Using LISP for Secure Hybrid Cloud Extension

draft-freitasbellagamba-lisp-hybrid-cloud-use-case-00

Santiago Freitas
Patrice Bellagamba
Yves Hertoghs

IETF 89, London, UK

A New Use Case for LISP

- It’s a use a use case draft.
- Covers the use of LISP to enable a secure layer 3-based Hybrid Cloud Extension.
  – Relevant for Cloud bursting, Workload migration, Rapid provision of new applications in the cloud and disaster recovery use cases.
- 67% of Enterprises expected to be pursuing a hybrid cloud computing strategy by 2015 (47% the year before)
  – Source: Gartner DC Summit 2012

A New Use Case for LISP

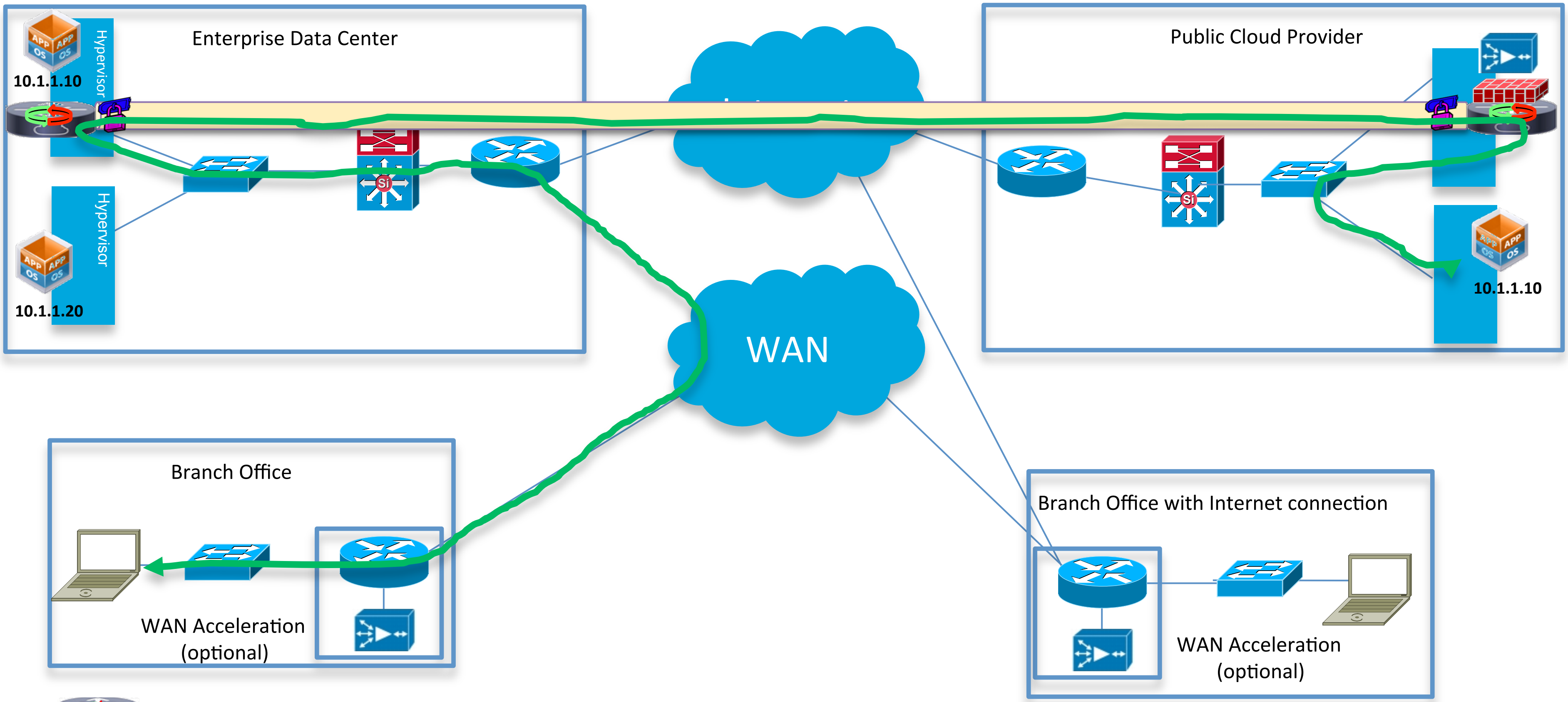
- LISP, in combination with IPsec or any other encryption mechanism, to be implemented on a virtualized router deployed on a public cloud and on the enterprise DC.
  - Allows virtual machines (VMs) to be moved to the cloud without changing the VMs IP Address / Mask / Default Gateway; Same subnet on both sites.

- Running code available and tested on large cloud providers.

Advantages over other proposals

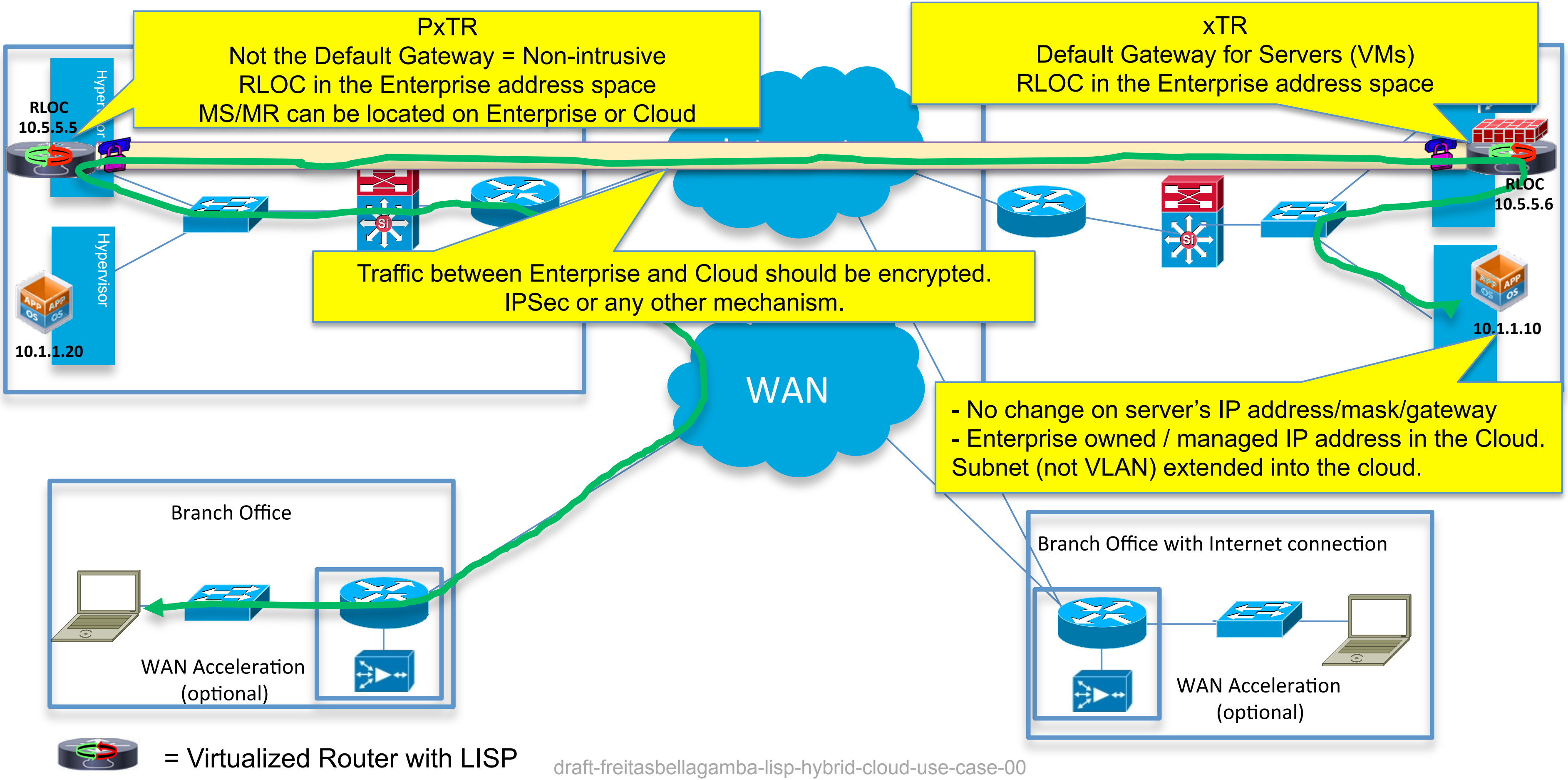
- Does not extend the failure domain
  - Total isolation of broadcast (Layer 2) domains between Enterprise and Cloud.
  - It allows a routed (Layer 3) connection between sites.
- Natively provides Gateway in the Cloud for optimal routing between servers moved to the Cloud.
  - No hair pining save “InterCloud” bandwidth / latency.
- Works with any standard VM in the Cloud, no need to modify the VM for migration.
- Ingress Path-Optimization from remote sites to the Cloud easily achievable.

Using LISP for Secure Hybrid Cloud Extension



= Virtualized Router with LISP

Using LISP for Secure Hybrid Cloud Extension


RLOC
10.5.5.5
Hypervisor
APP OS
10.1.1.20
Si
WAN
RLOC
10.5.5.6
10.1.1.10
Branch Office
WAN Acceleration (optional)
Branch Office with Internet connection
WAN Acceleration (optional)

PxTR
Not the Default Gateway = Non-intrusive
RLOC in the Enterprise address space
MS/MR can be located on Enterprise or Cloud

xTR
Default Gateway for Servers (VMs)
RLOC in the Enterprise address space

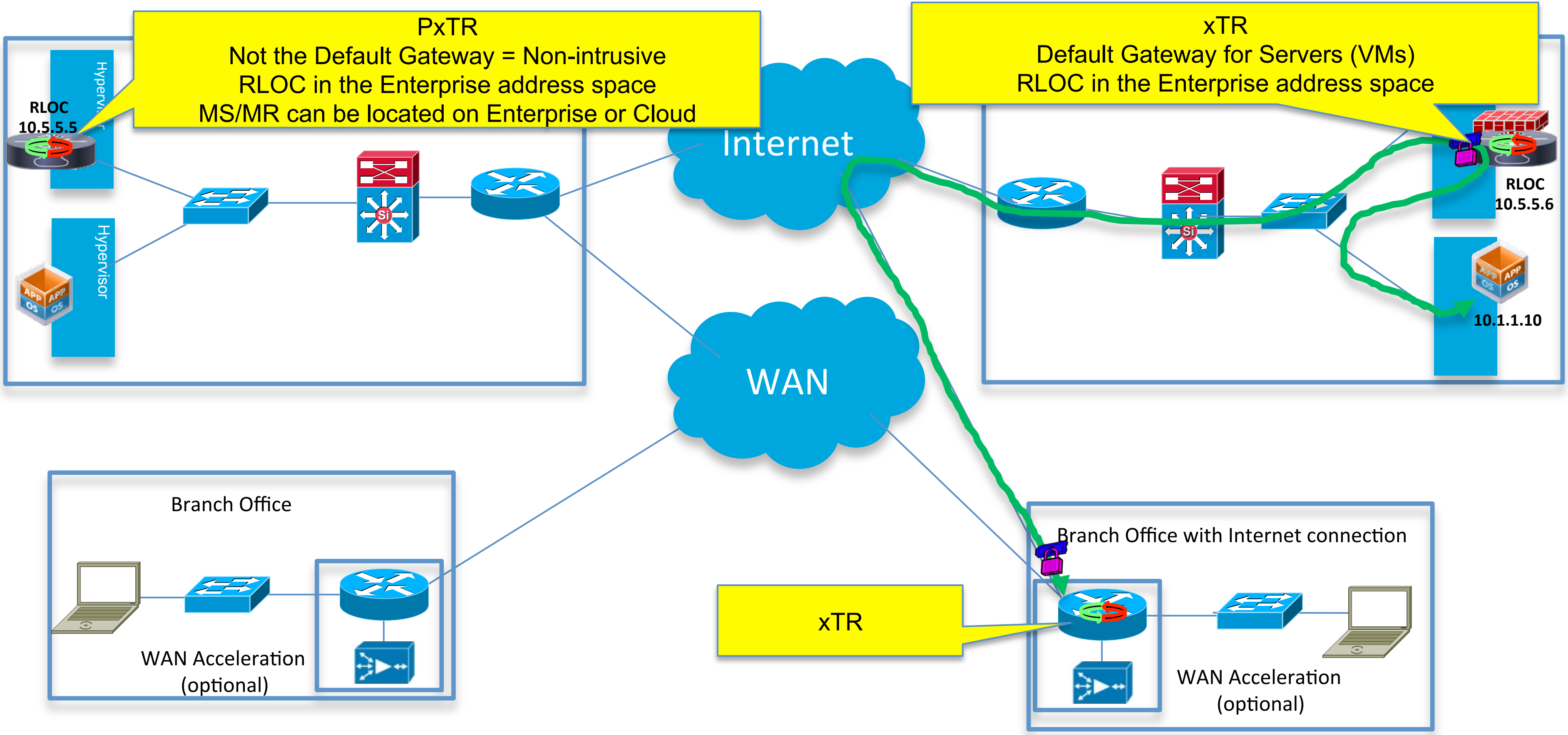
Traffic between Enterprise and Cloud should be encrypted.
IPSec or any other mechanism.

- No change on server’s IP address/mask/gateway
- Enterprise owned / managed IP address in the Cloud.

Subnet (not VLAN) extended into the cloud.

= Virtualized Router with LISP

Using LISP for Secure Hybrid Cloud Extension



PxTR
Not the Default Gateway = Non-intrusive
RLOC in the Enterprise address space
MS/MR can be located on Enterprise or Cloud

xTR
Default Gateway for Servers (VMs)
RLOC in the Enterprise address space

xTR

= Virtualized Router with LISP

Feedback received on Mailing List

- Concern with the use of pre-established IPsec tunnels
  - Secure connection (encryption) between enterprise and cloud is needed, IPSec used as a transport to encrypt the LISP flow. It's one option, other options will be incorporated into future versions of the draft.
  - How to extend the RLOC space into the cloud should also be considered; IPsec allows NAT, native LISP data plane and control plane address translation to be further investigated.
- Document should be more explicit about what the resulting message stack looks like.
  - Will be covered on version 01.

Areas to be included on version 01

- More explicitly stating where the IPsec tunnel is and incorporating other options for encryption where IPSec tunnel becomes optional.
- Discuss how private IPv4 addresses will be handled and where NAT devices will be deployed.
- Performance and Scalability Considerations
- Management and Automation Considerations
- Document the resulting encapsulation stack.

Ask to the Working Group

- Adopt this draft as one of the use cases for LISP.
- Consider the Secure Hybrid Cloud Extension Use Case to aid in future evolution of the protocol.