Sécurité du réseau fixe d'un opérateur : focus sur les dénis de service

Orange Expert Security

David Roy et Pascal Nourry,
Orange France / Direction Technique

orange™

Plan de la présentation

Réseau d'un opérateur

Politique de sécurité

Attaques de dénis de service

Contre-mesures statiques pour les DDoS par amplification

Contre-mesures dynamiques pour les DDoS de botnets

Attaques au cœur des offres Wholesale

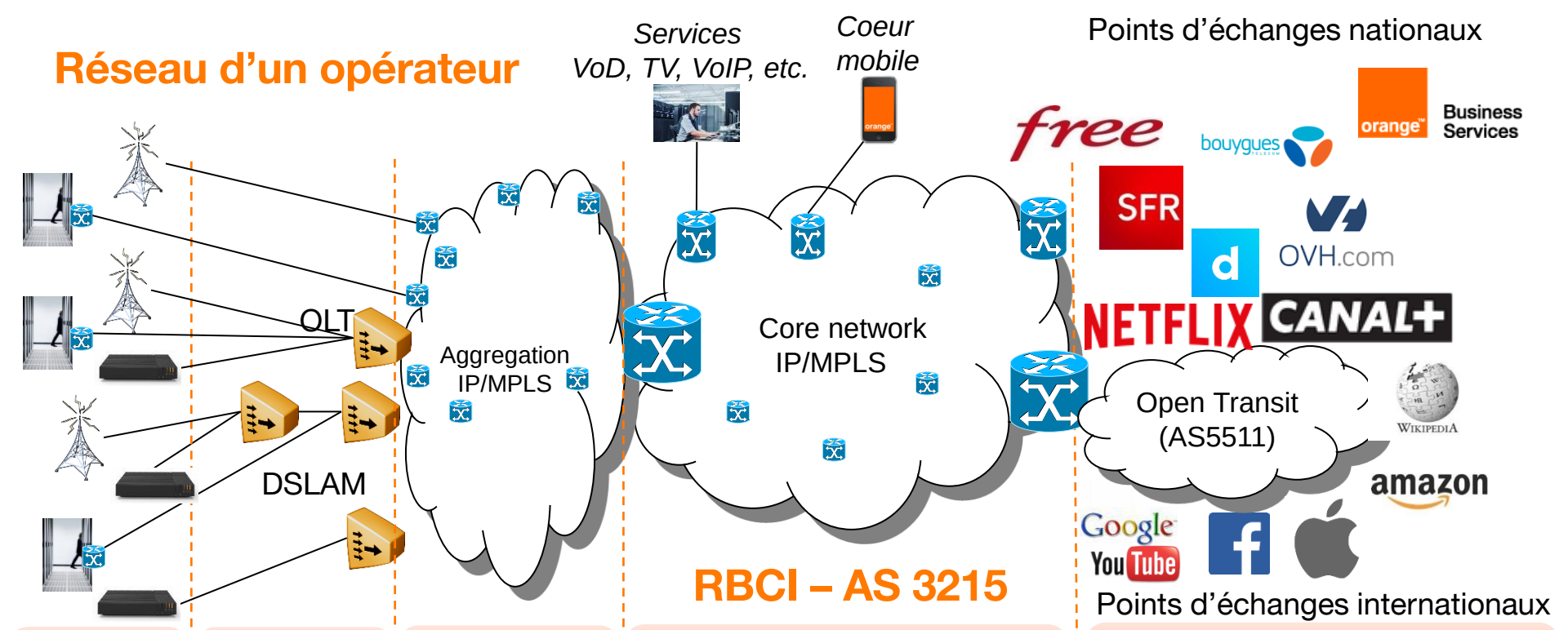
Réseau fixe d’un opérateur

Réseau fixe d'un opérateur

RBCI = AS 3215 = support de multiples offres réseaux : Ethernet, IPv4, IPv6, TV (multicast), etc.

- **Offres triple play Orange Internet / VoIP / TV**
- **Besoins internes Orange France**
  - VPN (par routage) pour le fonctionnement de services VoIP ou pour le cœur du réseau mobile
  - Raccordement des plateformes Orange comme le portail Orange.fr, les plateformes TV&VoD/CDN, etc.
- **Offres de transit IPCI (IP Connexion Internet)**
- **Offres de collecte régulés (pour des opérateurs tiers comme SFR, BYT, OBS, Orange « Mobile », etc.)**
  - Collecte des antennes mobiles (CEMx)
  - Collecte de clients entreprises
  - Collecte des clients résidentiels

Réseau d'un opérateur



Clients	Réseau d'accès	Réseaux de collecte	Réseau de cœur	Internet Opérateurs/Entreprises tierces
+12M Actifs +30M Prises	xDSL : 50 Mb/s FTTH : 1 Gb/s	Nx10 Gb/s Nx100 Gb/s	Nx100 Gb/s	

+50k équipements

+2k équipements

Politique de sécurité

Politique de sécurité

Constat

- **Les opérateurs subissent des attaques qui visent leurs clients ou qui visent l'opérateur lui-même**

Sécurité du RBCI - AS 3215

- **La sécurité est partie intégrante du réseau depuis sa création du réseau en 1998-1999 avec un accent très marqué sur la disponibilité du réseau**
- **La première politique de sécurité date de 2004 puis elle a évoluée en 2008 et en 2012-2013**
  - Travail collectif : ingénierie + exploitation

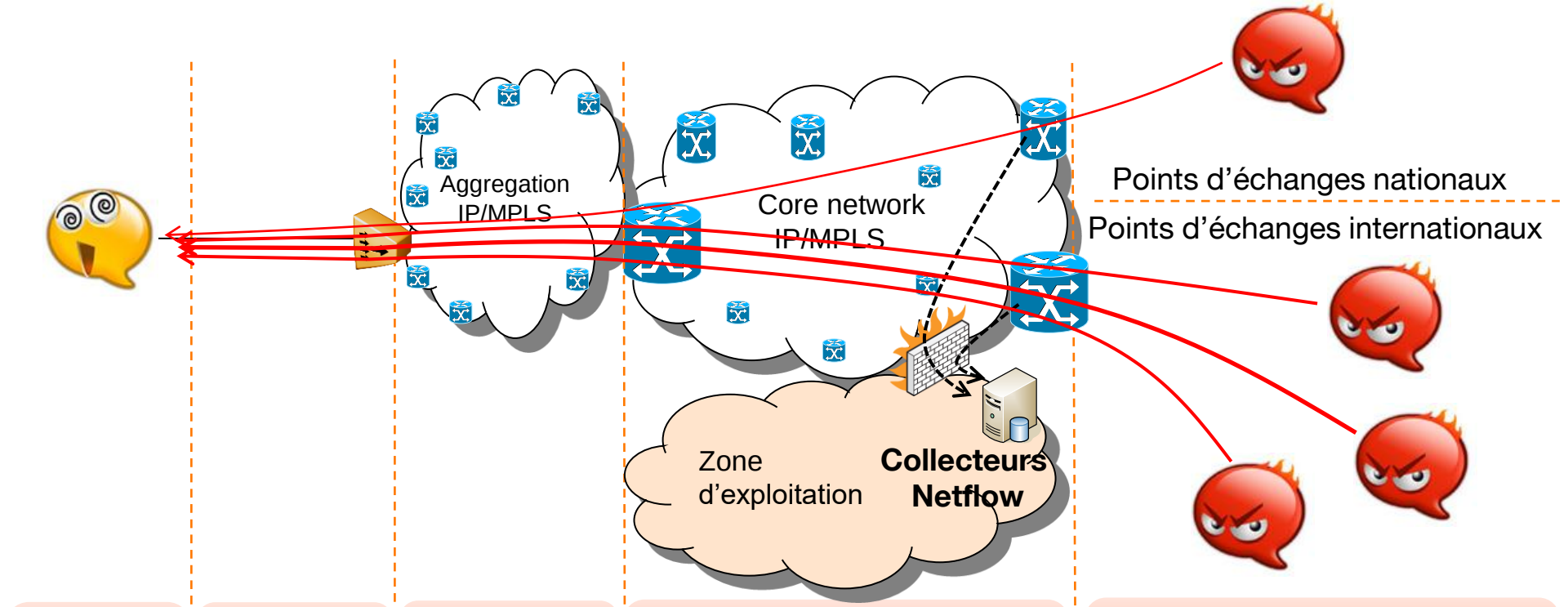
Politique de sécurité

Sécurité du RBCI = AS 3215

- **Les principaux axes**
  - Les équipements en périphérie du RBCI doivent protéger le RBCI des agressions extérieures
    - fiabilisation des en-têtes IP (anti-spoofing, marquage QoS, etc.),
    - destruction du trafic non légitime (adresse IP source privée, mécanismes anti-DoS, etc.),
    - limitation de la visibilité du RBCI vis-à-vis de l'extérieur,
    - fiabilisation du plan de contrôle en mettant en œuvre notamment les bonnes pratiques BGP,
  - Chaque équipement du RBCI doit se protéger en contrôlant toute information à destination de son plan de contrôle ou de son plan de management
    - mise en place de fiiltres sur la base de l'en-tête IP avec dans certains cas des limitations en débit,
    - exploitation des équipements en utilisant des protocoles sécurisés (par exemple SSHv2 avec une vigilance particulière sur les suites cryptographiques utilisées) et permettant un contrôle fin des accès
    - mise en œuvre de la QoS afin de privilégier par exemple le plan de management et le plan de contrôle aux dépens du plan de données,
  - Le RBCI doit être intégralement redondé pour être résilient dans tous les cas de panne simple, y compris en cas de "coup de pelleteuse" (ou de coup de disqueuse) sur un axe de transmission.

Attaques de dénis de service

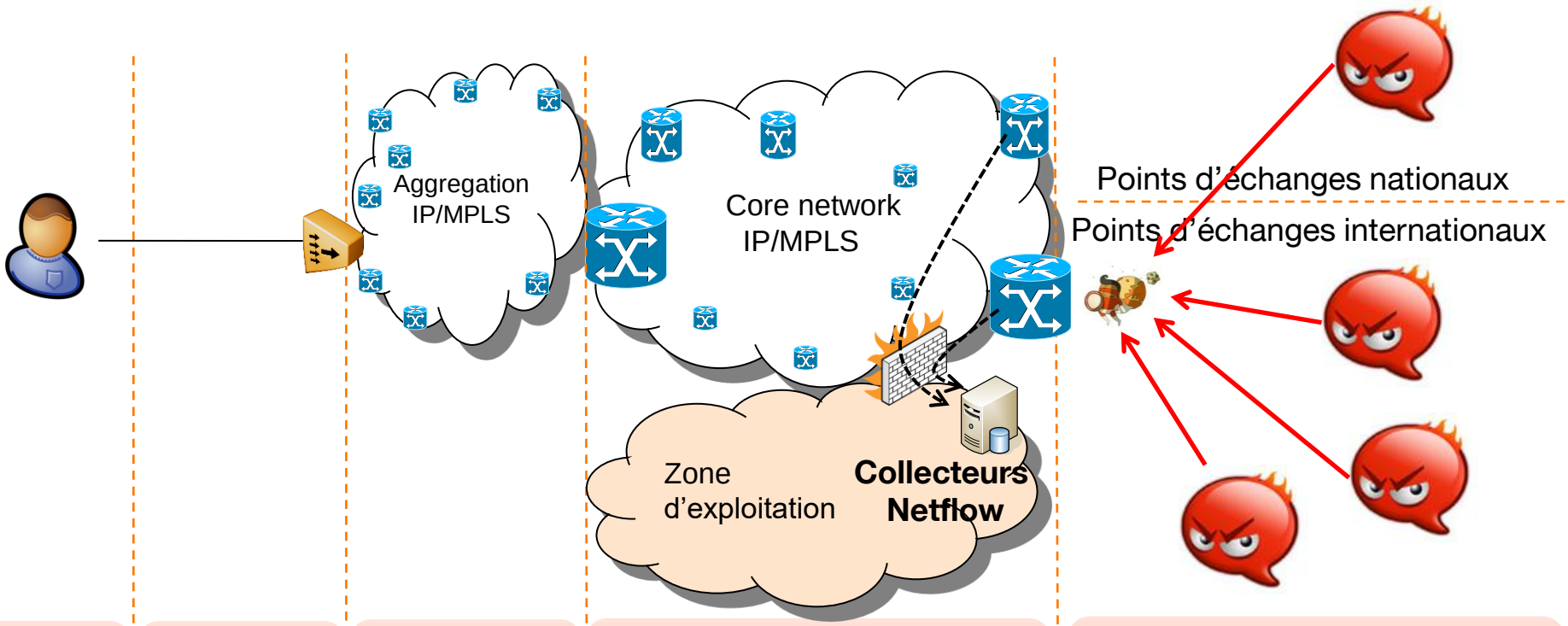
Attaques de dénis de service



Attaques de dénis de service

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
2 Gb/s > Attacks > 1 Gbps	2		15	224	8307	12026	13808	12974				
4 Gb/s > Attacks > 2 Gb/s	0		23	79	3903	5181	11108	14386	7786	6220	11001	2622
8 Gb/s > Attacks > 4 Gb/s	0	1	6	59	1072	2210	7310	12720	4877	5827	6924	1810
16 Gb/s > Attacks > 8 Gb/s		0	2	19	227	715	2857	9200	1322	2602	4612	1536
32 Gb/s > Attacks > 16 Gb/s			0	11	19	166	430	1582	245	684	1788	692
64 Gb/s > Attacks > 32 Gb/s				6	7	25	97	62	40	57	359	325
128 Gb/s > Attacks > 64 Gb/s				0	1	4	8	6	0	6	18	169
Attacks > 128 Gb/s				0	0	0	0	0	0	0	4	6

Attaques de dénis de service



Contre-mesures statiques pour les DDoS par amplification

Contre-mesure DDOS par amplification : filtres statiques

- **La première contre-mesure mise en place par Orange a été le positionnement de filtres statiques en entrée de son réseau**

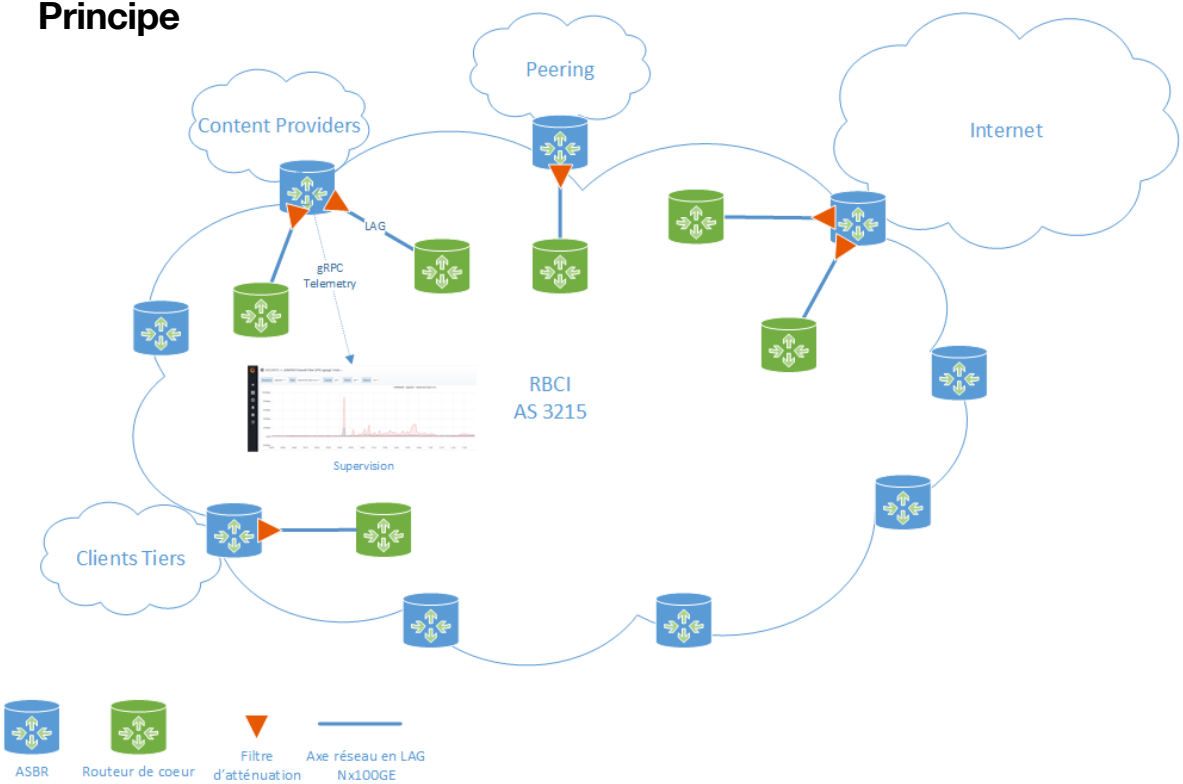
- **Ces filtres permettent:**
  - D'identifier des signatures réseaux d'attaques par Amplification bien connues:
    - Référencées entre autre par le CERT US.
  - De mesurer le volume de ces attaques
  - D'atténuer ces attaques par un mécanisme de « policing » (rate-limiter de trafic)

- **Une quinzaine d'attaques sont ainsi en permanence atténuées en entrée du réseau.**

- **Ces filtres sont mises à jour périodiquement en fonction des nouvelles signatures identifiées.**

Contre-mesure DDOS par amplification : filtres statiques

- **Principe**



A noter

- **Les filtres sont positionnés en « output » sur les liens ASBR > POP**
- **Les « policer » possèdent une valeur absolue – indépendante du nombre de liens dans les bundle Ethernet (LAG)**
- **Les statistiques des filtres: volume reçu Vs volume policé sont collectées en Telemetry (gRPC – gNMI).**

Contre-mesure DDOS par amplification : filtres statiques - exemple

```
term NTP {
    from {
        protocol udp;
        source-port ntp;
    }
    then {
        policer DOS-NTP;
        count DOS-NTP;
        accept;
    }
}
[...]
policer DOS-NTP {
    shared-bandwidth-policer;
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 625000;
    }
}
[...]
```

Signature

Contre mesure et statistiques

Bande passante autorisée

Contre-mesures dynamiques pour les DDoS de botnets

Contre-mesures dynamiques pour les DDoS de botnets

- **Depuis 2015: de plus en plus de dynamicité dans les signatures des attaques est observée**
- **Le couple: attaque par amplification + attaque sur ports dynamiques (aléatoires) est devenu quelques choses de très commun**
- **Les amplifications classiques restent atténuées par les filtres statiques.**
- **Pour les attaques sur ports dynamiques:**
  - Orange s'appuie sur la solution d' Netscout/ARBOR pour détecter les attaques dites dynamiques. La solution permet :
    - Détection rapide des attaques sur la base d 'échantillons réseaux transmis par les routeurs (protocole Netflow/IPFIX)
    - Fourniture de la signature réseau via une API
  - Orange utilise les signatures temps réels pour supprimer ces attaques (« blackholing ») avec :
    - Un outils maison de pilotage des contres mesures
    - Du protocole BGP Flowspec pour la diffusion des filtres (contres mesures) dynamiques sur le réseau

Contre-mesures dynamiques pour les DDoS de botnets

- **La détection des attaques dynamiques par la solution Arbor se fait en 3 temps:**

  — Phase 1 : L'heuristique sur la **première minute** consiste à détecter/-pondérer les **attaques par le débit**. Détection rapide des attaques les plus importantes en débit : **signature macroscopique,** à savoir uniquement les informations de types IP (adresses IP impliquées et protocole utilisé).

  — Phase 2 : Entre **1 et 2 min après** le début de la détection, la solution continue son apprentissage sur l'observation suspecte et fournit **une version plus détaillée** de l'attaque notamment avec les informations
  des **couches TCP/UDP**.

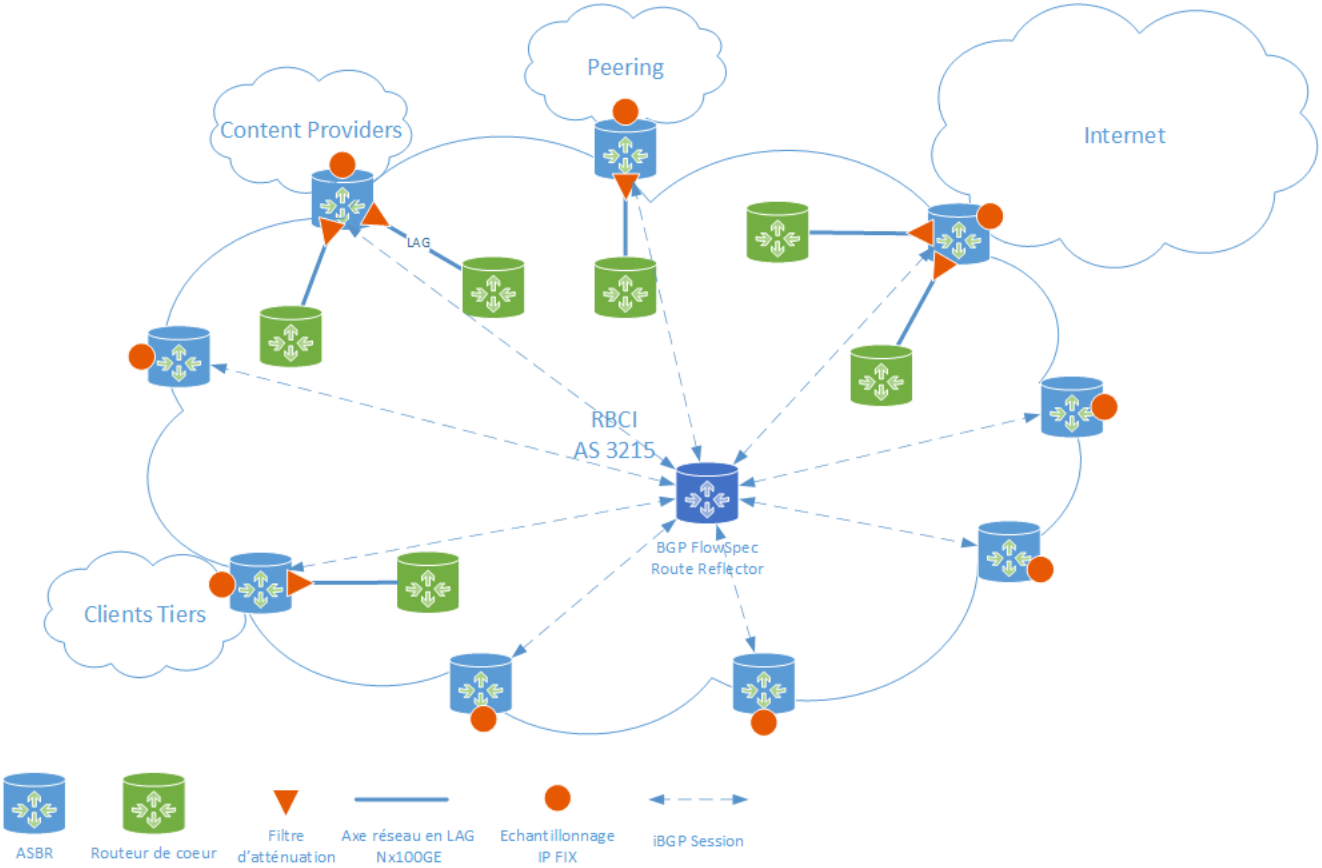
  — Phase 3 : **au-delà de 2 min**, la solution effectue **une mise à jour périodique de la signature** de l'attaque jusqu'à ce que celle-ci s'arrête.

- **A chaque phase les sondes Netscout/Arbor fournit ses informations au travers de notification ou d'une API.**

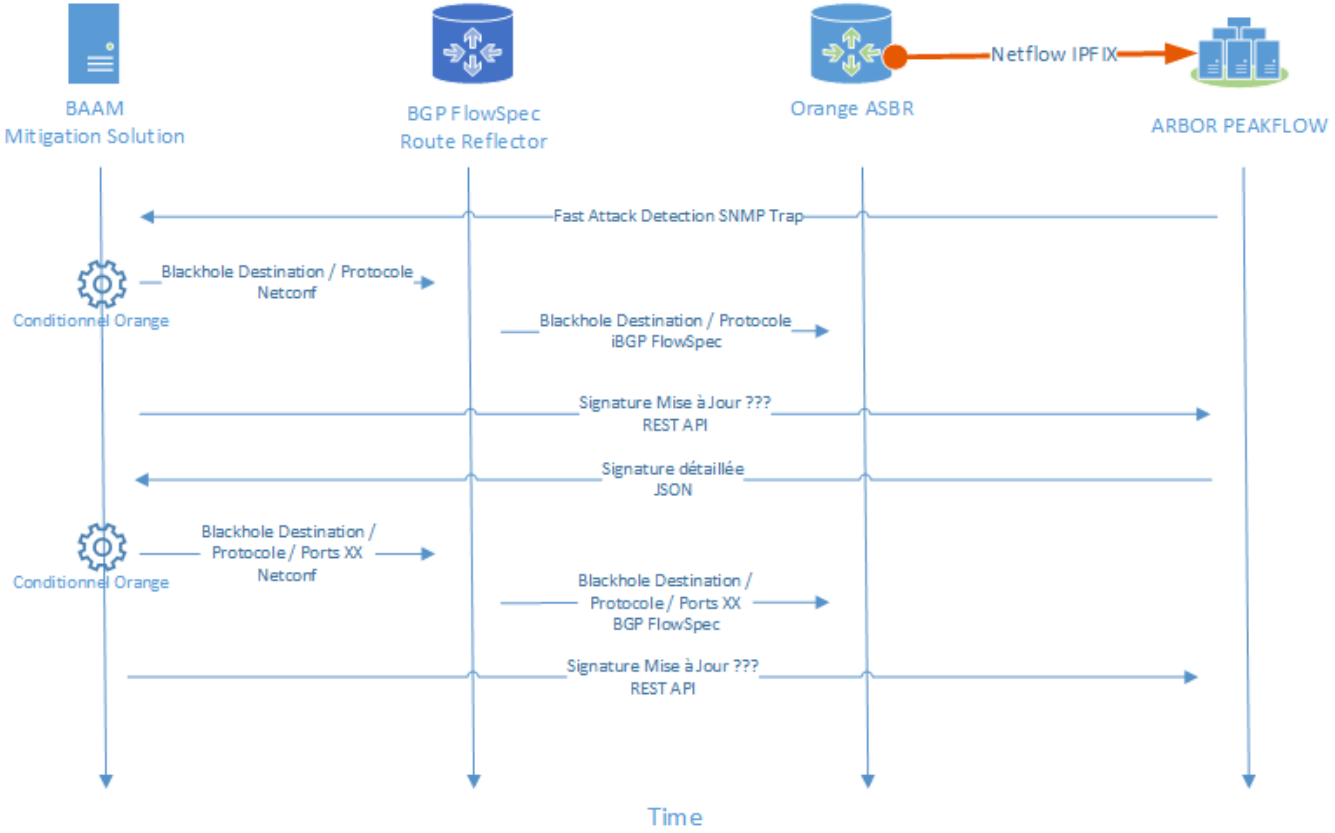
Contre-mesures dynamiques pour les DDoS de botnets

- **L'outil d'Orange (nom de code: BAAM) écoute les notifications / puis interroge périodiquement Arbor via son API.**
- **L'outil sur la base de contraintes propres à Orange va prendre ou non la décision de déclencher la suppression de l'attaque**
- **Cette suppression passe par :**
  - La pose d'un élément de configuration via une RPC Netconf sur un équipement réseau spécifique (routeur) : le route reflector BPG Flowspec
    - La configuration représente la signature de l'attaque
  - Automatiquement le routeur maillé avec l'ensemble des ASBR du réseau Orange diffuse l'information via la protocole BGP Flowspec.
  - Les ASBR concernés par l'attaque installe le filtre dynamique reçu via Flowspec: l'attaque est supprimée en entrée du réseau.
  - L'outil met à jour périodiquement la signature si celle-ci évolue – jusqu'à la suppression du filtre lorsque l'attaque est terminée.

Contre-mesures dynamiques pour les DDoS de botnets : Architecture

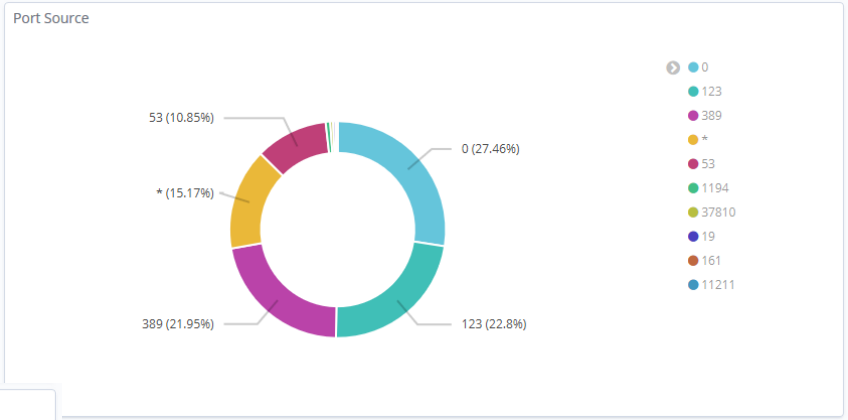


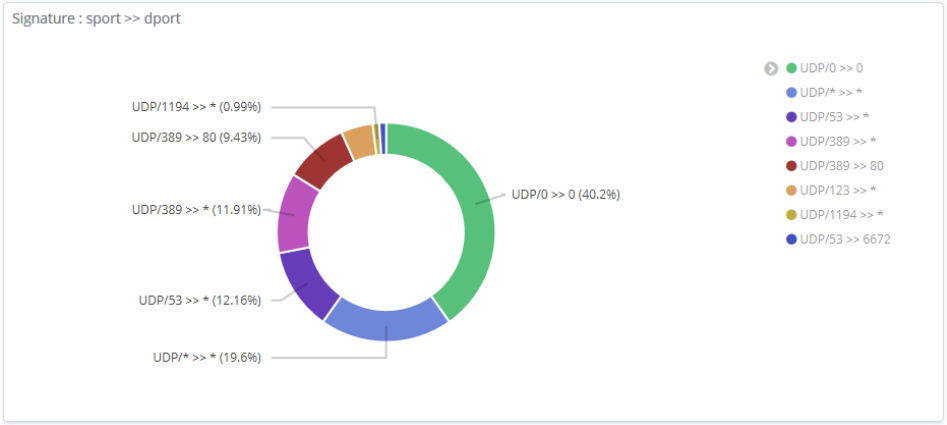
Contre-mesures dynamiques pour les DDoS de botnets : Macro algorithme



Contre-mesures dynamiques pour les DDoS de botnets : quelques stats

Statistique sur 7 jours





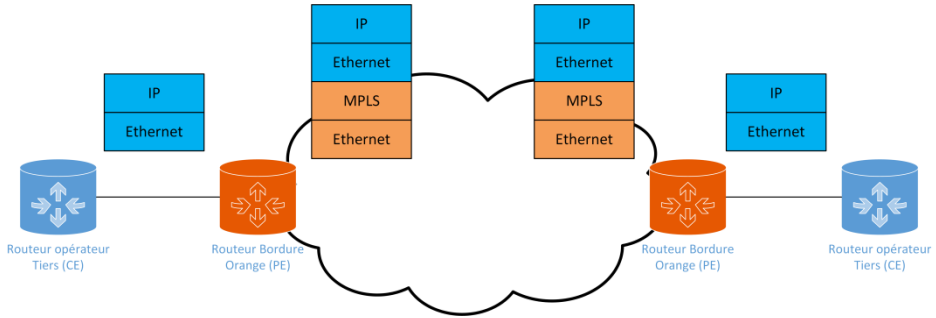
Contre-mesures dynamiques pour les DDoS de botnets : Extrait de l'IHM

DEMO DU PORTAIL BAAM

Attaques au cœur des offres Wholesale

Attaques au cœur des offres Wholesale : Principe

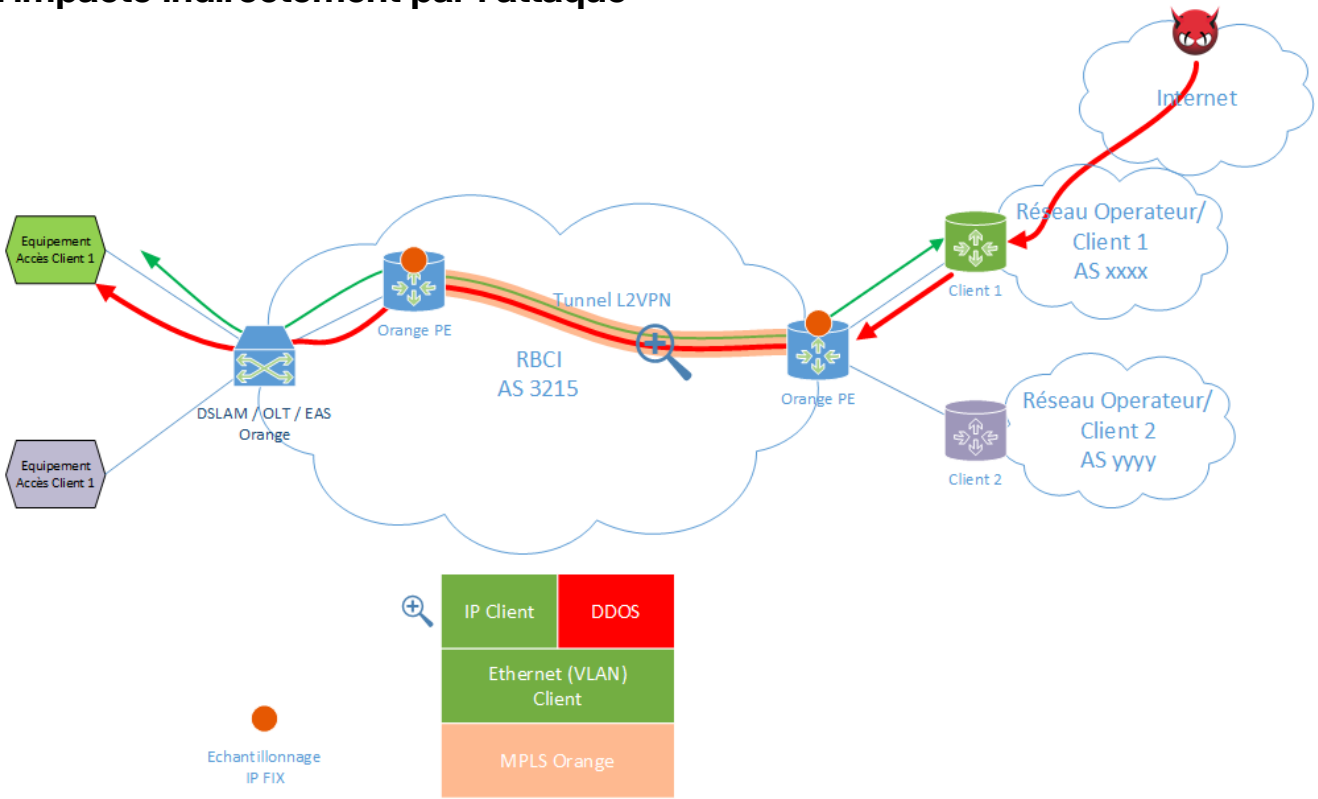
- Le réseau d'Orange (AS 3215) supporte de nombreuses offres dites de « gros » ou Wholesale
- L'opérateur Tiers utilise ainsi le réseau d'Orange pour augmenter sa capillarité réseau
- Ces offres de transport réseau s'appuient sur l'infra réseau d'Orange – infra mutualisée avec le réseau domestique grand public.
- Le transport des flux des opérateurs tiers se fait via la technologie L2VPN. On transporte la trame Ethernet de l'opérateur tiers dans une trame MPLS (maitrisée par Orange): on parle de Tunnel MPLS.



- Orange n'a pas la maitrise de la couche IP sur ce type d'offre.

Attaques au cœur des offres Wholesale : Principe

- **Comme Orange : ces opérateurs tiers subissent des attaques par déni de service sur leur réseau**
- **Si l'attaque véhiculée dans le réseau de l'opérateur tiers utilises les « fameux » tunnel MPLS Orange est impacté indirectement par l'attaque**



Attaques au cœur des offres Wholesale : Contre mesure

- **Orange a tout d'abord mise en place de l'échantillonage réseau (Netflow IPFIX) sur ces équipements (PE) d'interconnexion avec les opérateurs tiers:**
  - Afin de travailler avec Arbor sur le décodage de ces échantillons de trafic de type L2VPN (non supporté au départ par Arbor)
  - Puis identifier le profil/les signatures de ces attaques.
- **Orange s'appuie sur un nouveau template d'échantillonage L2VPN. Pour chaque paquet échantillonné on dispose de ces informations:**

MAC Src Addr	IPv4 Src Addr	TCP control Bits (Flags)
MAC Dest Addr	IPv4 Dest Addr	Protocol
Ingress Physical Interface	IPv6 Src Addr	IPv6 Option Header
Egress Physical Interface IPv6	Dest Addr	IPv6 Next Header
Dot1q VLAN ID	Packet Count	IPv6 Flow Label
Dot1q Customer VLAN ID	Byte Count	TOS
Post Dot1q VLAN ID	Flow Start Milliseconds	IP Version
Post Dot1q Customer VLAN ID	Flow End Milliseconds	
Dest Port	Src Port	

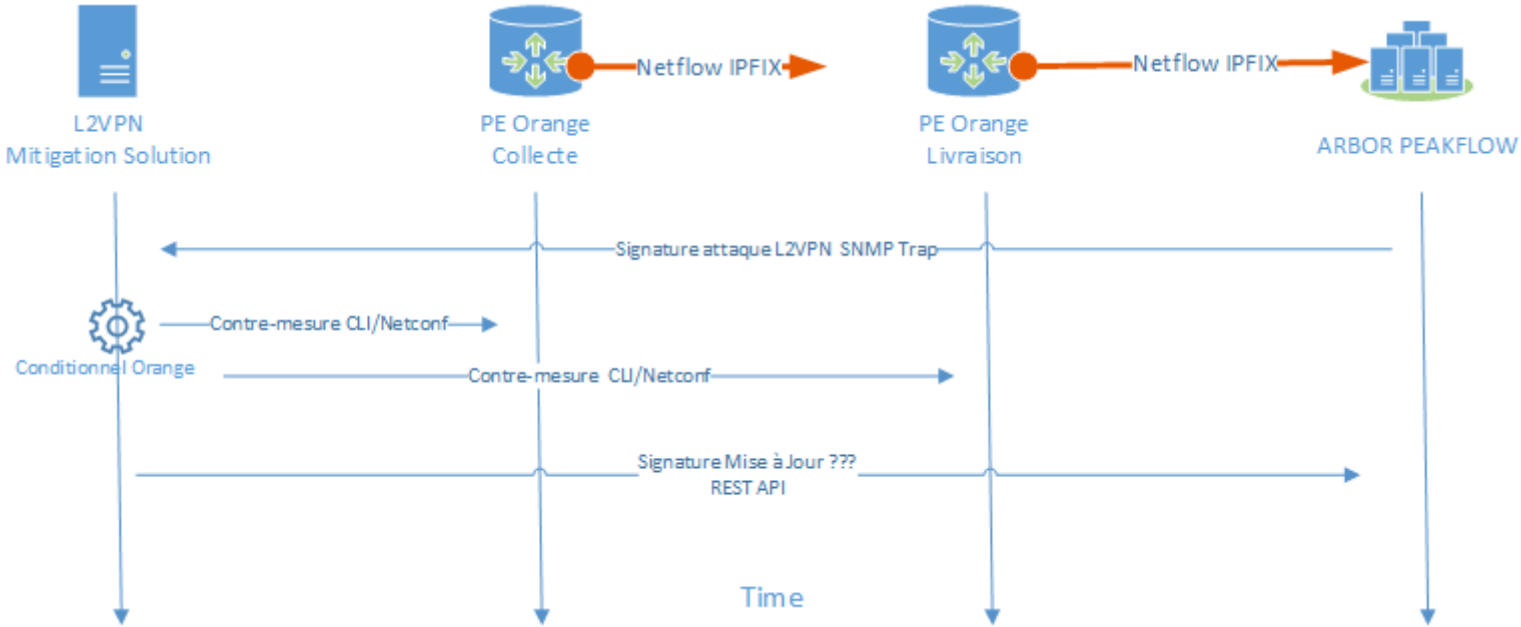
Attaques au cœur des offres Wholesale : Contre mesure

- **A l'issue de cette collaboration entre Orange et Arbor la solution était en mesure de fournir une détection rapide des attaques dîtes « tunnelées » et de proposer les mêmes mécanismes de notification/API sur les signatures de ces attaques.**
- **Malheureusement: pas de spécification Flowspec pour les services L2VPN disponibles aujourd'hui**
- **Orange a donc fait évoluer son outil pour proposer de nouvelles contres mesures associées à ces attaques spécifiques:**

  – Shutdown du port de livraison ou shutdown du port de collecte
  – Shutdown du VLAN de livraison ou shutdown du VLAN de collecte
  – Application d'un filtre de suppression de trafic Ethernet basé sur les adresses MAC src/dst sur le port de collecte ou de livraison.

- **Ces actions de contre mesure sont réalisées directement sur le ou les équipements d'Orange (d'entrée) impactés par l'attaque. L'outil réalise ces changements au travers de RPC/Netconf.**

Attaques au cœur des offres Wholesale : Macro algorithme



Merci