Citypassenger

Mr Bruno DUVAL

To ensure isolation and trust of professional digital devices with the « Network as a Dongle » solution

End of project :
November 2018

Ddos mitigation strategy based on the use of BGP to diffuse attack signal on a large scale

End of project : **initially April 2019**

Definition of the problem

- The security level of Digital Devices authentication relies on the non-diffusion of credentials from person-to-person
- To improve this security level physical « dongle » are used
- However, this is not a flexible solution in the context of modern IT

Solution: Network-as-a-dongle

- This solution reflects a demand of Citypassenger’s customers
- It was fully developped from scratch in the context of ODSI project
- The R&D works focused onto network isolation and authentication features
- Collaboration with WP3 and WP4 partners

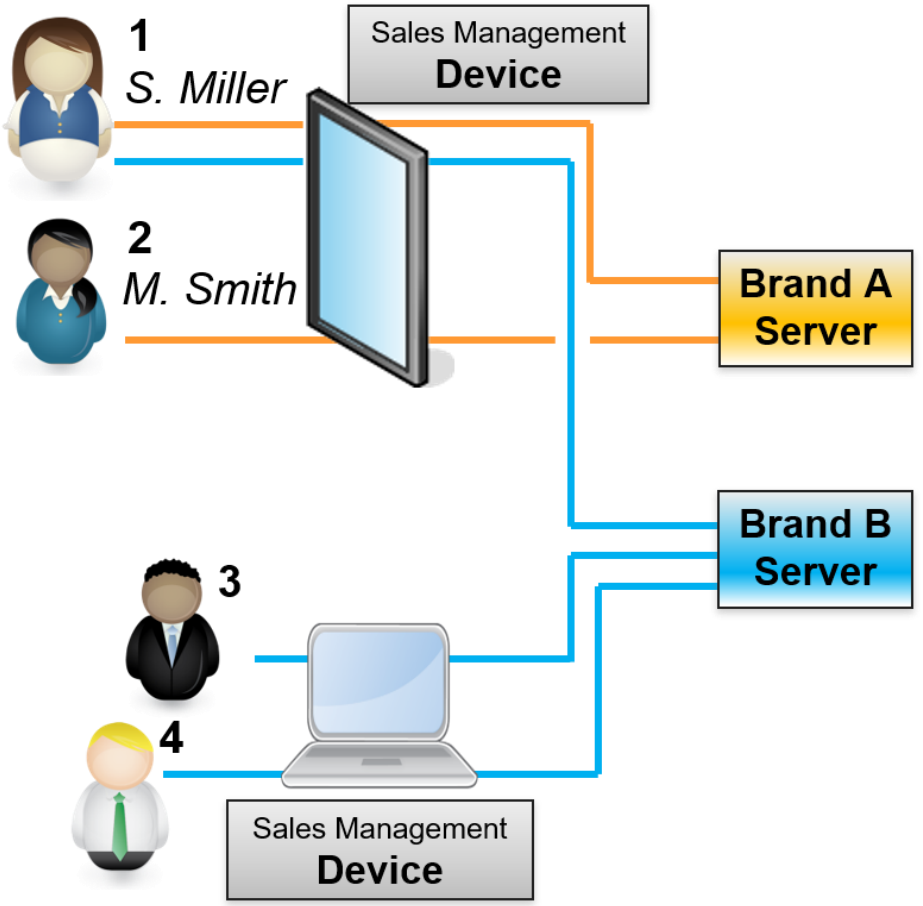
Concept and advantages

- The network infrastructure is used as an authentication tool when a user accesses a remote resource.
- No need for USB ports or other interfaces
- Configuration and user management : remotely, safely and at any time by a web interface
- Stealing the « dongle » is impossible

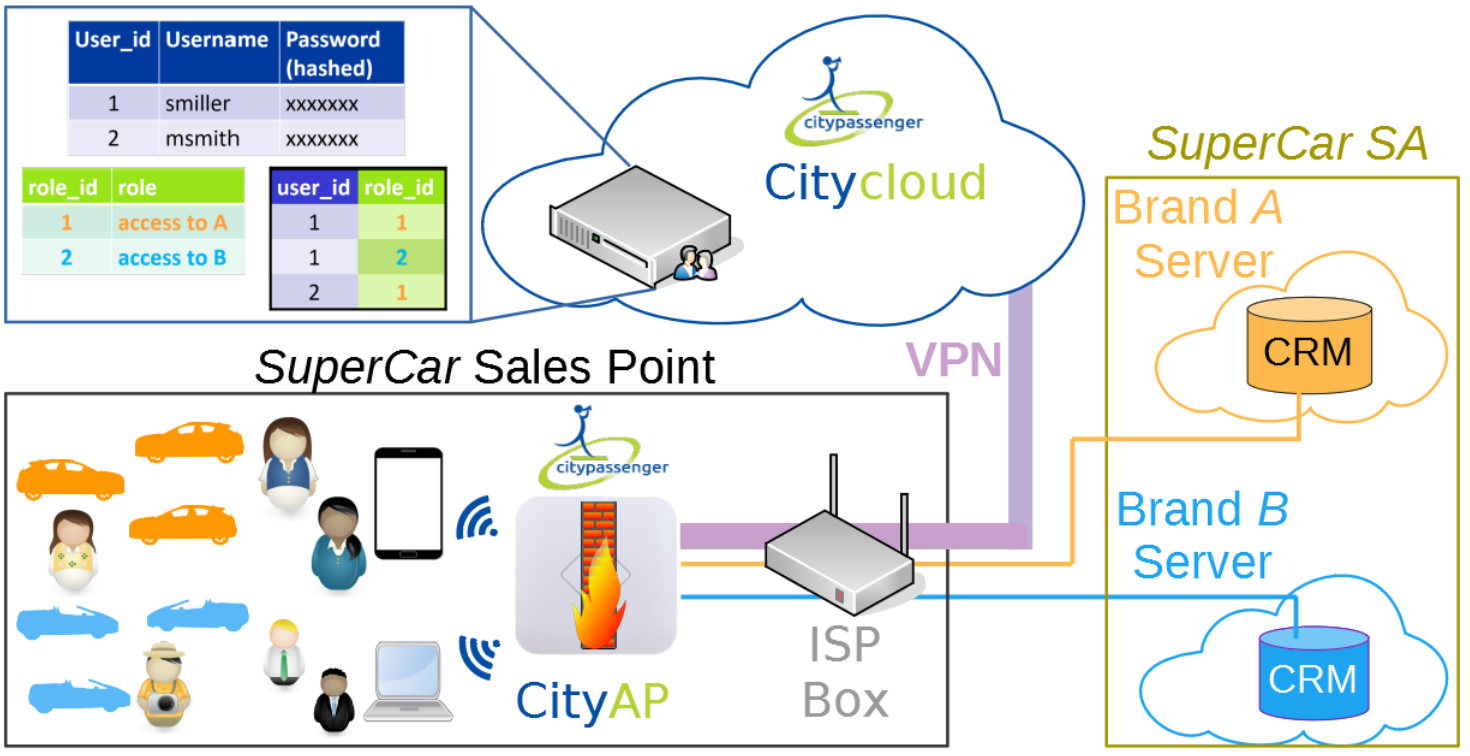
Automotive Retail Use-case

- Automotive Groups include various car brands, sometime sold in separate showroom on the same site but sharing the same IT infrastructure

Use case schematic representation



Network architecture



Commercial & technological advantages

- Minimizes the use of physical interfaces: reduces material and operating costs
- Secure-by-design thanks to the combination of authentication and network isolation mechanisms
- Responds to multi-tenant scenarios with high flexibility: users can be added or banned easily
- Directly relevant for the automotive industry and applicable to other sectors

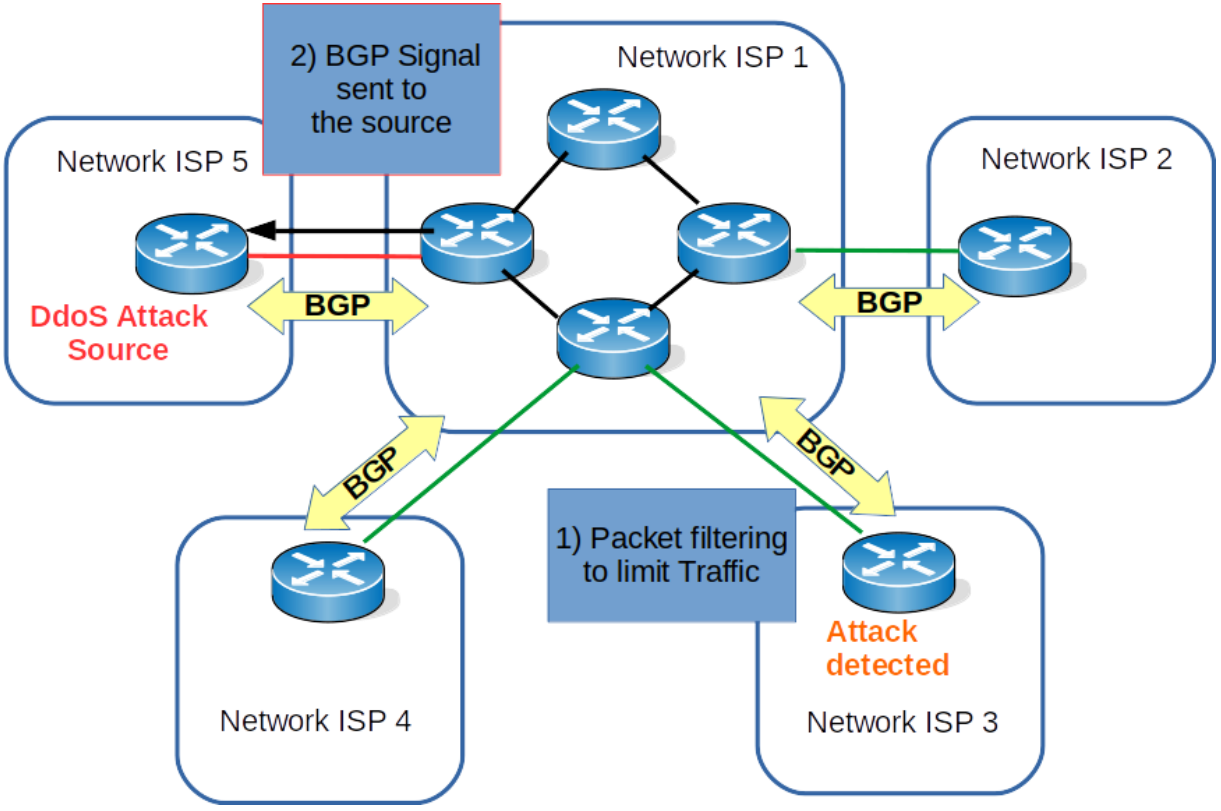
How to stop Ddos attack ?

SENDATE TANDEM

- Ddos is a major threat requiring costly dedicated hardware and maintenance operations
- Our suggestion: to use BGP3 to distribute the IP adresses and the protocoles in use in real time
- Advantages: no specific hardware needed, adapted to SDN infrastructure

Diffusion of the warning signal

- Proposition: to use BGP TRAPPED lists to forward warning signal



Advantages of the implementation

- Any router is able to at least forward the warning information
- Easily adaptable for an implementation on third party hardware
- Adaptation to SDN context is on going

Future directions

- Should be rapidly adopted by third-party vendors
- A community listing bad trafic as well as white lists of trusted sources should be setted-up
- BGP modifications and extension for a better integration of our solution
- A SBGP should be developped to forward other security information: bad flux, bad e-mails...