Concevoir et déployer ses protections anti-DDoS

Deux ans de recherche sur les attaques DDoS et de développement d'un système de défense

Antoine VERSINI, Resp. Réseau & Télécom, NERIM SAS
(antoine.versini@corp.nerim.net)
( @nerim_net)

AGENDA

1. Le contexte
   - La menace
   - Les infrastructures et services à protéger
   - Les choix possibles à ce stade
   - Let's do it !

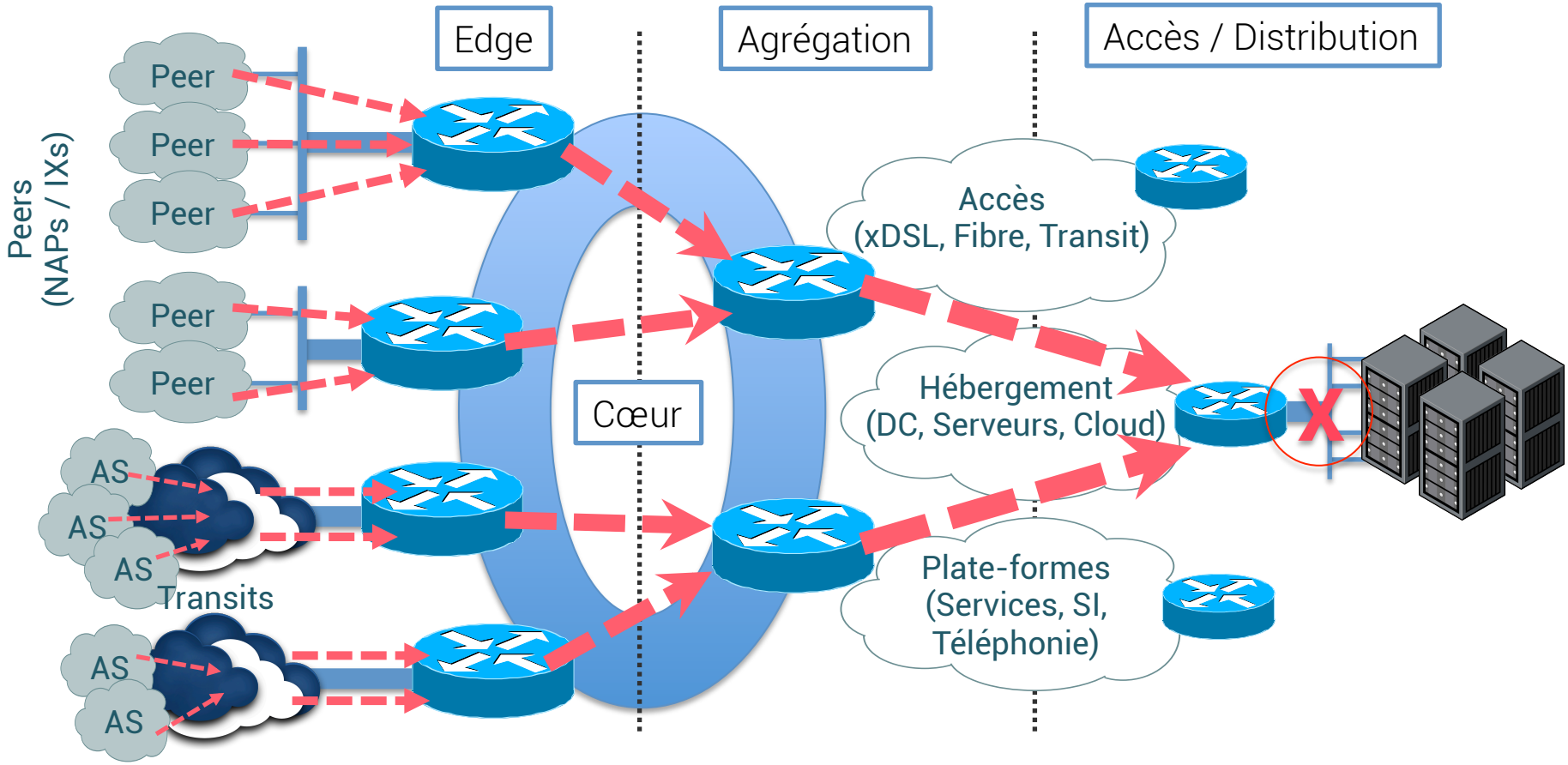
2. Le projet
   - La métrologie et la défense : deux objectifs indissociables
   - L'architecture générale
   - Les difficultés rencontrées & les solutions
     - Détecter une attaque ? Pas si simple…
     - Bloquer ce qui doit réellement l'être
     - La réactivité temporelle et comportementale
     - L'analyse temps-réel et ses contraintes

3. Et à présent… ?
   - Le chemin restant à parcourir

LE CONTEXTE: LA MENACE

Caractéristique principale de ces attaques: la distribution des sources.

Les sources se trouvent disséminées partout sur Internet. Chaque réseau hébergeant l'une d'entre elles expédiera le trafic illégitime par un chemin différencié de celui des autres réseaux infectés.



LE CONTEXTE: LA MENACE

Préparer l'infrastructure et ne pas se reposer sur un seul mécanisme de défense.

Paradoxalement, la plus grande force de ces attaques est leur plus grande faiblesse. Sur un réseau à la connectivité très diversifiée, il n'y a finalement qu'assez peu de trafic illégitime à détruire à chaque point d'entrée possible.

Le phénomène est d'ailleurs devenu une barrière à l'entrée : prétendre résister à ces attaques nécessite de démultiplier sa connectivité à Internet en transit et *peering*, dans le seul but de pouvoir les absorber. Cela à un coût qu'un nouvel entrant ne peut se permettre. Ni en infrastructures, ni en service de transit protégé.

De nombreuses autres techniques doivent venir s'ajouter à la détection et mitigation de DDoS : uRPF, bogon filters, anti-spoofing AS local & AS clients, filtres et polices des plans de contrôle des actifs réseau.

Et potentiellement d'autres méthodes moins tendres pour la neutralité du réseau : rejet des fragments, UDP et TCP port 0, options IP.

Une fois ces premières lignes mises en place, la partie peut commencer.

LE CONTEXTE: QUOI & QUI PROTEGER ?

- Infrastructures

  Plus de 200 routeurs en production, répartis sur une cinquantaine de sites situés dans 5 pays.

- Services

  Tout ce qui est fondé sur IP et qui expose au moins une adresse à Internet. Connexions, transit, hébergement, collectes opérateurs, télécommunications publiques, Jean-Claude *computing*, passerelles Internet de réseaux privés, …

- Qui ?

  Plusieurs dizaines de milliers de clients entreprise: de la TPE aux grands groupes, institutionnels, organismes d'état, opérateurs, hébergeurs, sites… Sans distinction.

  Vendre à ses utilisateurs un service protégé plus cher que le service sans protection, ou les laisser mourir sous les attaques pour les forcer à basculer vers le service protégé *in fine,* revient à les prendre en otage.

LE CONTEXTE: LES CHOIX POSSIBLES

- Réaction manuelle ou semi-automatisée

  Installation de routes pour détruire le trafic de l'attaque (risque de concentration sur le ou les routeurs injectant ces routes dans le cœur.)

  Installation de filtres *ad hoc* sur l'ensemble de la bordure. Nécessite une analyse humaine des caractéristiques du trafic illégitime et la conception de règles à la volée.

  RTBH sur les liaisons de transit. Quid des *peerings* ?

  Temps de réaction humain incompressible. Certaines plate-forme ne résistent que quelques secondes avant de céder (ex: agrégation L2TP.)

  Solution hautement inconfortable: dans l'immense majorité des cas, il en résulte aussi un filtrage et une destruction du trafic légitime et l'attaquant est parvenu à ses fins.

  Il s'agit du modèle antique, celui que précisément nous cherchons à abandonner. Poursuivre ainsi était insensé.

LE CONTEXTE: LES CHOIX POSSIBLES

- Les vendeurs d'alarme

  Promesse d'une boîte noire installée quelque part sur le réseau qui opère toute la magie et vous soustrait de la menace.

  Conçue par définition par des équipes d'ingénierie qui ne sont pas opérationnelles sur un réseau d'opérateur.

  Capacité d'intégration des solutions du marché allant de mauvaise à moyenne.

  Quid des réactions face aux menaces inexistantes au moment de la conception ? Le temps pour disposer de mise à jour de ces systèmes afin de les rendre capables de gérer une menace innovante est inconnu (comprendre: au mieux aléatoire.)

  L'alarme ultime n'existe pas. À quoi bon acheter un mécanisme dont l'on sait déjà qu'il sera dépassé le jour de son installation, et se rendre dépendant d'autrui ?

  Savoir cliquer sur la WebUI d'un système sur lequel la Network Security Association a plus de privilèges que vous ne fait pas de vous un spécialiste de la question, capable de réellement aider vos utilisateurs…

LE CONTEXTE: LES CHOIX POSSIBLES

- Let's fucking do it !

  L'on n'est jamais si bien servi que par soi-même, alors nous allons faire ce que nous savons faire de mieux: créer nos propres outils.

  Choix de partir de zéro. Nous n'utiliserons aucun code existant car pour une telle menace l'indépendance doit être totale.

  Il nous faudra comprendre, jour après jour, attaque après attaque, de quoi elles sont constituées, les vecteurs possibles, les types de cibles (et pourquoi ces cibles le deviennent,) ainsi que les protections possibles et comment les déployer.

  Il y aura des moments pénibles à traverser, avec des échecs et le réseau sera torturé avant que les premiers effets positifs ne se fassent sentir.

  Mais le jeu en vaut la chandelle : indépendance, connaissance affinée de la menace et des réactions à adopter, interopérabilité optimale avec les équipements du réseau, protections parfaitement adaptées aux infrastructures et aux services, évolutivité inégalable et réactivité imbattable en cas de nouveau vecteur.

AGENDA

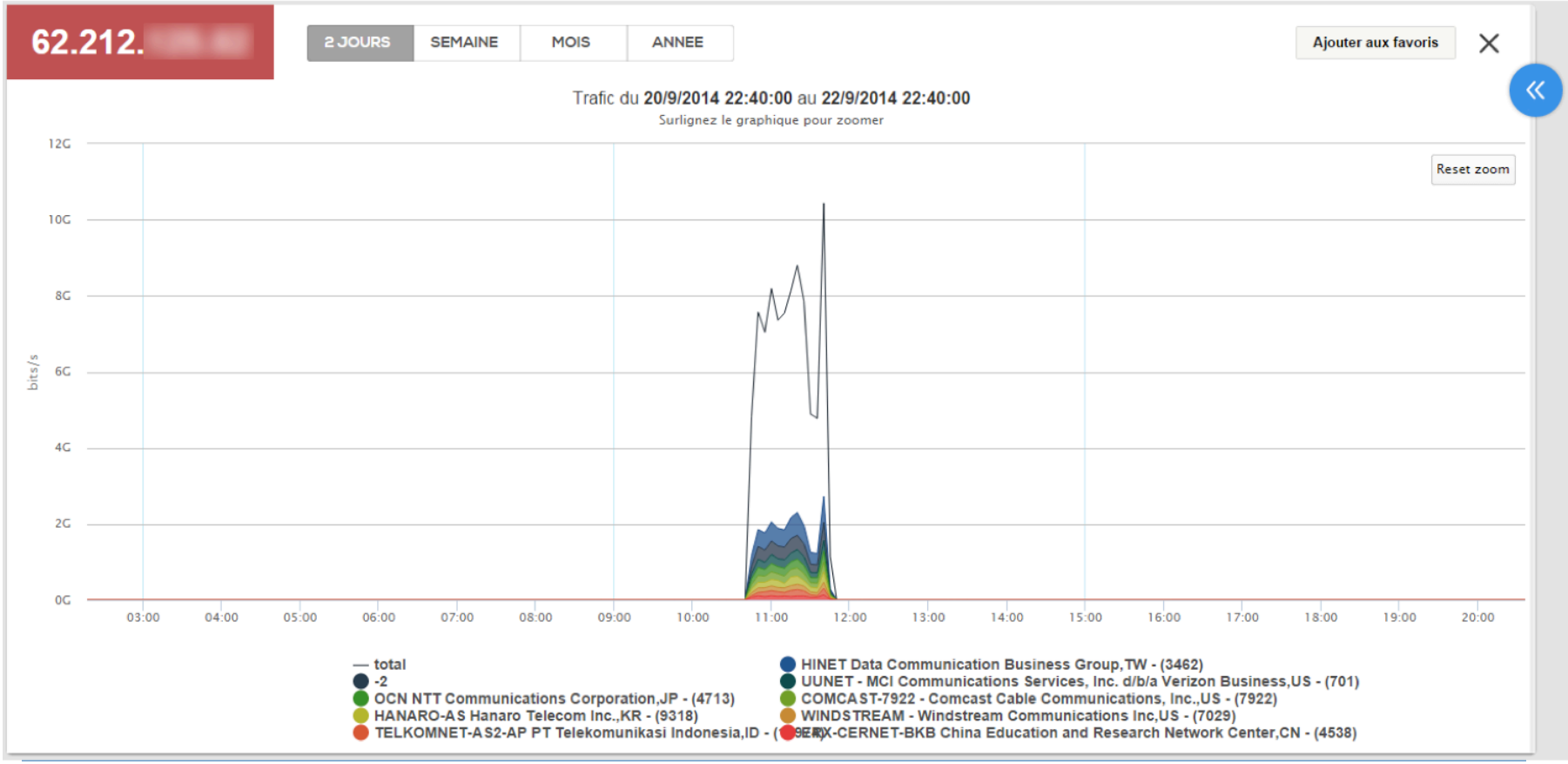
2.

Le projet

- La métrologie et la défense : deux objectifs indissociables
- L'architecture générale
- Les difficultés rencontrées & les solutions
  - Détecter une attaque ? Pas si simple…
  - Bloquer ce qui doit réellement l'être
  - La réactivité temporelle et comportementale
  - L'analyse temps-réel et ses contraintes

La métrologie : FSB (Flexible Statistics Backend)

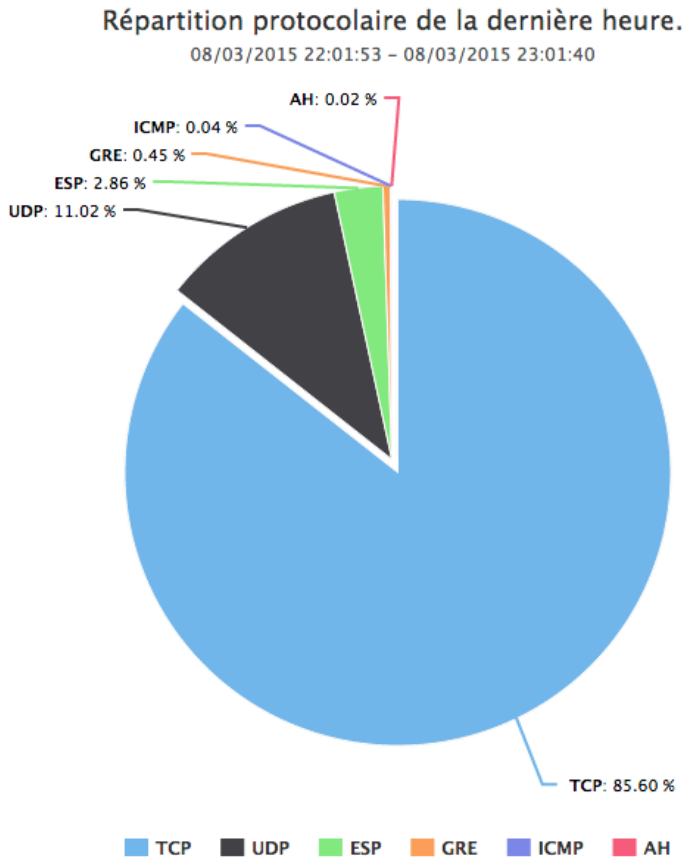
Pour neutraliser les attaques, il est essentiel de les comprendre. Cela implique de savoir d'où elle proviennent, de quoi elles sont constituées et quels sont leurs caractéristiques comportementales typiques.



LE PROJET: LA MÉTROLOGIE ET LA DÉFENSE

- Caractéristiques du trafic : la métrologie en assistance de la détection

  Apprentissage des composantes de volumétrie (octets, paquets) et des caractéristiques de trafic vers chaque destination.



10 DESTINATIONS AVEC LE PLUS DE TRAFIC SUR LES 39 DERNIÈRES MINUTES

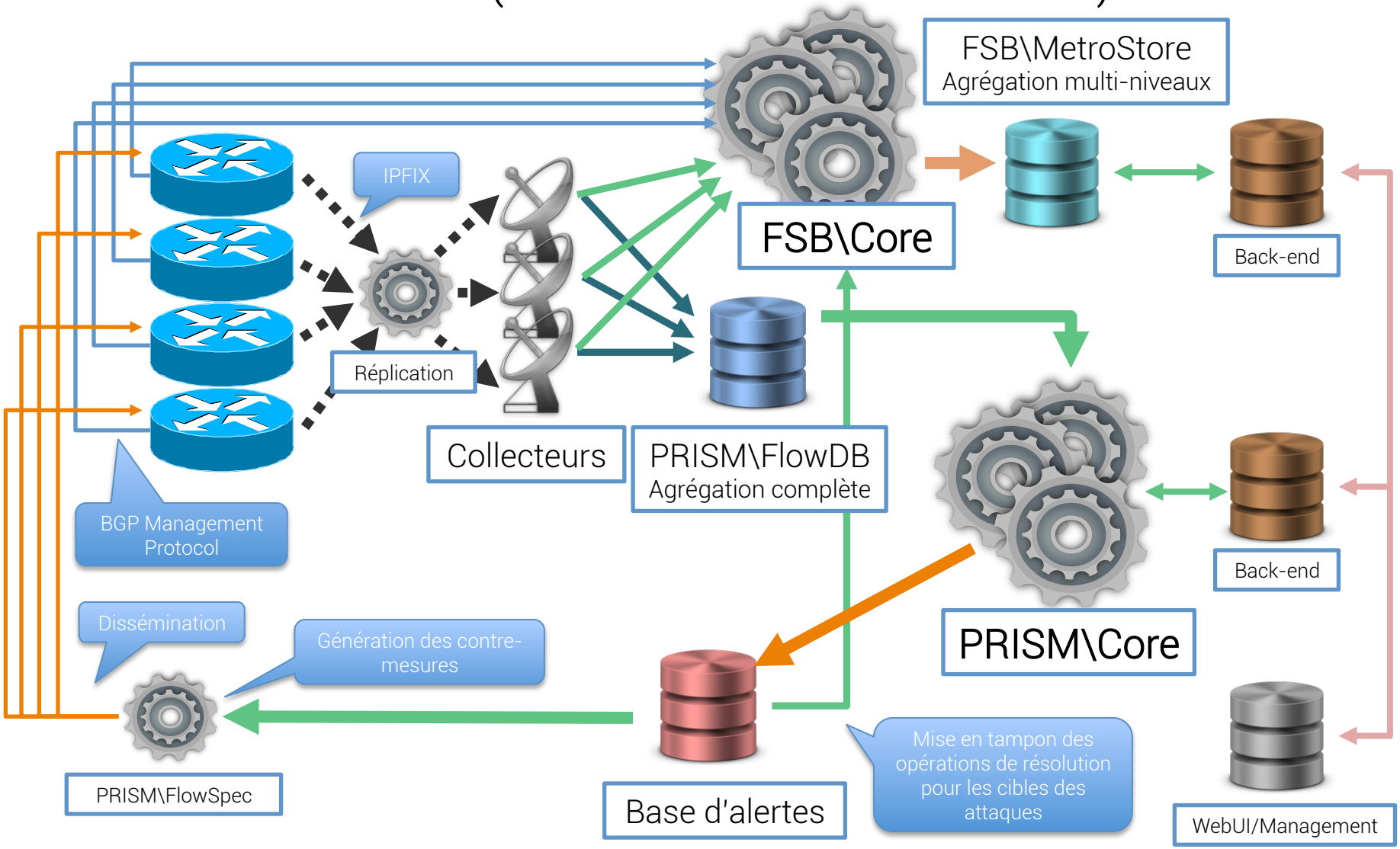
IP	Avg Kb/s	Avg Packets/s
195.5. (195.5)	68 534,39	6 570
178.132. (122.fib.nerim.net)	53 421,30	5 399
80.65. (.hst.nerim		
80.65. (nst.nerim.		
178.22. (178.22.		
195.5		

10 TOP SOURCES POUR 195.5.

IP	Avg Kb/s	Avg Packets/s
8.254. (8.254.)	5 830,62	503
37.187. com)	3 670,78	315
173.194. (173.194.)	2 574,02	220
8.254. (8.254.)	2 285,58	196
80.239. (teliacarrier.com)	2 283,17	200
8.254		

LE PROJET: ARCHITECTURE GENERALE

Protection anti-DDoS : PRISM (Protection de Réseaux IP Sur Mesure)



DÉTECTER UNE ATTAQUE: PAS SI SIMPLE…

Certaines attaques sont vicieuses et ne sont pas volumétriques

Les DoS ne sont pas systématiquement des attaques ayant pour objectif la saturation du réseau. Les attaques destinées à épuiser toutes les ressources systèmes d'autres types d'actifs sont tout aussi dangereuses et moins évidentes à détecter.

Il faut alors réagir en cas de changement significatif de nombreux critères prédéterminés, et considérer l'ampleur de la menace en fonction de leur concordance.

- Distribution protocolaire au niveau 3,
- Augmentation du nombre de sources (cf. planche métrologie) en peu de temps,
- Dépassement de la volumétrie acceptable dans un intervalle de temps faible,
- Changement majeur de la dispersion (par exemple la variance σ de la distribution gaussienne) de paramètres de niveau 4 (ports TCP, type ICMP, …)

Détecter une attaque est donc le plus souvent le résultat d'une pondération de plusieurs facteurs, la volumétrie étant l'un d'entre eux et n'est pas l'unique déterminant.

DÉTECTER UNE ATTAQUE: PAS SI SIMPLE...

Exemple d'une attaque composite

L'analyse suivante montre que l'attaque est composée de deux vecteurs: UDP/123 et UDP/80. UDP/123 se conforme au débit maximal possible pour cet accès DSL (25Mbit/s) mais est bloqué car considéré comme composante de l'attaque.

■ Blocage dynamique ■ Redirection dynamique ■ Blocage statique ■ Redirection statique

	IP	Protocole	Port	Template	Date de début
■	62.212. (.nerim.net)	UDP	80	25 Mb/s (18 750 p/s)	22-09-2014 10:40:39
■	62.212. (.nerim.net)	UDP	123	25 Mb/s (18 750 p/s)	22-09-2014 10:40:50

Date de fin	Durée du blocage	Kb/s lors du blocage	Paquets/s lors du blocage
22-09-2014 11:42:57	1 h 2 min 17 s	1 174 287,21	313 715
22-09-2014 11:41:52	1 h 1 min 1 s	16 147,60	4 288

BLOQUER CE QUI DOIT L'ÊTRE: AU NIVEAU 4

Encore une fois: exploiter la faiblesse inhérente de la distribution

Après l'échec d'une attaque volumétrique, les attaquants les plus déterminés vont tâcher de provoquer une réaction néfaste du mécanisme de protection envers la cible.

Typiquement, tenter de faire bloquer le protocole et le port du service ciblé.

Dans le cas d'une attaque à ports aléatoires, les cas sont :

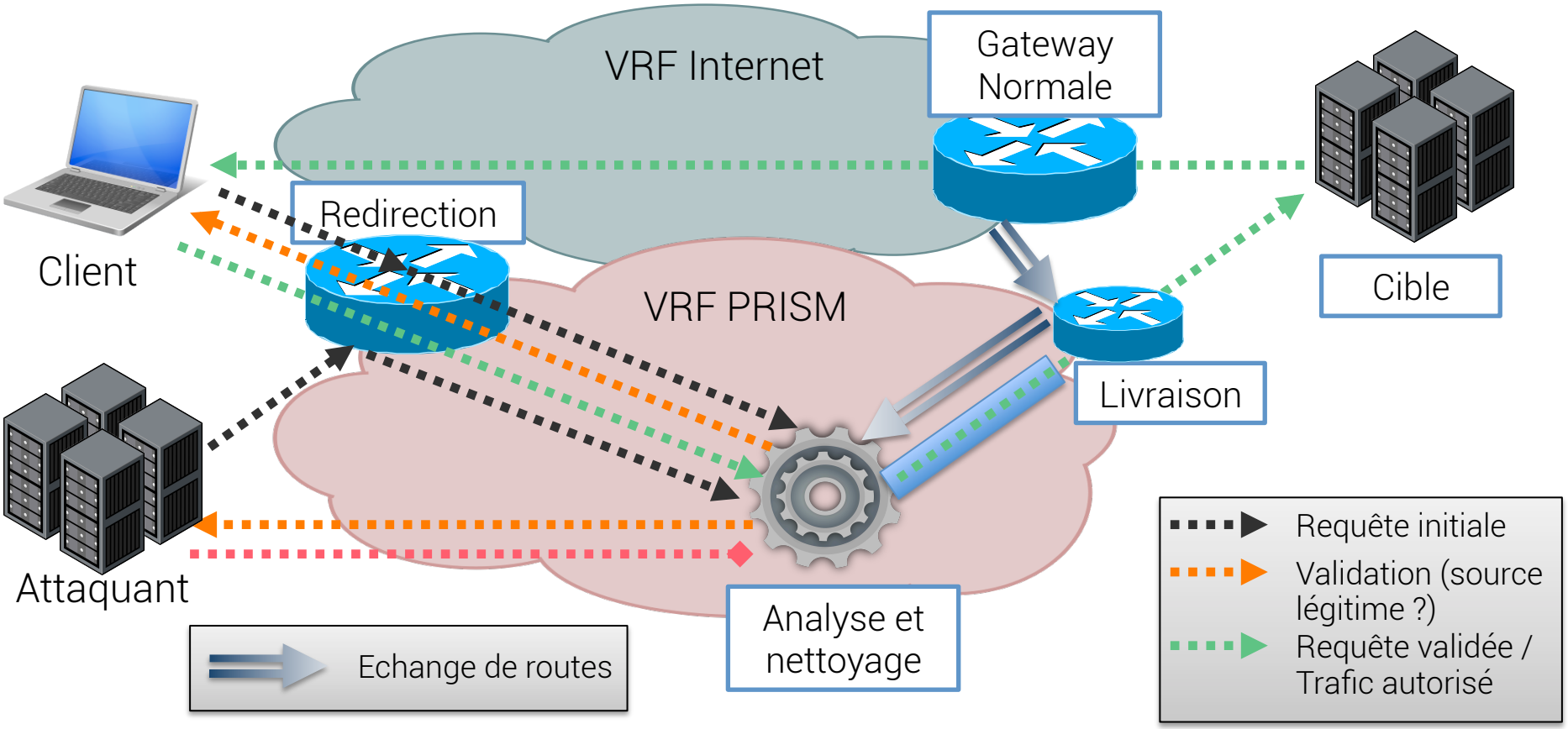
- L'écart-type de la distribution se rapproche de l'espace interquartile : bloquer l'ensemble des ports, sauf celui du service. Ainsi on ne laisse passer potentiellement que 1/65535^{ième} (soit 610Kbit/s d'une attaque de 40Gbit/s.)

- L'écart-type est plus faible :

  - $\overline{x} - 2\sigma > 1024$: blocage des ports de l'étendue maximale,
  - sinon : décision de filtrage niveau 7 si $\overline{x}$ est proche du port du service à défendre.

BLOQUER CE QUI DOIT L'ÊTRE: AU NIVEAU 7

- **Etape 1** : Détection d'une attaque à destination d'un service supporté (ex: HTTP)
- **Etape 2** : Installation d'une redirection de ce trafic dans une VRF de nettoyage
- **Etape 3** : Vérification que la source de chaque requête n'est pas un drone
- **Etape 4** : Installation d'un *fast-path* en cas de vérification réussie
- **Etape 5** : Renvoi des requêtes légitimes vers la cible



S'adapter aux comportements des attaquants

Il est rare qu'une attaque soit lancée sur un mode *fire & forget*. Souvent les attaquants suivent d'assez près les effets de leurs attaques. Et ceux qui ne le font pas apprennent vite à le faire, après avoir dépensés en pure perte 1/n *Bitcoins* dans une attaque d'une heure fondée sur de la volumétrie UDP.

La réactivité de l'ensemble du dispositif lors du début de l'attaque est cruciale. Il ne faut pas attendre la consolidation depuis l'ensemble des sources de métadonnées car souvent les équipements n'exportent pas les *flows* actifs à moins de 10 secondes.

En revanche, lorsqu'une attaque se termine, il faut entrer dans une période de *cooldown.* Sinon, en lançant des attaques cycliques sur des vecteurs différents, l'attaquant peut provoquer une indisponibilité continue par superposition.

Le système doit donc continuer à protéger une cible même si l'attaque se termine, et tenter de prévoir le vecteur suivant si un motif répétitif a pu être repéré dans les attaques précédentes.

L'ANALYSE TEMPS-RÉEL ET SES CONTRAINTES

Un ***not-so-big-but-really-painful data*** !

Stocker n x 10^6 *flows* est à la portée de n'importe quel système.

Les analyser pour produire des séries en moins de 100ms l'est déjà nettement moins.

Tous les *No-SQL* testés ont échoué (même ceux travaillant en RAM.)

Il nous a fallu créer notre propre stockage *No-SQL* adapté à la situation. Il est fondé sur un algorithme de type *B-tree* qui permet entre autre de réaliser des résolutions dans une dizaine de tables de routage de 500k entrées et de procéder à des indexations sur plusieurs dimensions de collections hachées.

Son avantage est aussi de pouvoir paralléliser les traitements à l'extrême, notamment sur l'aspect temporel des informations stockées. Ce qu'un stockage classique ne peut pas faire lors de traversées séquentielles.

L'ANALYSE TEMPS-RÉEL ET SES CONTRAINTES

La métrologie doit survivre au stress des attaques

Où l'on découvre que tenter de classifier en temps-réel toutes les sources de DDoS en cas d'attaque est absurde.

Lors des attaques, un effondrement général du système de métrologie fut observé, peu importe les réglages essayés (nombre de threads, tolérance à l'échec, …)

L'effet néfaste est que les flux légitimes n'étaient sont plus résolus ni classifiés et que les statistiques vers l'ensemble des destinations (dont celles non-impliquées dans les attaques) devenaient graduellement distordues.

Nous avons donc appris à faire avec la limite de la technologie, malgré des machines à 32 cœurs et 512GB de mémoire vive : mettre en file les *flows* impliqués dans une attaque pour résolution/agrégation/insertion parallèle par des cœurs dédiés.

Ainsi le traitement du trafic légitime reste déterministe dans son temps d'exécution et n'est pas influencé par les attaques. Mais l'effet rétroactif des résolutions retardées sur les graphiques est contre-intuitif…

AGENDA

3. Et à présent… ?

   Le chemin restant à parcourir

LE CHEMIN RESTANT À PARCOURIR

Quid du ***Big One*** ?

Il arrivera irrémédiablement… S'imaginer en sûreté derrière 300, 1500, … Gbit/s de surcapacité serait une erreur funeste.

La question est donc: à partir de quel stade, pour le bien de tous les autres utilisateurs, ne doit-on plus chercher à défendre la cible, mais l'infrastructure ?

- Activer automatiquement les communautés RTBH en cas de saturation d'une interconnexion de transit,
- Couper les sessions vers les serveurs de routes des points d'échange, pour ne conserver que des sessions de *peering* vers des pairs avec un certain niveau de confiance,
- Idéalement, détecter les AS voisins (hors transit) participant à l'attaque et couper les sessions BGP afférentes pour forcer le trafic vers les RTBH des transitaires.

En bref: inculquer une connaissance du réseau aux analyseurs.

LE CHEMIN RESTANT À PARCOURIR

La question de l'analyse des charges utiles

La législation en vigueur entend arrêter l'analyse aux en-têtes.

Pourtant, toutes les méthodes mises en œuvre par des systèmes discrets ou dits UTM, fondées sur des heuristiques ou des comparaisons de motifs connus, ne s'y conforment guère…

Cette méthode crée une bijection entre la puissance de traitement utilisée et l'ampleur de l'attaque. Et donc une faiblesse intrinsèque, pour un apport qui peut être faible si un attaquant éduqué élabore un générateur capable d'influer négativement sur le *scoring* par implémentation malicieuse des principes et techniques utilisés par les analyseurs de contenu.

Exemple: un système anti-spam fondé uniquement sur l'analyse des messages est utile, mais ne doit être utilisé conjointement qu'avec nombre d'autres méthodes.

Cette voie dans laquelle s'engouffrent les systèmes commerciaux pour justifier des coûts matériels élevés n'est qu'une partie relativement restreinte de la solution.

END & THANKS