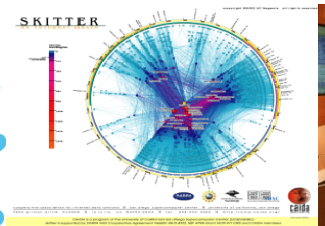
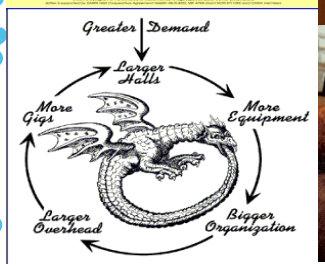
Comment répondre à une attaque DDOS (édition fournisseur de services)





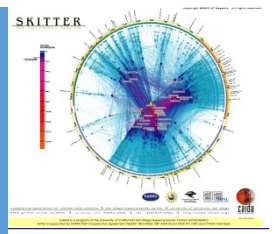
Grandes lignes

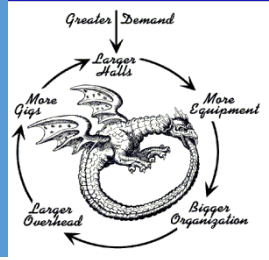
- Principes de base pour lutter contre une attaque DoS
- Mettre les outils à contribution - Attaque DDOS

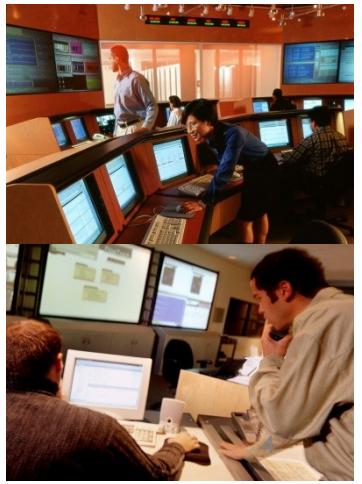
Une longue histoire - Formation en ligne

- NANOG 23 - Sécurité des ISP - Techniques du monde réel II - par Barry Raveendran Greene, Cisco Systems ; Chris Morrow, UUNET/Verizon ; Brian W. Gemberling, UUNET
- NANOG 25 - Mise à jour de la sécurité BGP - par Barry Raveendran Greene, Cisco Systems
- NANOG 26 - Sécurité ISP - Techniques du monde réel - par Barry Raveendran Greene, Cisco Systems ; Kevin Houle, CERT
- NANOG 28 - Sécurité des FAI : Déploiement et utilisation des failles de sécurité par Barry Raveendren Greene, Cisco Systems ; Danny McPherson, Arbor Networks
- NANOG 36 - Introduction à la sécurité ISP 101 par Barry Greene, Cisco Systems et Roland Dobbins, Cisco Systems
- NANOG 47 - Les dix principales techniques de sécurité de NSP-SEC par Barry Greene, Juniper Networks
- NANOG 54 - Kit d'outils de "sécurité" des fournisseurs de services par Barry Greene, ISC (partie 1) et (partie 2)
- **MAAWG 26 - Atelier sur la sécurité des SP**
- Atelier CommunicAsia 2015

Principes de base pour lutter contre une attaque DoS

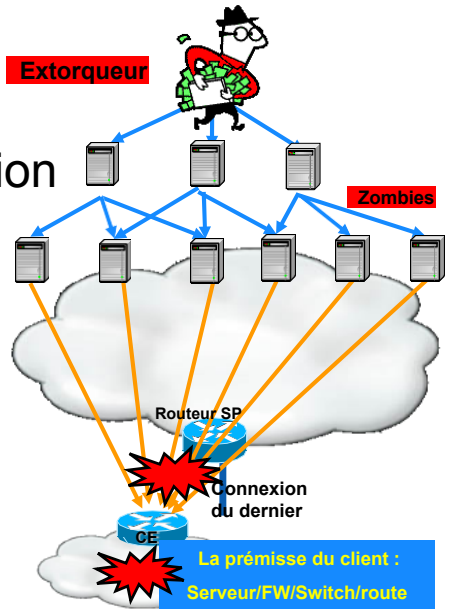






Comment arrêter réellement une attaque DDOS ?

- Les Clean Pipes, Scrubbing Centers et autres outils "anti-DDOS" *n'arrêtent pas les attaques DDOS*.
- Ces outils sont essentiels, mais ils ne doivent être utilisés que pour fournir :
  Restauration de services complets pour certains services essentiels à la mission
  Il est temps de remédier à l'attaque DDOS



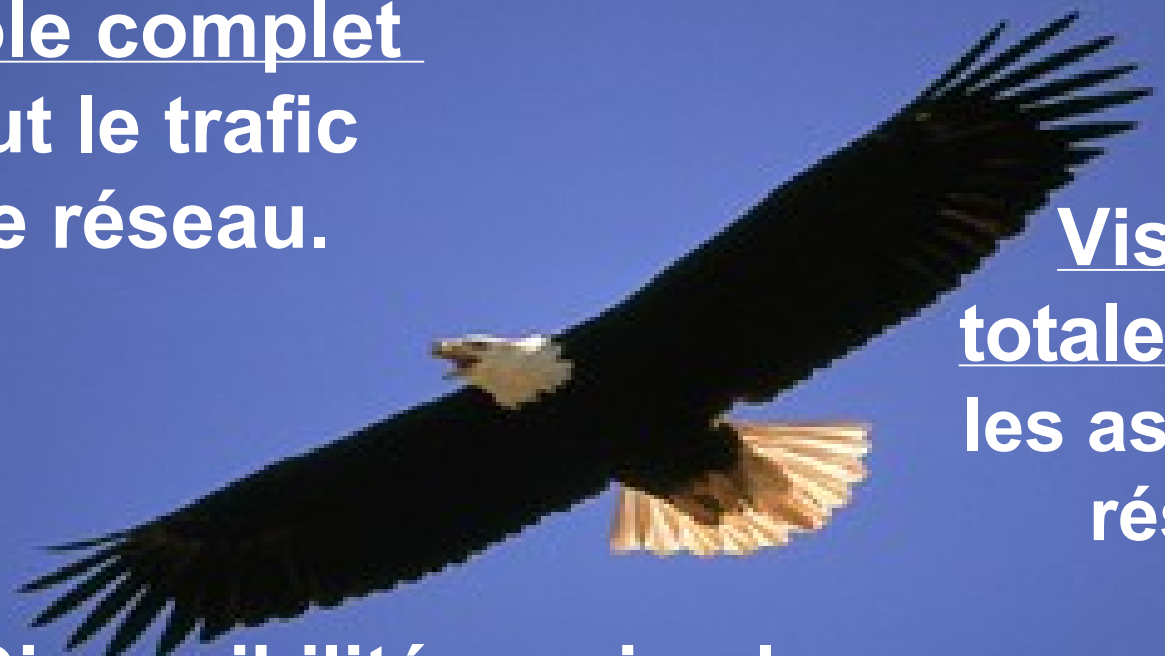
- Arrêter une attaque DDOS nécessite une capacité à faire :

1. Résister à l'attaque et ne pas céder à l'extorsion/la menace.
2. Visibilité/traçage des sources de l'attaque
3. Remédier aux outils utilisés dans l'attaque (BOTNETs et réflecteurs).
4. Backtracing jusqu'au C&C utilisé pour conduire l'attaque.
5. Trianguler sur la ou les personnes qui lancent l'attaque.

Essential Principe de la résilience du EssentialDoS

Construire une infrastructure sécurisée pour des services rentables

Contrôle complet de tout le trafic sur le réseau.

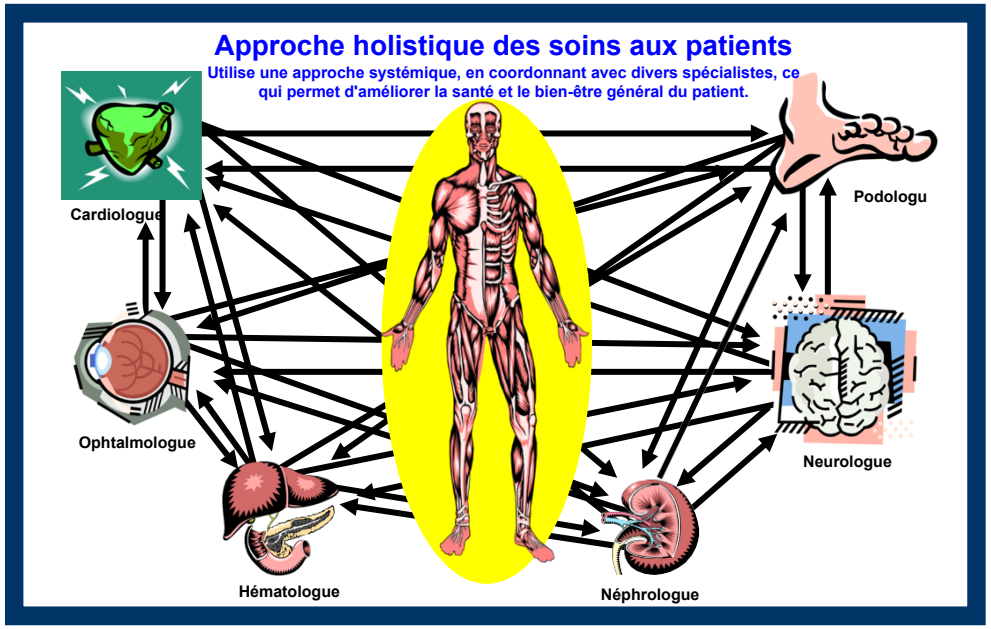


Visibilité totale sur tous les aspects du réseau.

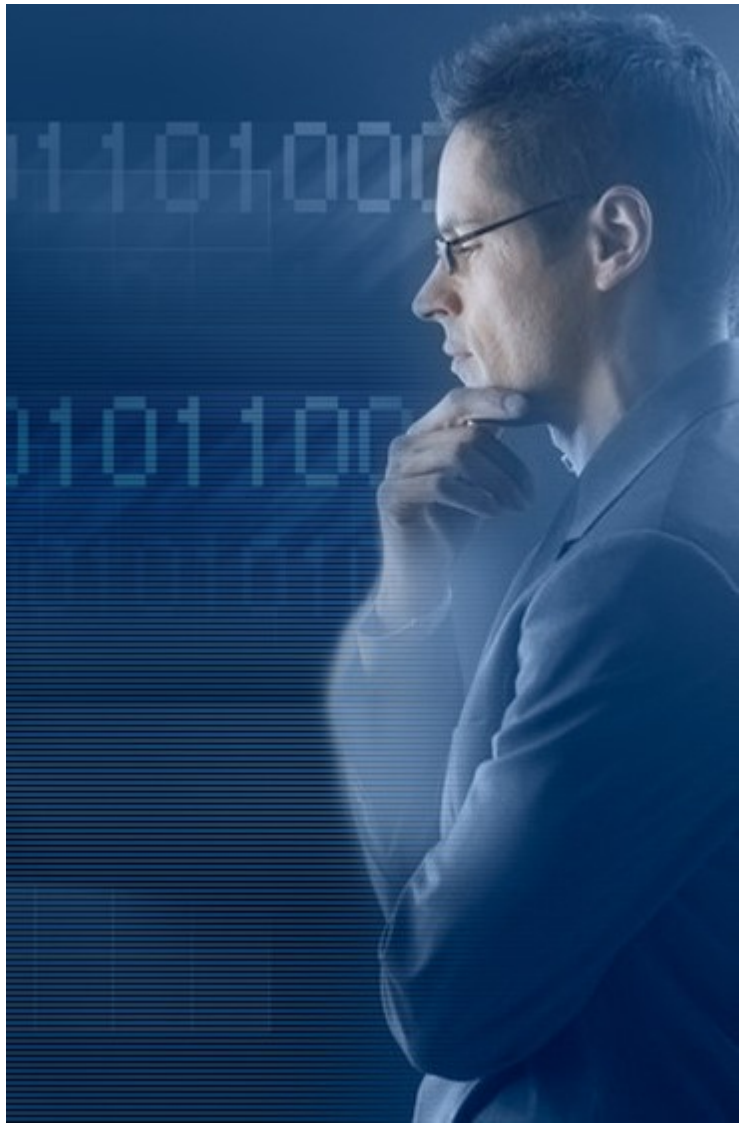
Disponibilité maximale de tous les services.

Que signifie la visibilité ?

- La visibilité est un élément fondamental de l'industrie des télécommunications.
- Vous devez savoir tout ce que font vos clients, quelles applications pilotent votre réseau, et comprendre la direction que prend votre entreprise.
-

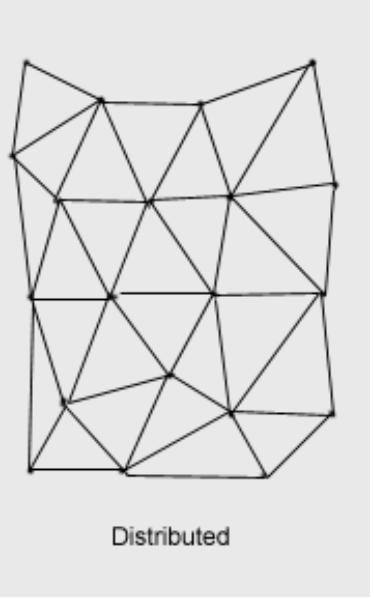


1. **Vous devez savoir exactement ce qui se passe avec vos clients et votre réseau.**
2. **Vous devez être capable de façonner, de manipuler et de servir vos clients sur la base de ces connaissances.**
3. **Vous devez faire en sorte que votre réseau reste en place au-delà de *cinq 9s.***

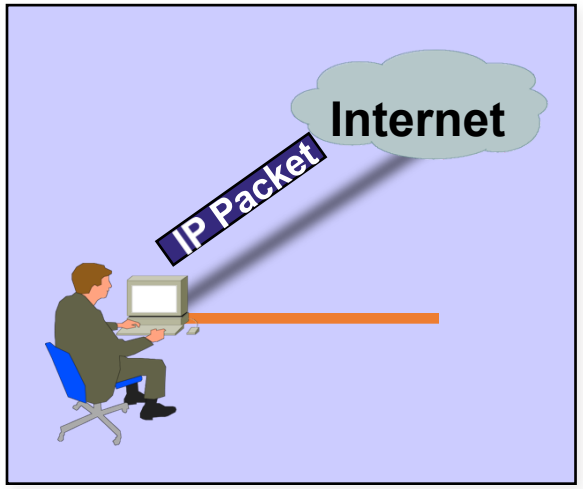


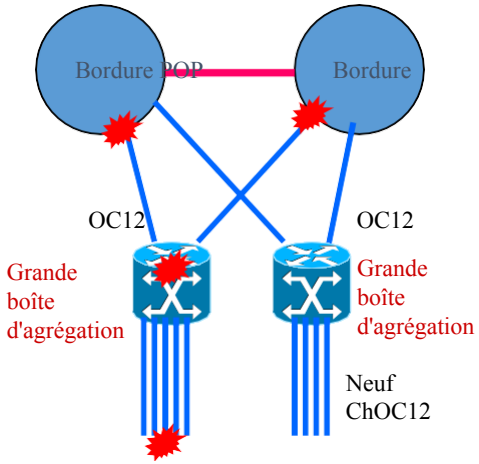
Que signifie la disponibilité ?

- Le réseau doit être opérationnel à 99,999%.
- Pour ce faire, nous utilisons le modèle de disponibilité et de résilience de Paul Baran.
- Problème : la majorité des ingénieurs IP ne connaissent pas les principes du modèle de disponibilité et de résilience de Paul Baran.



Il s'agit all du paquet ……..





Tout est dans le paquet .....

Une fois qu'un paquet arrive sur Internet, quelqu'un, quelque part, doit faire l'une des deux choses suivantes :

- ***Livrer le paquet***
- ***Déposer le paquet***

Dans le contexte des attaques DoS, les questions sont les suivantes : *qui* et *où* l'action "drop the packet" aura-t-elle lieu

La *boîte à outils de* la sécurité des opérateurs - *Tout utiliser*

BGP

La fiabilité de Five 9s

Haute disponibilité

OSPF

Netflow

OER

MPLS

FPME

ACLs

Conception du fond de panier

QOS

Conception ASIC

CoPP

GTSM

Sécurité SP

Les widgets

NAM

PIX

Trous d'évier

ISR

CRS

CSM

RTBL

Sup720

Moteur 3

Moteur 5

Communications Inter - CNO

ASWAN

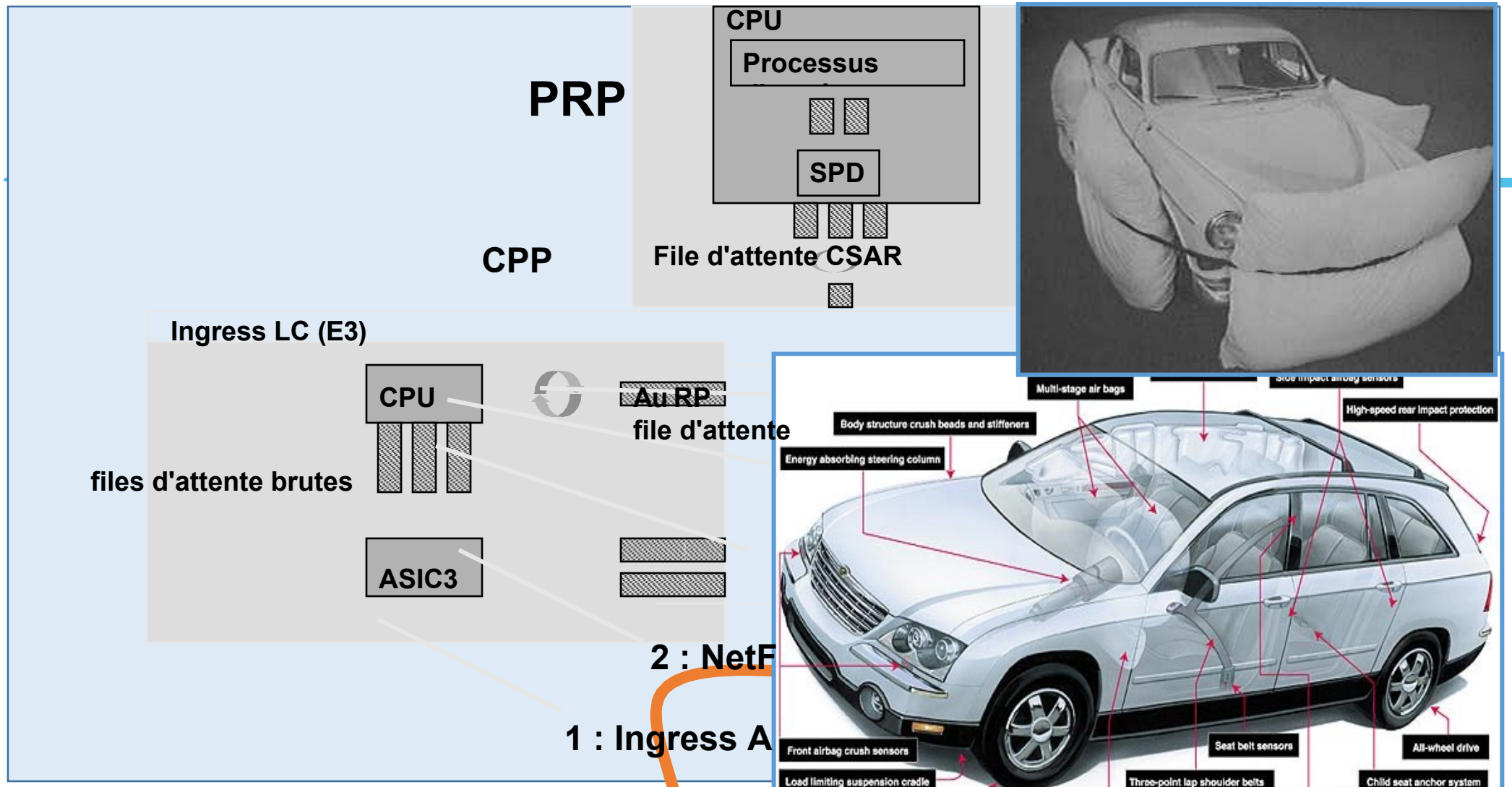
Compartimentage

Contrôle des frontières

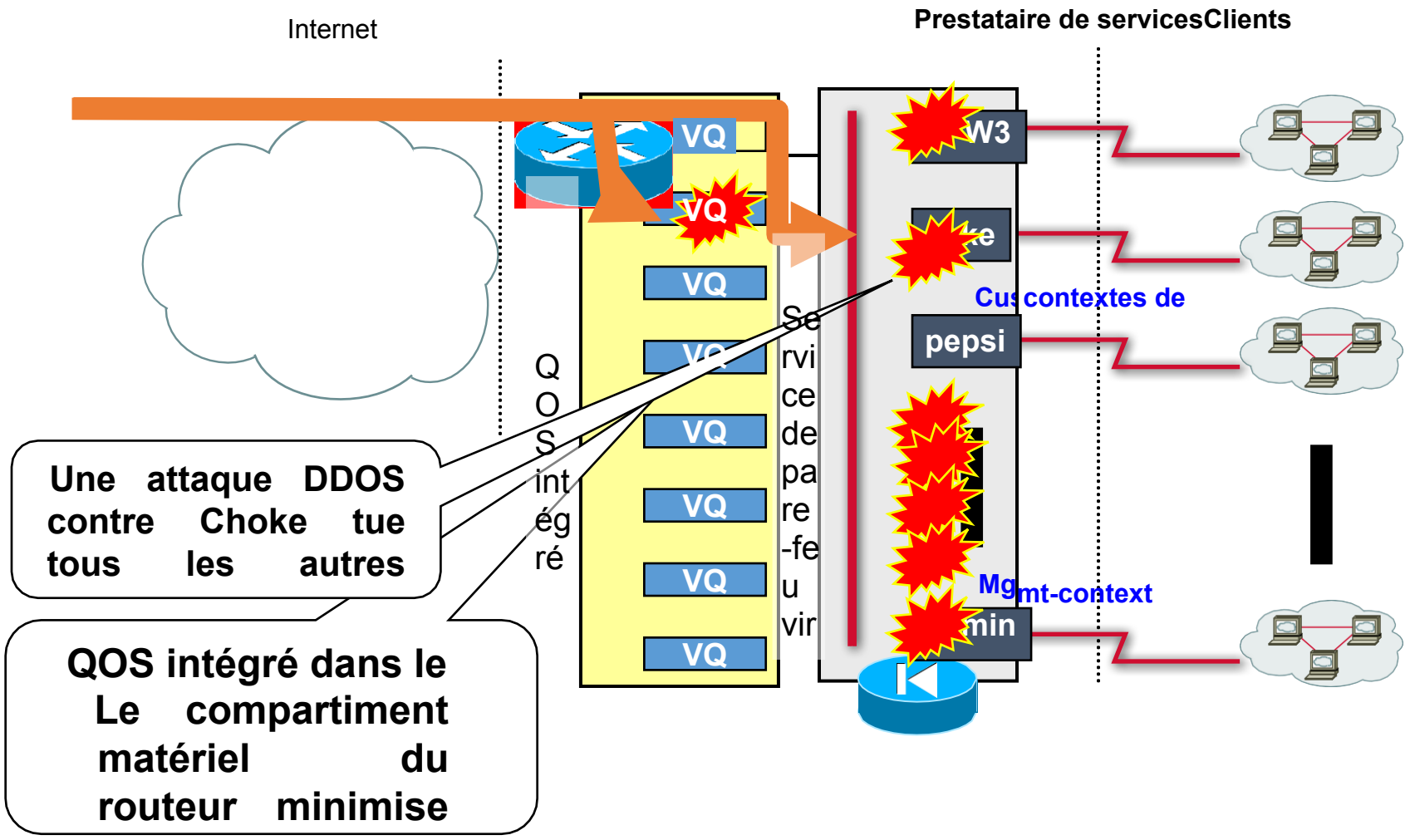
Conception modulaire

Contrôle des services/Quarantaine

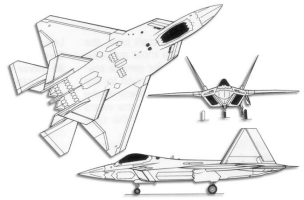
La sécurité ne peut pas être une réflexion après coup !



Un problème de matériel ?

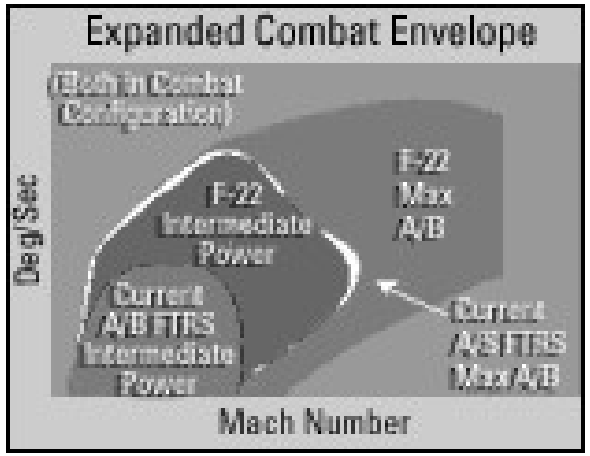


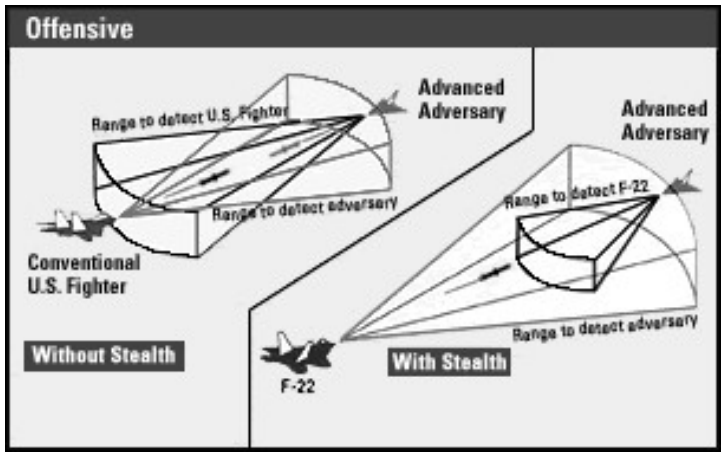
Repoussez-vous les limites ?

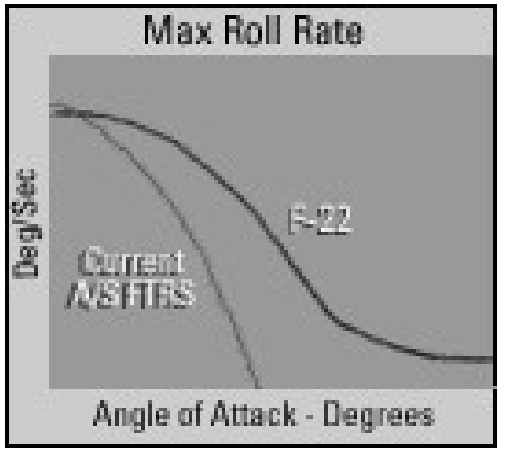


- Connaissez votre équipement et votre infrastructure :
  - Connaissez l'enveloppe de performance de tous vos équipements (routeurs, commutateurs, postes de travail, etc.). Vous devez savoir ce que votre équipement est réellement capable de faire. Si vous ne pouvez pas le faire vous-même, faites-en une exigence d'achat.
  - Connaissez les capacités de votre réseau. Si possible, testez-le. Les surprises ne sont pas agréables lors d'un incident de sécurité.

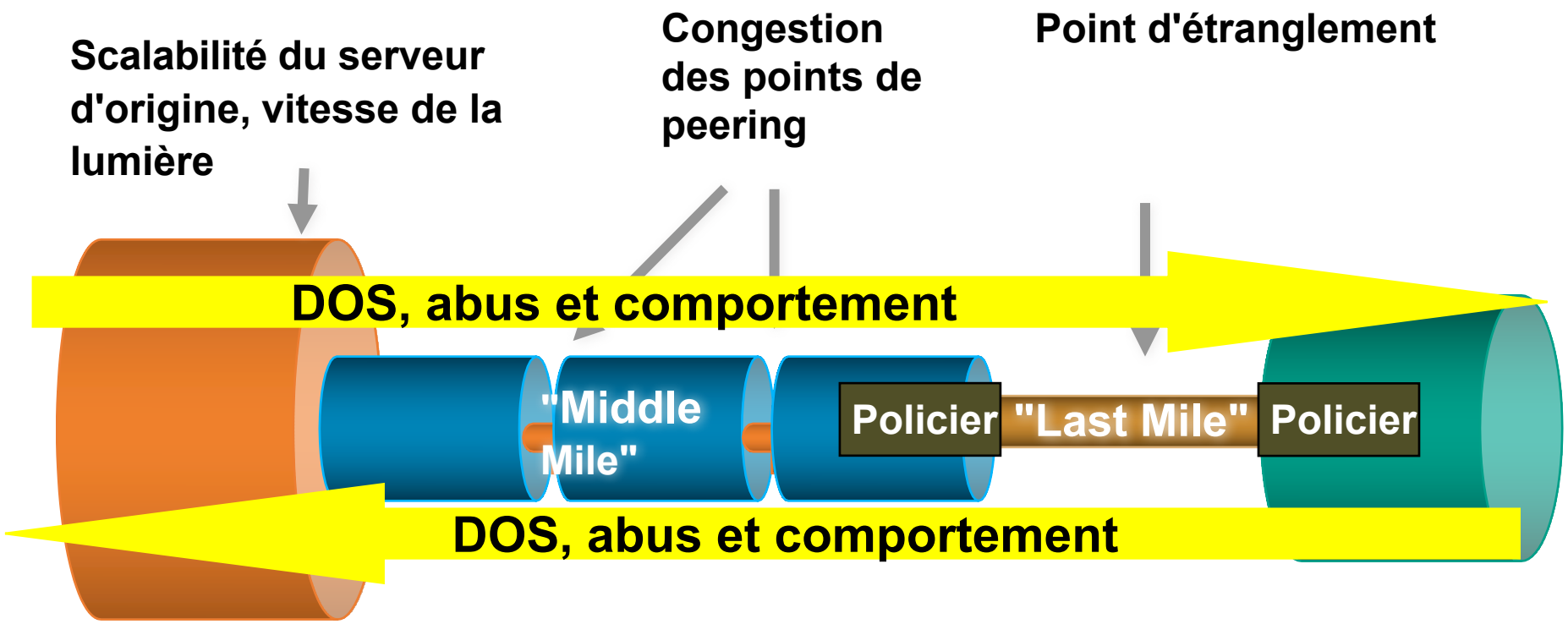
Repoussez-vous les limites ?







Points d'étranglement = Collateral

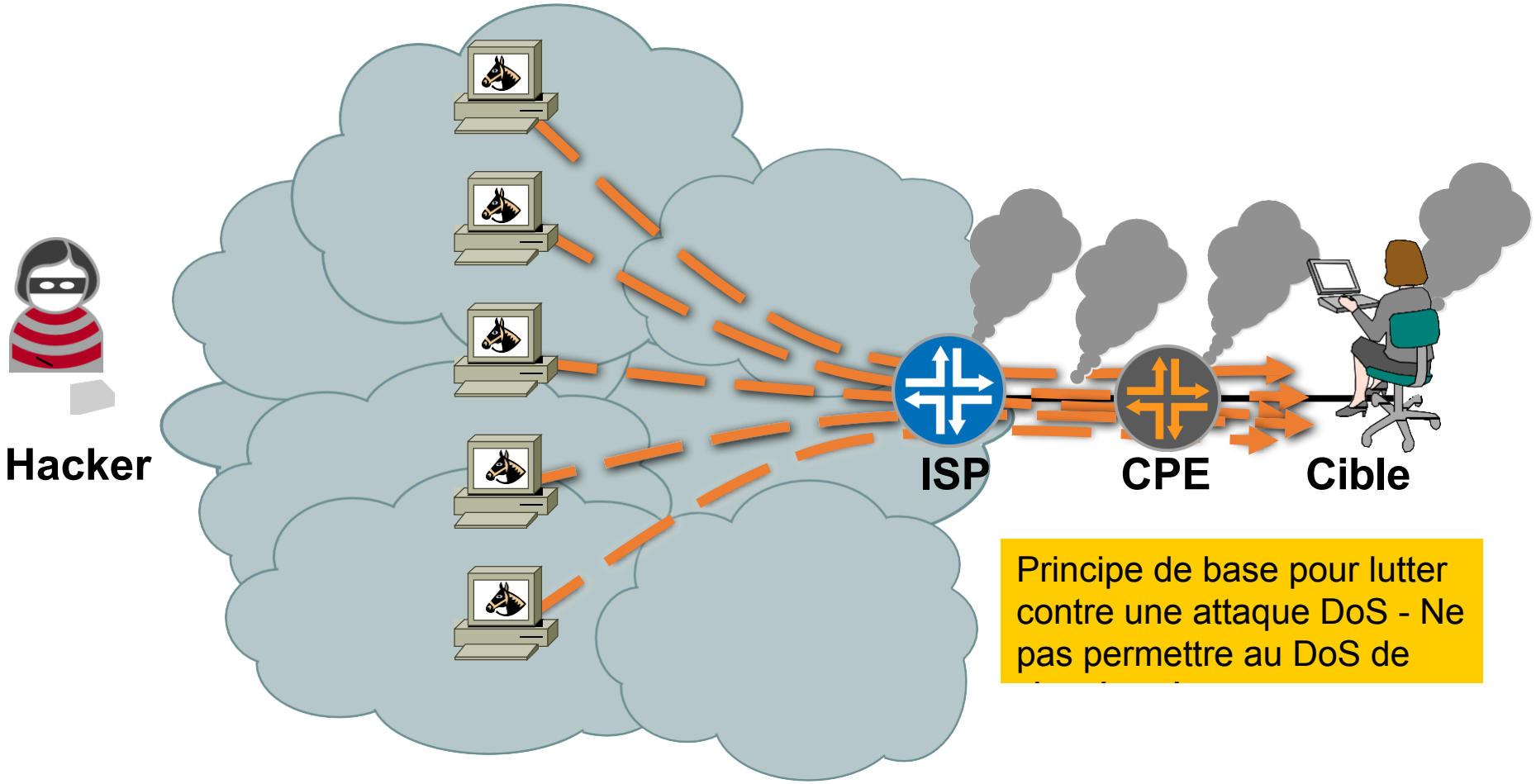


Backbone Internet Cross-Internet connexions

Boucle locale

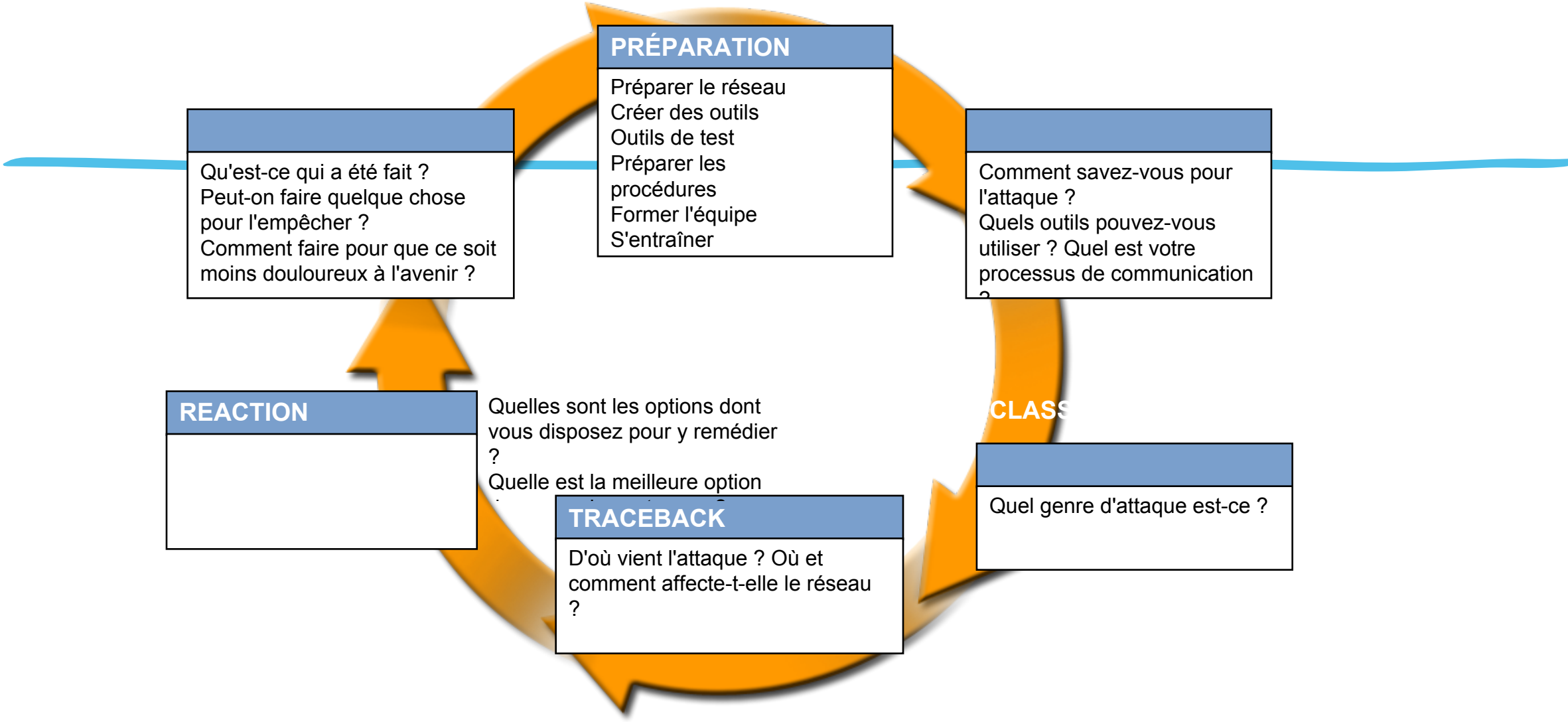
Réseau des locaux

Point d'agrégation DoS

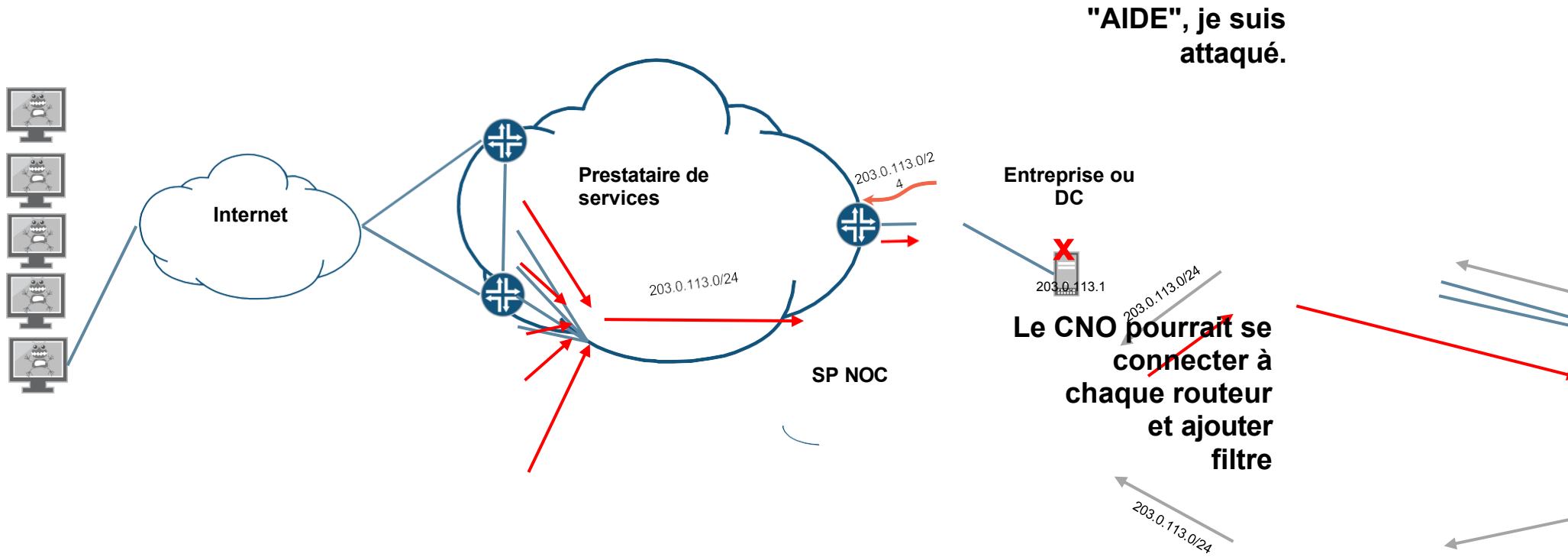


Principe de base pour lutter contre une attaque DoS - Ne pas permettre au DoS de

Les six phases de la réponse aux incidents



Bloquer les DDoS dans le "bon vieux" temps

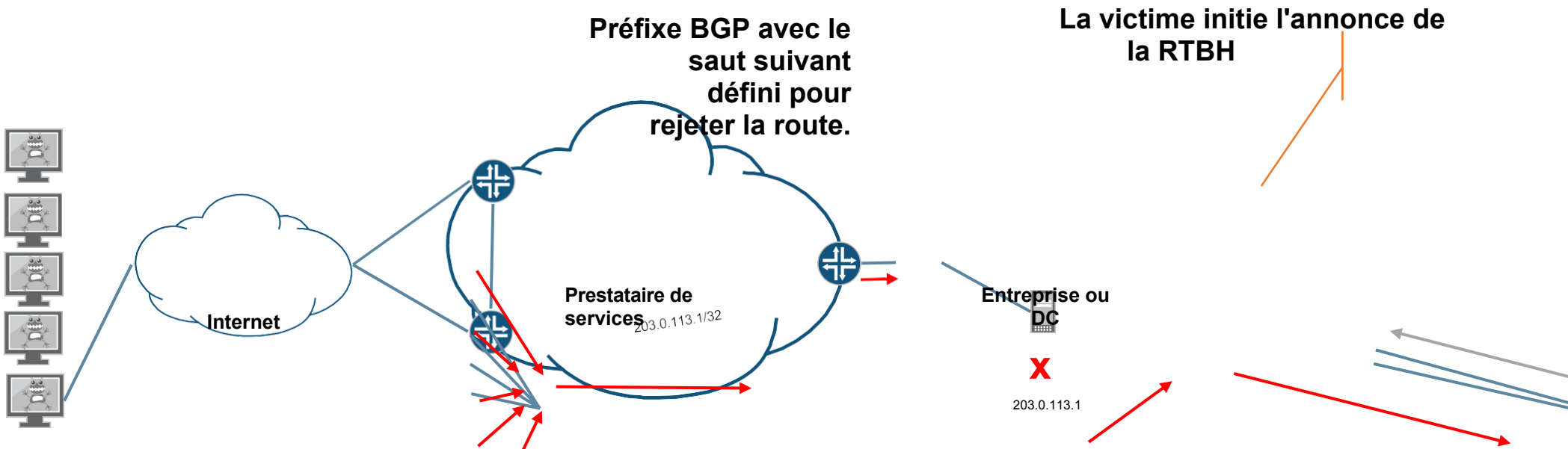


- Facilité de mise en œuvre et utilisation de concepts bien compris.
- Nécessite un degré élevé de coordination entre le client et le fournisseur.
- Il est difficile de faire évoluer le périmètre d'un grand réseau.

Bloquer les DDoS dans le "bon vieux" temps

- Mauvaise configuration possible et coûteuse

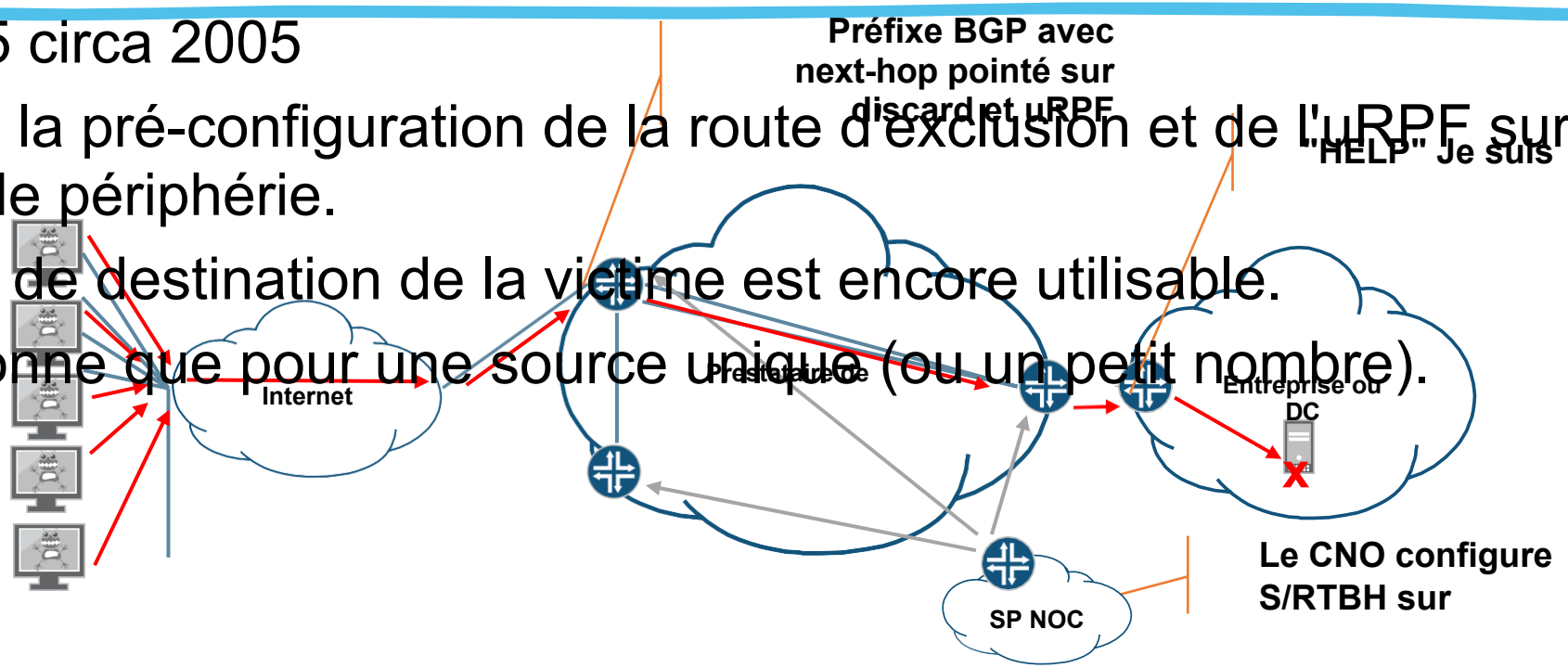
Trou noir déclenché à distance par la destination (D/RTBH)



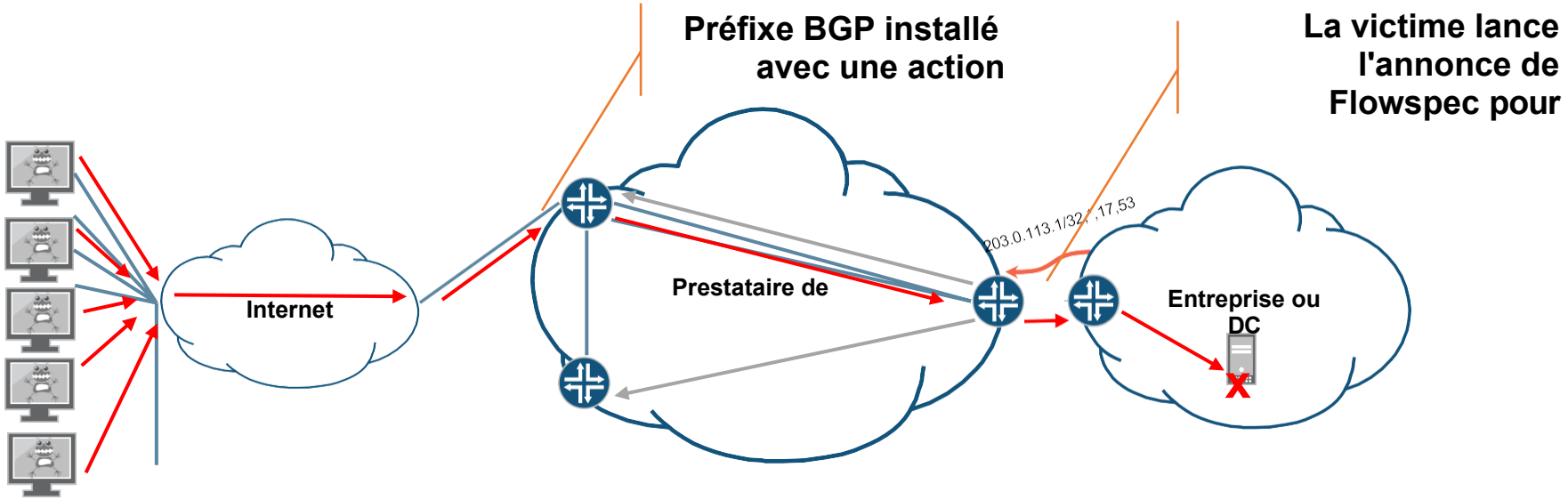
- RFC 3882 circa 2000
- Nécessite la pré-configuration de la route de rejet sur tous les routeurs de périphérie
- L'adresse de destination de la victime est totalement inaccessible mais l'attaque (et les dommages collatéraux) est arrêtée.

Trou noir déclenché à distance par la source (S/RTBH)

- RFC 5635 circa 2005
- Nécessite la pré-configuration de la route d'exclusion et de l'uRPF sur tous les routeurs de périphérie.
- L'adresse de destination de la victime est encore utilisable.
- Ne fonctionne que pour une source unique (ou un petit nombre).

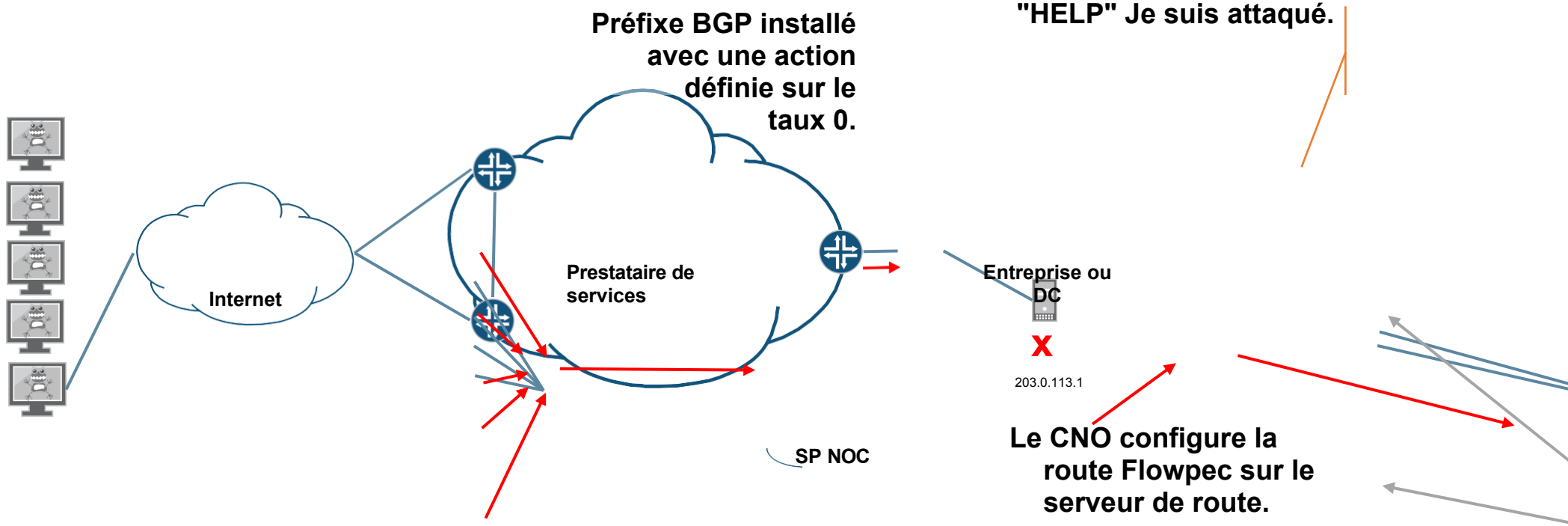


Atténuation des DDoS inter-domaines à l'aide de Flowspec



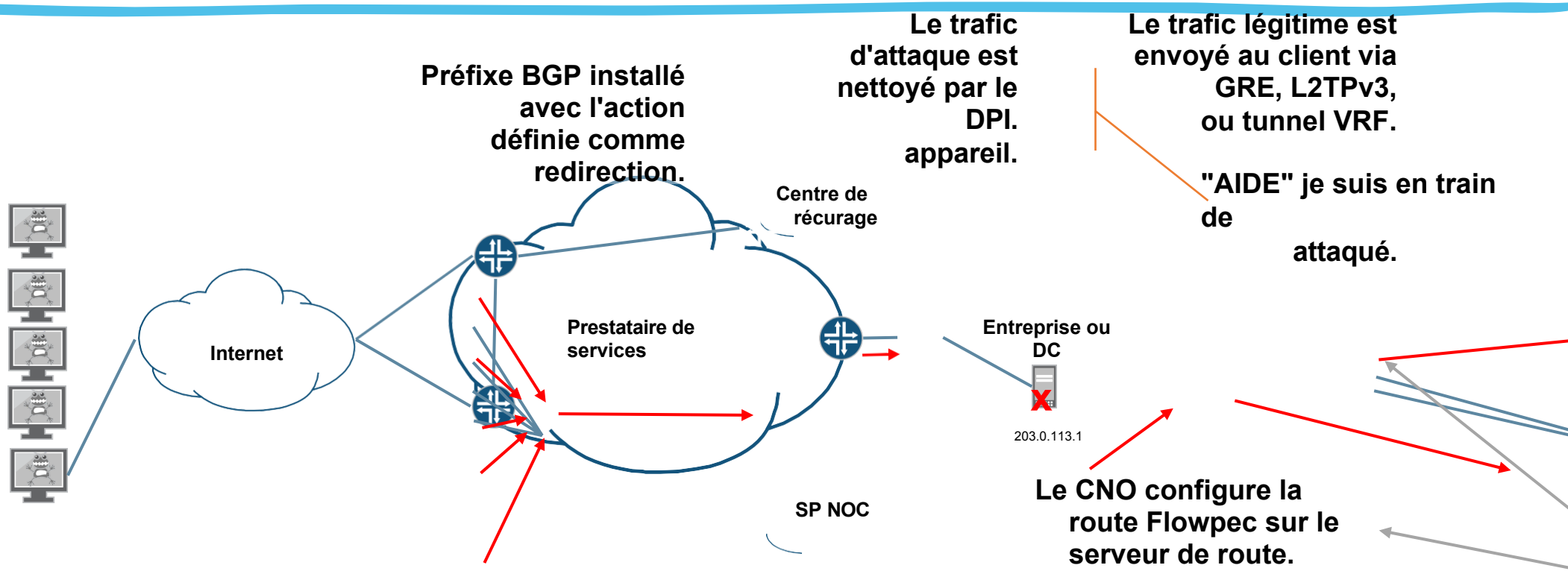
- Permet au client du FAI d'initier le filtre.
- Nécessite un filtrage sain à la périphérie du client.

Atténuation des DDoS intra-domaine à l'aide de Flowspec



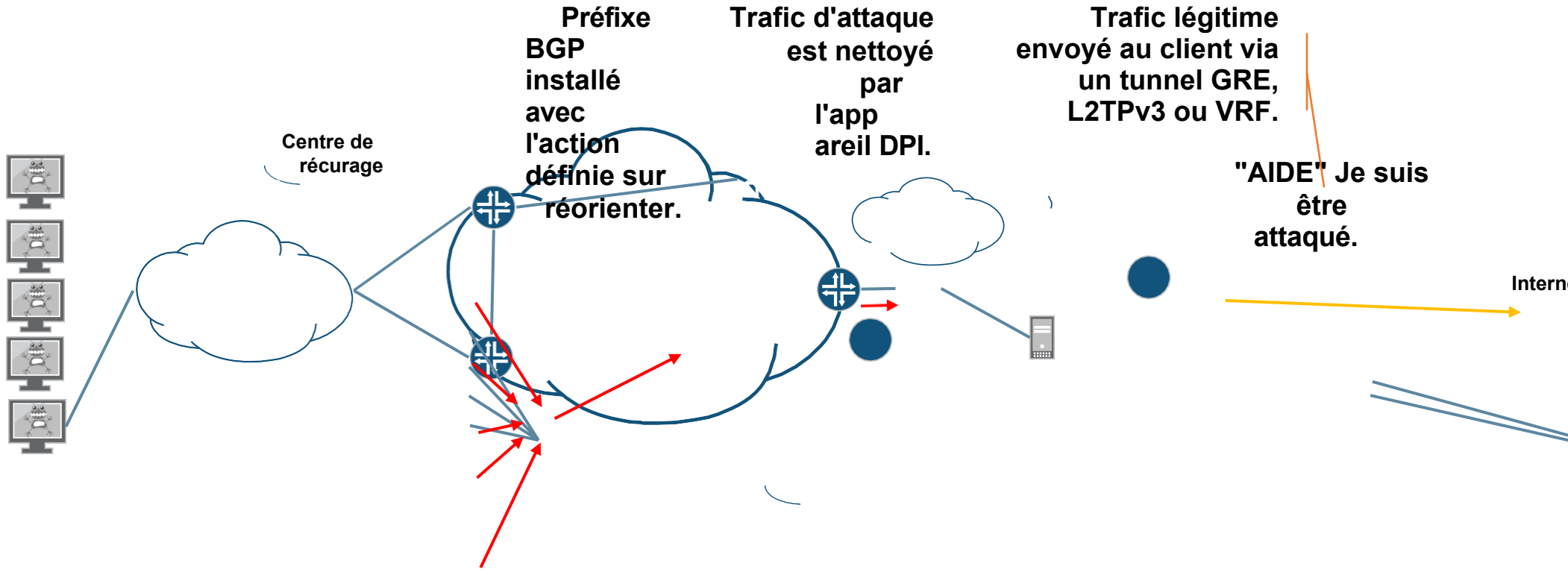
- Elle peut être initiée par un appel téléphonique, une détection dans le réseau SP, ou un portail web pour le client.
- Nécessite une coordination entre le client et le fournisseur.

Atténuation des DDoS grâce à Scrubbing Center



- Elle peut être initiée par un appel téléphonique, une détection dans le réseau SP, ou un portail web pour le client.
- Permet d'atténuer les attaques de la couche applicative sans mener à bien l'attaque.

Atténuation des DDoS grâce à Scrubbing Center



Atténuation des DDoS grâce à Scrubbing Center

Fournisseur de services en amont

Entreprise ou DC

Flowspec sur le serveur de route.

SP NOC

203.0.113.1

X

Le CNO configure la route Fl

Atténuation des DDoS grâce à Scrubbing Center

- Elle peut être initiée par un appel téléphonique, une détection dans le réseau SP, ou un portail web pour le client.
- Permet d'atténuer les attaques de la couche applicative sans mener à bien l'attaque.

DDOS aujourd'hui - Nous pouvons riposter

DDOS aujourd'hui - Surmonter l'attaque - Nettoyage sur place

DDOS aujourd'hui - Surmonter l'attaque - Hors site

DDOS aujourd'hui - Construire des services plus résilients

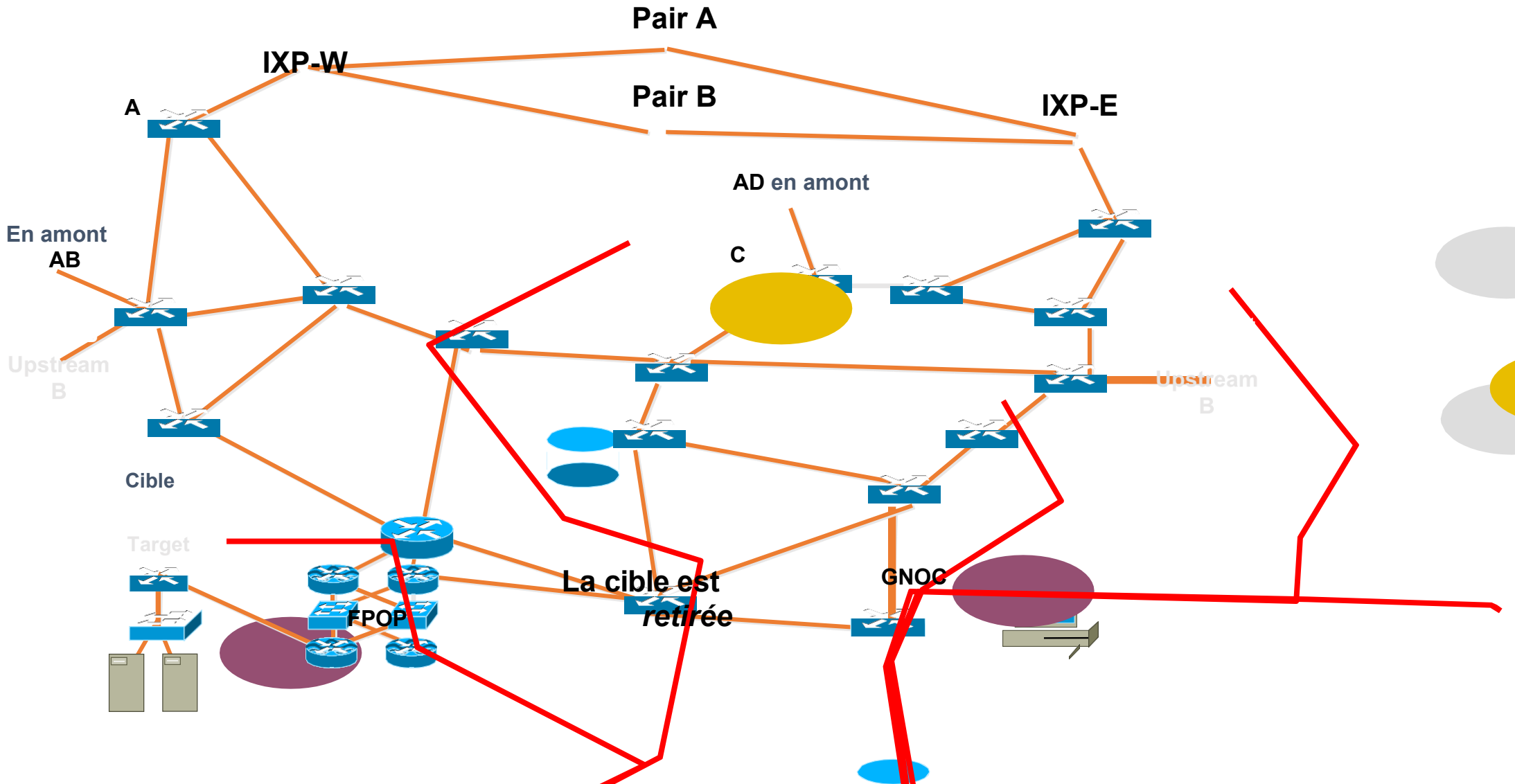
Now nous pouvons y remédier dans le cadre d'une fédération

Pause pour les questions

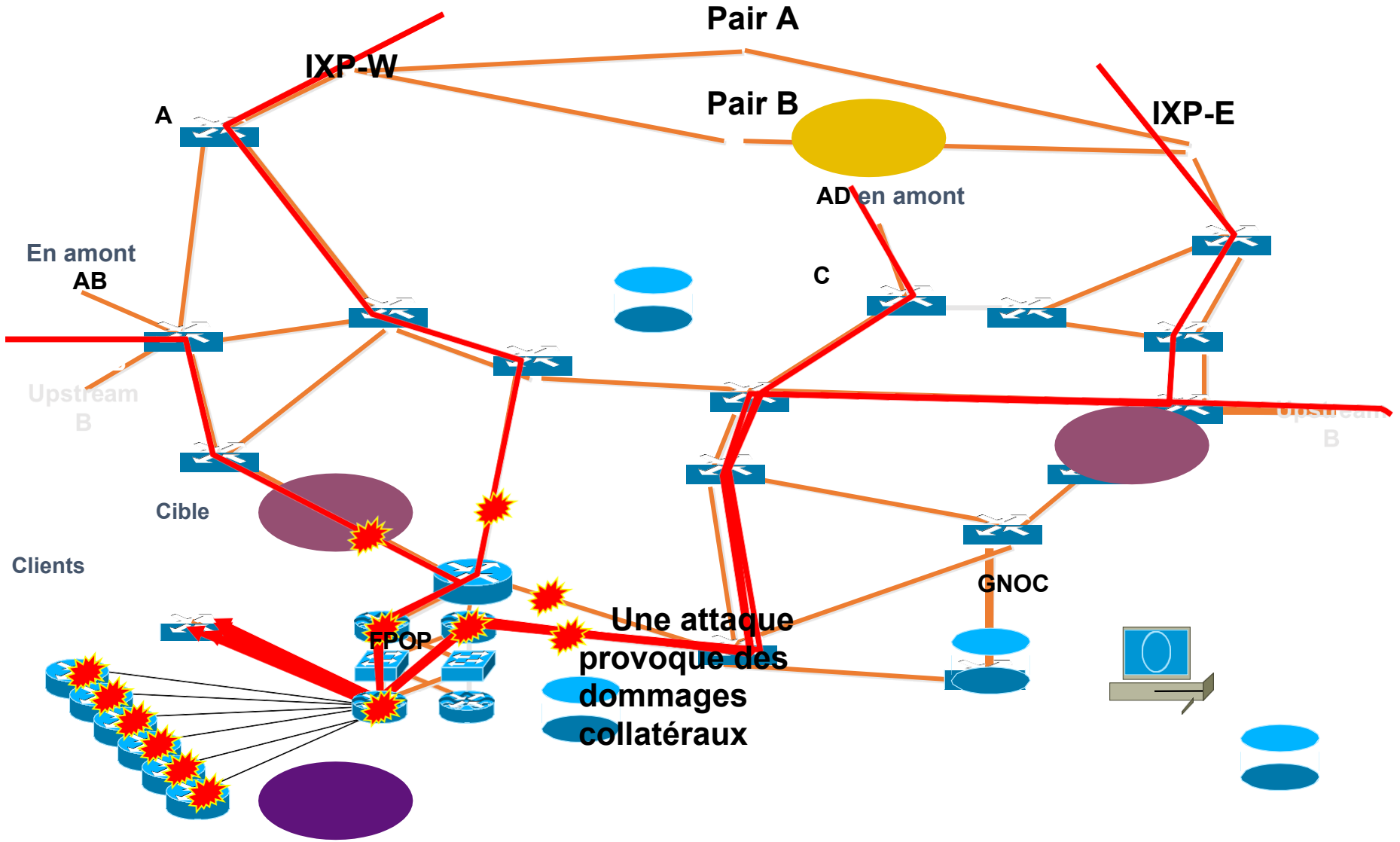
SITREP

- Tout est normal dans le réseau.
- Puis les alarmes se déclenchent - quelque chose se passe dans le réseau.

Le client est DOSé avant



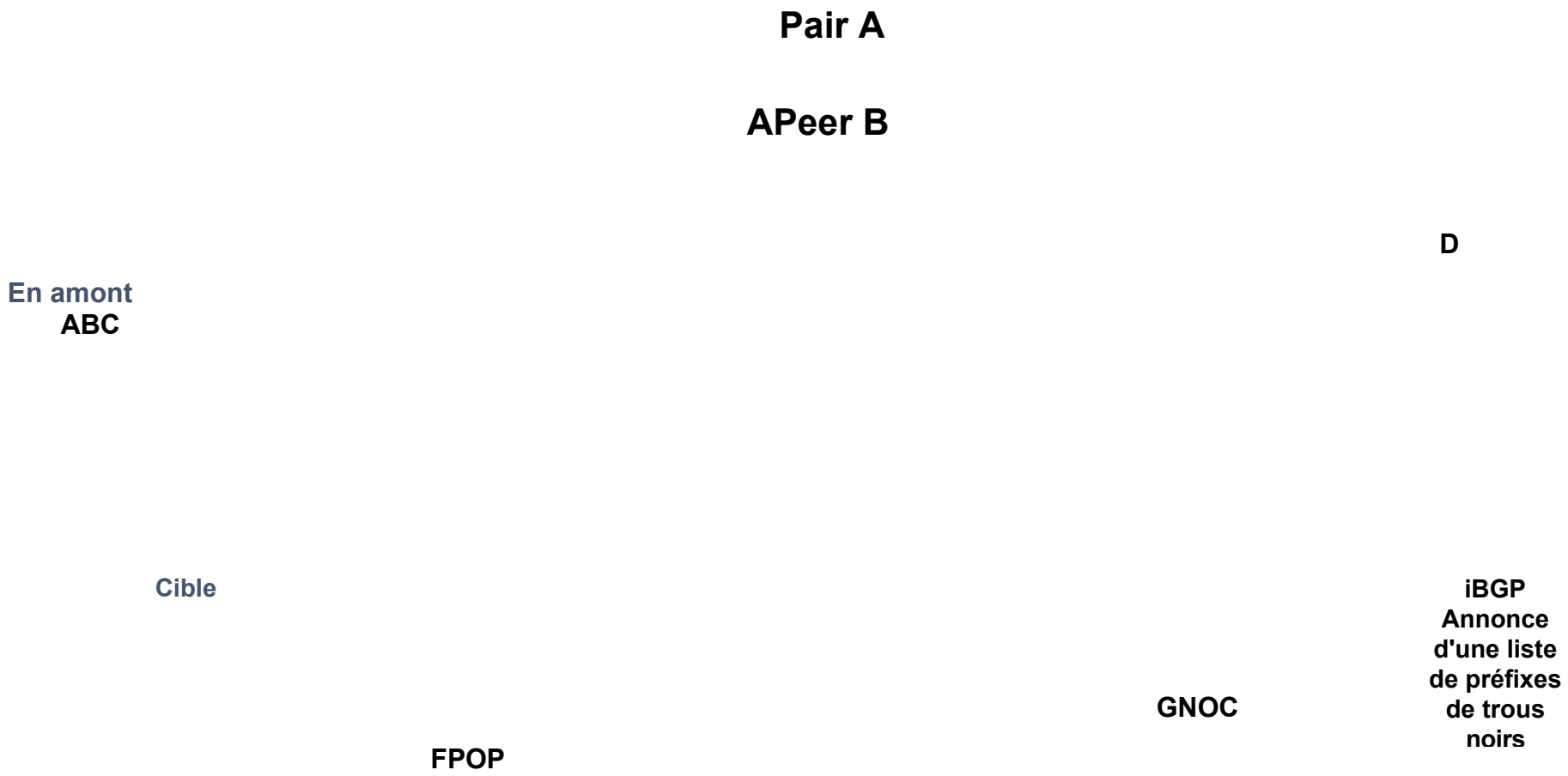
Le client est fichu avant les dommages collatéraux.



SITREP - Attaque en cours

- L'attaque contre un client a un impact sur un certain nombre de clients.
- INCIDENT DE DOMMAGE COLATÉRAL !
- Action immédiate : Résoudre les problèmes de dommages collatéraux.

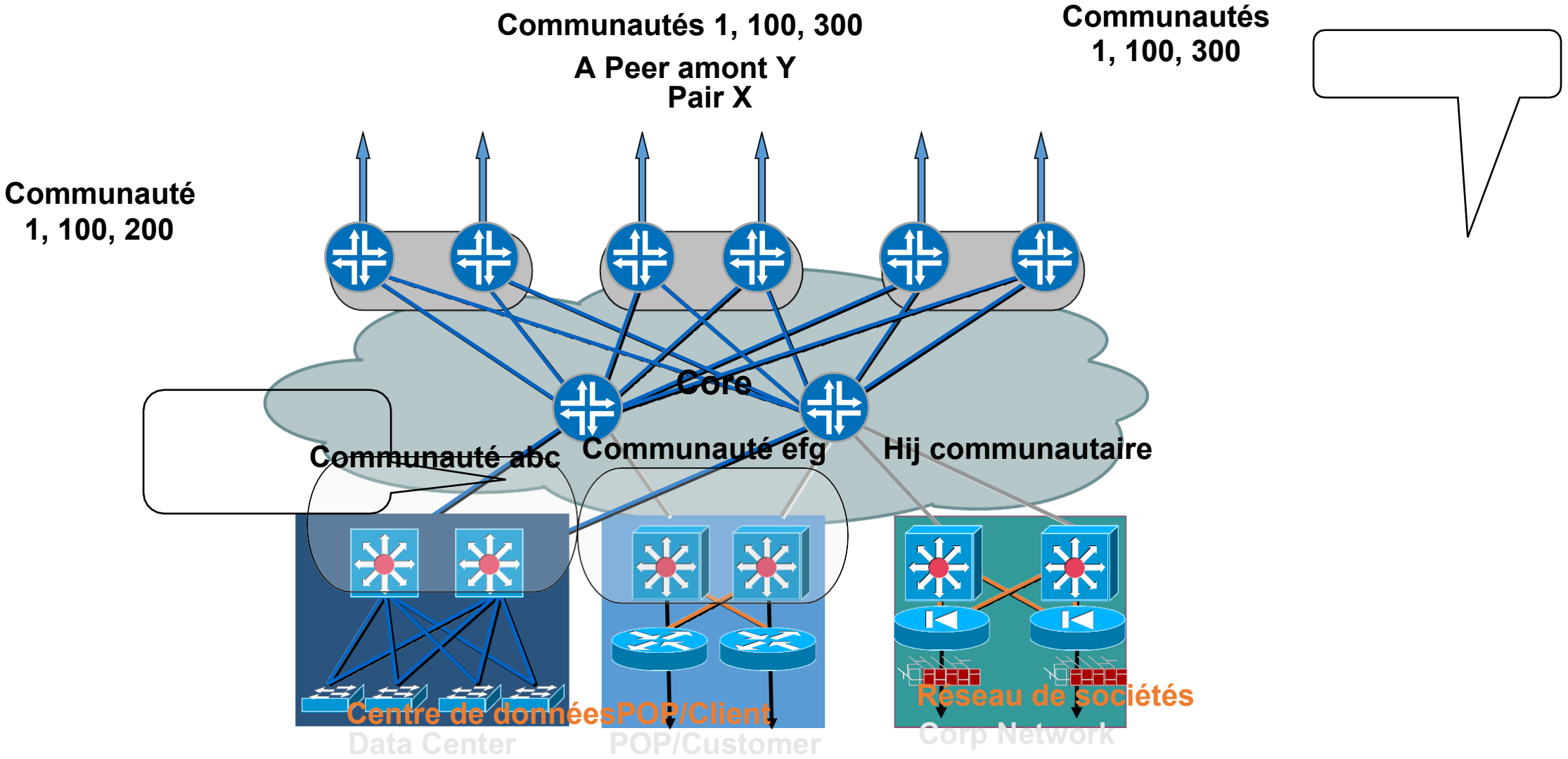
Un client est victime d'un DOS après que des chutes de paquets l'aient poussé à la limite.



SITREP - Attaque en cours

- Atténuation des dommages collatéraux
- Le client qui a été attaqué a un SERVICE PARTIEL.
- L'attaque DOS est toujours active
- Options :
  - Sink Hole une partie du trafic à analyser.
  - Surveillez l'attaque DOS et attendez la rotation de l'attaque ou son arrêt.
  - Activez "Clean Pipes" pour une restauration complète.

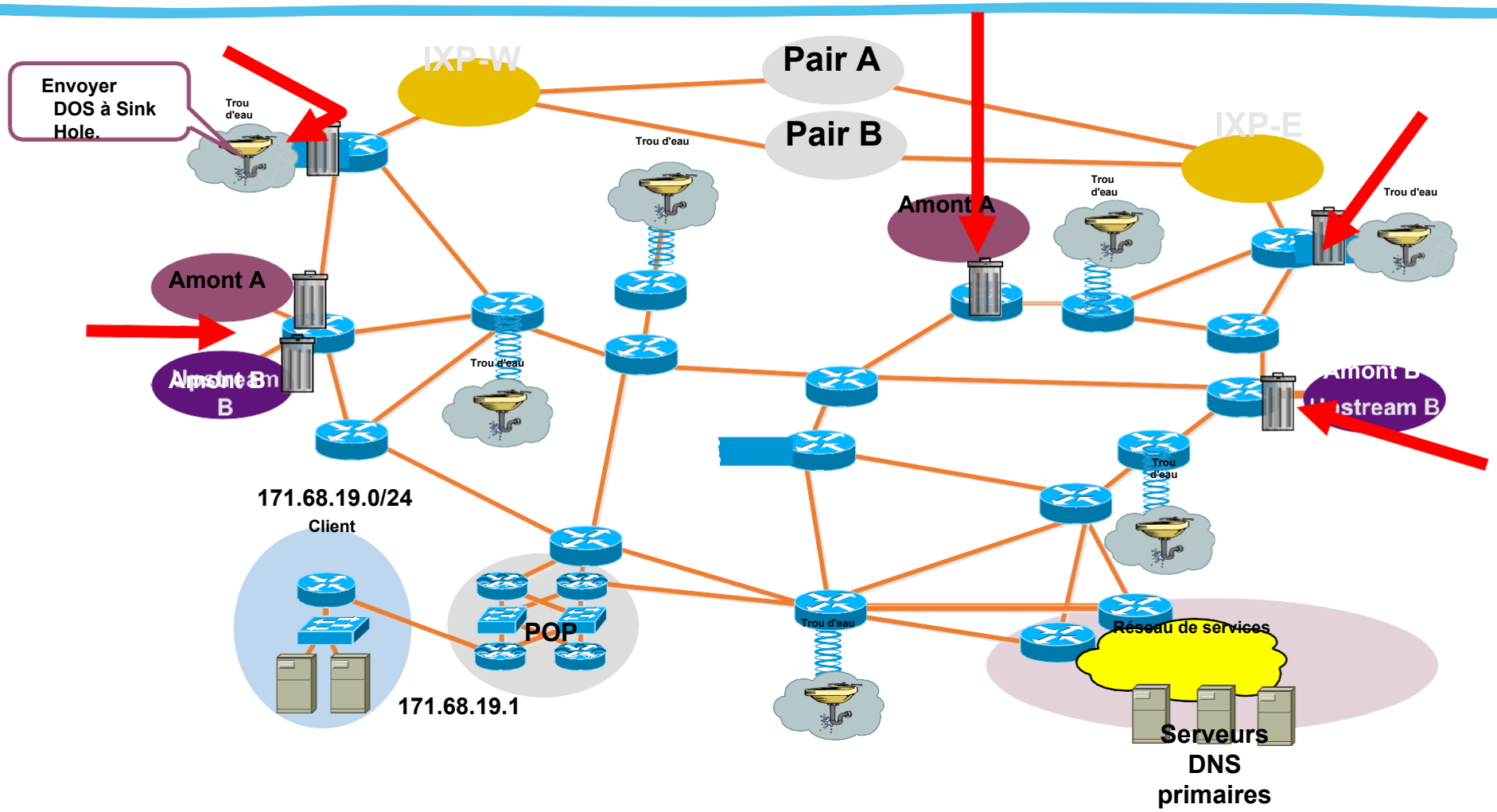
Drops déclenchés à distance et



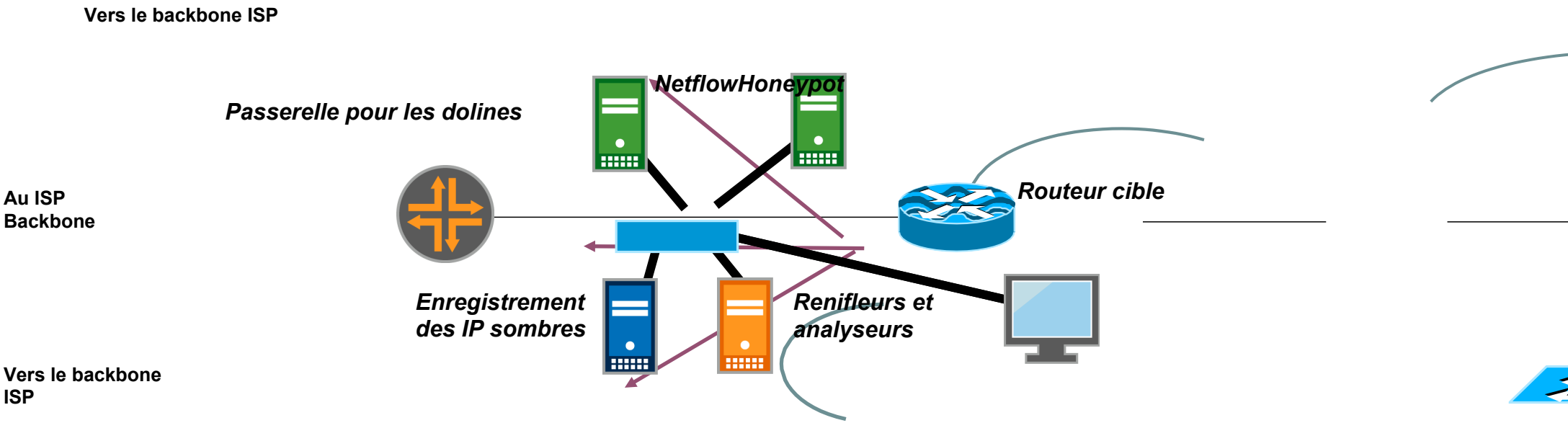
SITREP - Attaque en cours

- Atténuation des dommages collatéraux
- Le client qui a été attaqué a un SERVICE PARTIEL.
- L'attaque DOS est toujours active
- Action : Surveiller l'attaque et obtenir plus de détails sur l'attaque.
  - Utiliser le déclenchement basé sur la communauté BGP pour envoyer un flux de régions dans un Sink Hole.

Déclenchement de la communauté



Analyser l'attaque



- Utilisez les outils disponibles sur Internet et auprès des fournisseurs pour analyser les détails de l'attaque.
- Vous obtiendrez ainsi des informations sur ce que vous pouvez ou ne pouvez pas faire ensuite.

SITREP - Attaque en cours

- Atténuation des dommages collatéraux
- Le client qui a été attaqué a un SERVICE PARTIEL.
- L'attaque DOS est toujours active
- Action : Fournir au client qui est la victime une RÉCUPÉRATION DE SERVICE COMPLÈTE de Clean Pipes (hors détails spécifiques au fournisseur).

Qu'est-ce que la reprise de

- "Clean Pipes" est un terme utilisé pour décrire la *reprise complète du service*. Les attentes pour un rétablissement complet du service sont les suivantes :
  - L'attaque DDOS est en cours et TOUS les services clients fonctionnent normalement, conformément à l'accord de niveau de service contractuel.
  - Le dispositif utilisé pour le rétablissement complet du service n'est pas vulnérable au DDOS et l'infrastructure n'est pas vulnérable aux dommages collatéraux.
- Les produits de récupération et de nettoyage des canalisations à service complet sont très spécialisés. Adressez-vous au fournisseur approprié.

Full par rapport au

- La récupération partielle du service est facile ... repousser l'attaque vers l'ASN Edge.

- Le recouvrement intégral des services exige une planification ciblée autour des services clés.

Pause pour les questions

Quelle est la prochaine étape ?

- Téléchargez les livres blancs, les blogs et le matériel d'atelier sur www.senki.org.

- Connectez-vous ! Barry est en contact avec ses pairs, ses collègues et les talents en herbe via Linkedin (www.linkedin.com/in/barryrgreene/). Vous pouvez également suivre Barry sur Twitter (@BarryRGreene) ou ses blogs sur Senki (www.senki.org).