CPE, Normandy regional network - SYVIK

Alain BIDAUD (CTO), Sébastien VIGNERON (system and network admin)
CRIANN

GÉANT Infoshares, December 8th 2021

Public

www.geant.org

CRIANN – SYVIK – Normandy Region

- SYVIK is the Normandy regional network for Education and Research, connected to RENATER (the French NREN)

- CRIANN is the pilot of the SYVIK network

- One of SYVIK's clients (and funder) is the Normandy Region, which manages all the CPE routers in Normandy high schools, which themselves connected to the SYVIK network

Normandy CPE - use case & goal

- CRIANN has been mandated by the Normandy Region to evaluate whitebox solutions in order to renew the CPE routers in Normandy high schools.

- goal: to replace old vendor-locked routers in Normandy high schools with
  - vendor-free (virtualized) routing devices,
  - adding features (network functions) at no extra cost over time,
  - at the same or lower cost than the previous infrastructure (Cisco routers)

- basic needs
  - basic routing capabilities (including BGP, PBR and VRF lite), filtering, separate management, …
  - the objective was a bandwidth of 1 Gbps with the possibility of 10 Gbps.
  - remote management (in-band and out-of-band if possible)

Why Whiteboxes as CPE routers?

- To avoiding vendor lock-in and restrictive licensing
  - Why pay for unnecessary functions? Or for basic functions any Linux box can do?
  - Why pay for extra bandwidth when the hardware can already do it without breaking a sweat?
  - Whitebox servers currently equipped with 10 Gbps SFP+ can provides near-line speed (9.4 Gbps measured) with IOMMU (PCI-e passthrough)

- To consolidate Network Functions
  - Why buy physical appliances (firewall, network routers, monitoring servers, VoIP gateways, ...) when one White Box server can do it all using virtualization?
  - One device takes up less space in a rack than several

- Centralized CPE routers management
  - A single Ansible server can manage them all at a fixed initial cost (initial development, basic Ansible training) and reduced maintenance costs (if some features become necessary, we will only have to do a little extra development)
  - System and network administrators work together toward a common goal, each contributing their expertise
  - Can use DevSecOps techniques to automate and secure

Easy to change one part to keep the objective

- Commodity x86 server with appropriate SFP+ and copper ports
  - *today* Dell Virtual Edge Platform 4600/1485,
  - *tomorrow* who knows (HPE Edgeline, Lenovo ThinkSystem-SE350 Edge server, …)
- Open source/Free virtualization software
  - *initially* Proxmox VE,
  - *today* Citrix Hypervisor (Region choice for production),
  - *tomorrow* who knows (VMware ESXi, …)
- Open source/Free routing software
  - *today* FRRouting
  - *tomorrow* who knows (Bird, RARE?, …)

GÉANT

Dell EMC VEP 4600 specifications

- Intel Xeon-D 2100 (4, 8 and 16 cores models)
- Up to 64 GB RAM (4x DIMMs)
- Up to 960 GB SSD storage (2x M.2 SATA slots)
- 4x copper DATA ports (right front side)
- 2x SPF/SPF+ ports
- 4x copper MGMT ports (left front side)
  - BMC ports: serial and Ethernet
  - MGMT ports: serial and Ethernet (in-band access)
- 2x USB 3.0 ports
- Power consumption [16 cores]: typical 206.5W max 311W
- Suitable for demanding high schools but expensive
- About 3000€/unit

6

GÉANT

Dell EMC VEP 1485 specifications

- Intel Atom processor C3958
- 32 GB DDR4
- 16 GB eMMC
- 240 GB SSD
- 6x 1 Gbps Copper RJ45 ports
- 2x 10 Gbps SFP+ ports
- Micro USB serial (console) port hidden
- 2x USB 3.0 on sides
- Power consumption: 40 W typical, 50 W max
- rack mount using the optional dual-unit tray
- Suitable for most high schools needs
- About 1500€/unit

GÉANT

Easy to automate

- Ansible – an automation platform
  - You describe your network configuration intent within the scope of what ansible does,
  - you run the playbooks and your network is reconfigured.
- You can also take advantage of CI/CD techniques to delegate. For example:
  - A field IT technician can request network changes (ACL entries, new VLAN, port configuration, …) for the CPE of a high school using a merge request in the GitLab project of the high school CPE router.
  - A network administrator (Region's network team) reviews it and merges it into the main branch.
  - This triggers a dedicated deployment where everything is traceable.
    - What changes were made, who requested a change, who authorised it and when it was deployed
 - A rollback is also easy to trigger

www.geant.org

Ansible for initial setup and production operations

- After the initial configuration of the hypervisor (manual or automated with gPXE when possible)

- We can use Ansible to set up the Whitebox device
  - create the CPE router VM (using virtualization software API)
  - set it up for a specific site
  - can perform daily operations: routing and switching management, port configuration, ACL management, …

- When a white box device fails, a replacement device (with pre-installed hypervisor) can be ready in minutes (from a configuration backup or from scratch) and then sent for quick on-site replacement

Deployment model
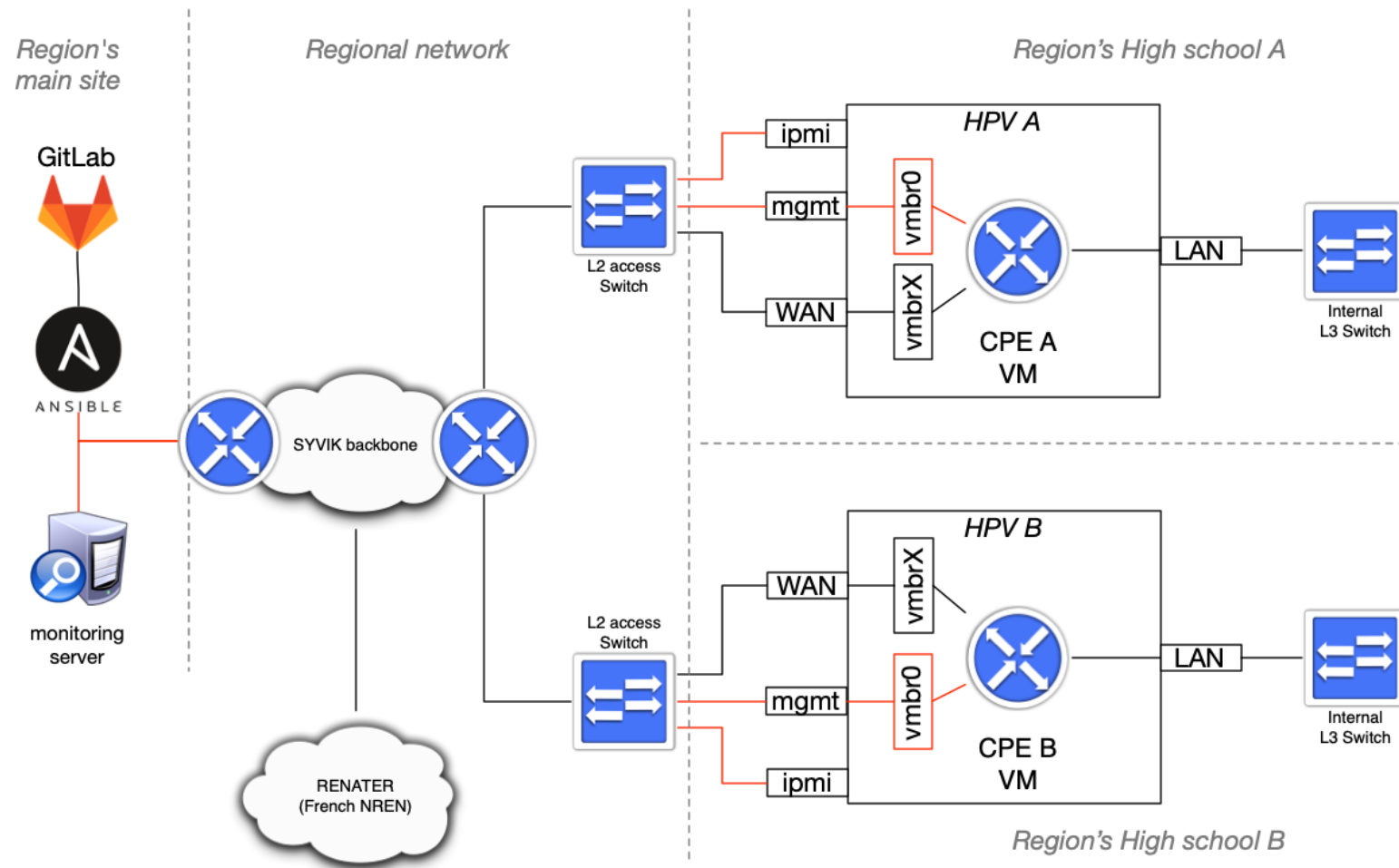
CPE virtual machine

- Debian OS with FRRouting software
- 3 vNIC: 1 for WAN, 1 for LAN and 1 for management
- 2 linux routing tables (rt_tables / ip rule / ip route): 1 for management, 1 for LAN-WAN traffic
- BGP peering with 1 or 2 PE routers in the regional network.
- we could have chosen a commercial (Cumulus VX, …) or an open-source (Open Network Linux, …) NOS but we had two constraints: time and budget
  - Time for first deployments
  - Time for training
  - Time to interface Ansible with a specific NOS
  - Budget for commercial NOS

GÉANT

CPE whitebox project history

- April to summer 2019: development and first tests on a test bed (first virtualised then proof of concept with physical white boxes)

- November 2019: 2 high schools were equipped with white boxes (in Caen)

- The COVID-19 pandemic put deployment plans on hold for a few months

- Summer 2020: training of the Region's teams - the Region is autonomous for the management of white boxes in production

- January 2021: another series of high schools were equipped (in Le Havre)

- December 2021: 10 high schools are equipped, 25 in the next months, 100 to go

What's next?

- CPE router function is working. Now it's time to do additional functions:
  - Firewall (OPNSense, PfSense, WatchGuard FireboxV or XTMv, ForcePoint, …),
  - Local network monitoring,
  - VoIP gateway,
  - Web proxy cache,
  - …
- To date, monitoring and firewall (Pfsense) VMs are deployed alongside the CPE router VMs

www.geant.org

Thank you

Any questions?

www.geant.org