KUDELSKI SECURITY

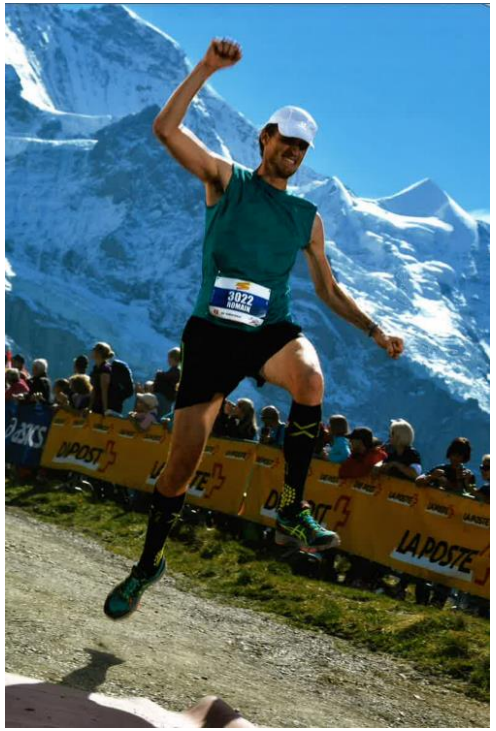
HACKING ARISTA APPLIANCES FOR FUN AND PROFIT

2015.05.11 - SwiNOG - Romain Aviolat

PERSONAL & COMPANY INTRODUCTION

KUDELSKI SECURITY

/ME



- Romain Aviolat
- Married / two years old daughter
- Love doing selfish sports
  - trail / running
  - ski-touring
  - ultra-marathon

- OpenSource advocate
- Void warranties
- Started to build a house with my wife for our family

MY ROLE INSIDE THE KUDELSKI GROUP

- Working for the Kudelski-Security group since 2013
  - System administrator
  - Work in a R&D team / always working with disruptive technologies
  - In charge of an infrastructure dedicated to KS
    - Architecture, design, deployment, maintenance, evolution
  - Built a:
    - Swiss-wide backbone
    - 2 regions private-cloud
    - Big-Data cluster

PERSONAL INTRODUCTION

Our Company

- 60+ years of innovative technology (founded in 1951)
- Independent Swiss listed company, (KUD: SIX Swiss EX)
- 895 M CHF revenue in 2014
- 4,500+ patents, 300 new patents yearly
- 3,000+ employees worldwide
- 200M+ annual R&D investment
- Over a dozen of innovation and technical excellence awards
- World leader in digital security and media convergence solutions

Our Business

- Integrated Digital TV
  - Securing >70B$ annual content revenues
- Public Access
  - Securing >10.000 locations in > 90 countries
- Cyber Security
  - Tailored cyber security services & solutions for key industries (Finance, Public, Defense, Media)

Our Mission

- Provide comprehensive and best in class security & privacy solutions

KUDELSKI GROUP STRUCTURE

DIGITAL TELEVISION

NAGRA KUDELSKI

conax

opentv

SMARDTV

CYBER SECURITY

KUDELSKI SECURITY

Customized Solutions:

- Financial Services
- Public and Defense
- Digital Media and Entertainment

PUBLIC ACCESS

SKIDATA
KUDELSKI GROUP

Parking management

Mountains destinations

Arenas and attractions

KUDELSKI SECURITY

KUDELSKI GROUP OFFICES AROUND THE WORLD

Headquartered in Switzerland and operating on five continents

MY TEAM

- RnDOI: R&D and Ops Infrastructure
  - Was formed the 1st of April 2015
  - Core team is composed of 5 ninja
    - 2 infra guys
    - 2 R&D engineers
    - 1 team leader
    - Reinforced with project-specific resources (masters thesis, …)
  - Missions:
    - Provide cyber-security infra to Kudelski-Security
    - R&D in threat intelligence
    - Internal consulting (network security, network forensic, high-speed networks, big-data, cloud, infrastructure design, …)

R&D PROJECTS & SERVICES

- SINN: wire-speed port-scanner
  - Able to scan the whole public IPv4 space on a specific port in <15 minutes.
  - We're able to quickly extract useful information based on the scan output and do some fingerprinting.

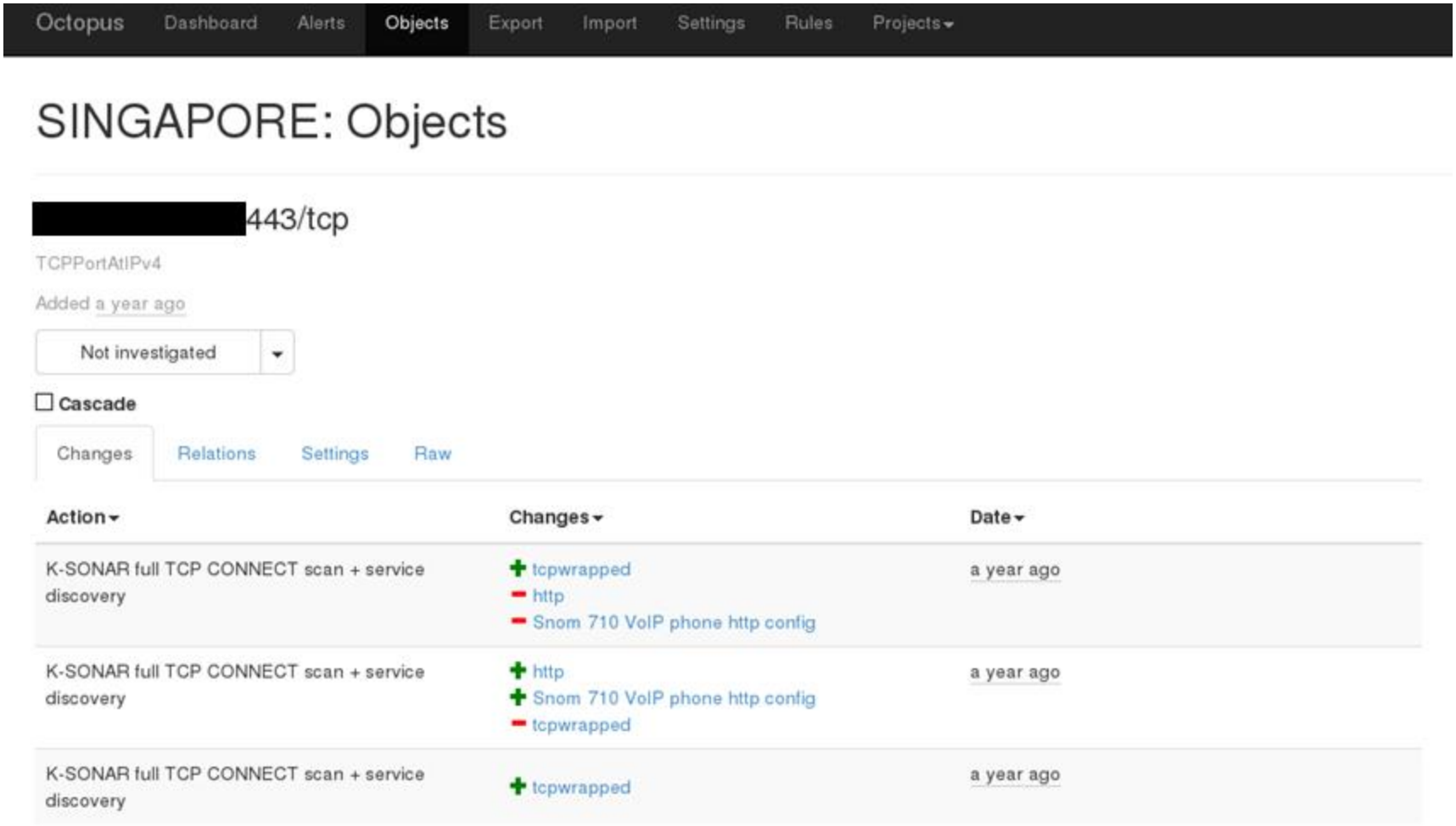
```
> 7 trigger(s) parsed from file "rdp_ms12_020.pld"
> 47 range(s) parsed from file "ips.rng"
> openfd limit set to 25600
> 2015-10-28.13:31
> scanning 203264 IP(s)
> done receiving recon packets

nb open port(s) found:          582
nb closed port(s) found:        6546
nb filtered port(s) found:      196136
> SYN scan duration: 0h:0m:0s

> starting service fingerprinting ...
 |=============================================>              | (408)
```

R&D PROJECTS & SERVICES (K-SONAR)

Network perimeter monitoring

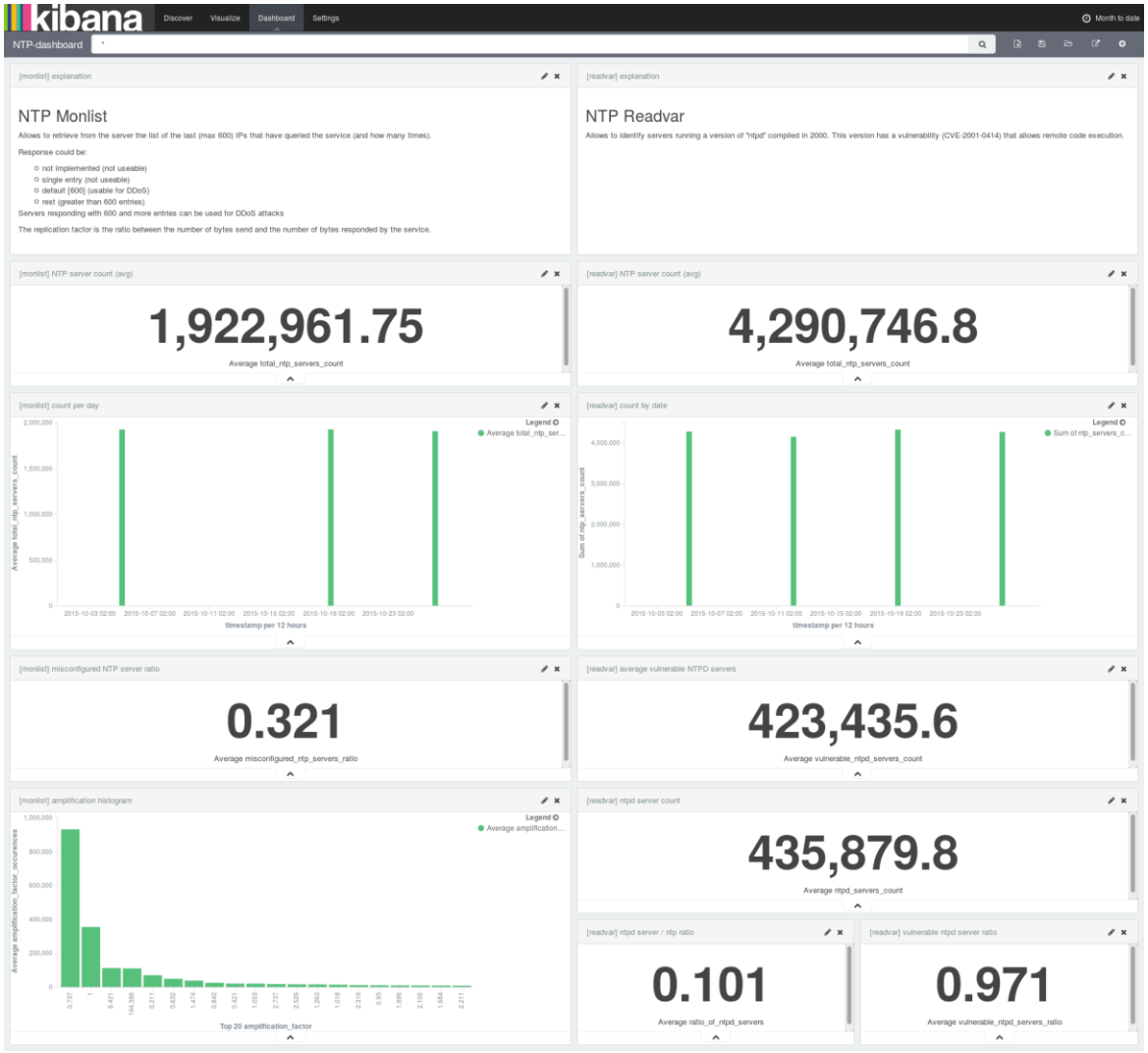


R&D PROJECTS & SERVICES

- BD3I: BigData Index of the Internet Insecurity

  - Combination of port-scanning and BigData analysis
  - Collect data from port-scan into our Hadoop cluster
  - Extract the interesting information
  - Highlight the relevant information

  (-> NTP protocol analysis)



SPECIAL INFRASTRUCTURE REQUIREMENTS

Those activities, and other outside of my team require a dedicated special infrastructure

- Big Internet pipes
  - 2x 10Gbit uplinks with different IP-Transit providers
  - And other smaller lines
- Large public IP space (v4/v6)
- +50 physical servers
- +150 VMs
- Robust network backbone (line-rate routing)
- Private-cloud (400 vCPU / 3TB of RAM)
- Big-Data cluster (1/2 PB)

TECHNOLOGIES IN USE

KUDELSKI SECURITY

LET’S GO BACK IN TIME…

KUDELSKI SECURITY

END 2013

We had growing and growing requirements in term of IP-Transit.

We were asked to make tests using a 10Gbp/s-flat Internet line for a POC

- Goal was to see how well our home-made port-scanner could scale, how fast we could port-scan the public IPv4 space. For now we only had 1Gb/s Internet uplink.
- We used a common 24x10Gb multi-layer switch to connect the line with our port-scanner.
- On the paper it was supposed to route packets a 10Gbit/s, yeah on the paper… But in fact …

IT BURNED…

KUDELSKI SECURITY

SYN SCAN

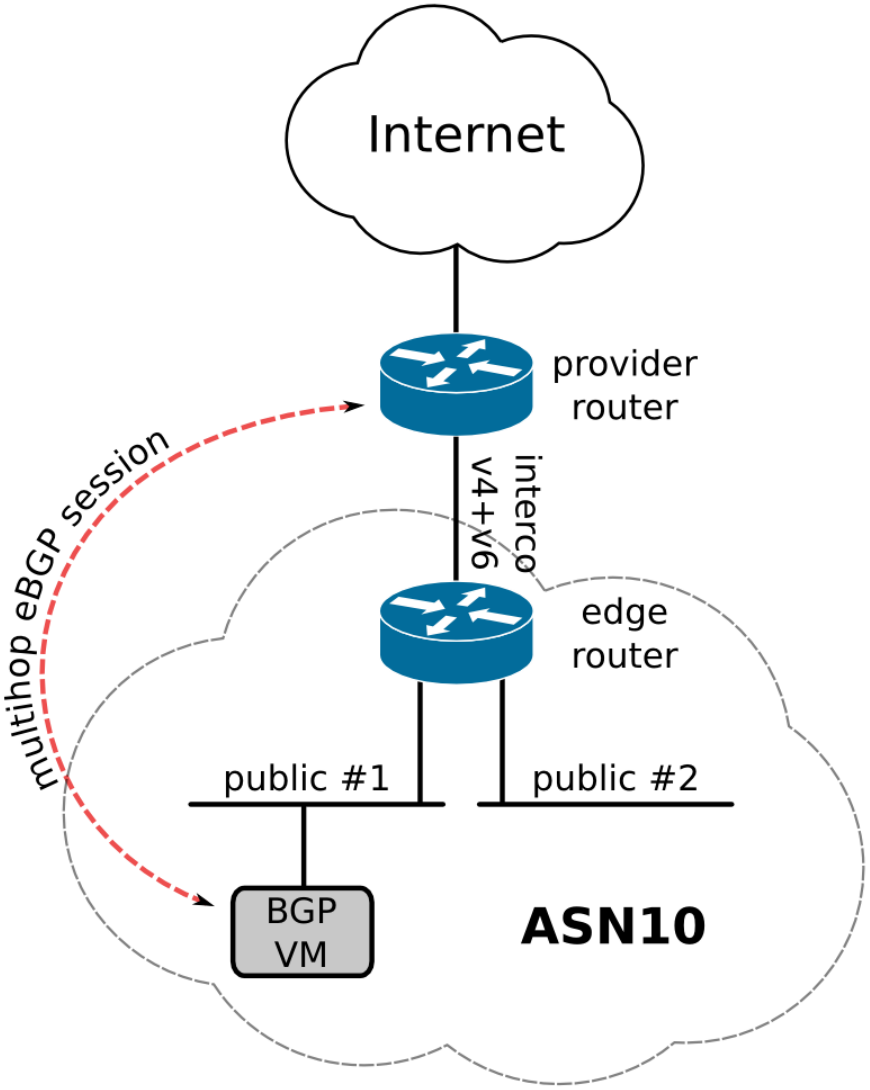
What happened is that those switches were able to route 10Gbit/s of standard packets with large payloads. Their limit was around 1-2Mpps.

- With our SYN scans, without payload, we generated packets of 84 Bytes, so at 10GBit/s it would mean 14’880’955 pps
- We tried a bunch of different brands without success, then we heard of Arista.
- They were kind enough to lend us a switch to make our tests.
- We weren’t able to kill it with our port-scanner… Even in our lab we achieved line-rate routing with it.

2014

So we ended-up with a setup like that:

- An Arista 7150S-24 MLS connected to the IP-Transit provider
- IPv4/v6 interconnection subnets between us and the provider
- Two Default routes (v4/v6) towards the provider-router
- Multi-hop eBGP configured between the provider and a VM on our side, we announced our IP resources from there. BGP tables were also stored there.
- This setup was rock solid, we achieved scans at 7Gbit/s. The limitation was our port-scanner this time and not the router.

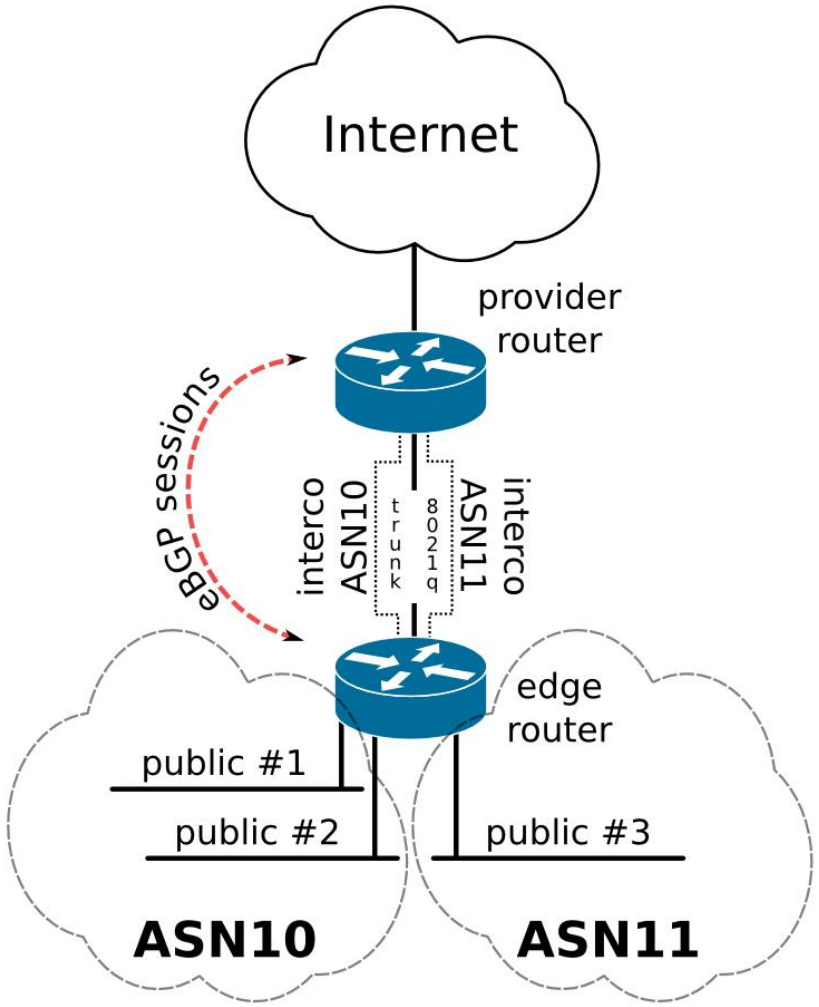


It was working so great that we started to use the line more and more internally, for other projects and for a more corporate usage.

So we wanted to push things a bit further:

2015

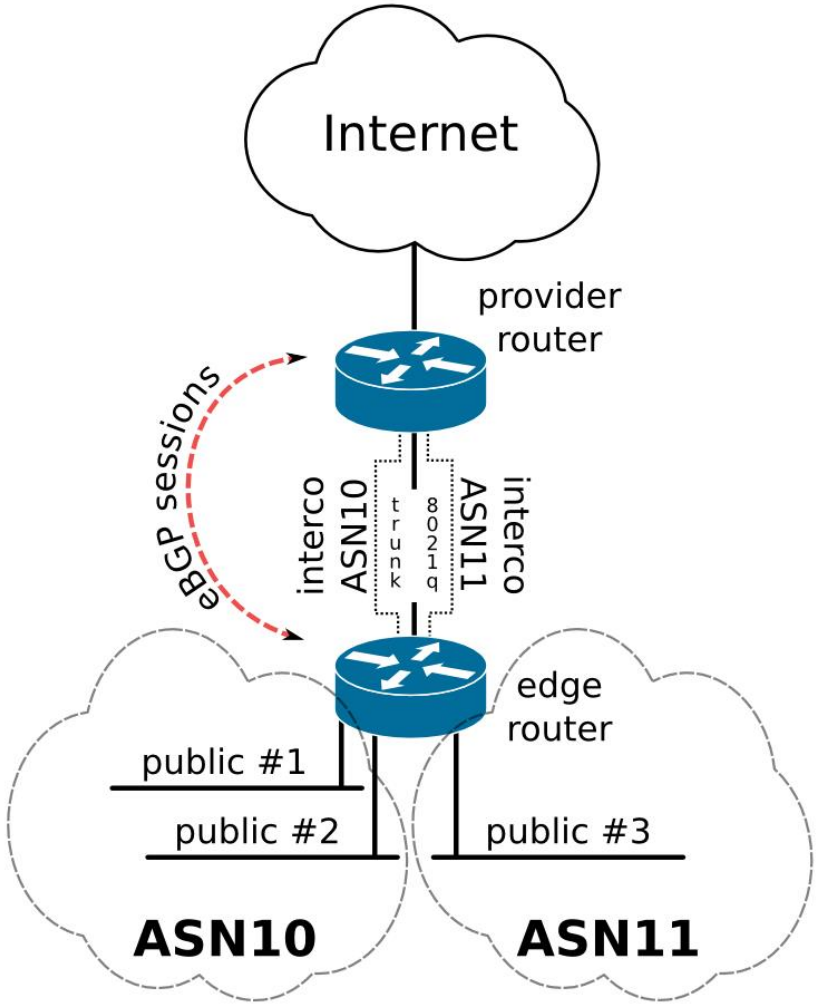
- Isolate as much as possible, the port-scanning and kinky activities from the “corporate” usage.
- Still needed the pps performances on the edge for our port-scanner.
- Multi-hop BGP wasn’t a long-term solution (**no supported by Cogent**)
- So here’s what I had in mind:
  - Create one BGP session directly from the edge-router, per AS.
  - Store the BGP tables on the edge. But don’t push them to the switch FIB.
  - Routing decision should be based on a static default route to avoid costly lookups.



We quickly faced two big problems:

- The impossibility to have multiple ASNs configured at the same time on the BGP daemon.
- The Arista 7150S-24 mls is only able to store 12’000 entries in its FIB, and there’s no way to store the tables into the RIB without pushing them into the FIB.

We’re far away from the +550’000 routes for IPv4 and the +20’000 for IPv6, and this is only for one ASN.



By curiosity I tried to remove the 12’000 entries soft-limit and I sent a full BGP table to the router FIB.

AGAIN …

KUDELSKI SECURITY

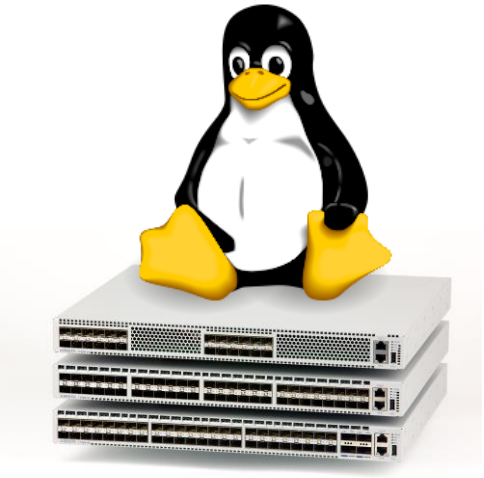
Believe me, you don’t want to do this…

- The process responsible for pushing routes into the TCAM was acting like crazy, eating all the CPU, trying desperately to push the routes into its hardware and then it decided to commit suicide after a few minutes of pure panic.

- So my setup was pretty screwed so far …

At that point I decided to replace the switch BGP engine ...

- To put something more customizable
- Those switches are running on GNU/Linux
- Hopefully not a striped-down version like it's often the case
- Full blown x86 Fedora distribution
- >bash
- #sudo –i
- You're root !
- Don't be scared…



```
admin@arista-7150S24:~
admin@arista-7150S24:~ 76x20
arista-7150S24>
arista-7150S24>
arista-7150S24>enable
arista-7150S24#
arista-7150S24#bash

Arista Networks EOS shell

[admin@arista-7150S24 ~]$ sudo -i

Arista Networks EOS shell

-bash-4.1# w
 08:59:36 up 507 days,  3:04,  1 user,  load average: 2.45, 2.00, 0.93
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
admin    pts/5    10.31.32.11      08:59    0.00s  0.56s  0.56s FastCli
-bash-4.1#
-bash-4.1# whoami
root
-bash-4.1#
```

BIRD ftw !

- Choose to install BIRD: http://bird.network.cz
  - Bird Internet Routing Daemon
  - BGP, OSPF, RIP, v4+v6
  - Powerful language for route filtering
  - Linux, *BSD,
- Question was: should I use the packaged version from Fedora repo or compile it from scratch ?

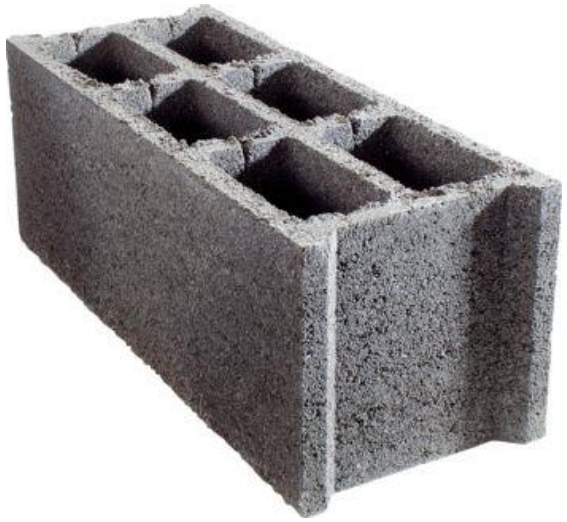
Compilation time !

- Packaged version in the repo was >2years old…
- Added Fedora 14 x86 repo to the distribution configuration and installed few dependencies:
  - $yum install vim readline-devel ncurses-devel flex bison autoconf gcc make
- Downloaded latest stable version from their git repo.
- #automake

```
./configure
make
cp bird /mnt/flash/persist/bird
cp birdc /mnt/flash/persist/birdc
cp birdcl /mnt/flash/persist/birdcl
make clean
./configure --enable-ipv6
make
cp bird /mnt/flash/persist/bird6
cp birdc /mnt/flash/persist/birdc6
cp birdcl /mnt/flash/persist/birdcl6
```

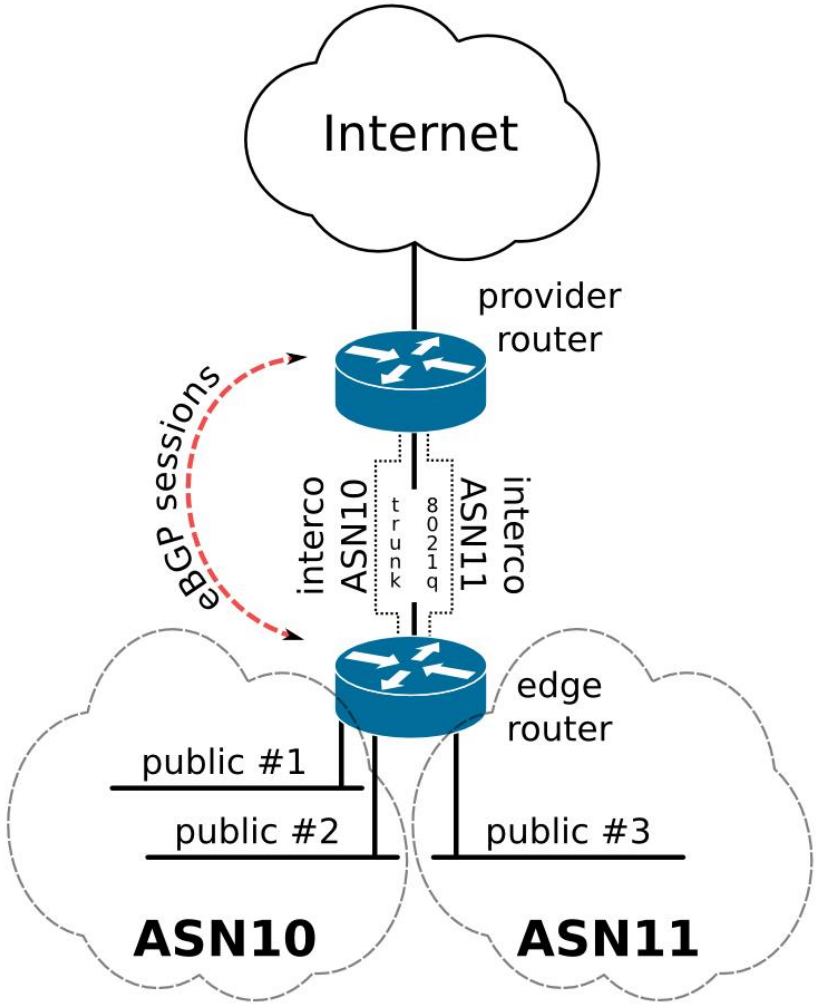
Make it persistent

- The switch OS is extracted from and image during each boot.
- So we have to make the BIRD setup persistent across reboot.
- Luckily Arista provides a R/W storage space, where we will put the compiled binaries and a script that put those binaries in the right place with the right permissions and then execute them.
- Of course you'll have to write two configuration files for bird and bird6 daemons.



Switch configuration

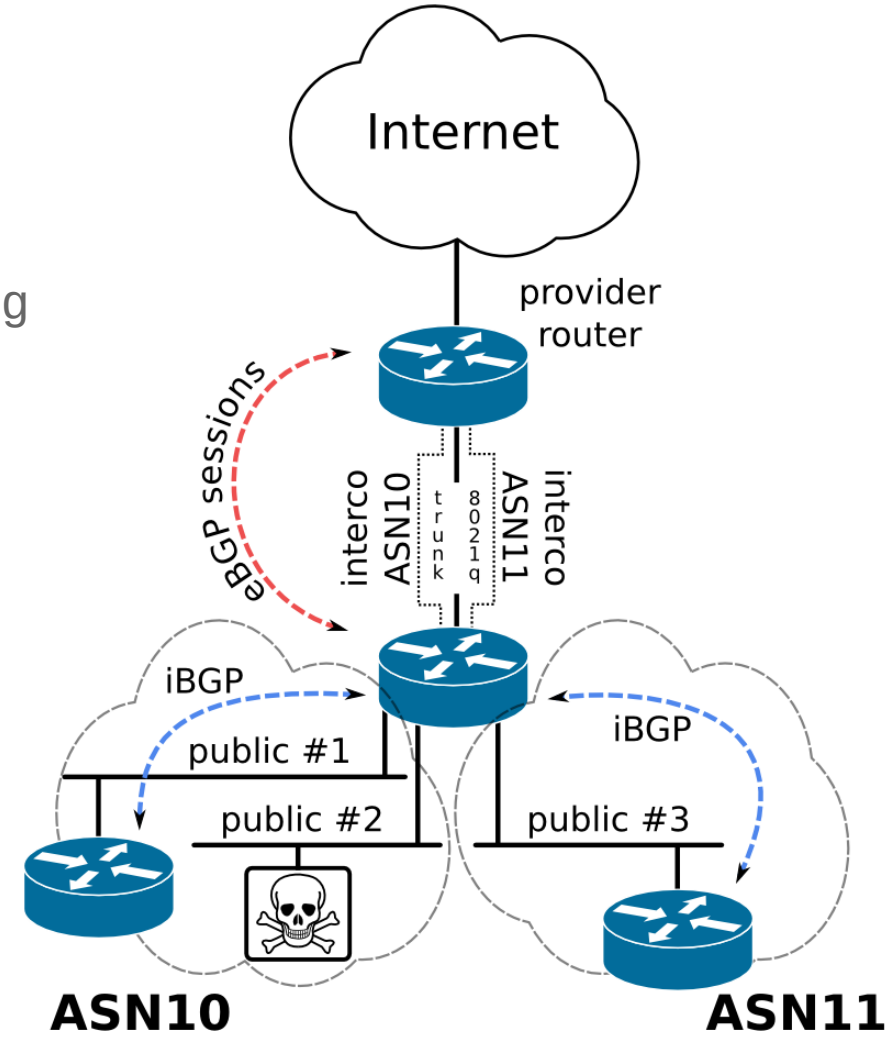
- The uplink with the provider has been converted to a trunk, with 4 interco subnets (1x v4+v6 for both ASNs)
- Four different default gateways pointing to the provider router (1x v4+v6 for both ASNs) using VRFs.
- **BIRD** is now configured to peer from both ASNs with the upstream router.
- It announces our public resources for each ASNs



Route server !

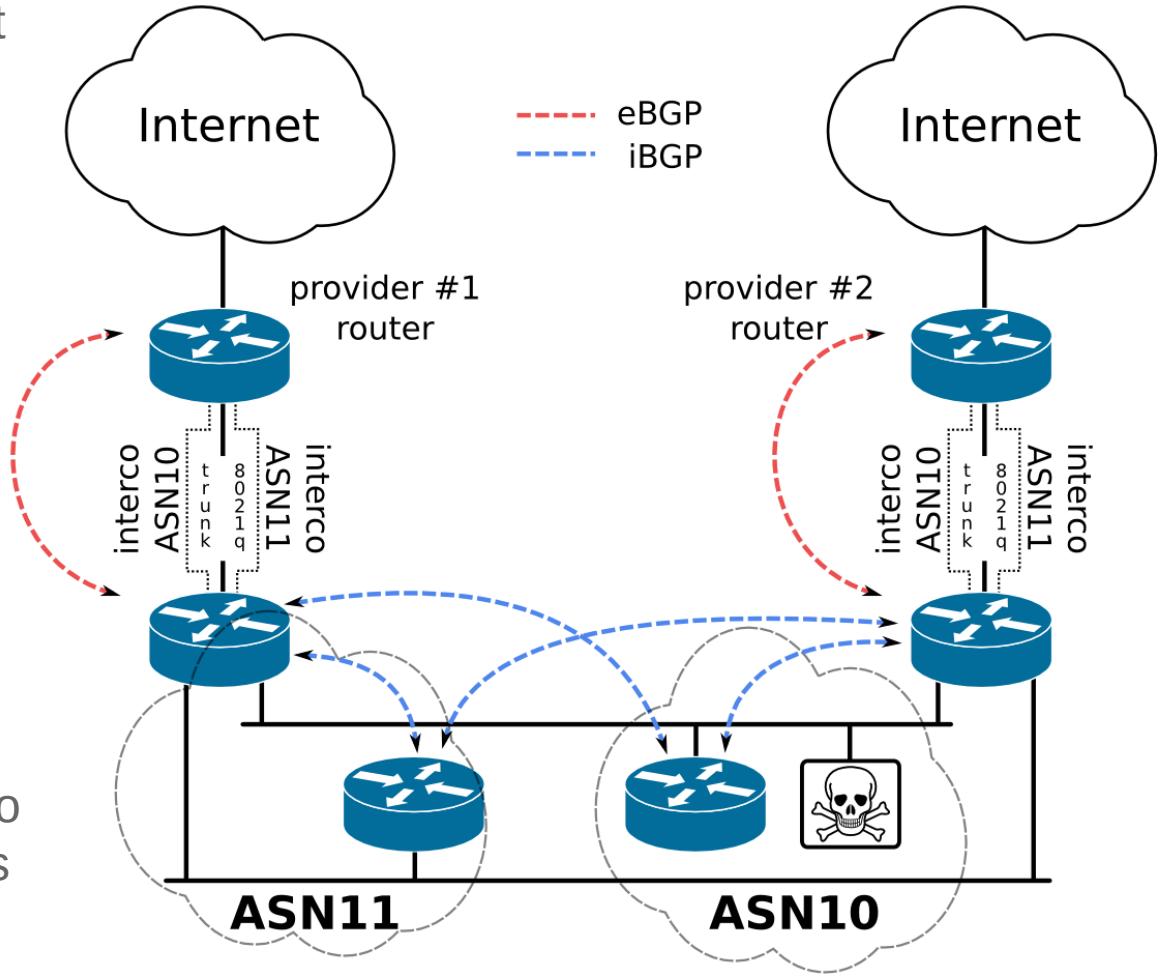
- At this point we added site routers behind each ASNs
- Configured the **BIRD** daemon to redistribute routes for each ASNs using **iBGP**

```
protocol bgp iASN10 {
        description "iBGP AS10";
        local as 10;
        neighbor 198.51.100.101 as 10;
        export where proto = "AS10;
}
protocol bgp iASN11 {
        description "iBGP AS11";
        local as 11;
        neighbor 198.51.100.111 as 11;
        export where proto = "AS11;
}
```



Multi-homed

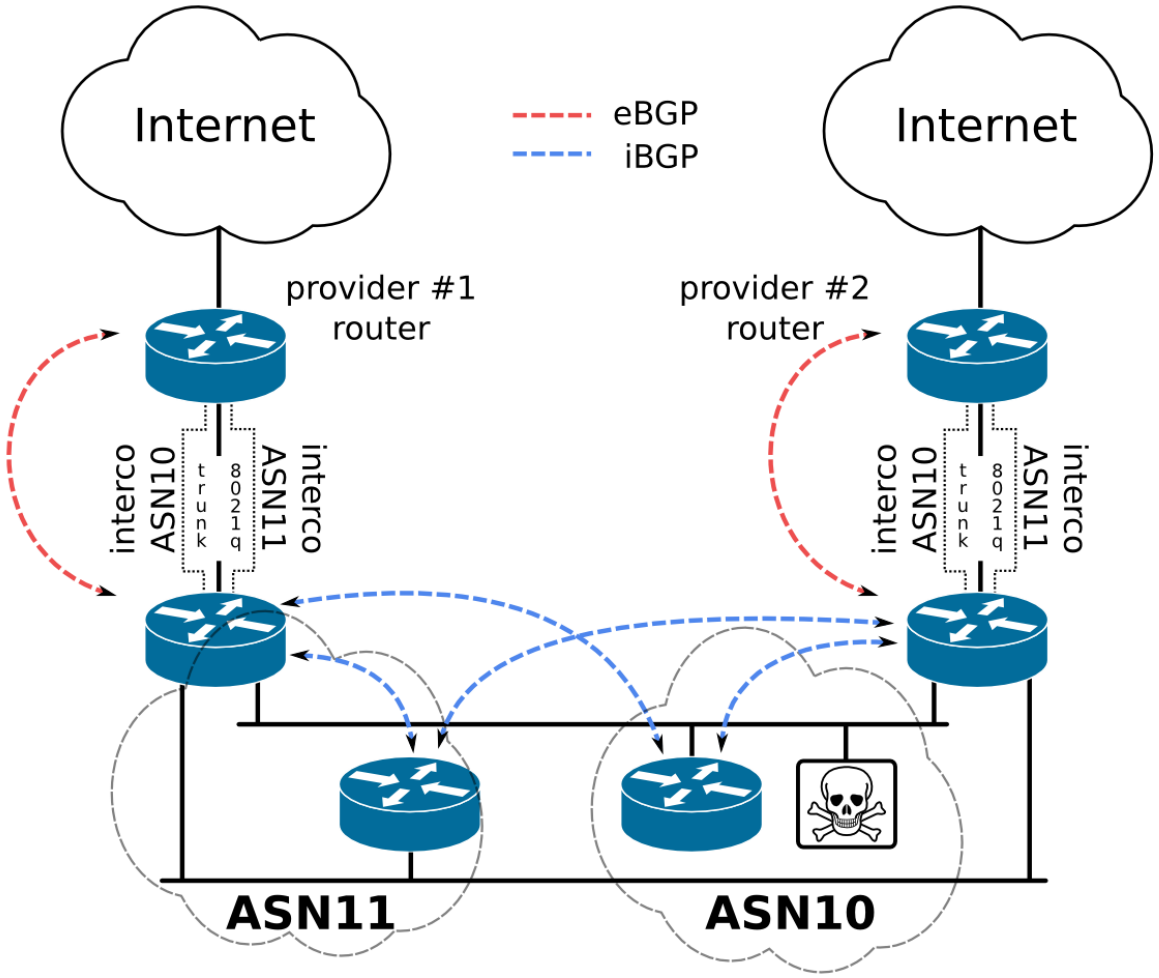
- Add another IP-Transit provider to announce our public resources for both ASNs
- Put the same tweaked Arista router on the edge of our network
- Start announcing our resources to the second provider
- Create the iBGP sessions with the downstream routers; now they will be able to choose the best routes
- Our port-scanner can use one or the other gateway



CONCLUSIONS

Moving the “real” BGP routers from the edge of our network to a lower layer and leaving dumb-but-powerful multi-layer switches in front of them was a great solution for our special requirements.

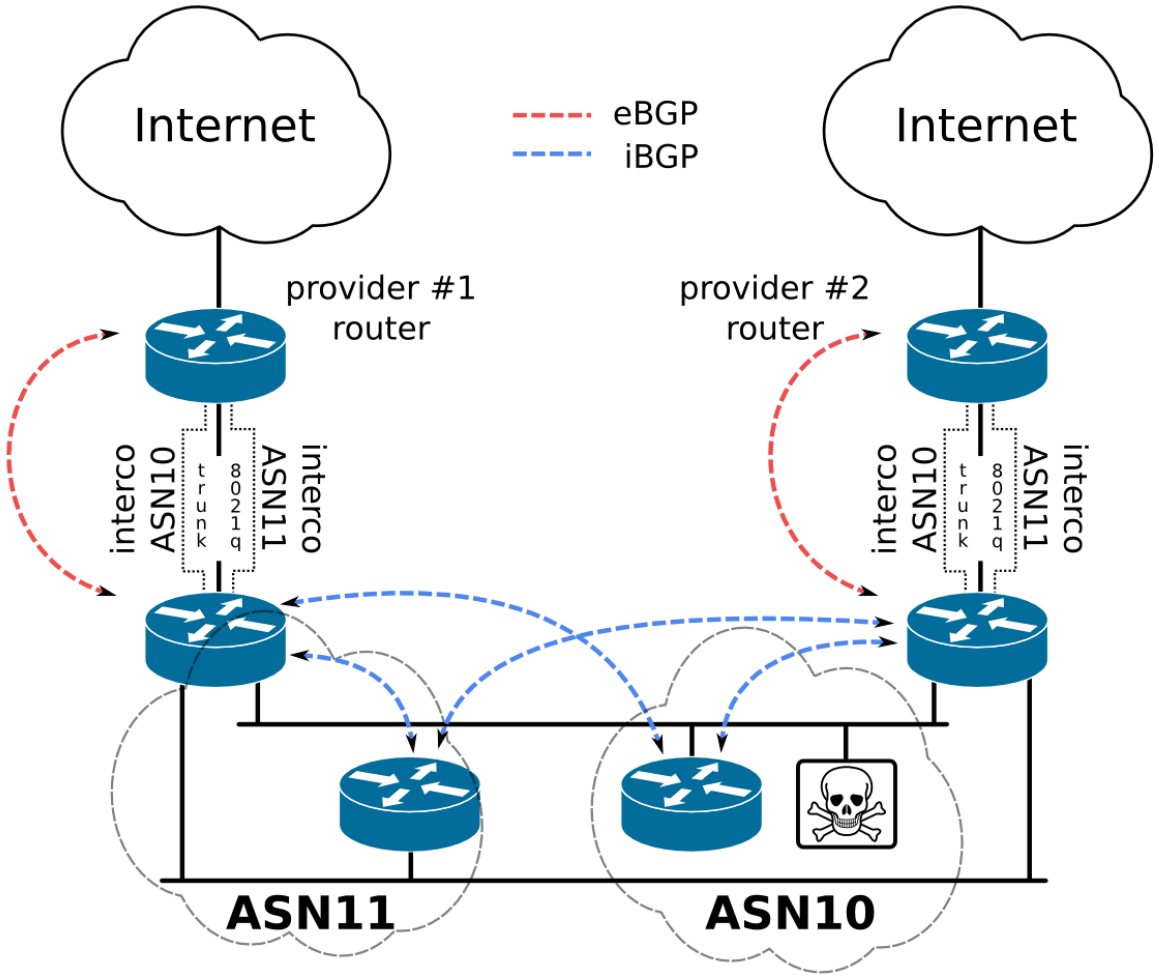
It allowed us to leverage the physical limitations of these routers. It created a kind of cheap pps-DMZ in front of the routing-decision-taking-routers.



CONCLUSIONS

Replacing all the routing engines (OSPF, RIP, …) is also something possible with this hack.

Replacing the BGP routing engine will remove the ability to push BGP learned routes into the ASICS switch, at least I haven't invested time in that, it might be doable.



WHAT'S NEXT ?

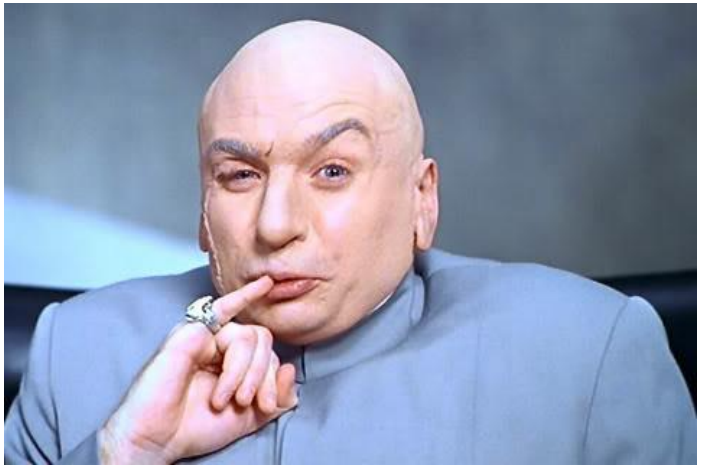
- Networking world is evolving like never before:
  - Whitebox networking / merchant silicon solutions
  - SDN / Orchestration
  - Separated control and data-plane
  - Linux distributions in the core: CumulusLinux / HP OpenSwitch initiative

- We want to explore as much as possible all the amazing solutions that are emerging.

- Replacing the Arista switches with cheaper mls like cumulus-linux-ready switches is definitely an interesting direction we should explore.

- More and more R&D around the Internet Insecurity.

If you still want to peer with us we would be **delighted** !
we plan to be in Equinix4 SwissIX soon …



We’re not evil (ASN42570)

TO READ

Kudelski Security blog, related articles:

- cybermashup.com/2015/08/17/knock-knock-whos-there-not-me
- cybermashup.com/2015/10/01/hacking-arista-appliances-for-fun-and-profit
- cybermashup.com/2014/01/20/first-steps-with-arista-networks

Others:

- bird.network.cz
- arista.com
- cumulusnetworks.com


KUDELSKI
SECURITY
THANK YOU!
www.kudelskisecurity.com
cyber security unit of Kudelski Group