) network
- Location independence: user's VMs and networks can be physically allocated anywhere in data center
- Easy policy control: users can change policy settings for cloud resources on the fly
- Scalability: service scale only restricted by total among of resources available, not dependent on customer composition
  - A few large enterprises vs. many small business or individual users
- Low cost: use off-the-shelf devices whenever possible

Provide Isolation in Traditional Data Center Architecture

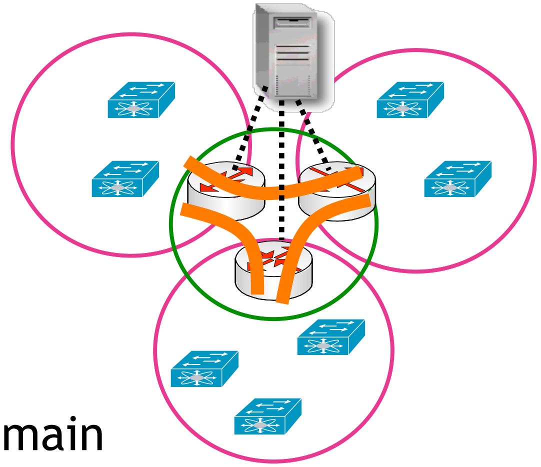


- Unique VLAN can be set up for each user
  - VLAN extended to hypervisors
  - Each VLAN can have its own IP address space
- VLAN extended beyond L3 boundaries via VLAN trunking

Constraints

- VLAN scalability
  - Maximum 4K VLAN Ids << number of users
- Per-user policy customization is difficult
  - E.g. port 80 traffic ⇨ firewall ⇨ NAT ⇨ load balancer ⇨host

Secure Elastic Cloud Computing (SEC2): Main Idea



Partition data center network into smaller domains

- Use VLANs to isolate customers within a domain
- No “global” VLANs
- VLAN ids reused across domains

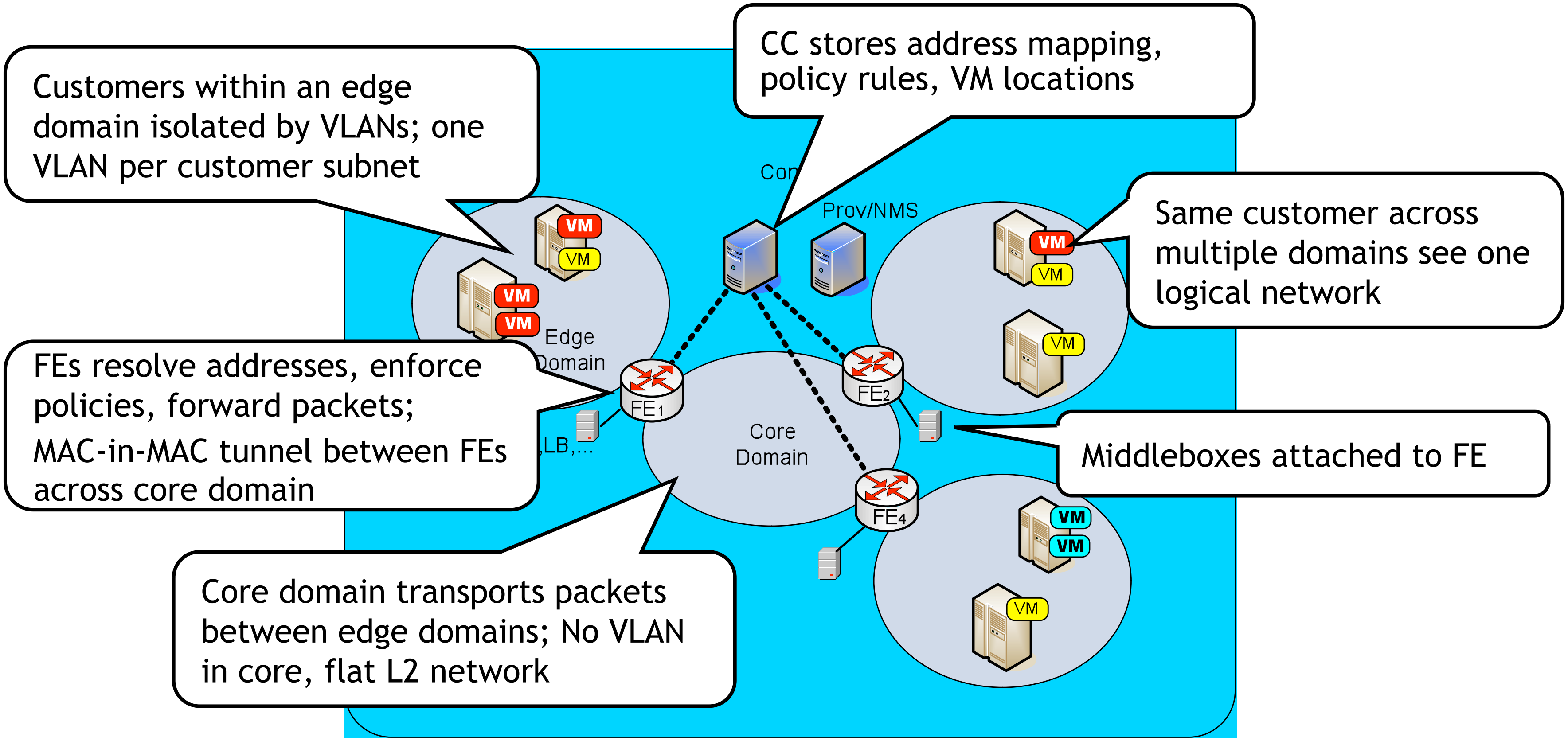
“Glue” different edge domains together via one central domain

- Special forwarding elements (FE) deployed at border of central and edge domain
- Central controller (CC) stores mapping between user and their VLANs in each edge domain
- Traffic between edge domains are tunneled through central domain by FEs

Per-user policy control

- Middleboxes attached to FEs
- Policy routing enforced by FEs
- CC stores per-customer policy, allow on-the-fly user configuration

SEC2 Architecture



Customers within an edge domain isolated by VLANs; one VLAN per customer subnet

CC stores address mapping, policy rules, VM locations

Same customer across multiple domains see one logical network

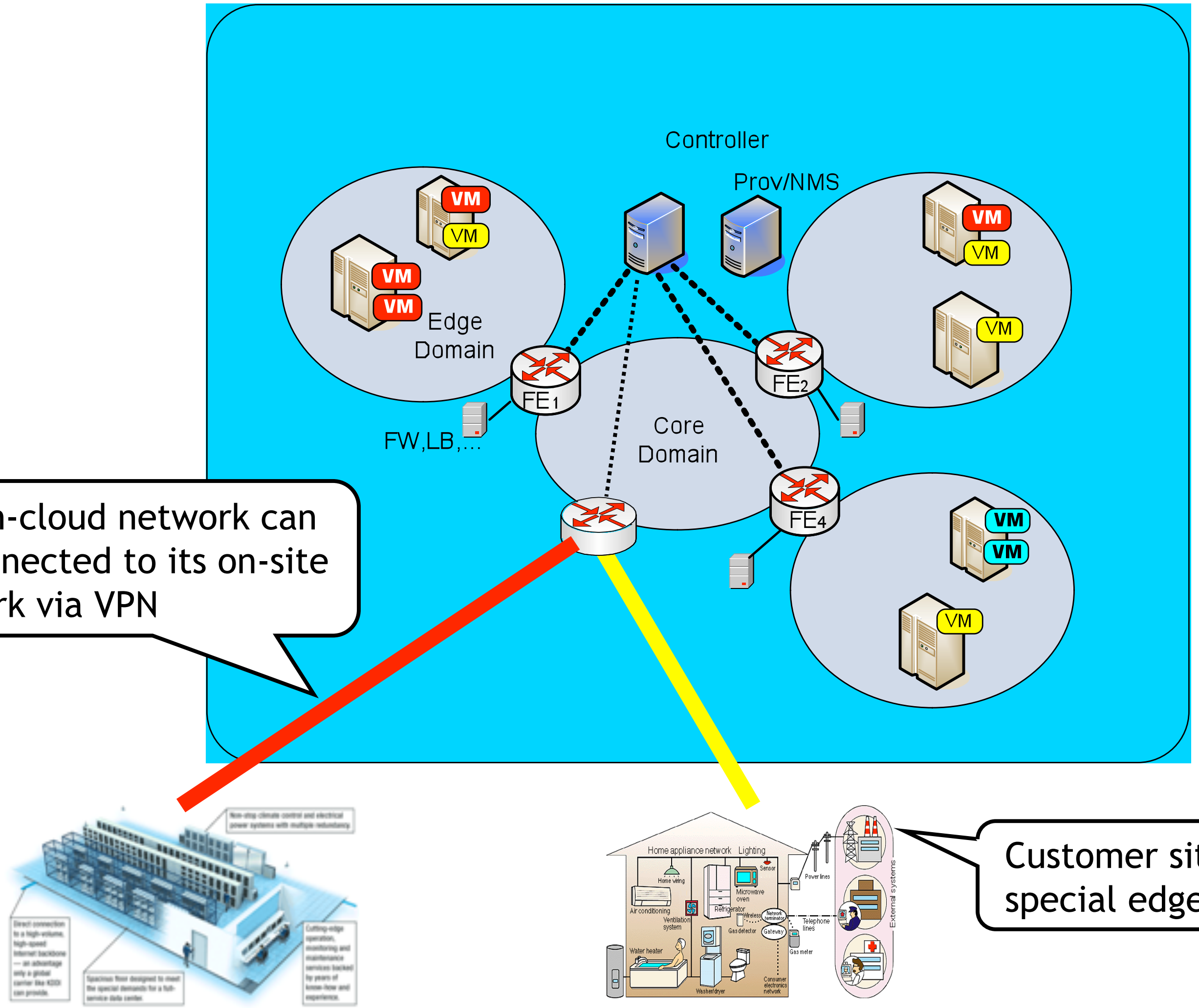
FEs resolve addresses, enforce policies, forward packets;

MAC-in-MAC tunnel between FEs across core domain

Middleboxes attached to FE

Core domain transports packets between edge domains; No VLAN in core, flat L2 network

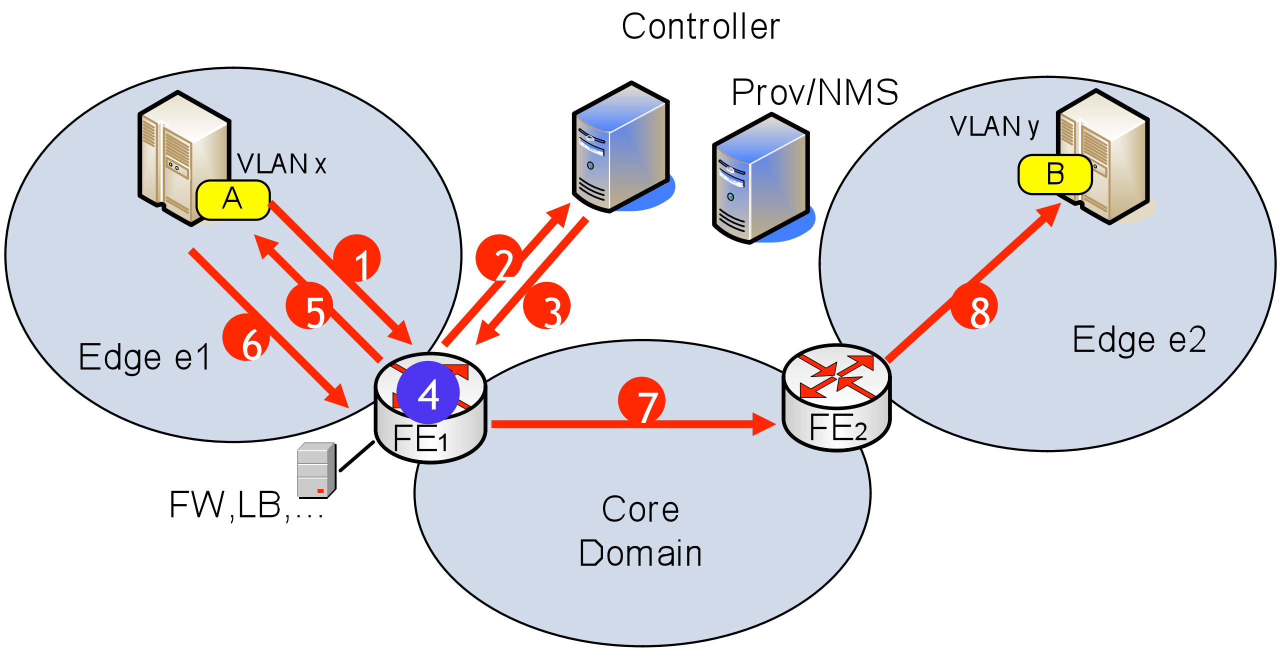
Integration with User’s On-Site Network



User in-cloud network can be connected to its on-site network via VPN

Customer site is a special edge domain

Data Forwarding



1) ARP on VLAN x: What's MAC for IP$_B$?
2) Query CC: IP$_B$,x ⇨MAC$_B$?
3) Reply from CC: MAC$_B$ in y, with MAC$_{FE2}$ as tunnel end
4) Install rule at FE1: "To MAC$_B$: set VLAN y, add tunnel header to MAC$_{FE2}$"
5) ARP reply: MAC$_B$
6) 7) 8) Data packet forwarding (tunnel header added by FE1, stripped off by FE2

Security via Isolation and Access Control

Potential attack on Amazon EC2 outlined by Ristenpart et al. CCS'09

- Key is to determine co-resident VMs by
  - Determine matching Dom0 IP address via traceroute
  - Test for small round-trip time
  - Check for numerically close IP addresses

- None of such attack works in SEC2
  - Traceroute is disabled between different users
    - They don't even know other's IP address
  - All packets across different users are forced to go through FEs ⇨round-trip time won't reveal location
  - Private IP addresses: no correlation between different users

Concluding Remarks

SEC2: a step towards “good enough”, low cost secure cloud solutions

- Security via isolation and access control
- Scalable: well beyond 4K limit imposed by VLAN
- Low cost
  - Allow high resource utilization
  - Most networking equipments are off-the-shelf, e.g., switches within both edge domains and core domain are regular L2 switches
    - FEs can be L2 switches enhanced with Openflow or SoftRouter like functions