Clouds and Governments

Cloud technologies are being adopted by governments around the world.

- "Recommended Security Controls for Federal Information Systems and Organizations" is a document with NIST's recommendations for governments, cloud technologies included (NIST 800-53), updated in April 2013.
- Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is currently supported by US General Services Administration.
- In September 2012, the EC has launched the "European Cloud Computing Strategy", just as commissioner Neelie Kroes endorses new open-source technologies

IPv6 Security Issues to Care About

IPv6 is here to stay. It is important to know what changes it triggers in your network's security configuration.

GEN6 aims to help you from the following perspectives:

- How to check thoroughly what security implementations are incorporated when you do provisioning. When new equipment is purchased, provisioning support for IPv6-ready equipment should be checked thoroughly.
- IPv4 to IPv6 transition technologies and the security issues that they introduce. What do expect when you use dual stack, tunnelling and translation technologies.
- Specific IPv6 security issues in a network and how they are addressed by the community.

GEN6 aims to give advice on how you can transition to IPv6 without decreasing the security of your services and system.

ABOUT GEN6

Work was in part supported by the European Commission as part of the project »Governments Enabled with IPv6« (GEN6). GEN6 is about stimulating EU-wide deployment of IPv6 by means of best practices and guidelines.

- National pilots to make a step further in IPv6 deployment in different sectors
- Cross-border pilots to demonstrate EU-wide interoperability of IPv6
- Communication activities and road shows to ensure dissemination in public administrations and with other relevant stakeholders

Supported by EC, Grant nr. 261584

Interdisciplinary Center for Security, Reliability and Trust

University of Luxembourg
4 Rue Alphonse Weicker
L-2721 Luxembourg

+352 46 66 44 5721
Visit us at http://uni.lu/snt

Secure Cloud Services with IPv6

Luxembourg Pilot

SnT, University of Luxembourg

IPv6 for Future-Proof Infrastructures

What is the pilot about?
The Luxembourg pilot focuses on the transition of an IPv4 to an **IPv6 private cloud**. A private cloud is generally operated for a single organisation. In this effort, SnT benefits from local support, by collaborating with the Centre de Communications du Gouvernement.

What is our vision?
IPv6 enabled clouds are **the infrastructure of the future**, and the public sector should benefit from its use.

What will the **output** be?
A set of guidelines for governments on how to do the transition, as well as tools for checking security properties of cloud services.

The Cloud for the Luxembourg Public Sector

For public administrations, deploying cloud computing has some advantages that are hard to beat:

- **Independence from hardware** that is difficult to maintain. Legacy software that is important can be turned into virtual machines, and thus can stay unchanged even if the underlying infrastructure changes.
- **Availability and reliability**. The 2011 report of activities of the Luxembourg Government, mentions that the Committee for Critical Infrastructures in ICT is coordinating the buildup of a crash center with a 99.995% availability, for critical IT services to the European Reliance Center East.
- Very **low maintenance costs**, as these efforts are shifted to the cloud hardware infrastructure provider.

Instead of outsourcing data and infrastructures over the borders, the local government can opt for a private cloud option (i.e., a cloud infrastructure operated solely for a single organisation). Very important is that in Luxembourg there is a large market for datacenters, with a number of big players of which EBRC, ClearStream, SecureIT, P&T.

IPv6 in the Cloud

The boost of addressability and flexibility offered by IPv6 couples well with the cloud's need for massive scalability (e.g., virtual interfaces).

With IPv6 in the cloud, NAT is eliminated and hence many awkward host accessibility problems disappear. Providers no longer need strategies of how to split internal address spaces into hierarchies. Provision is much easier, and virtual machine configuration can be made on demand, automatically.

Customer connectivity is improved by means of the "always-connected" seamless experience of mobile IPv6: virtual machines can be relocated without affecting user connectivity. In addition, it is now possible to have peer-to-peer communication among virtual hosts and systems.

However, the adoption of IPv6 is likely to impact current security configurations: firewalls and other network-level defenses should be rethought with IPv6. Thus, further work should be done in that direction to help cloud customers and providers.

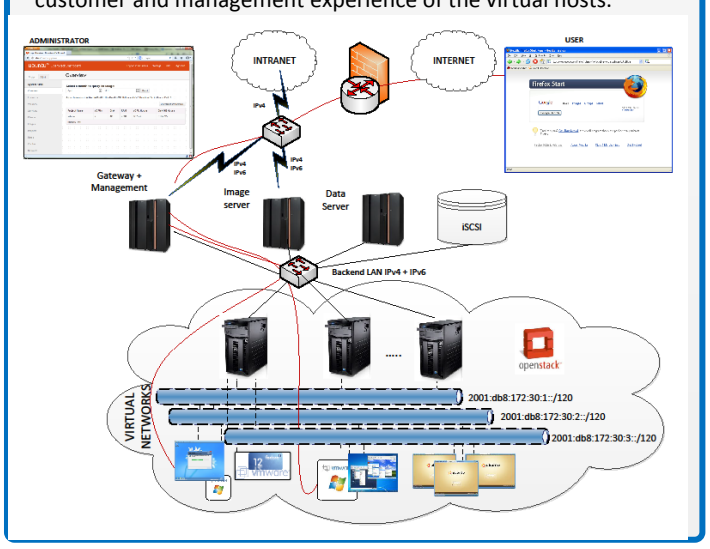
Luxembourg Pilot

The Luxembourg pilot is based on the open-source software called OpenStack.

Why open-source based private clouds?
OpenStack is one of the most popular open-source cloud distributions, and we have chosen it for our deployment because of its global community and its agility. OpenStack is a massively scalable cloud operating system, currently used by actors such as the US Department of Energy, San Diego Supercomputer Center, Intel, Cisco WebEx, or PayPal.

IPv6 transition of an open-source cloud
OpenStack supports IPv6 but provides little help in how to configure its use. With GEN6, UL will deliver a methodology for IPv6 transition that governments can use to migrate in-house cloud services, without losing their existing autonomy. The resulting methodology and guidelines will contribute to the global community as well.

Building blocks
UL's cloud computing pilot consists of a fleet of virtual machines deployed on existing hardware and managed by OpenStack APIs. These virtual hosts can support any OS and are connected in virtual networks. Such networks can be accessed through a dashboard by cloud administrators (internal) and by clients from the internet. New hosts can be deployed on demand. As mentioned above, IPv6 addressability will sensibly improve customer and management experience of the virtual hosts.



Usage on the Long Run

The common problem.
Any government service is deployed on a system with a certain configuration (e.g., a number of Windows servers currently using IPv4). If you are managing that service, you will meet with situations such as the following:

- Your network is upgraded to IPv6, and your software should speak IPv6 too;
- A new service is installed in the system and you need to know if that service would affect overall service stability;
- The OS or an existing application other than the service are patched/upgraded;
- You need to check IPv6 compatibility of software across your network.

Checking by hand if your service is unaffected in these cases is painstaking and error prone.

The vision.
Automating the testing of the cases above would be a great Step forward for both system administrators and managers who need to ensure the performance and reliability of the government service. With our pilot, GEN6 can bundle together a set of tools, test suites and guidelines that, in a private IPv6 enabled cloud context, can test IPv6 readiness and security of services that are offered by public administrations. The picture below shows a possible architecture of the internal cloud-based testbed that we are proposing with the Luxembourg pilot.