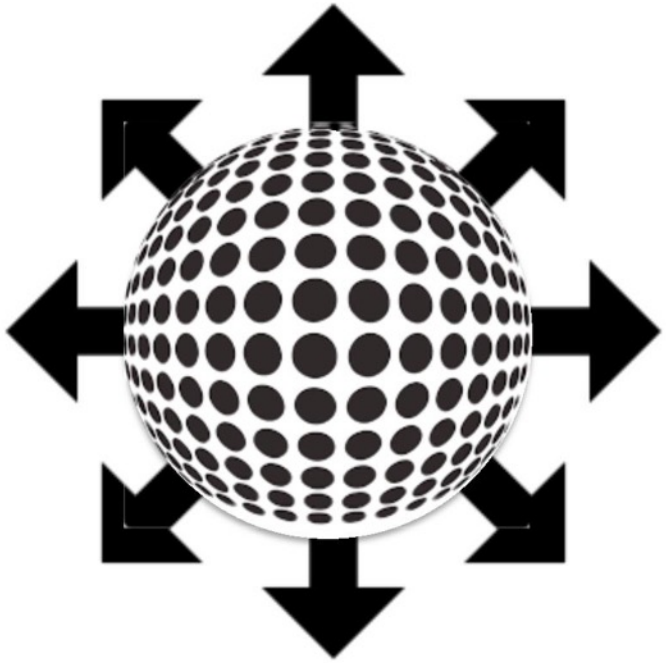


94th IETF
YOKOHAMA JAPAN
1-6 NOVEMBER 2015

Menace ouverte DDoS

Signalisation (DOTS)

Groupe de travail

draft-ietf-dots-use-cases-00

Roland Dobbins - Arbor Networks

Stefan Fouant - Corero Network Security

Daniel Migault - Ericsson

Robert Moskowitz - HTT Consulng

Nik Teague - Verisign

Liang "Frank" Xia - Huawei

Introduction et contexte

draft-ietf-dots-use-cases-00 Résumé

- Fournit des exemples de cas d'utilisation du DOTS (en fait, des catégories).

- Tous les exemples peuvent être CE/PE ou PE/PE.

- La possibilité d'une grande variation au sein de chaque catégorie (voir 4.1.1).

- Toutes les communications du DOTS dans chaque exemple peuvent être directement entre les serveurs DOTS et les clients DOTS, ou par l'intermédiaire de les relais du DOTS.

- Les relais DOTS peuvent transmettre des messages entre les clients DOTS et les serveurs en utilisant soit le transport sans état, soit le transport avec état, ou une combinaison des deux.

- Les relais DOTS peuvent regrouper les demandes de service, les statuts les messages et les réponses.

- Les relais DOTS peuvent filtrer les demandes de service, les messages d'état et les messages d'erreur.

réponses

94th IETF
YOKOHAMA JAPAN
1-6 NOVEMBER 2015

draft-ietf-dots-use-cases-00 Résumé (suite)

- Les cas d'utilisation en -00 ne sont pas exhaustifs, ils sont illustratifs.

- Les cas d'utilisation en -00 se concentrent sur l'atténuation des DDoS à l'aide de systèmes dédiés. Dispositifs d'atténuation. S/RTBH, flowspec, OpenFlow, etc. peuvent également être utilisé pour exploiter l'infrastructure du réseau pour les DDoS l'atténuation.

- 4.1.1 Le cas d'utilisation de cette présentation illustre un DOTS complet cycle de communication, variantes.

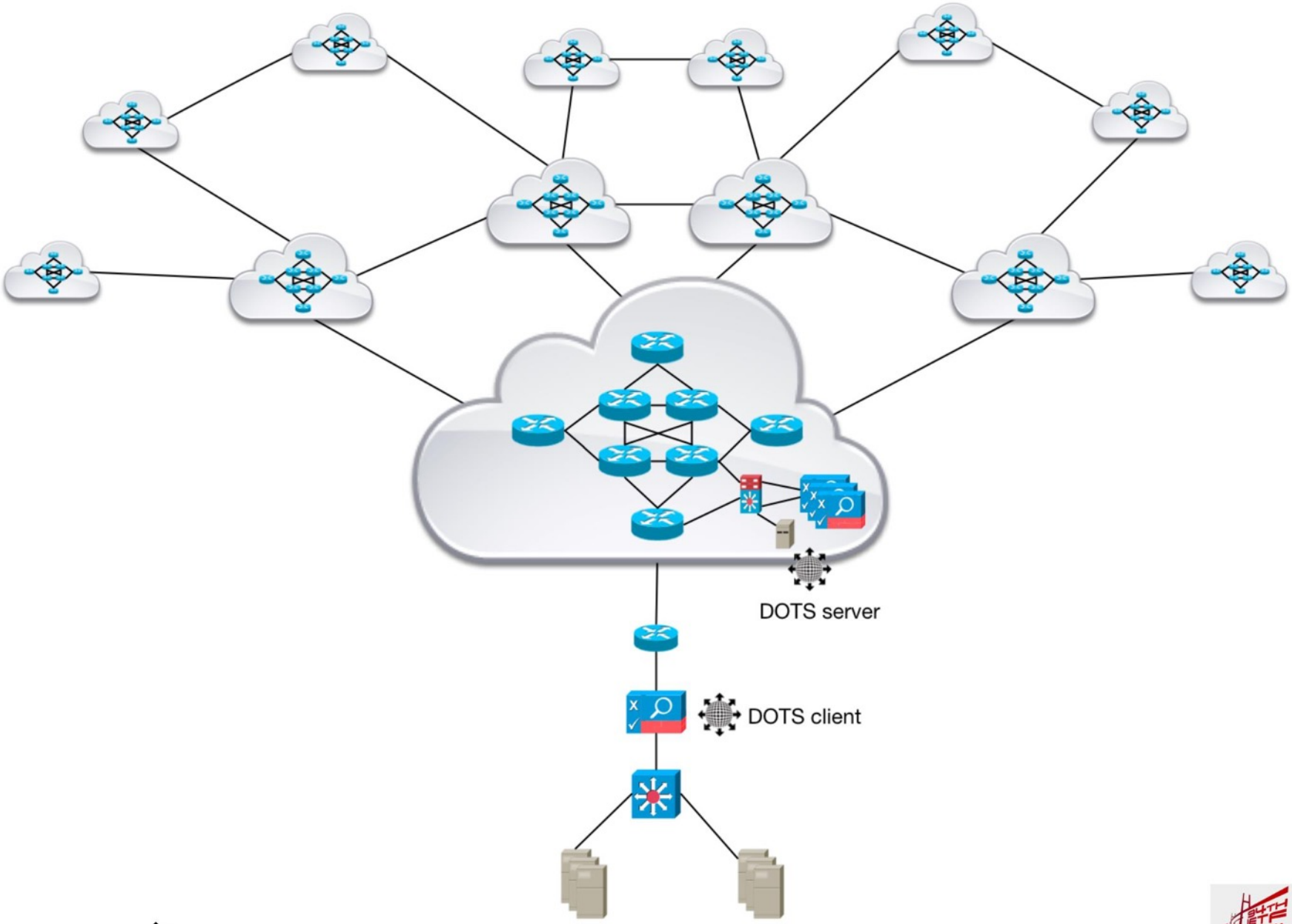
- D'autres cas d'utilisation dans cette présentation sont résumés dans les "diffs" illustrant le modèle de communication DOTS dans des contextes très différents circonstances.

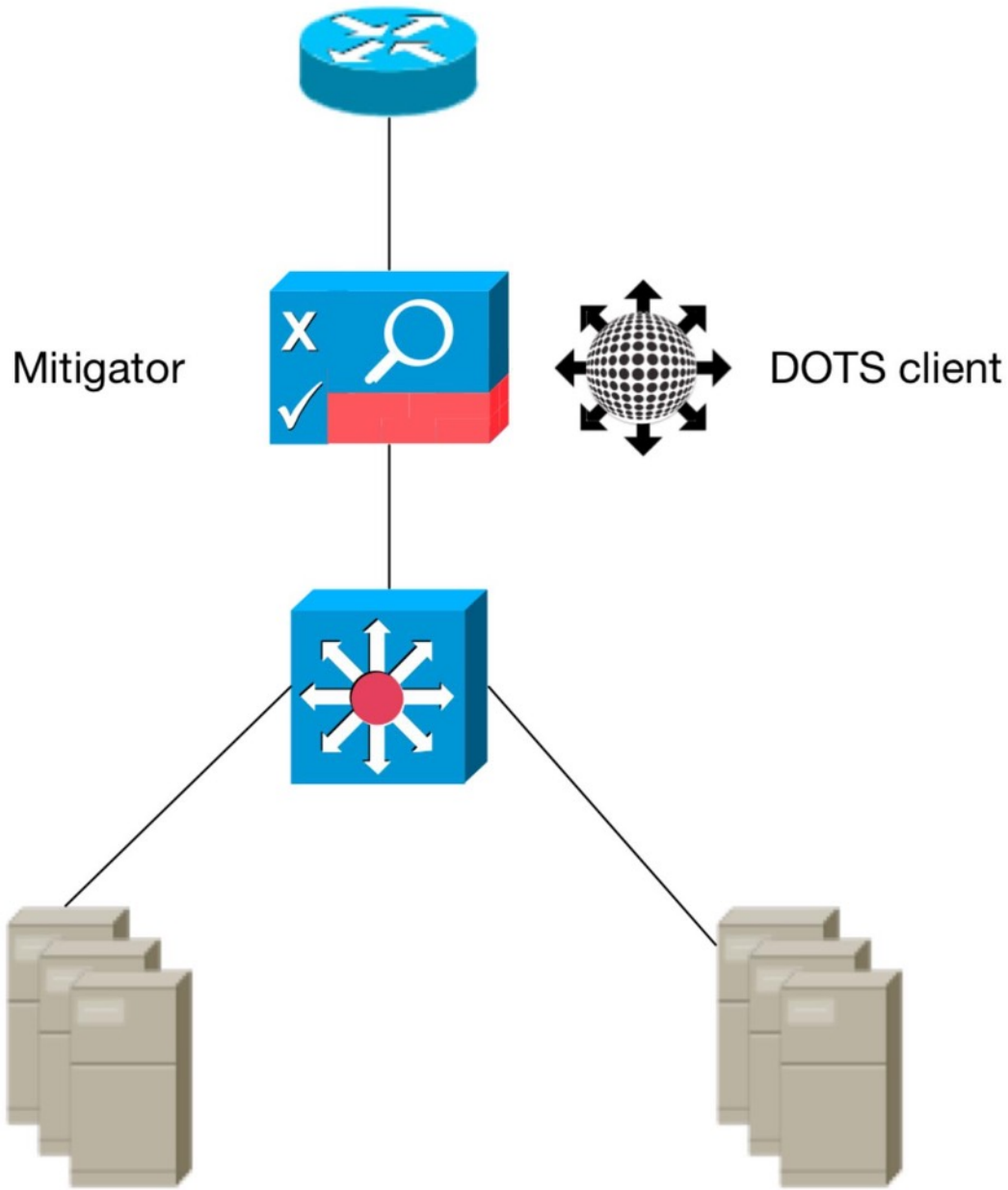
- Les cas d'utilisation de cette présentation portent sur la protection des serveurs sous attaque DDoS sur les réseaux de destination. DOTS peut également être utilisé pour supprimer le trafic d'attaque sur les réseaux d'origine ou comme il traverse des réseaux intermédiaires.

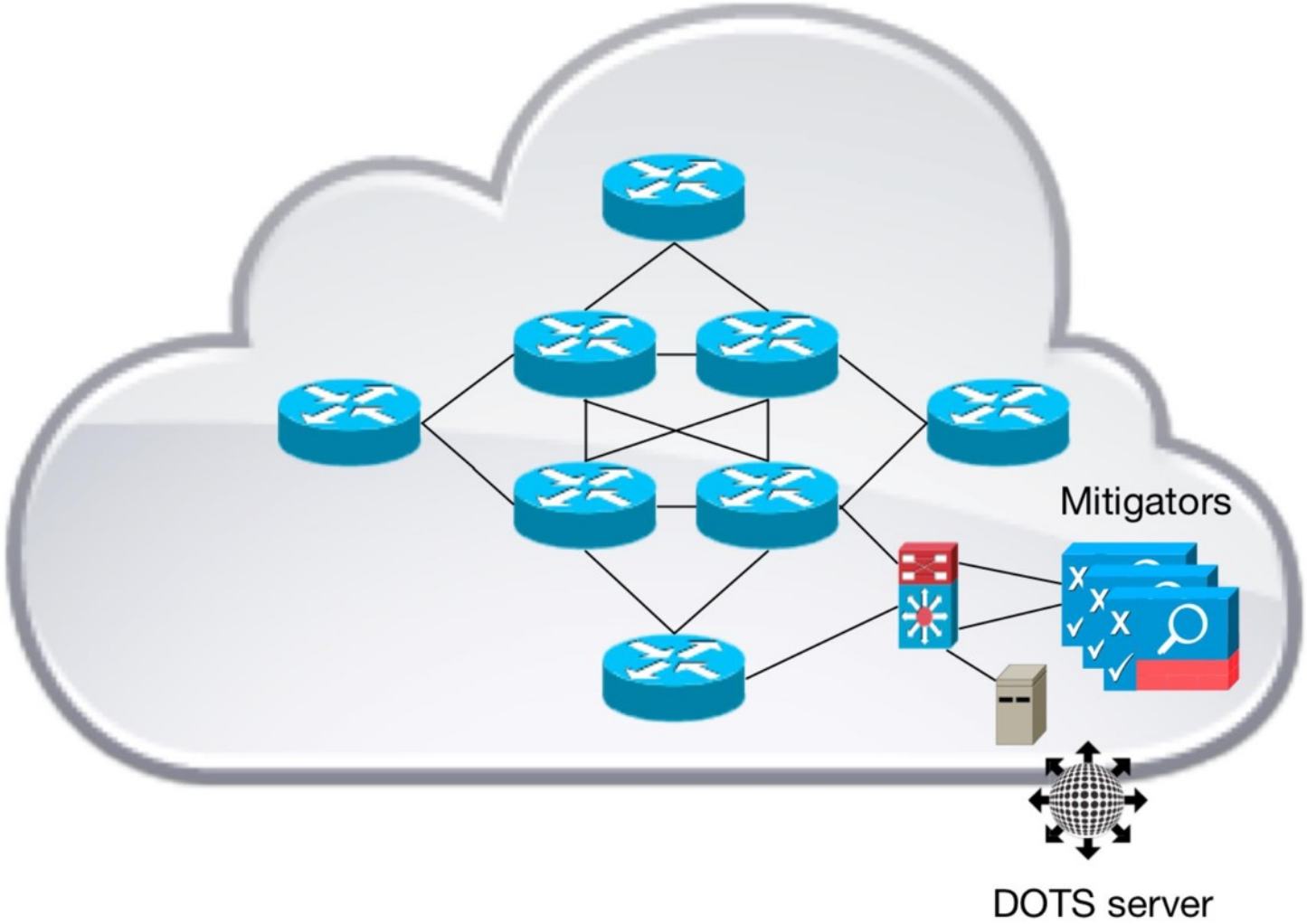
4.1 - Principaux cas d'utilisation

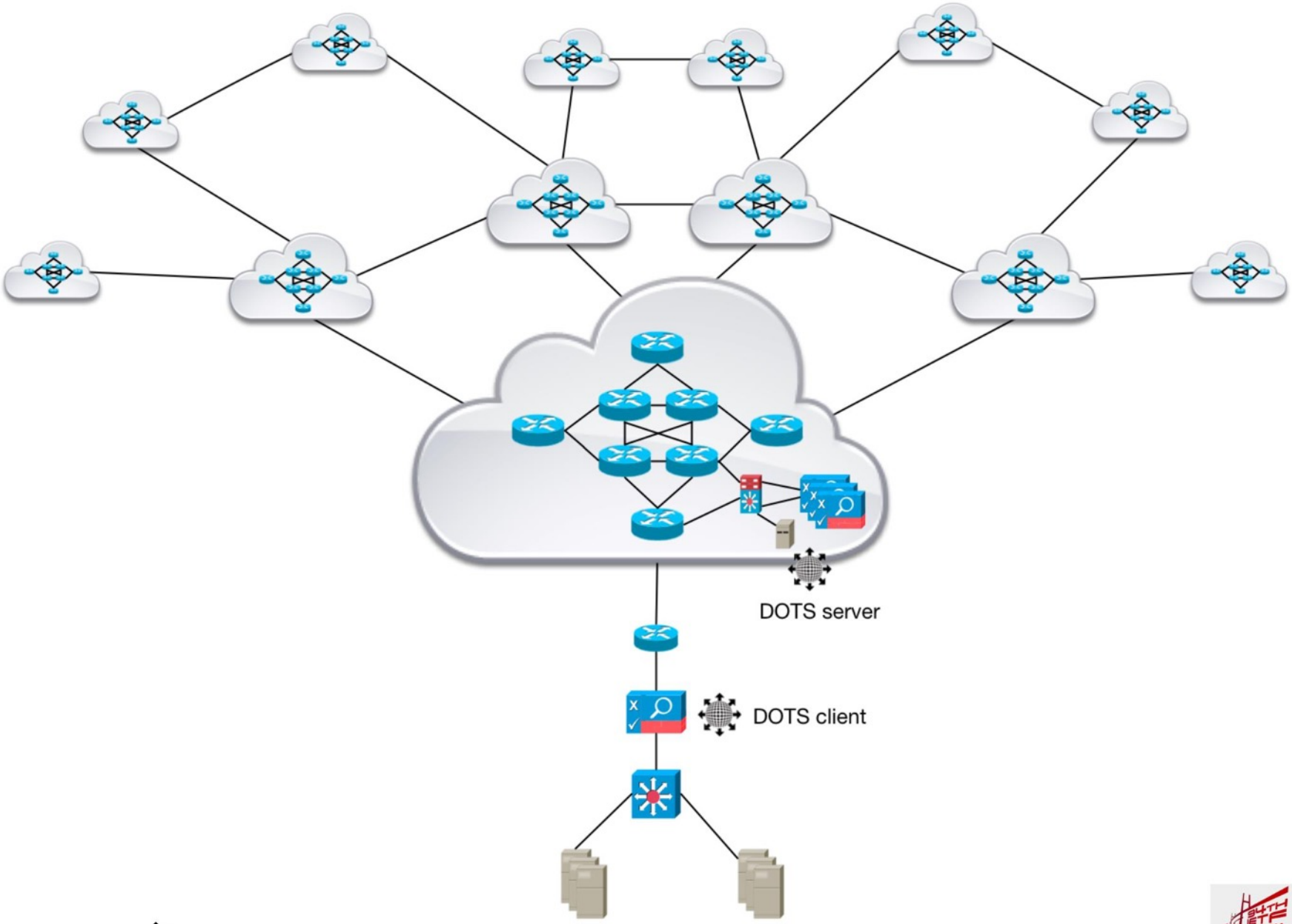
4.1.1 - Demande de CPE ou PE Mitigateurs

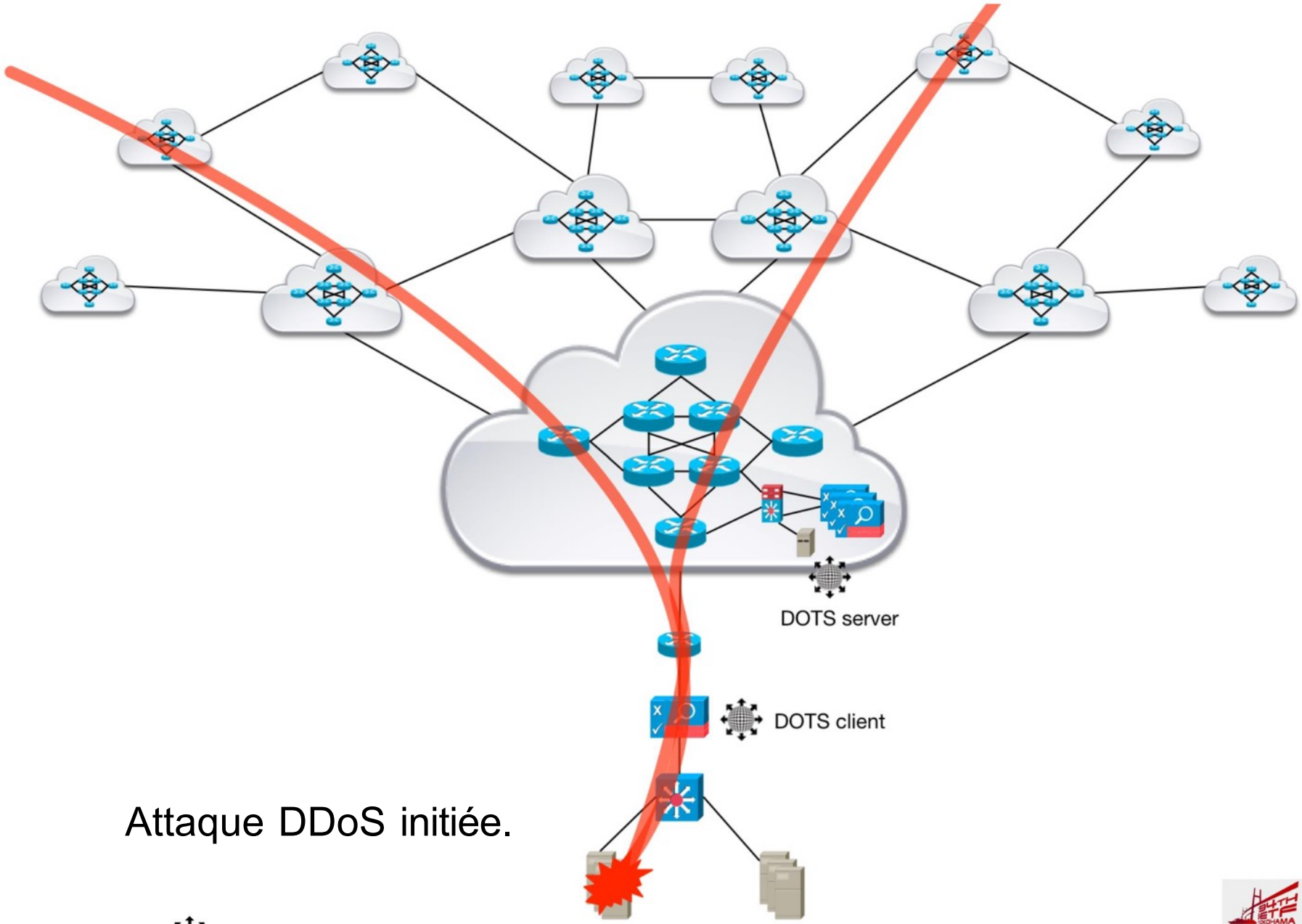
Atténuation des DDoS en amont


DOTS server
DOTS client

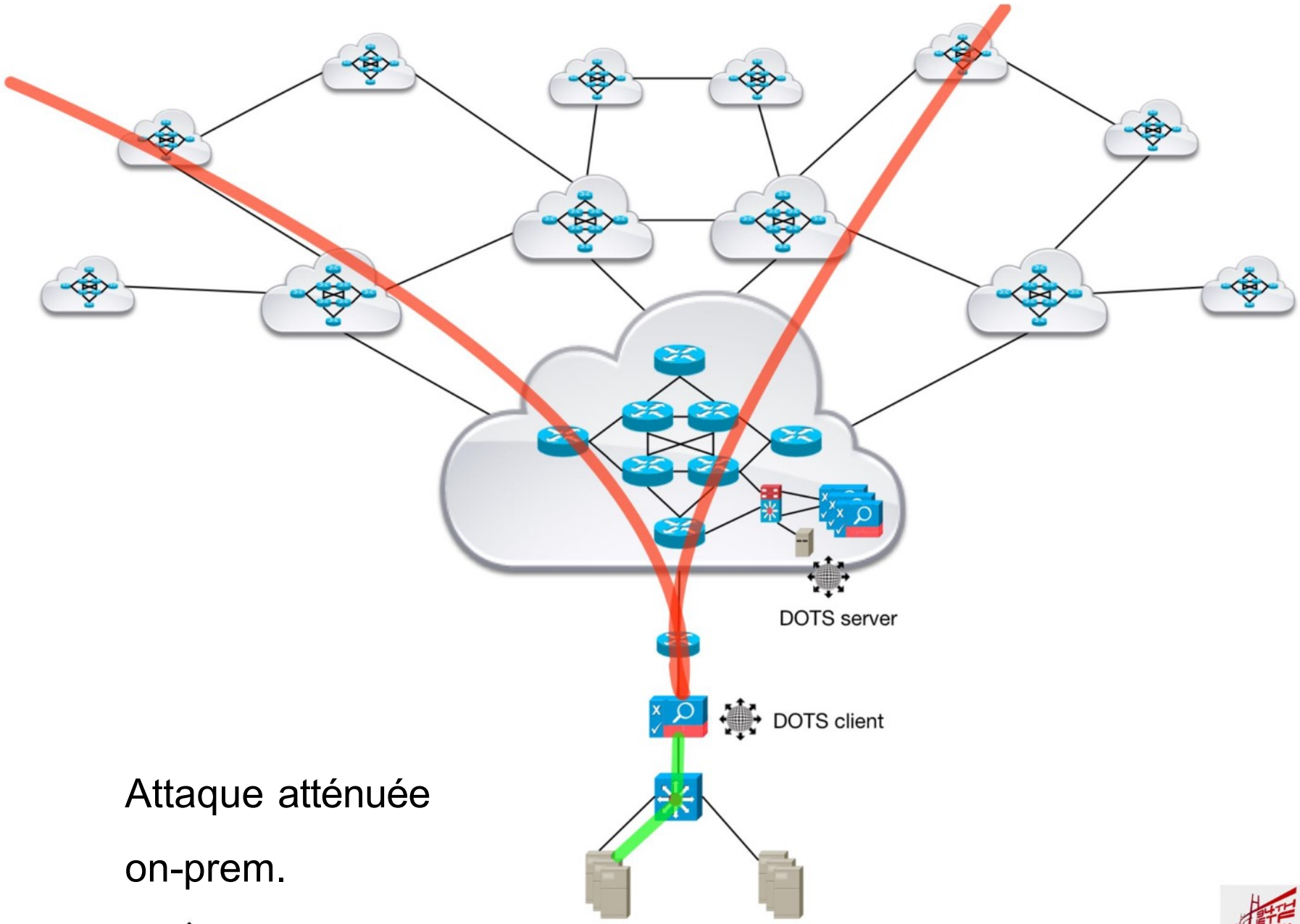

Mitigator
DOTS client


Mitigators
DOTS server


DOTS server
DOTS client

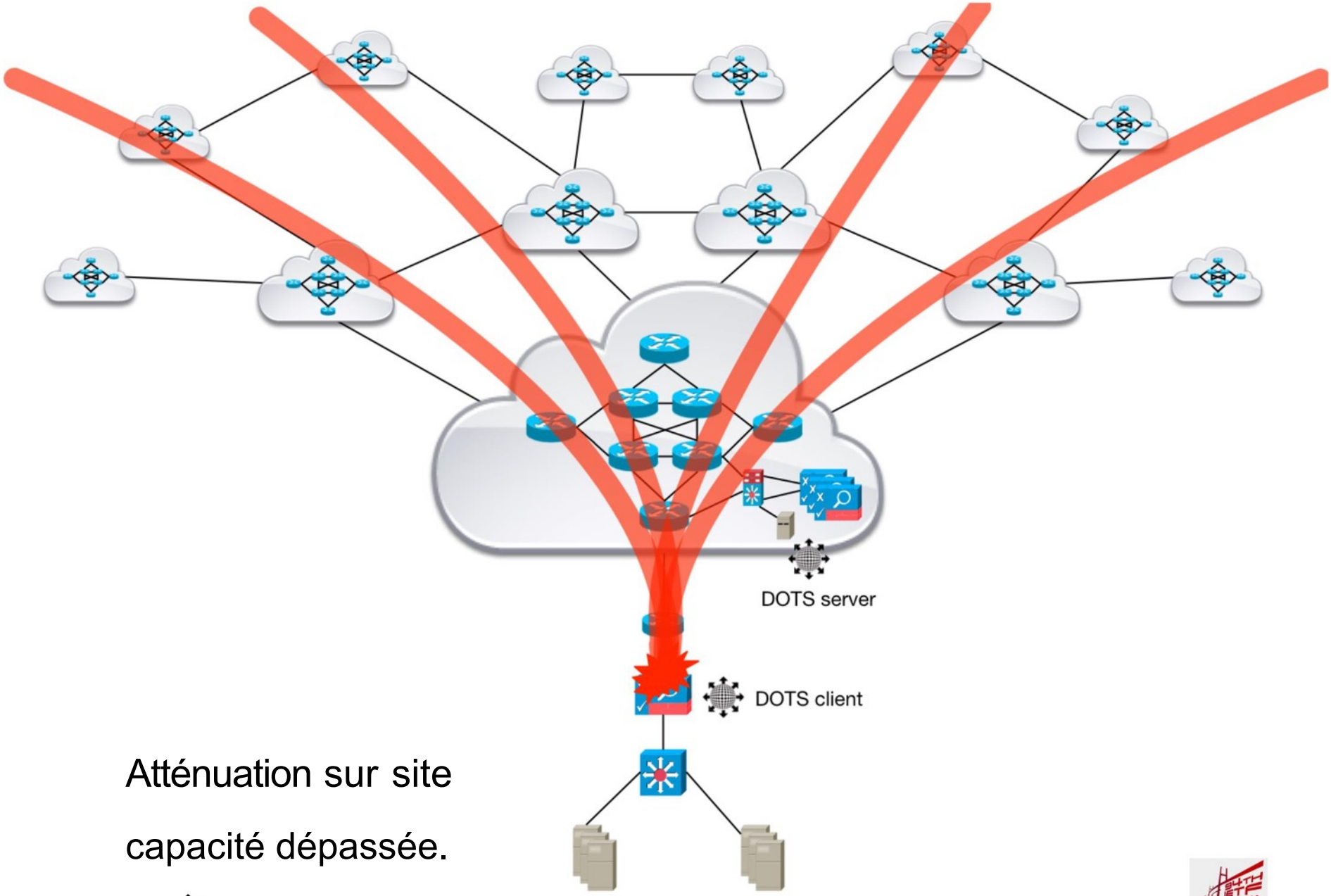


Attaque DDoS initiée.

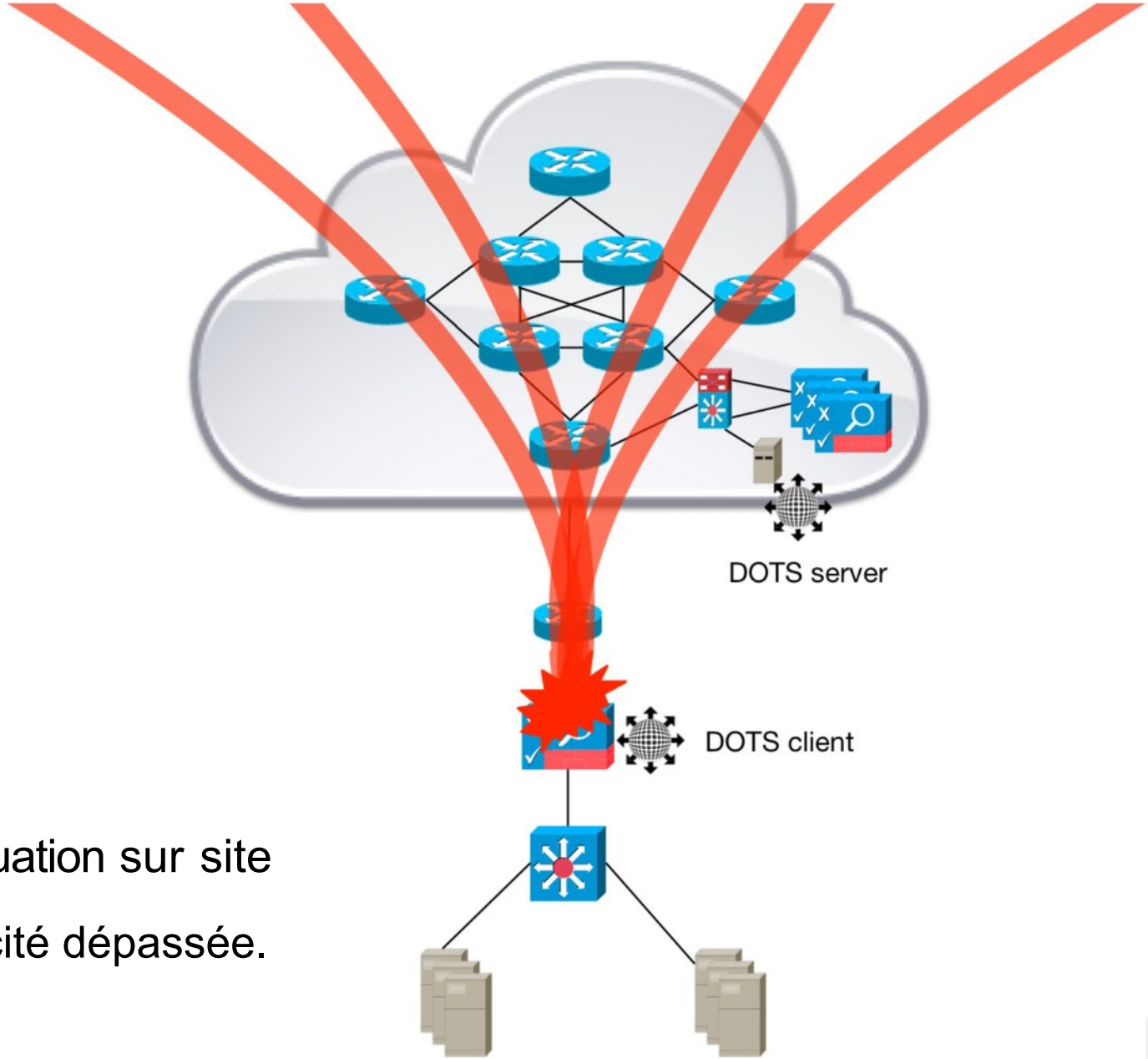


Attaque atténuée

on-prem.

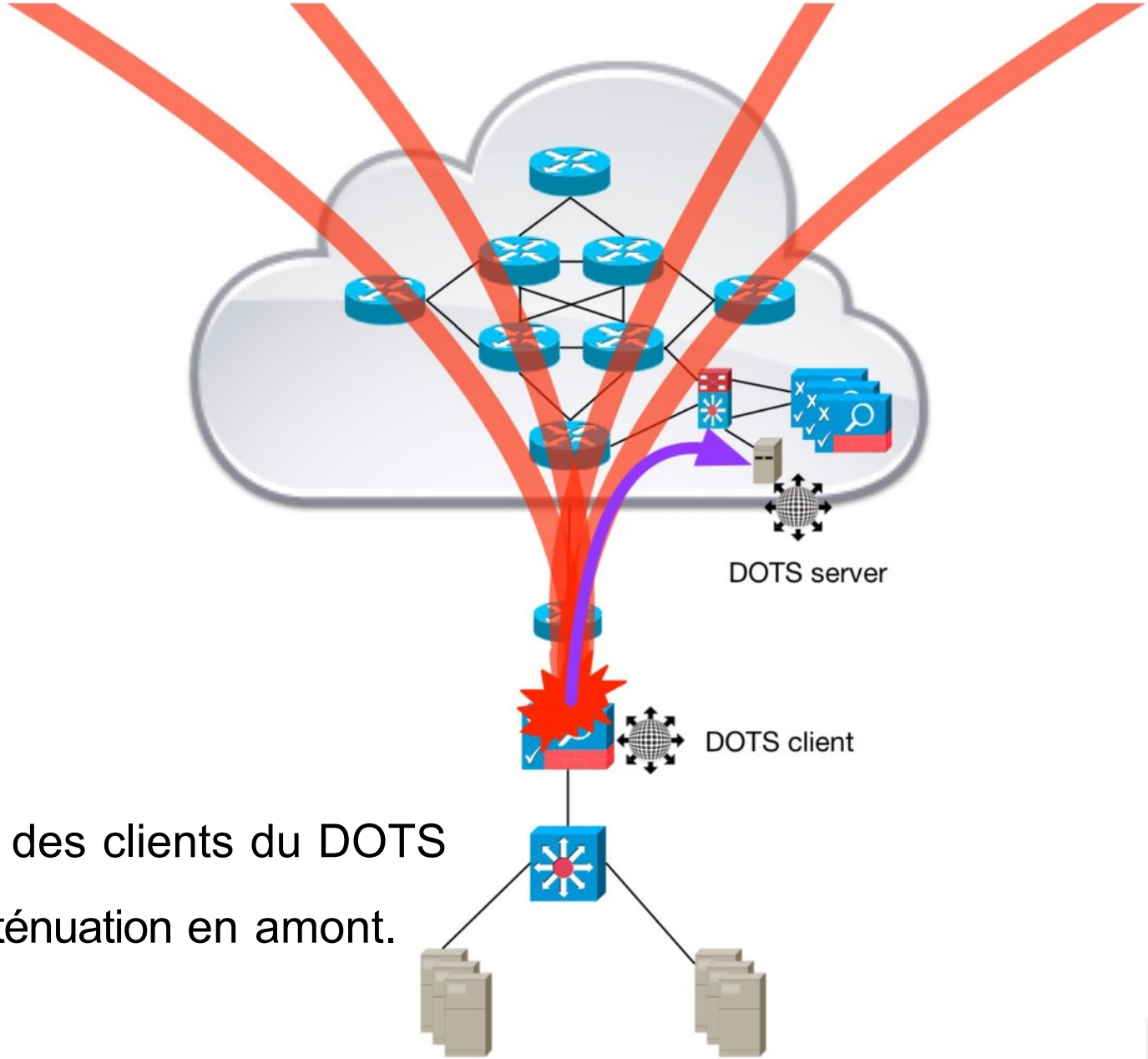


Atténuation sur site capacité dépassée.

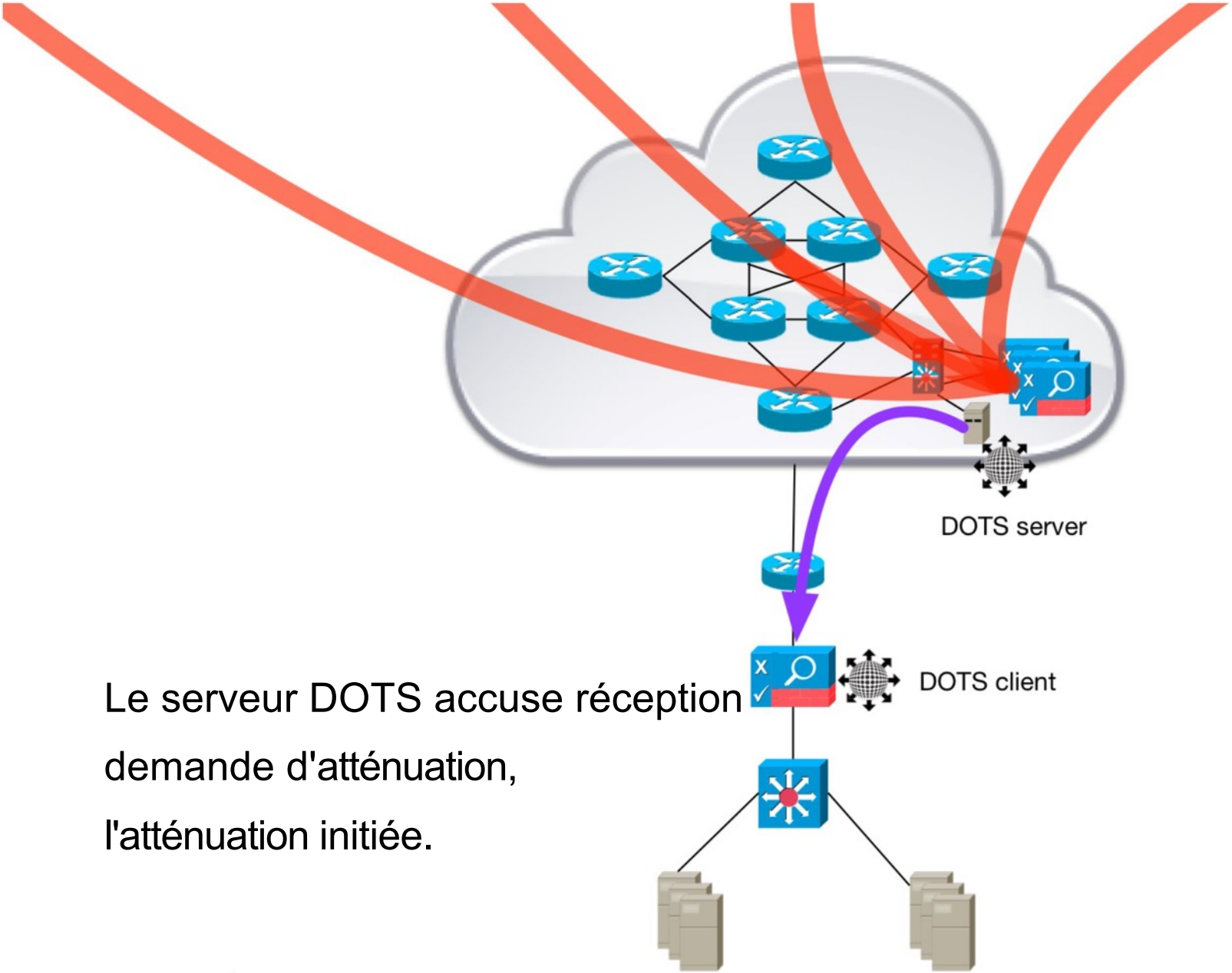


Atténuation sur site

capacité dépassée.



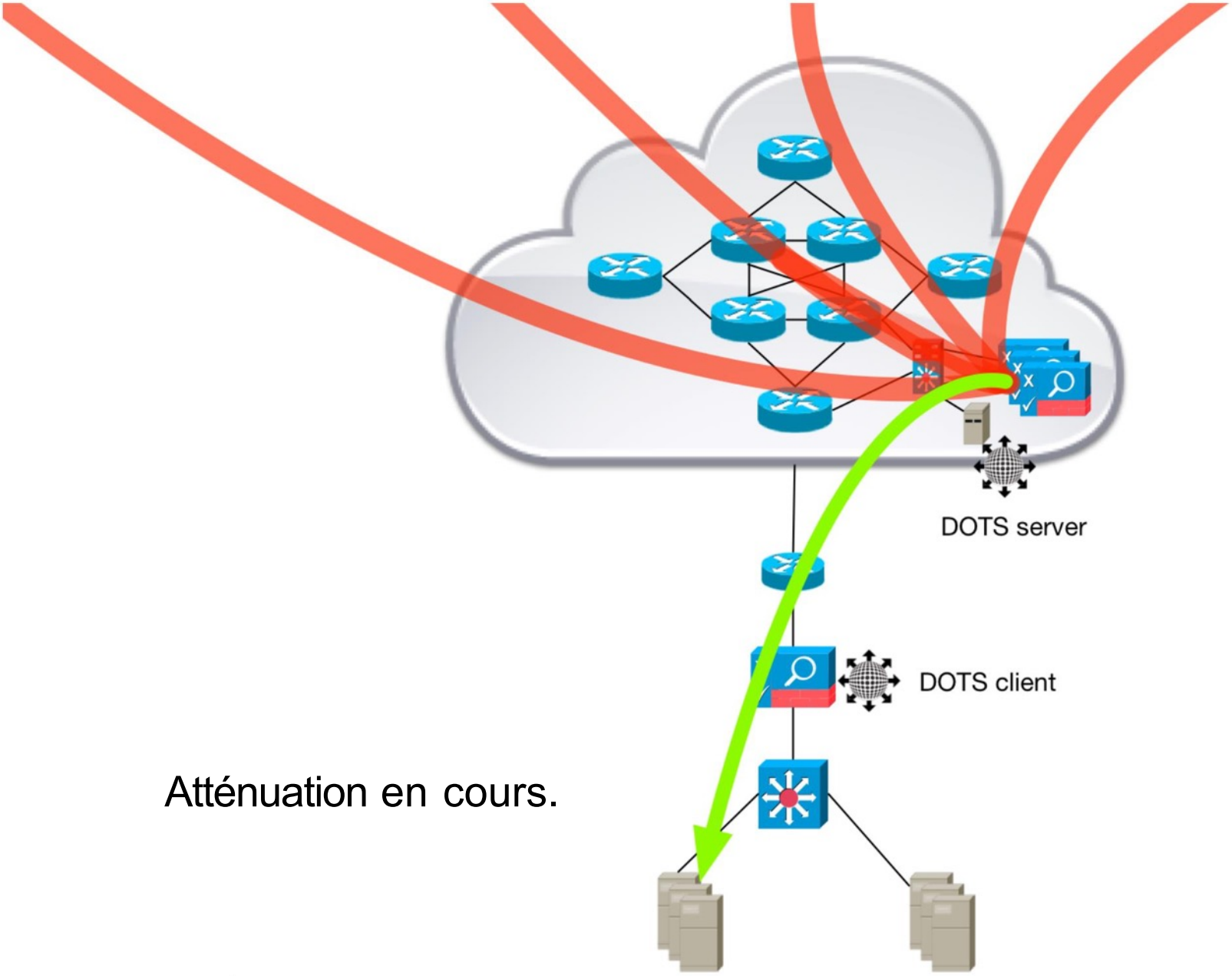
Signaux des clients du DOTS pour l'atténuation en amont.



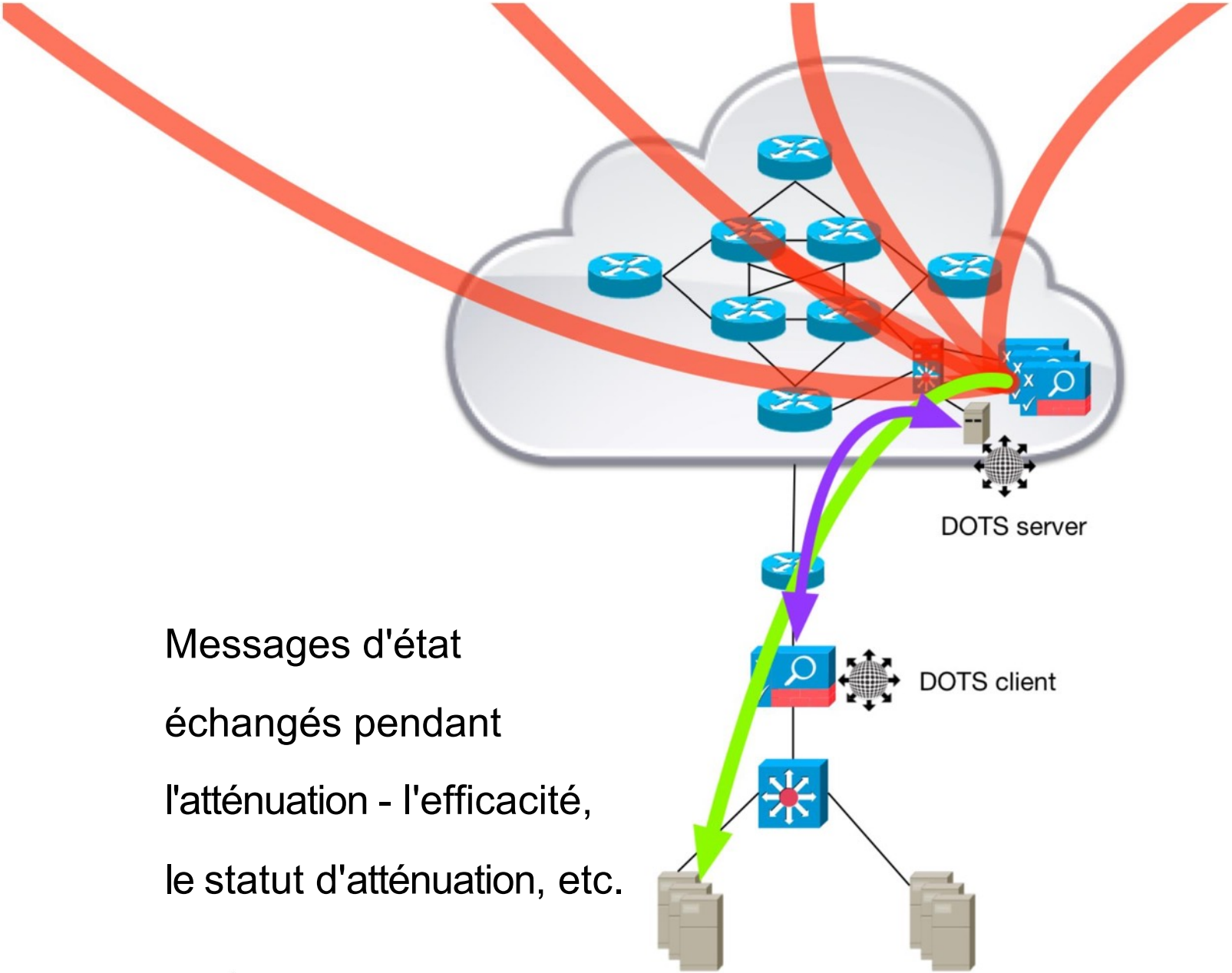
Le serveur DOTS accuse réception

demande d'atténuation,

l'atténuation initiée.



Atténuation en cours.

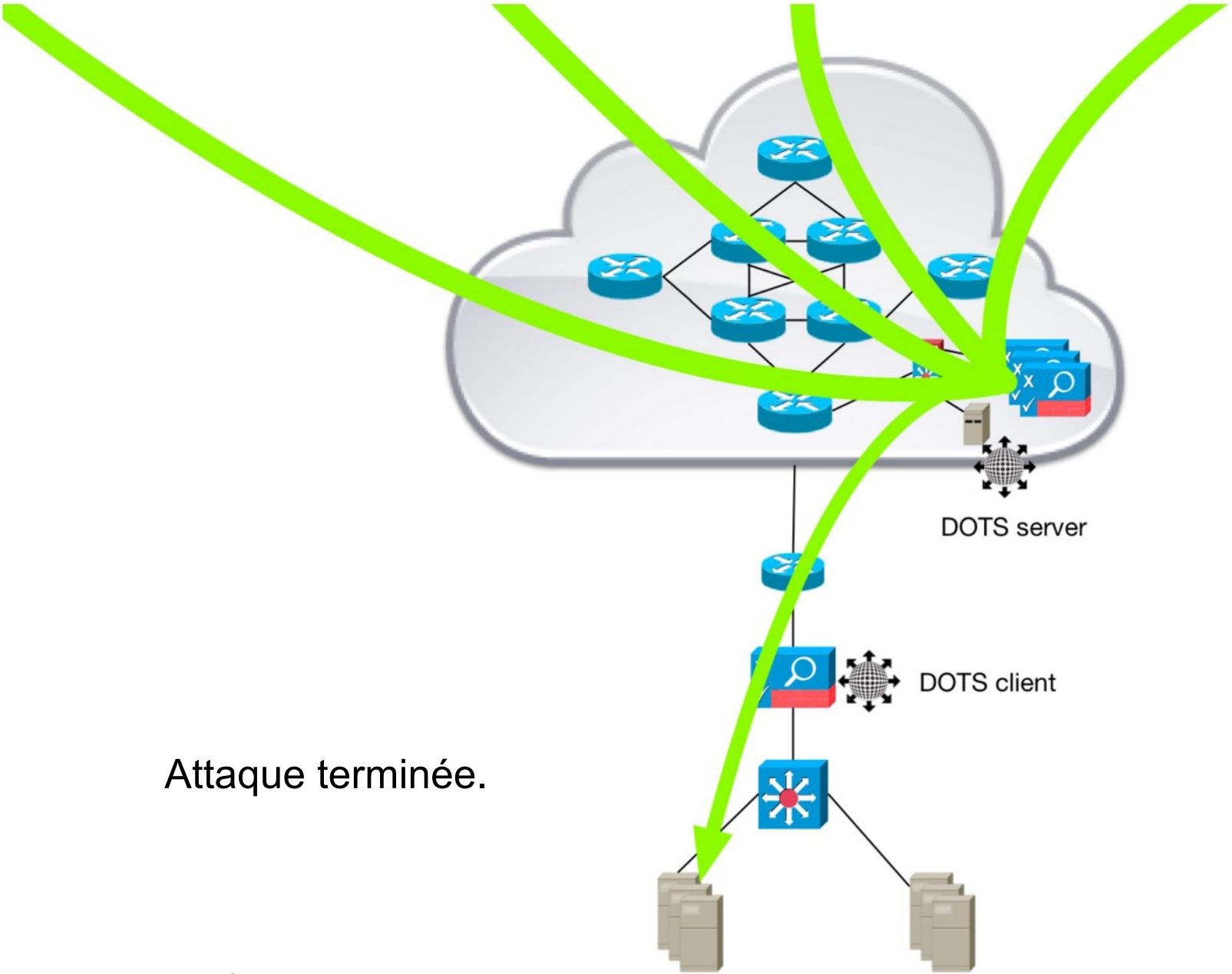


Messages d'état

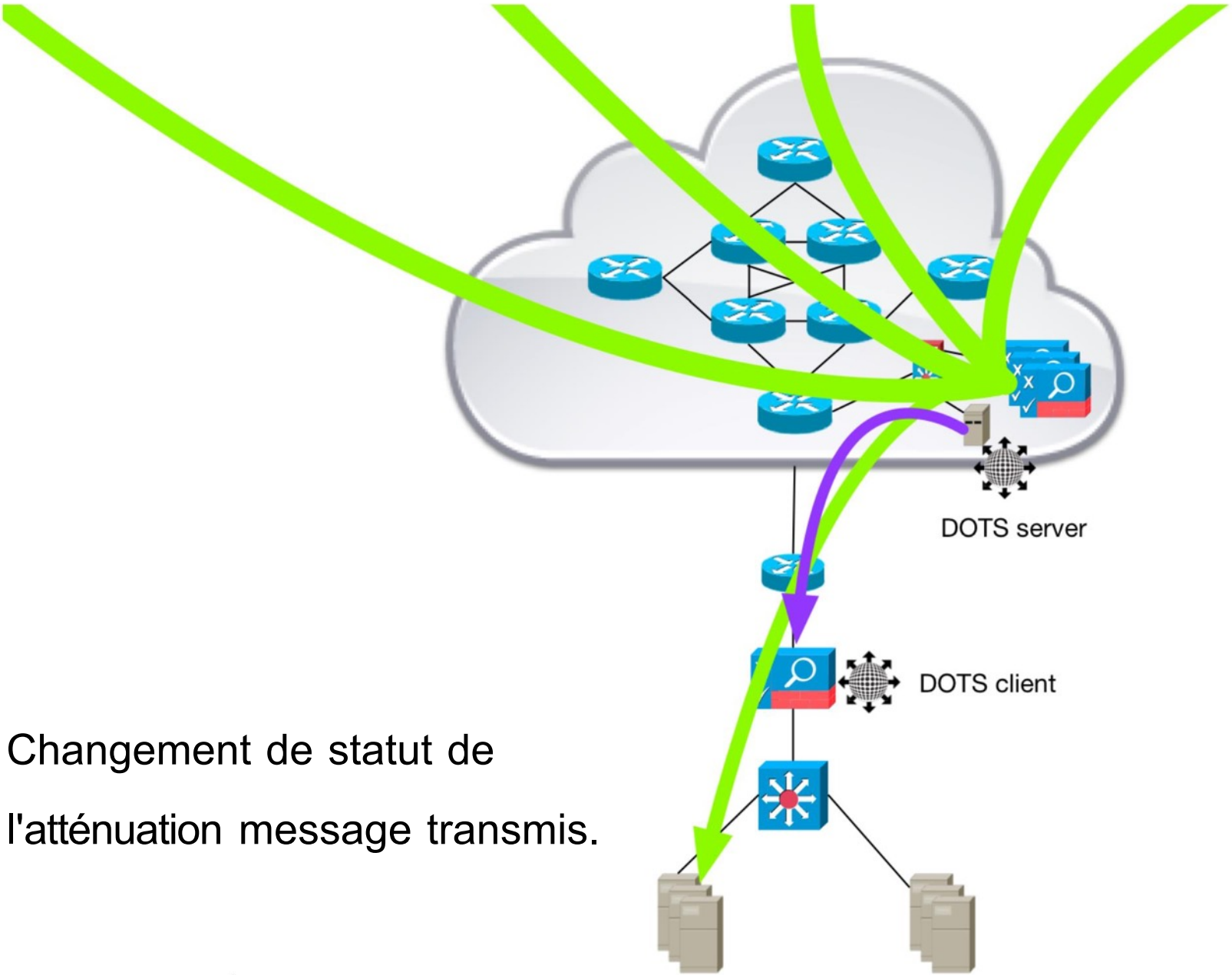
échangés pendant

l'atténuation - l'efficacité,

le statut d'atténuation, etc.

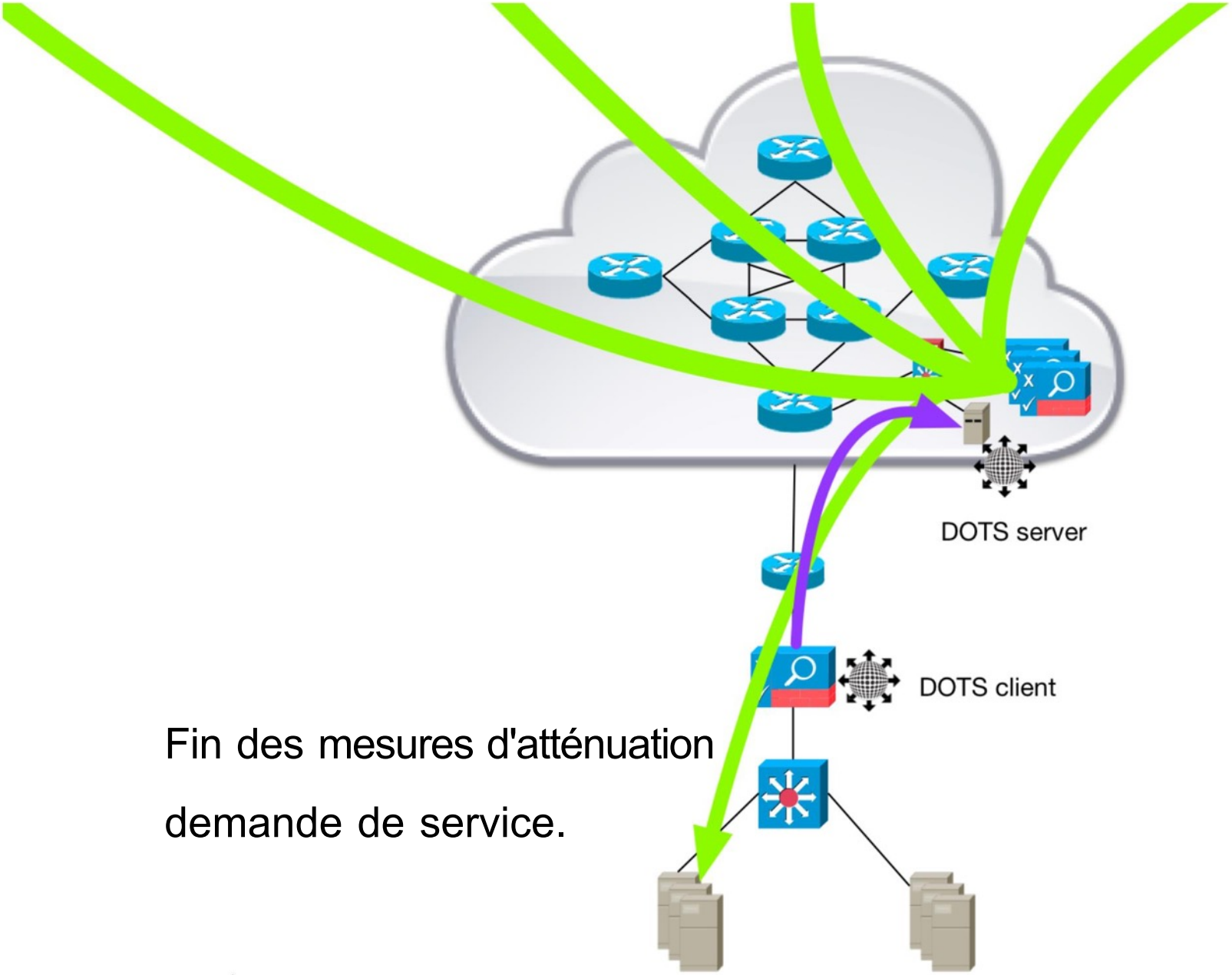


Attaque terminée.



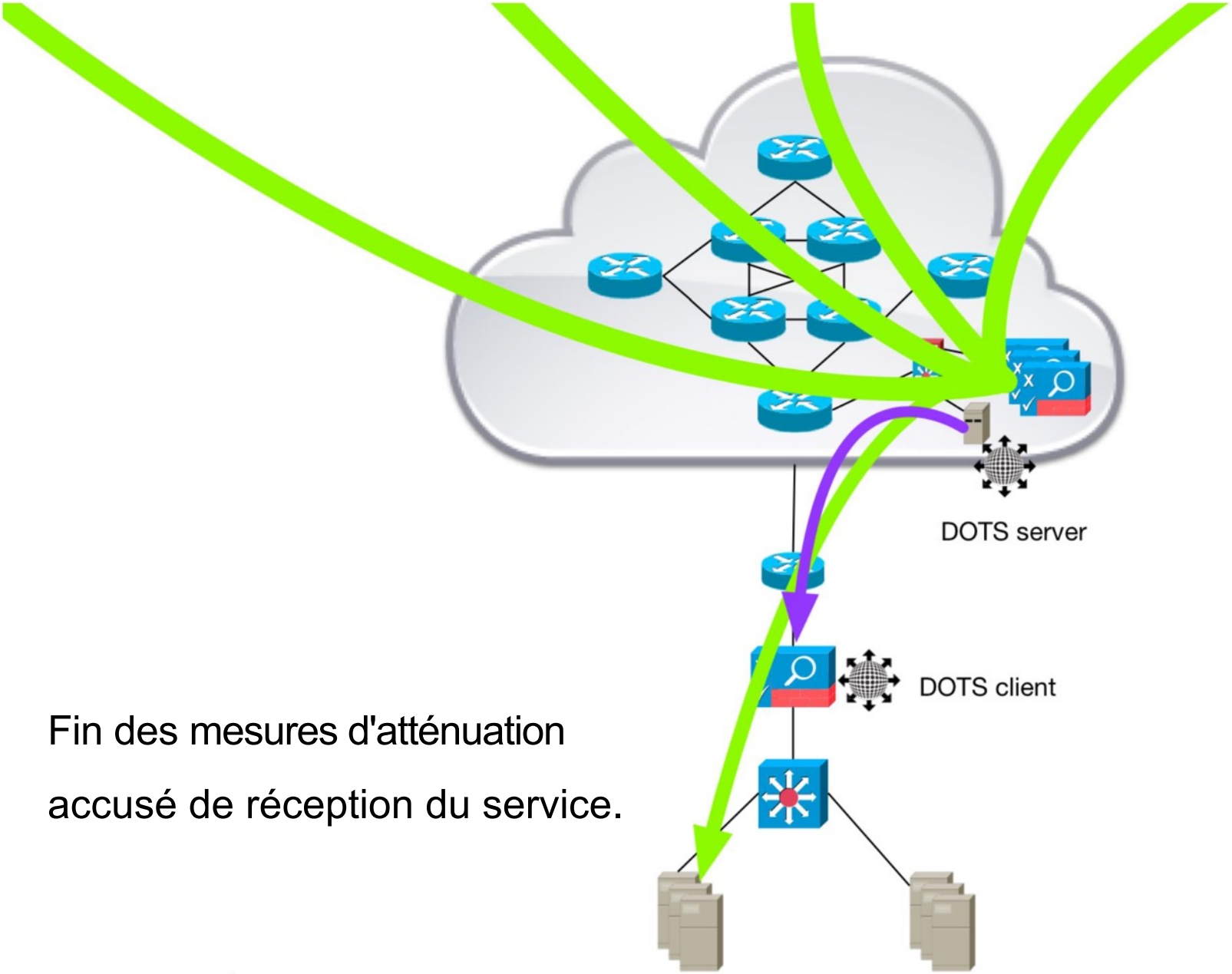
Changement de statut de

l'atténuation message transmis.



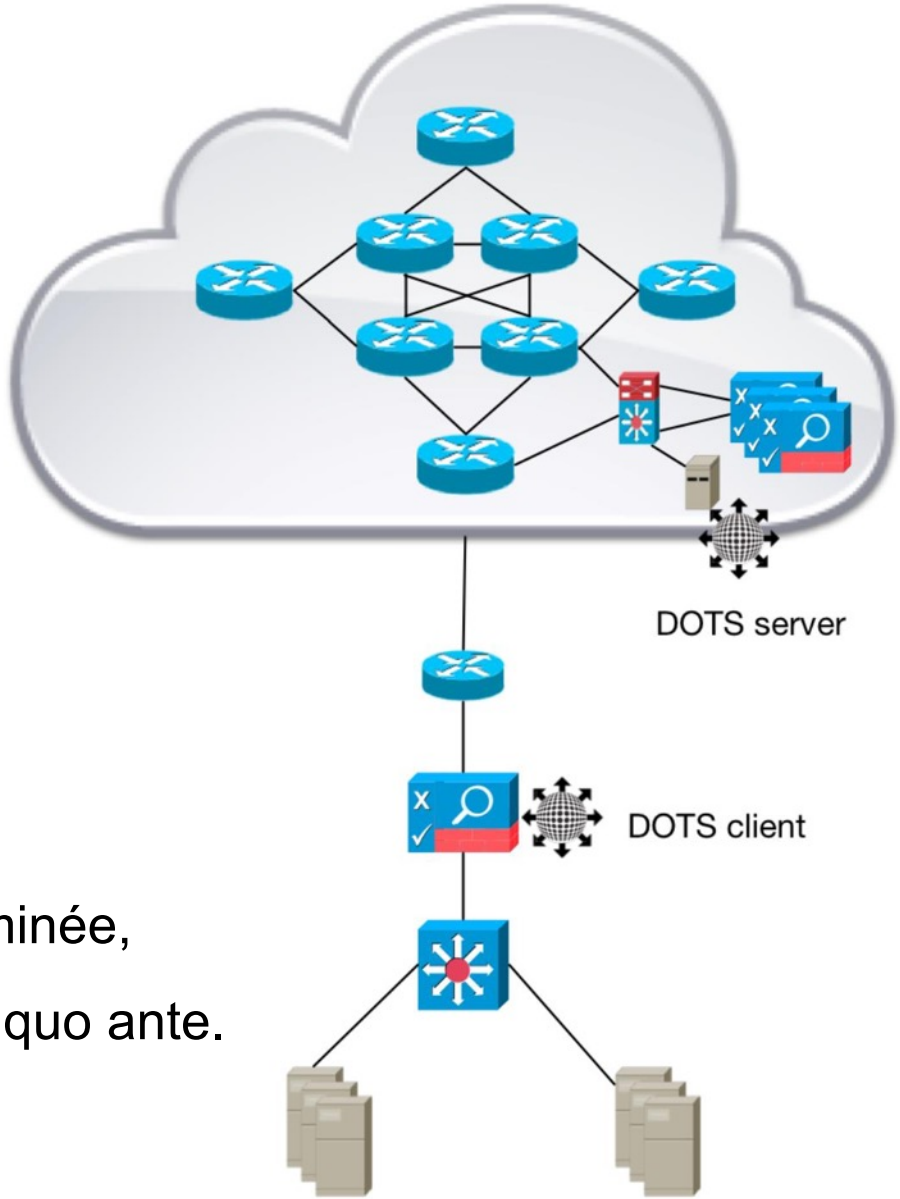
Fin des mesures d'atténuation

demande de service.



Fin des mesures d'atténuation

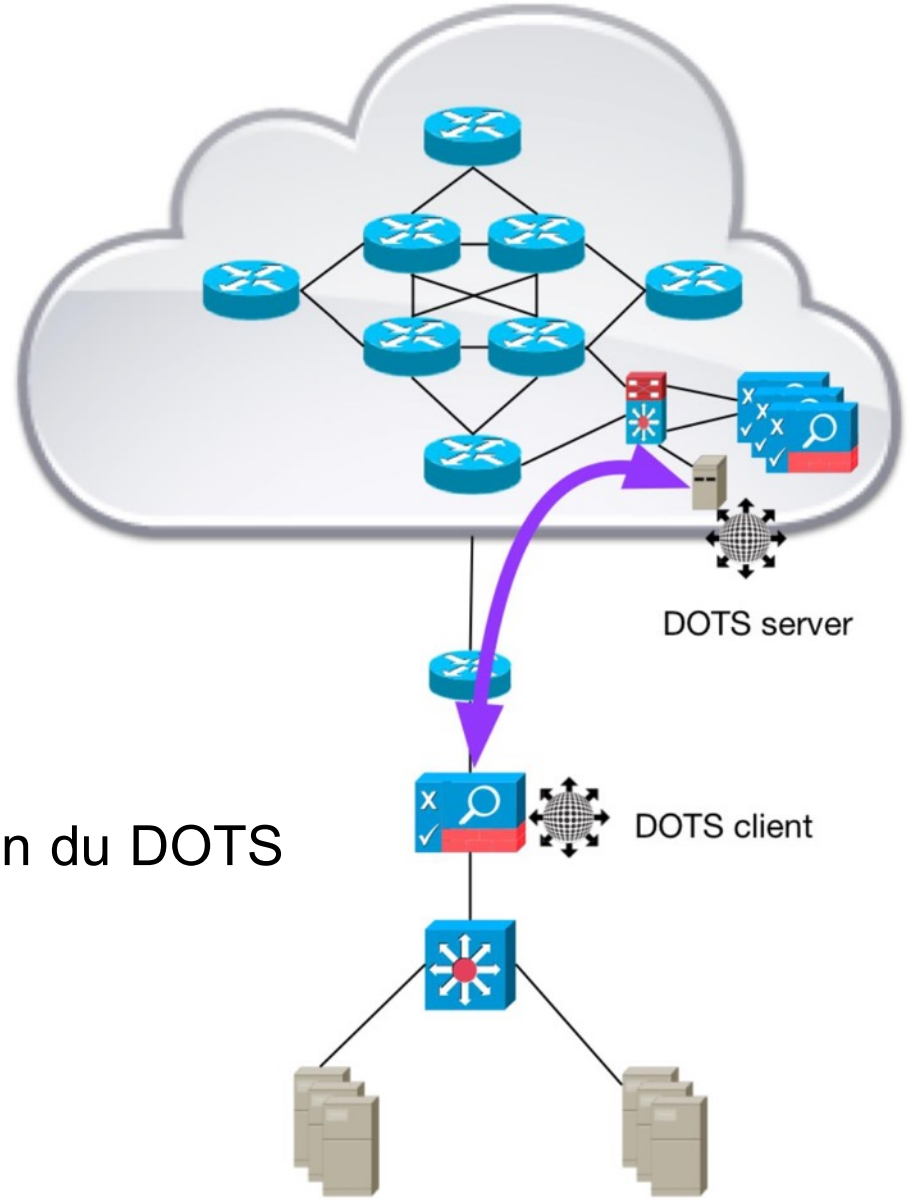
accusé de réception du service.



Atténuation terminée,

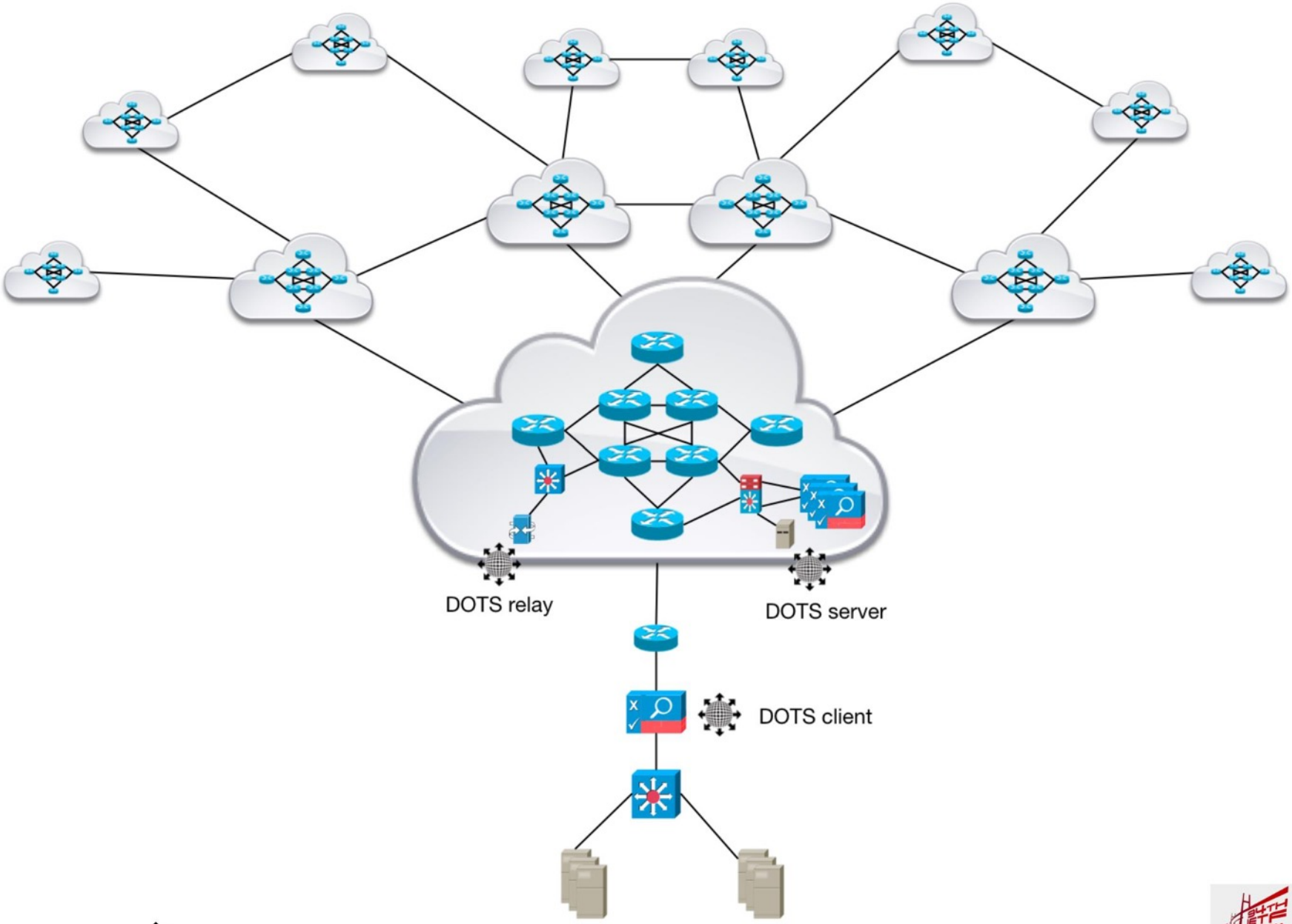
retour au statu quo ante.

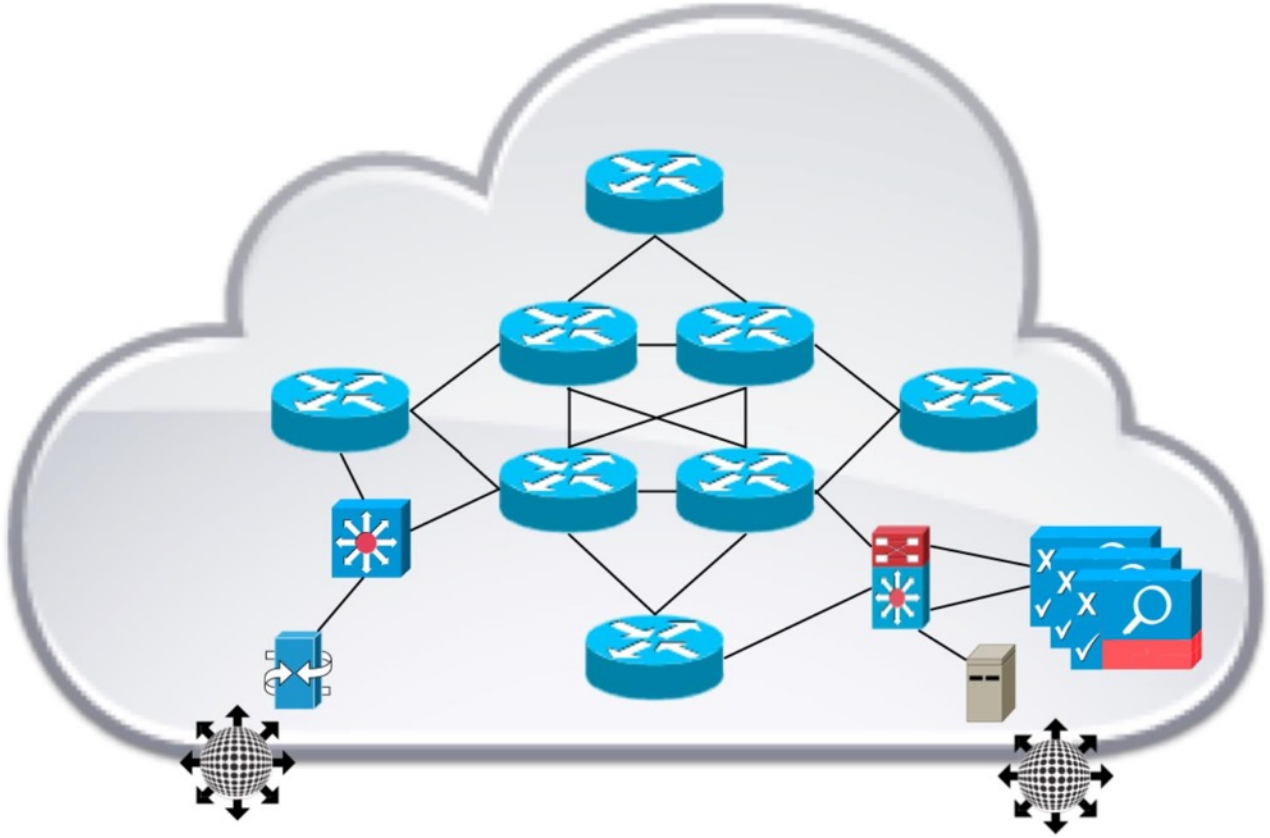
Communication du DOTS relations.

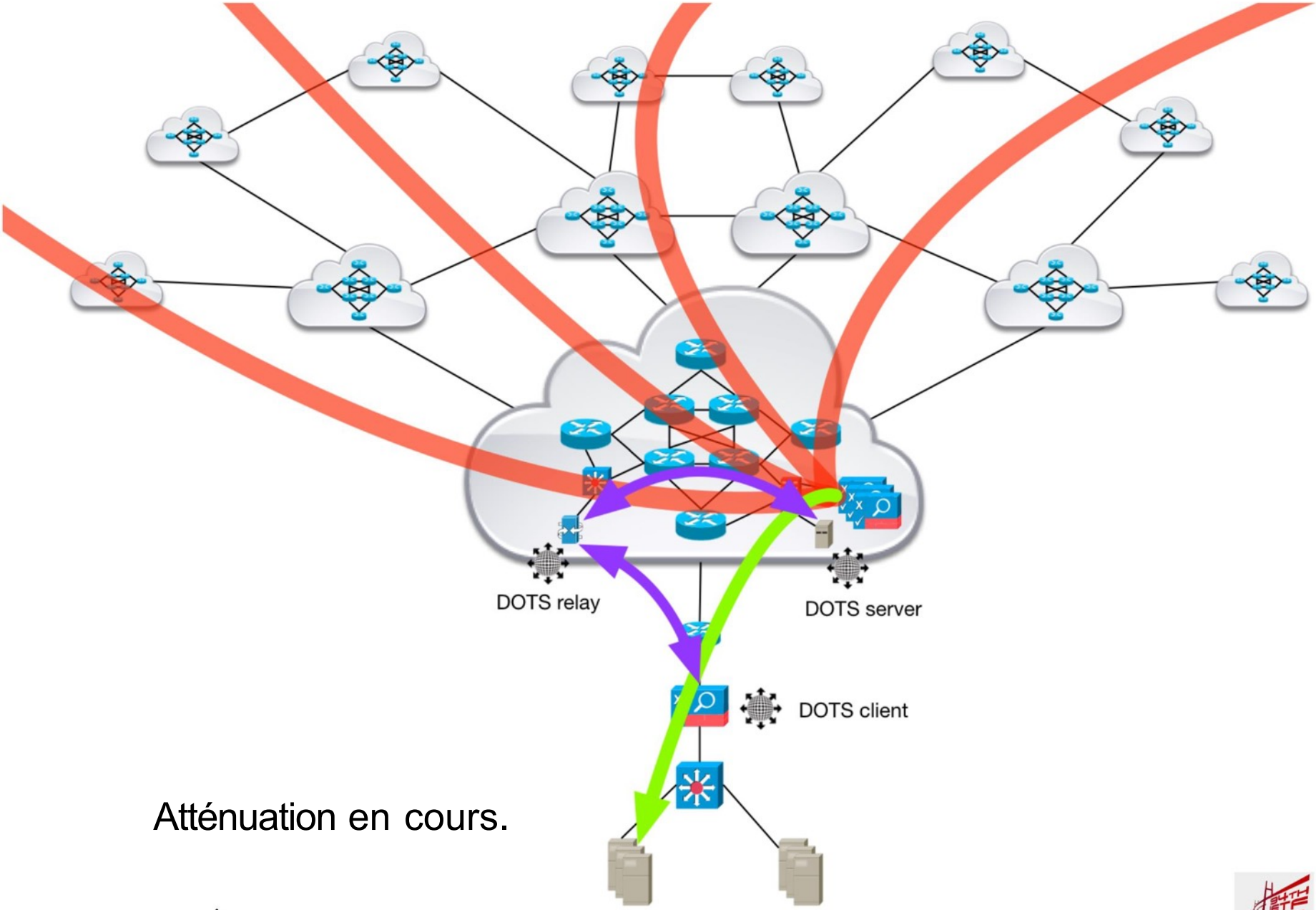


4.1.1 - Variation avec le relais DOTS

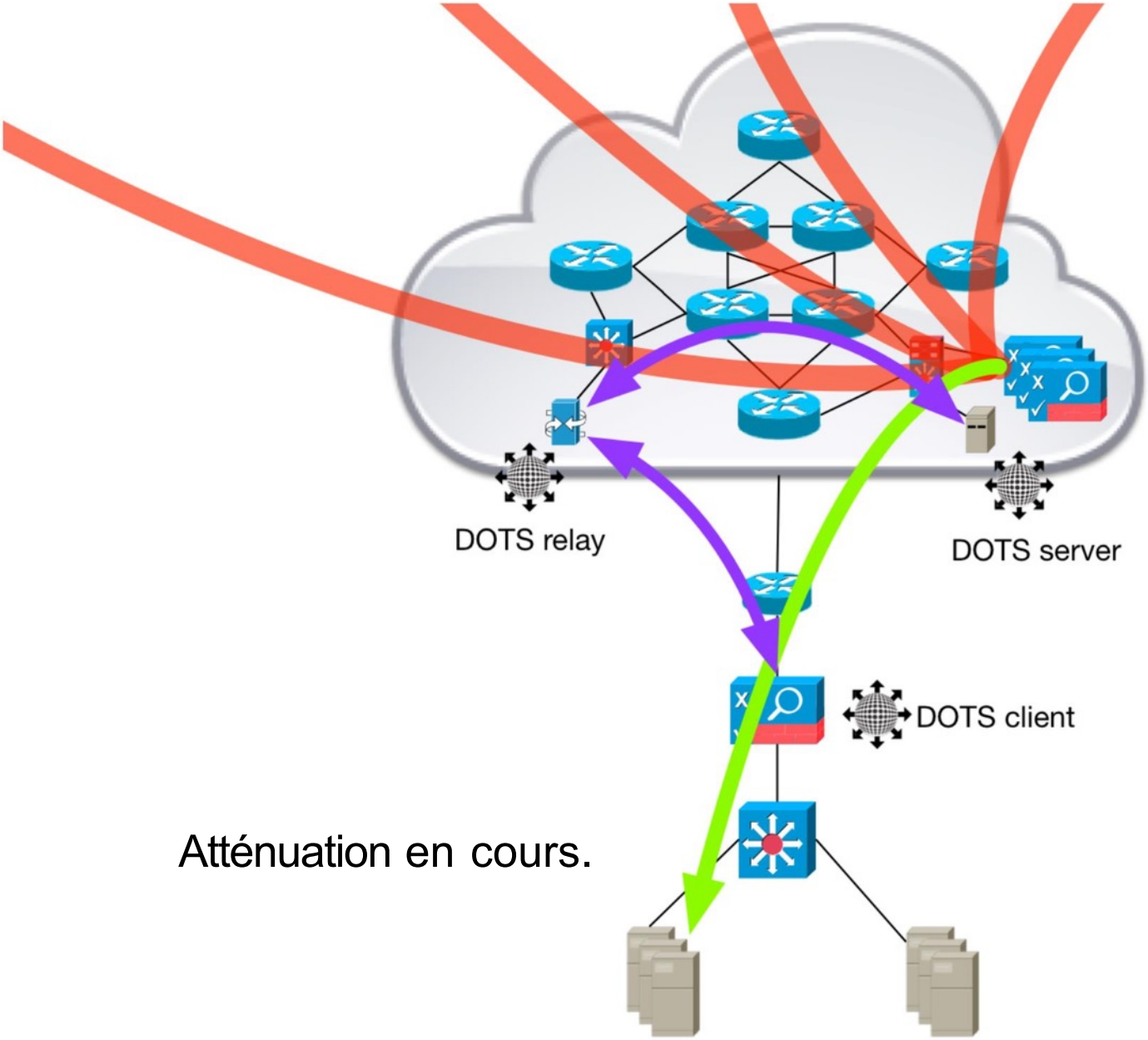
Communications


DOTS relay
DOTS server
DOTS client

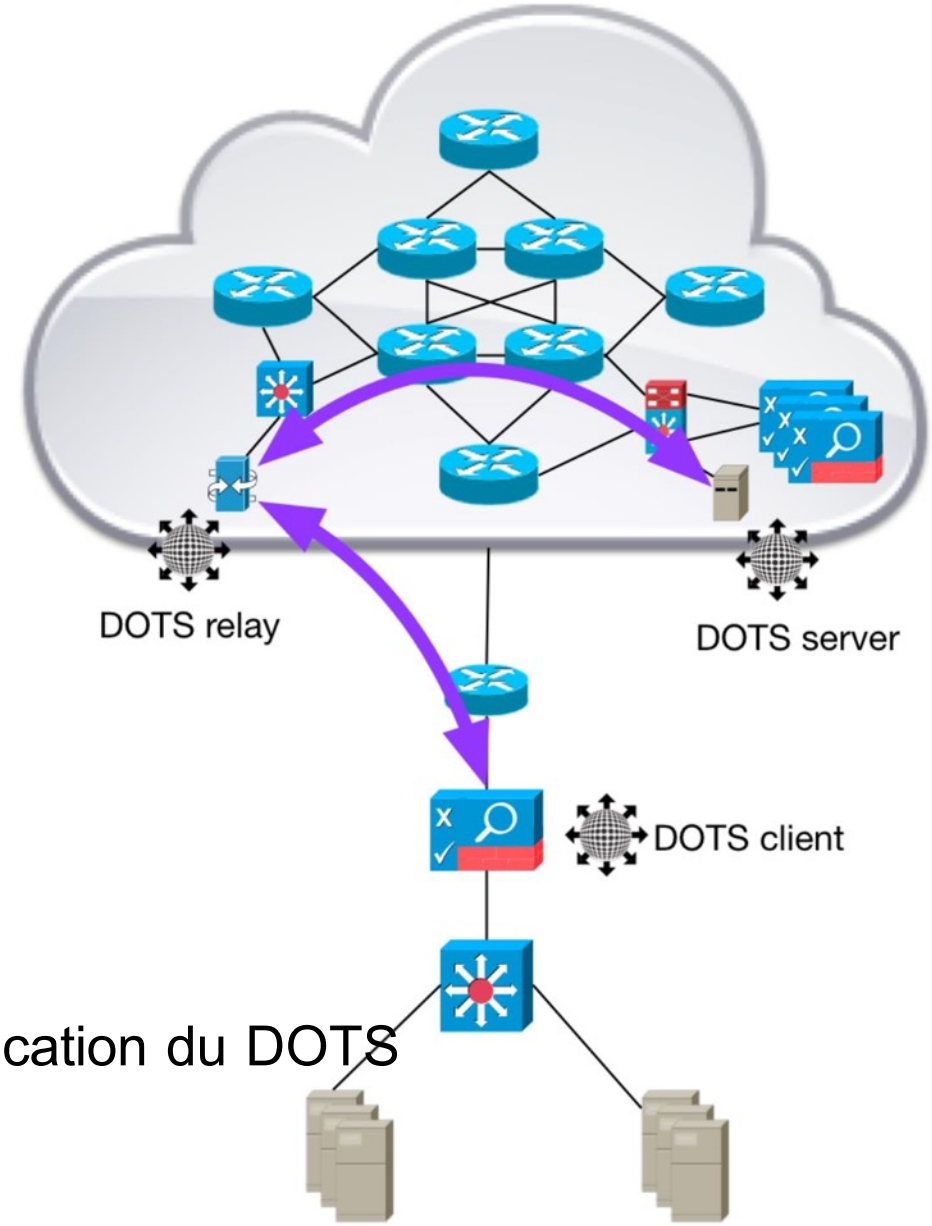

DOTS relay
DOTS server



Atténuation en cours.



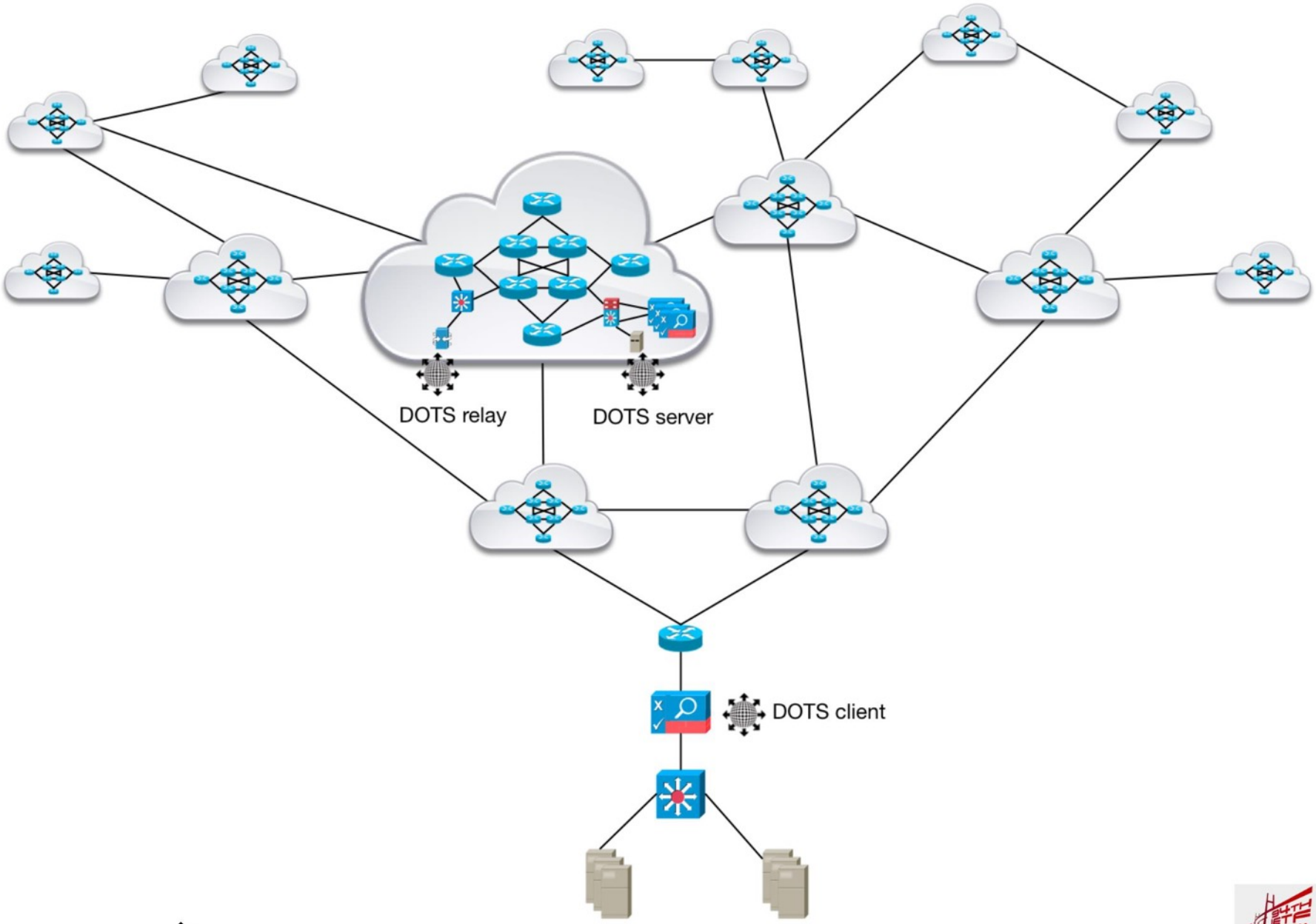
Atténuation en cours.

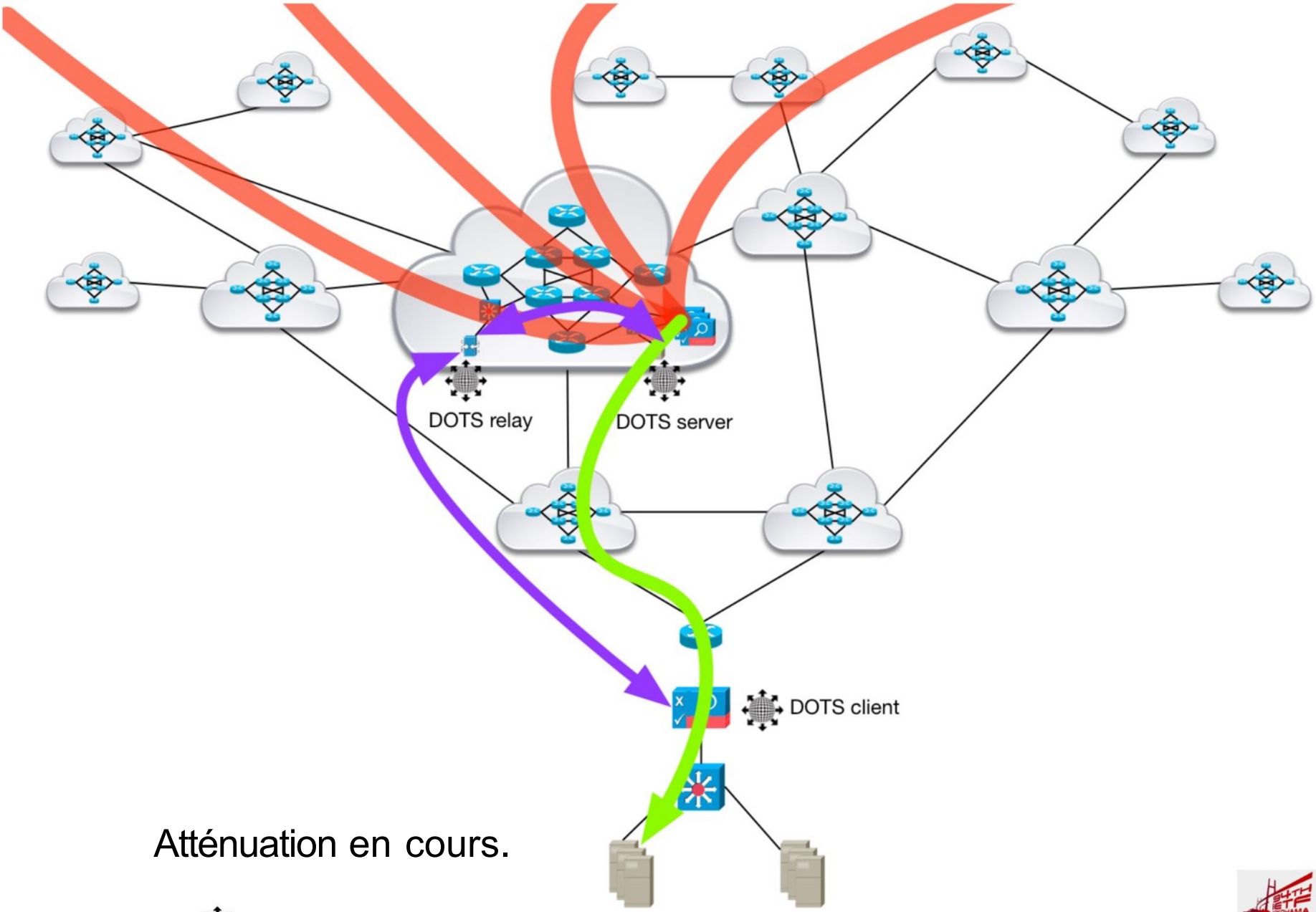


Communication du DOTS relations.

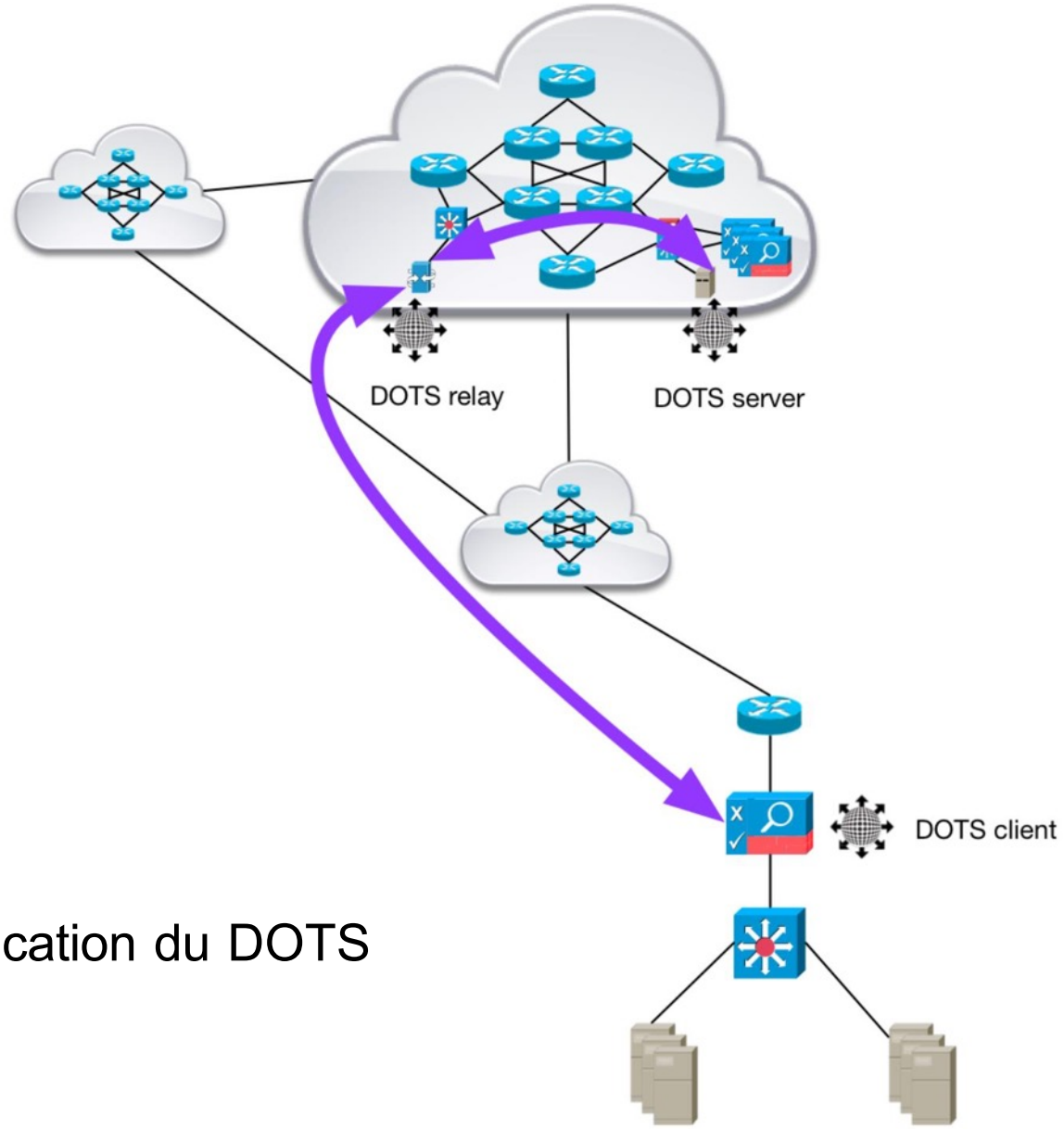
4.1.1 - Variation avec les DDoS superposés

Fournisseur de services d'atténuation


DOTS relay
DOTS server
DOTS client

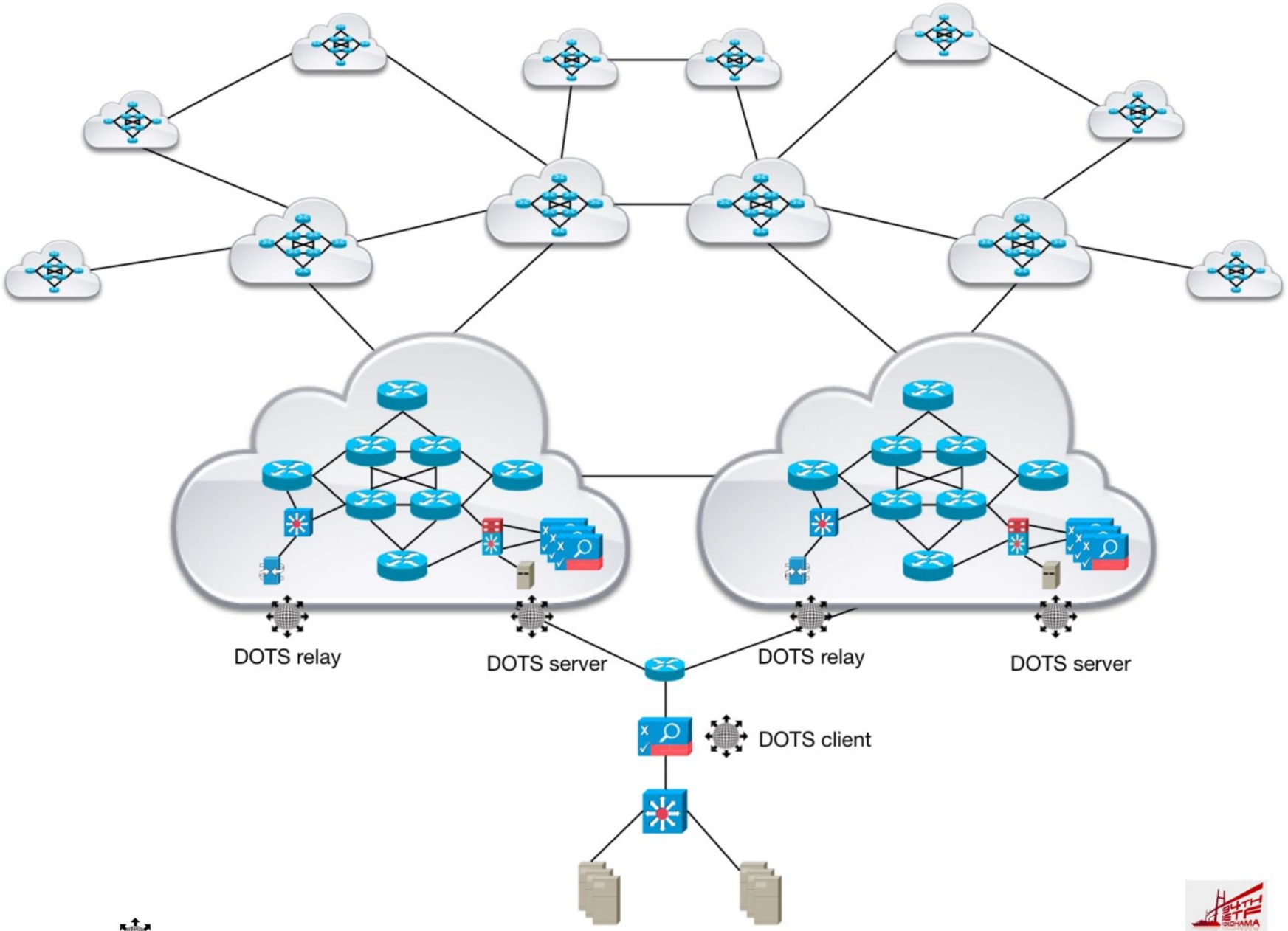


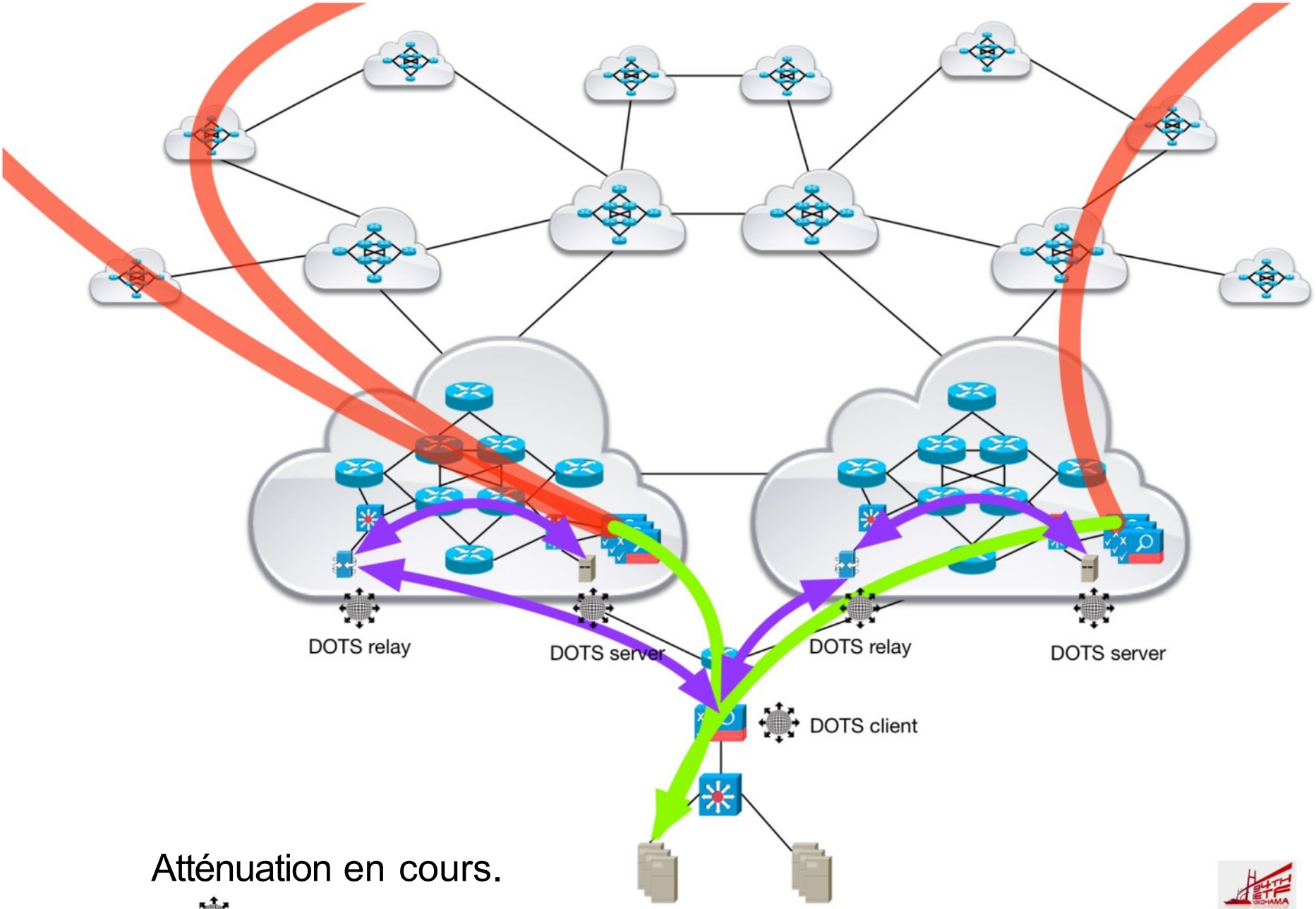
Atténuation en cours.



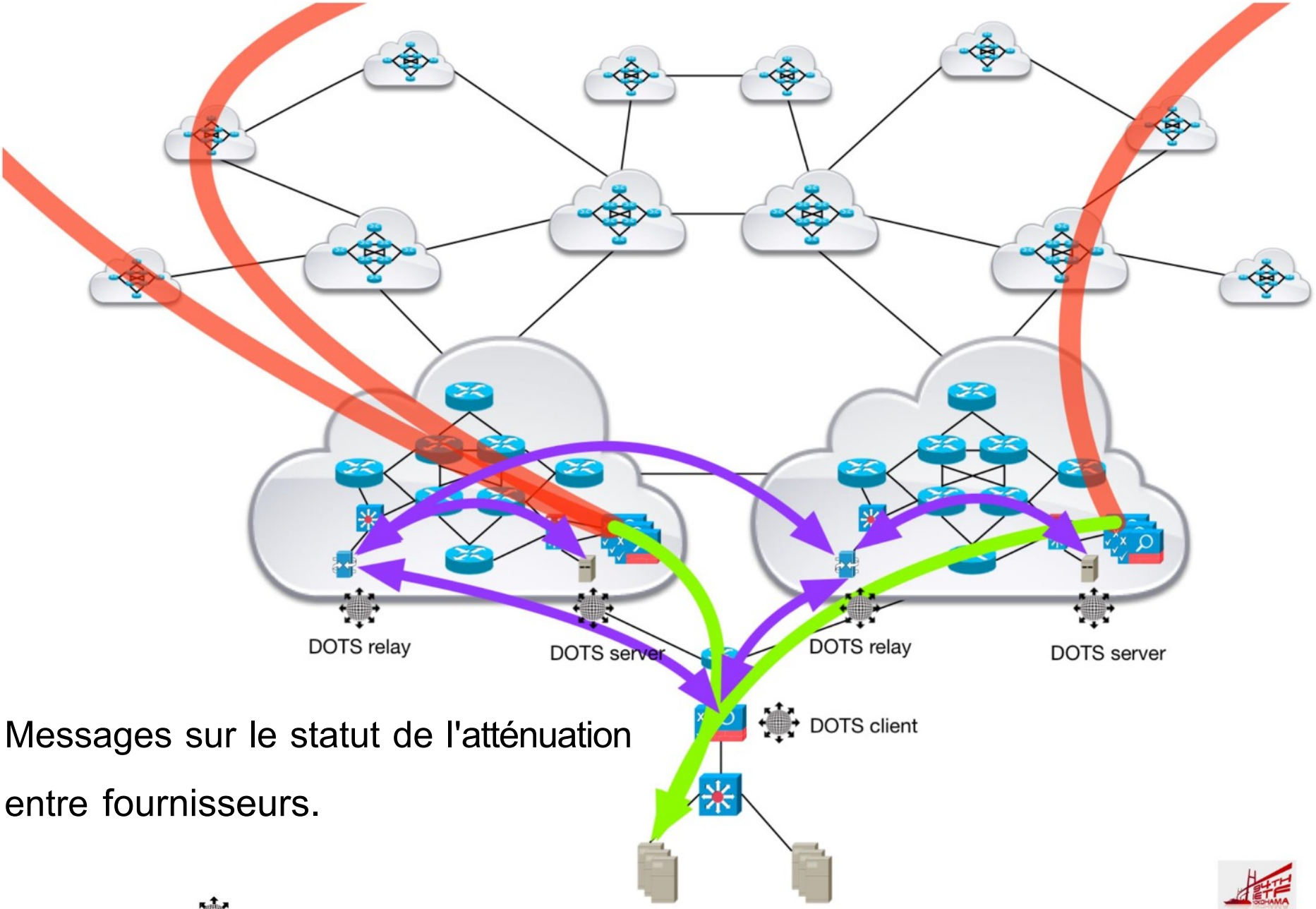
Communication du DOTS relations.

4.1.1 - Variation par rapport à Multiple Fournisseurs de solutions d'atténuation des DDoS en amont

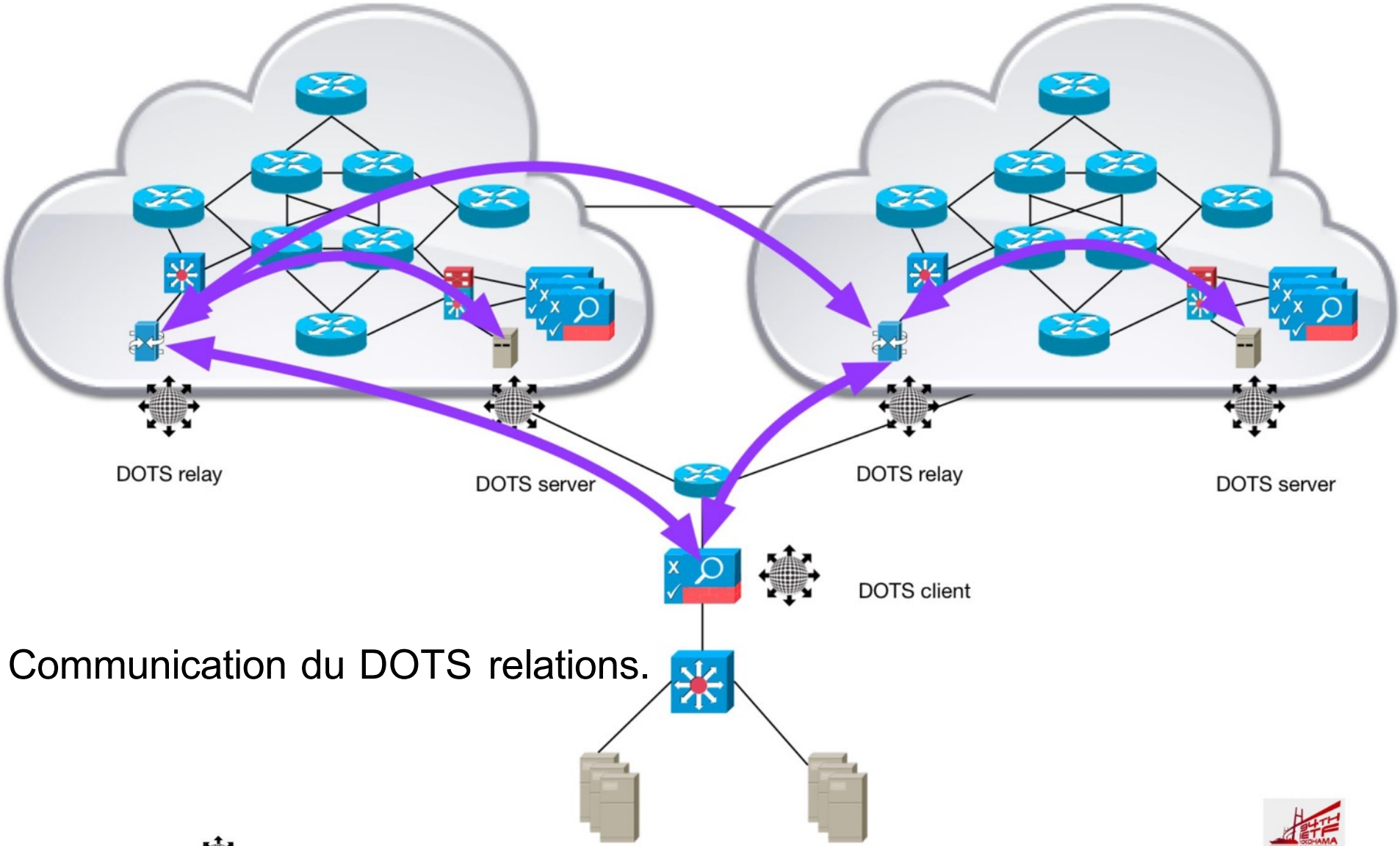

DOTS relay
DOTS server
DOTS relay
DOTS server
DOTS client



Atténuation en cours.



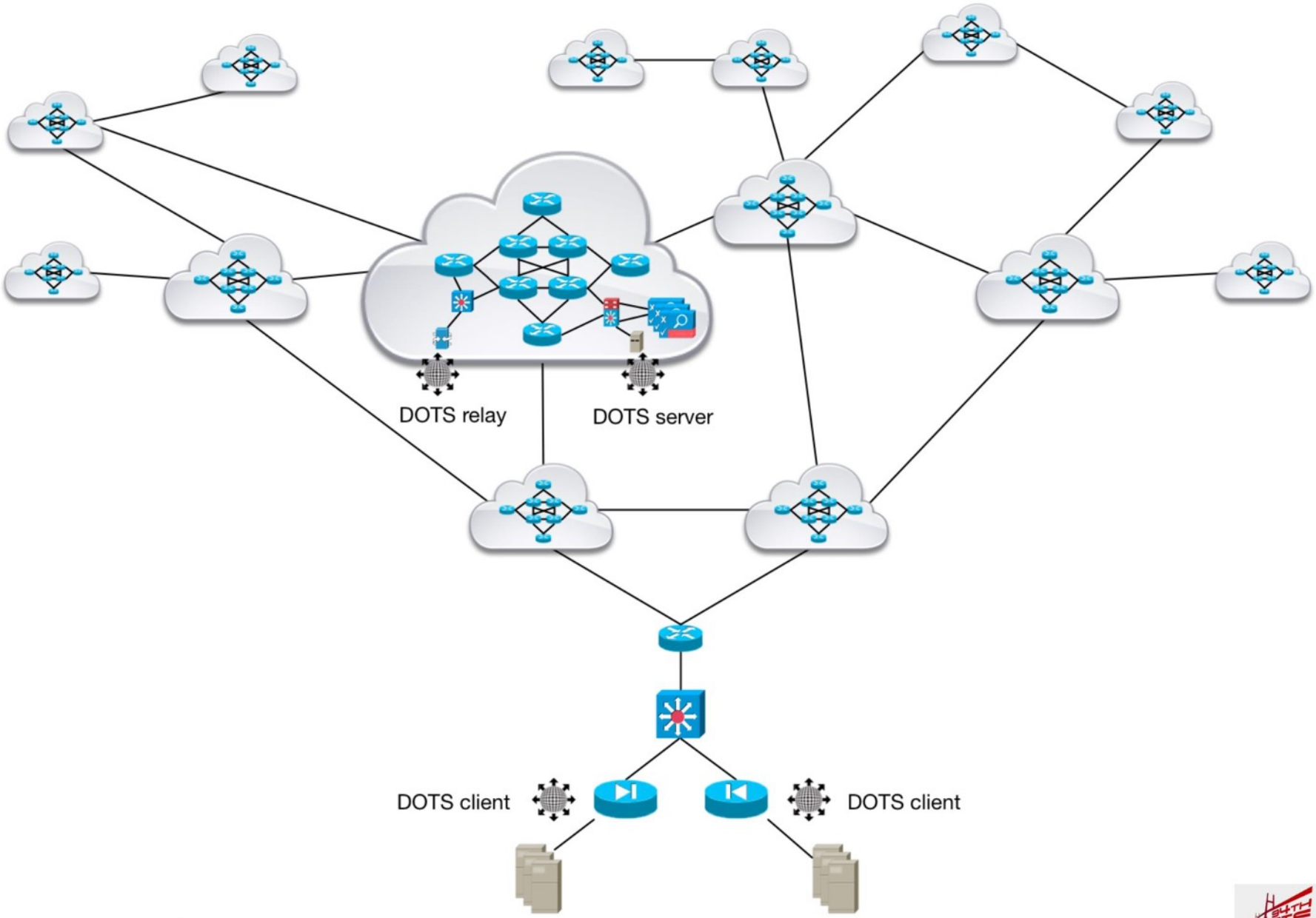
Messages sur le statut de l'atténuation entre fournisseurs.

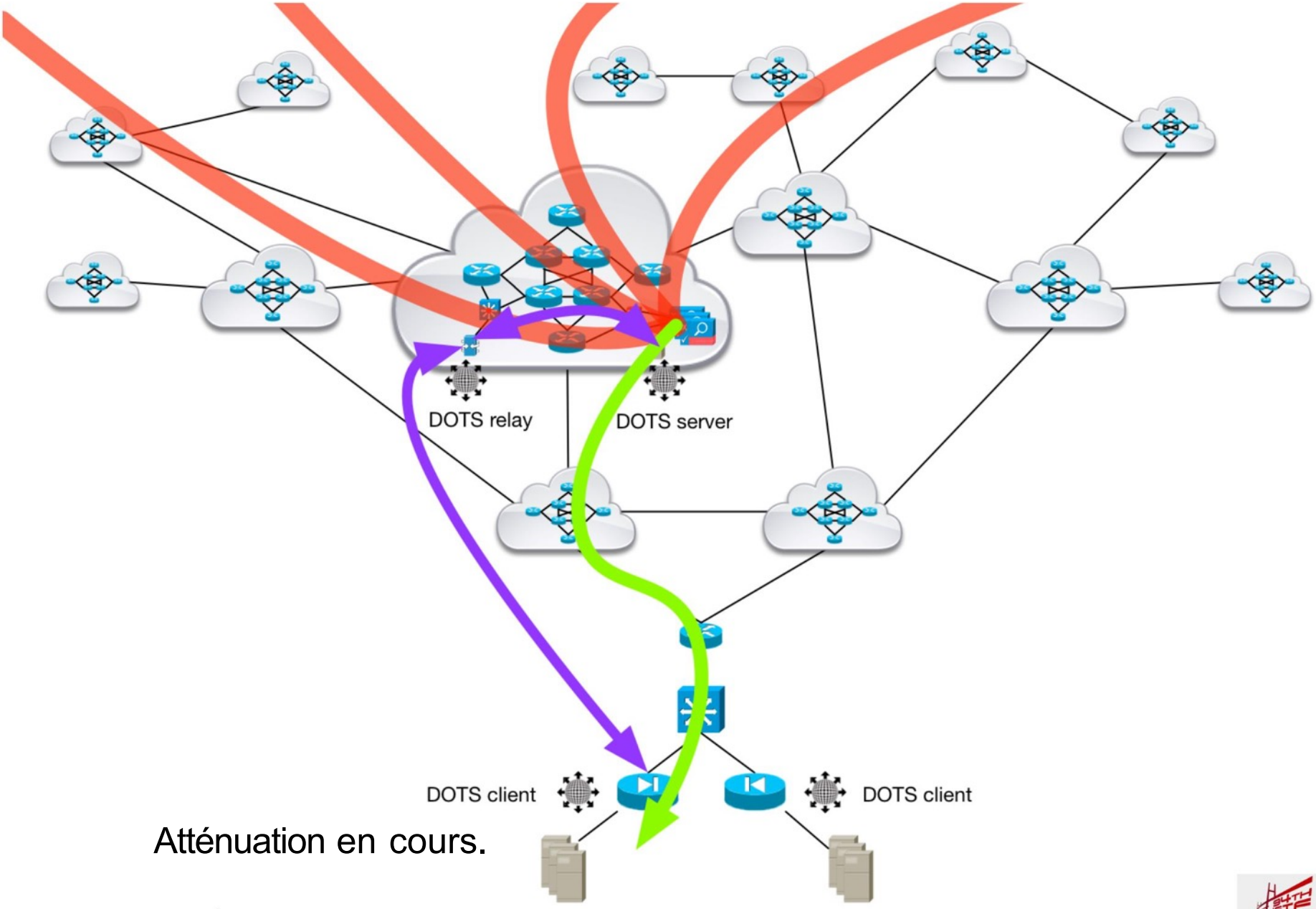


Communication du DOTS relations.

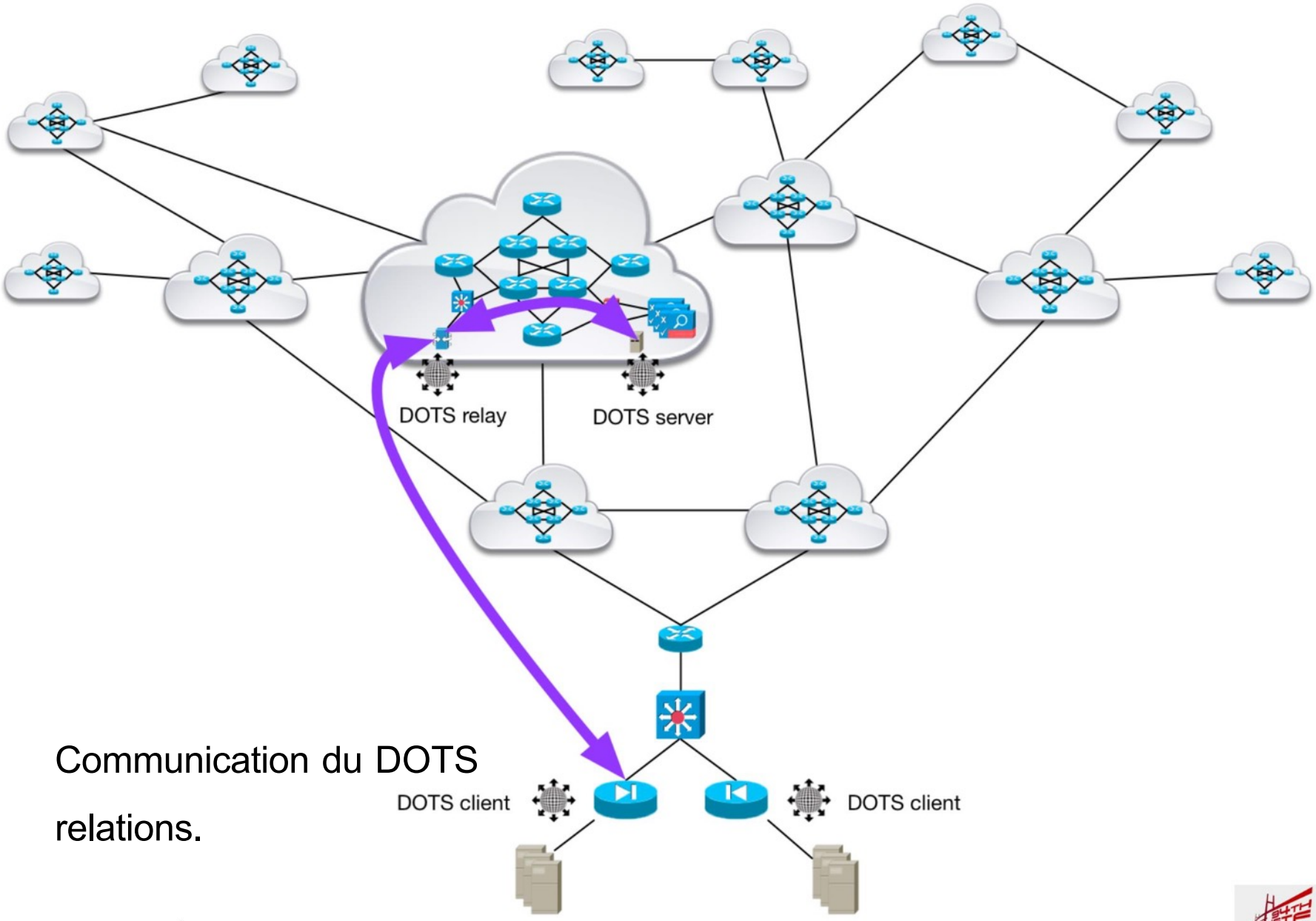
4.1.2 - Infrastructure de réseau

Demandes de dispositifs DDoS en amont


DOTS relay
DOTS server
DOTS client
DOTS client

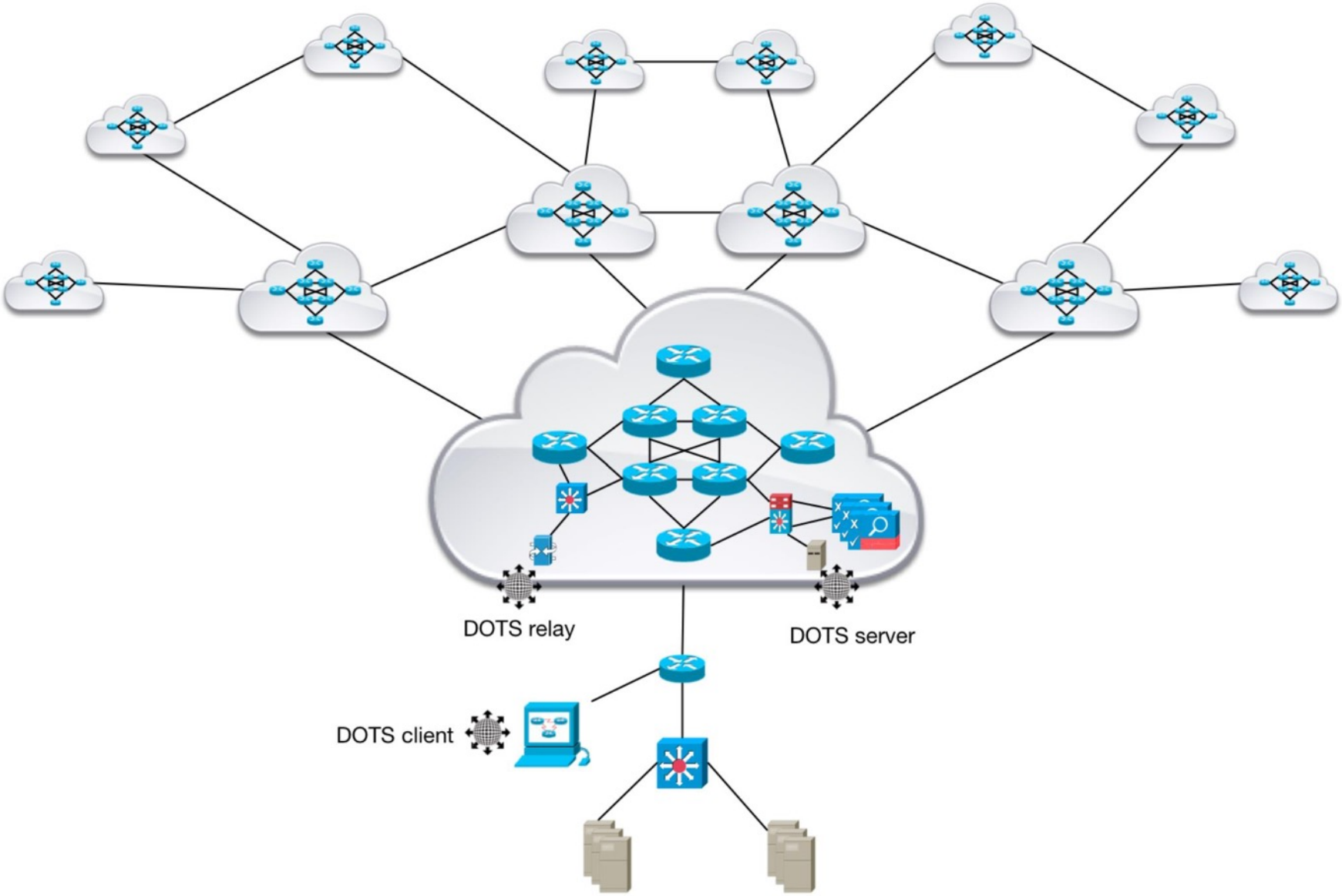


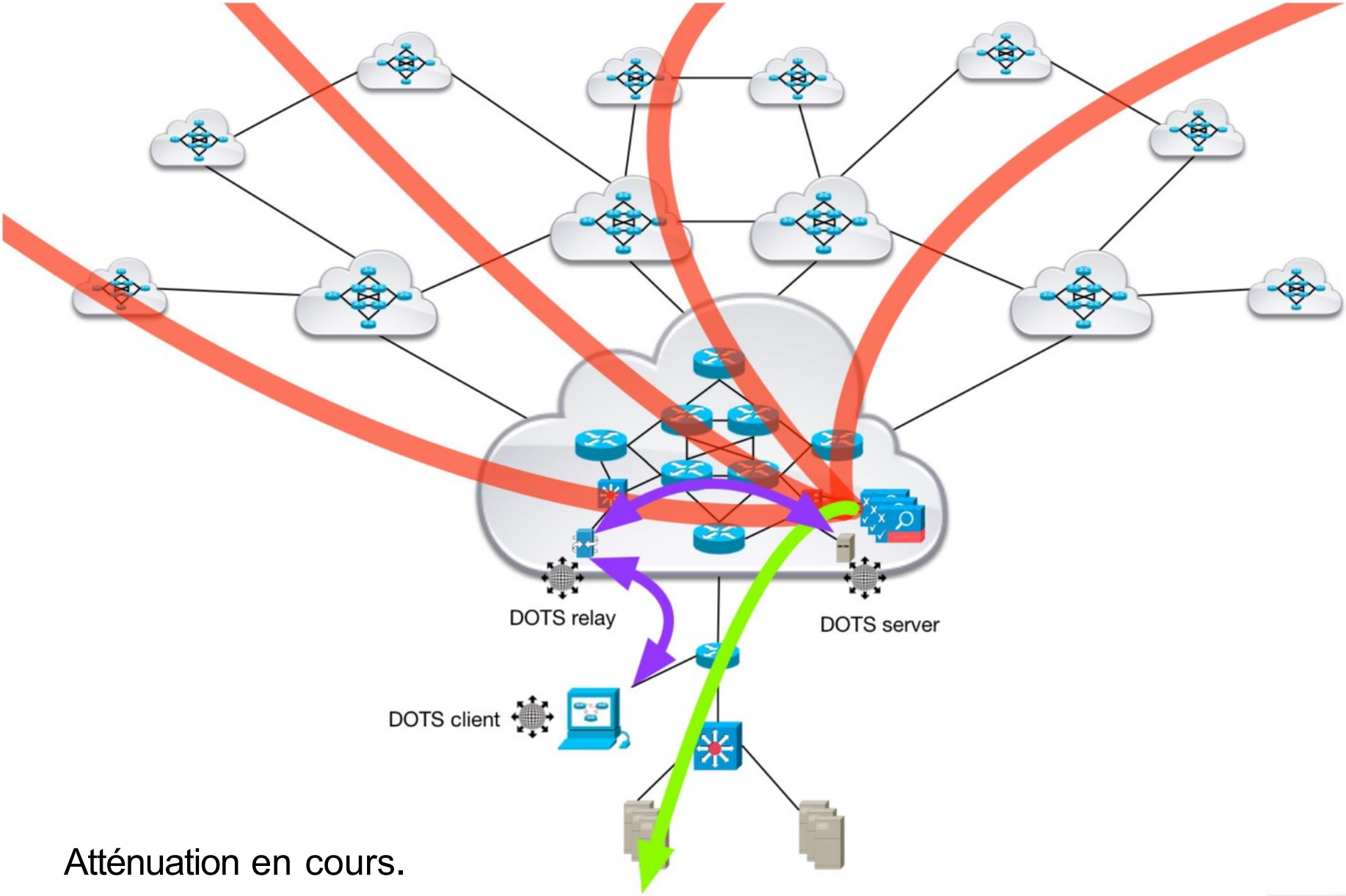
Atténuation en cours.



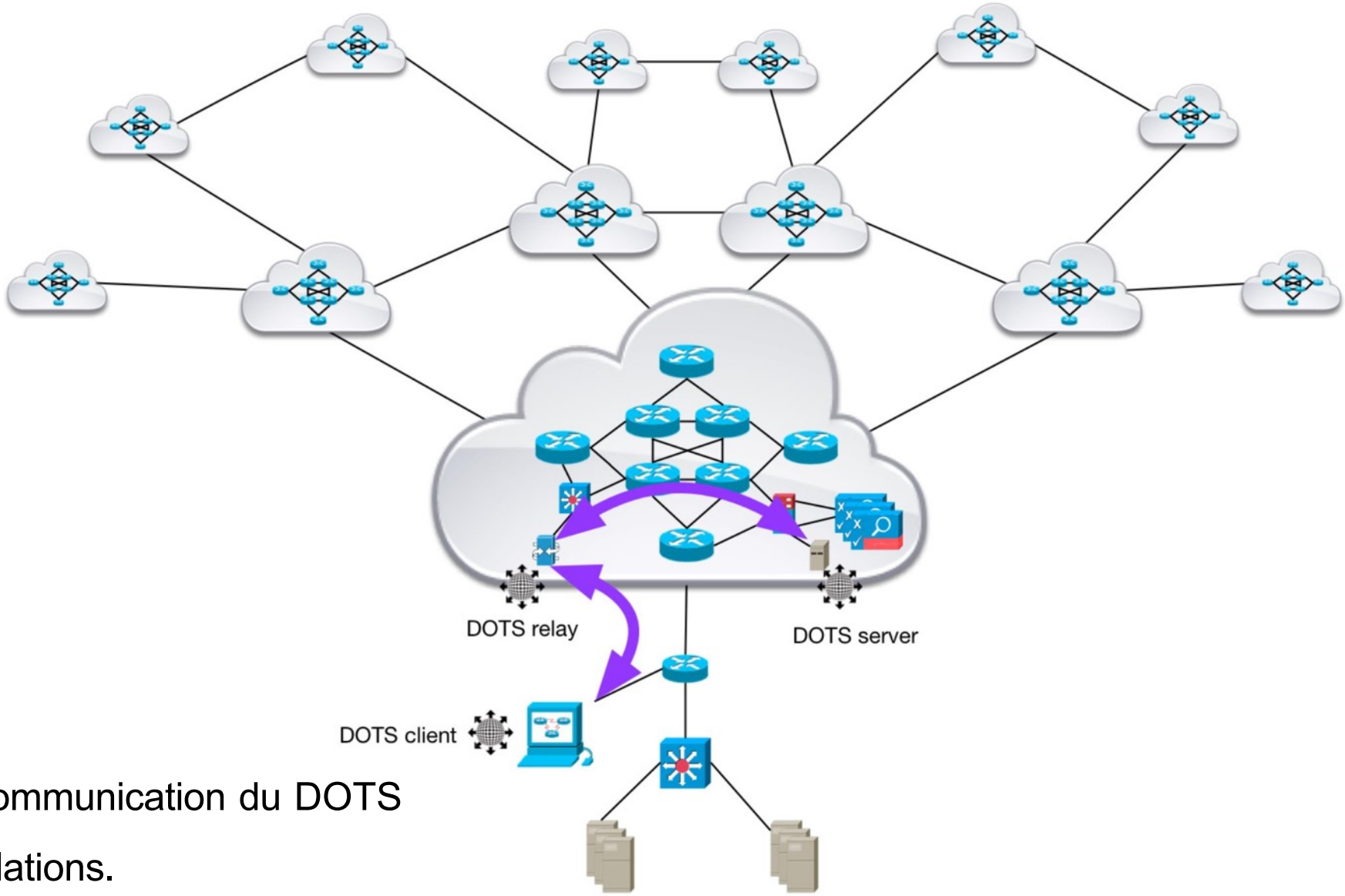
Communication du DOTS relations.

4.1.3 - Détection des télémétries d'acces/ Demandes de système de classification en amont Atténuation des DDoS


DOTS relay
DOTS server
DOTS client



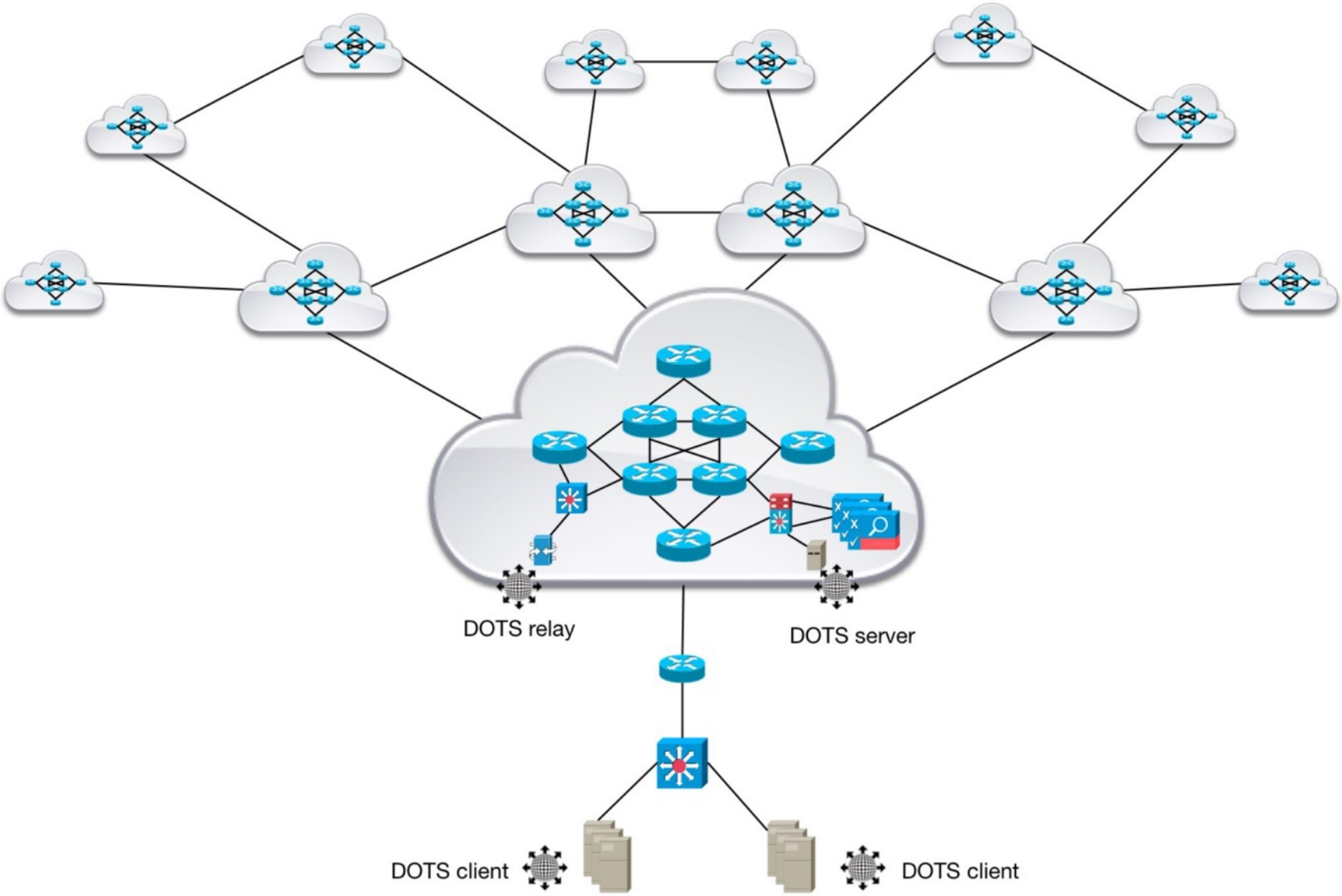
Atténuation en cours.

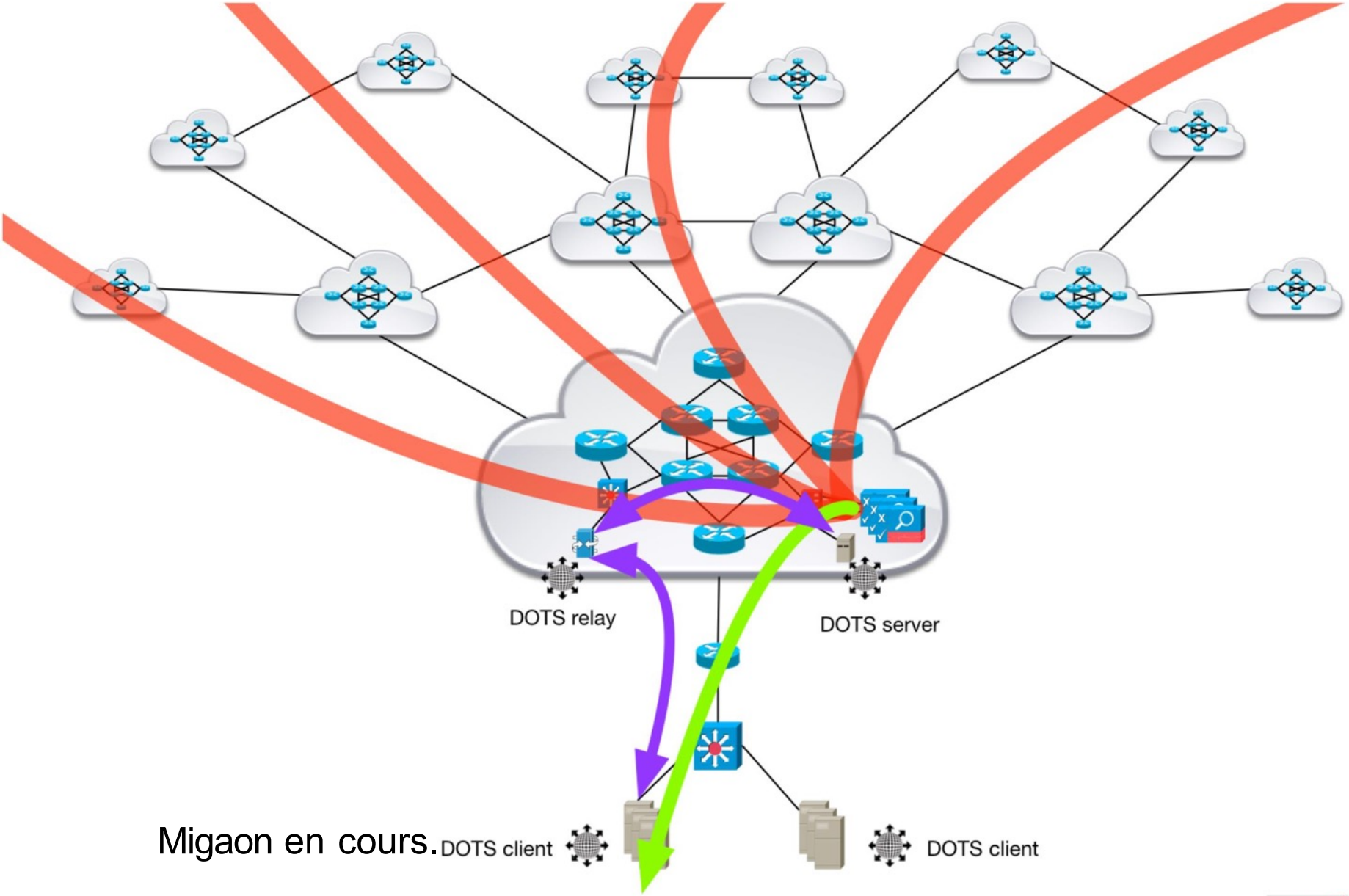


Communication du DOTS relations.

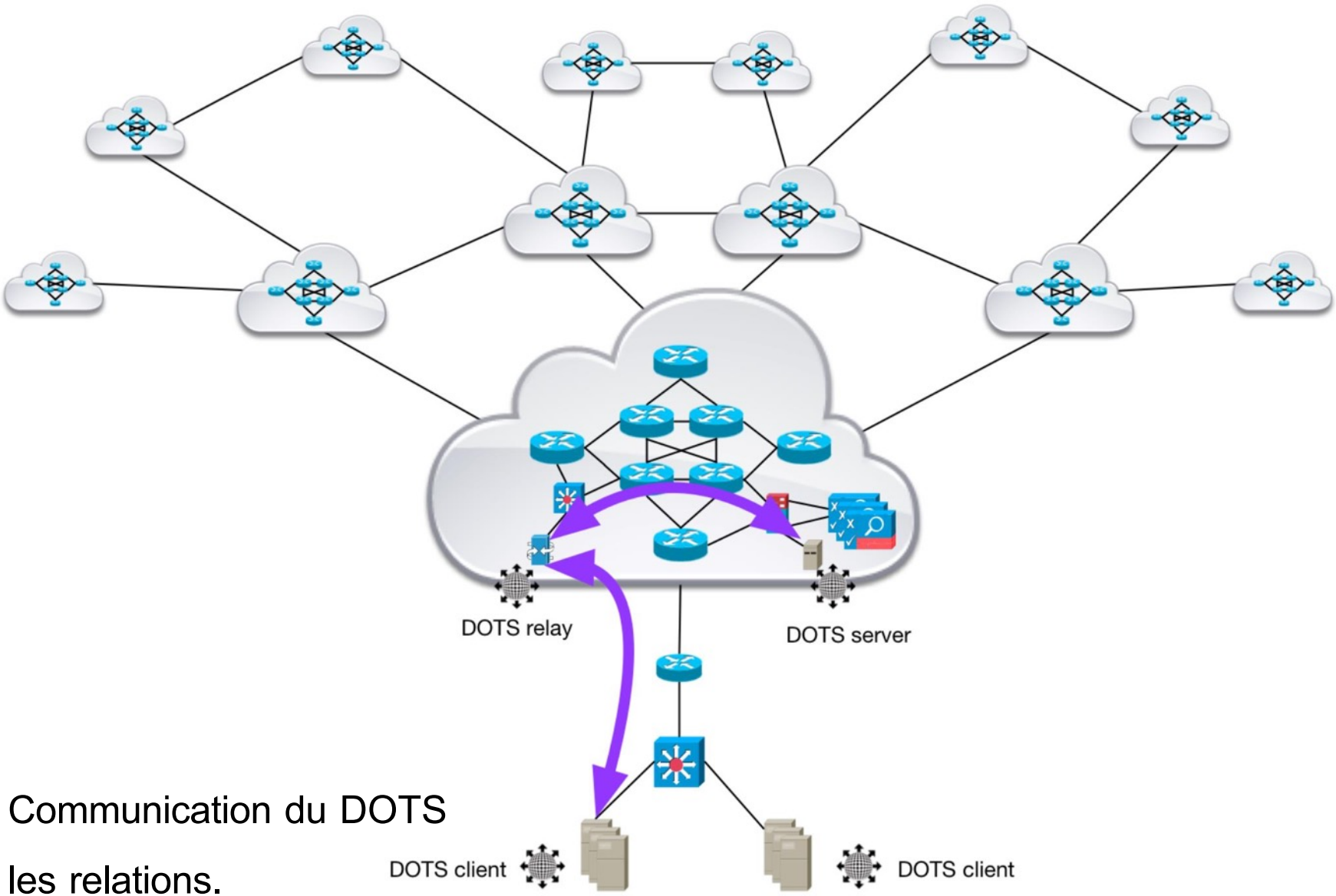
4.1.4 - Service/application ciblé(e)

Demande d'atténuation DDoS en amont


DOTS relay
DOTS server
DOTS client
DOTS client



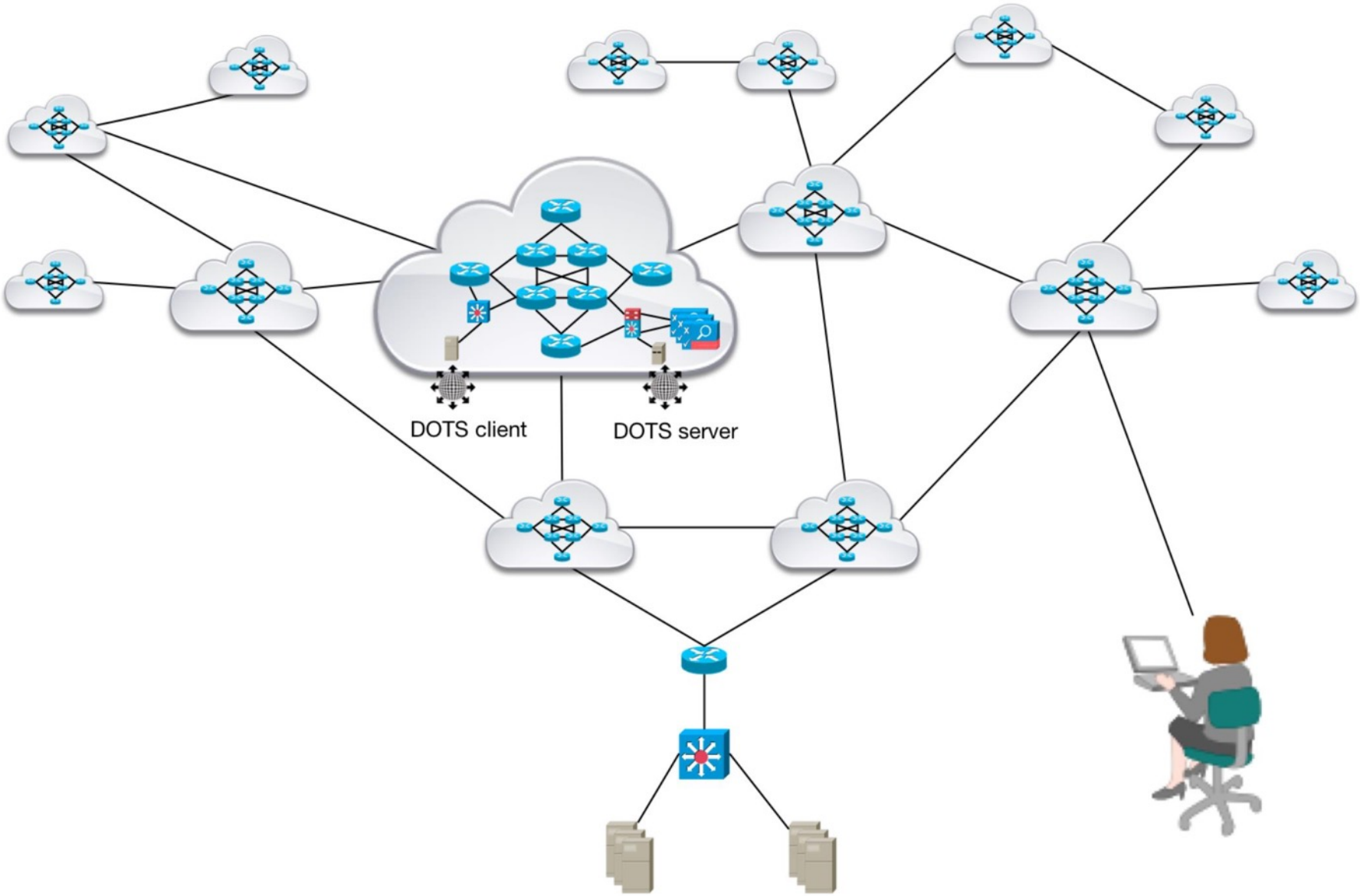
Migaon en cours.

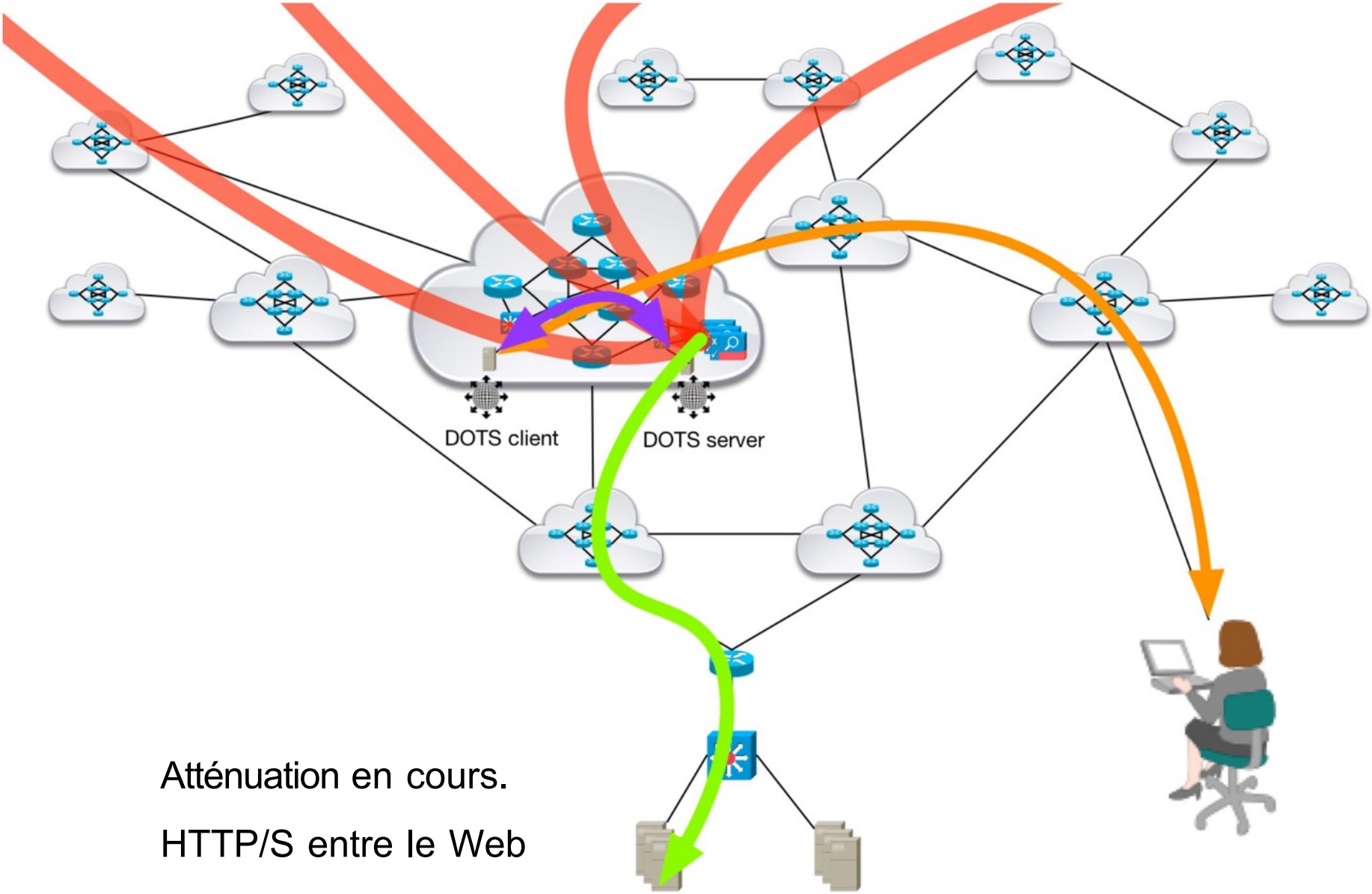


Communication du DOTS

les relations.

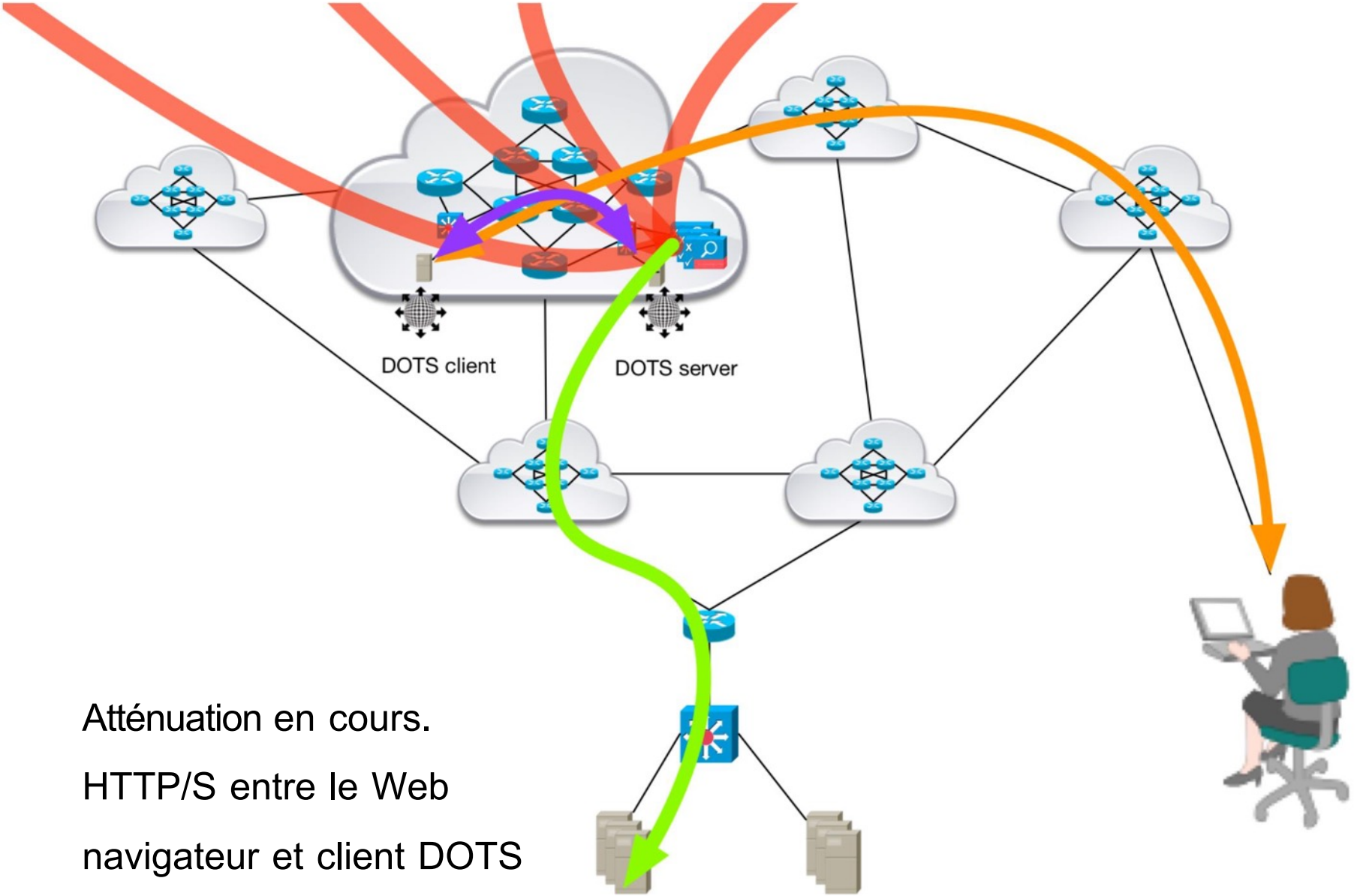
4.1.5 - Demande manuelle de portail Web à l'Atténuateur en amont


DOTS client
DOTS server



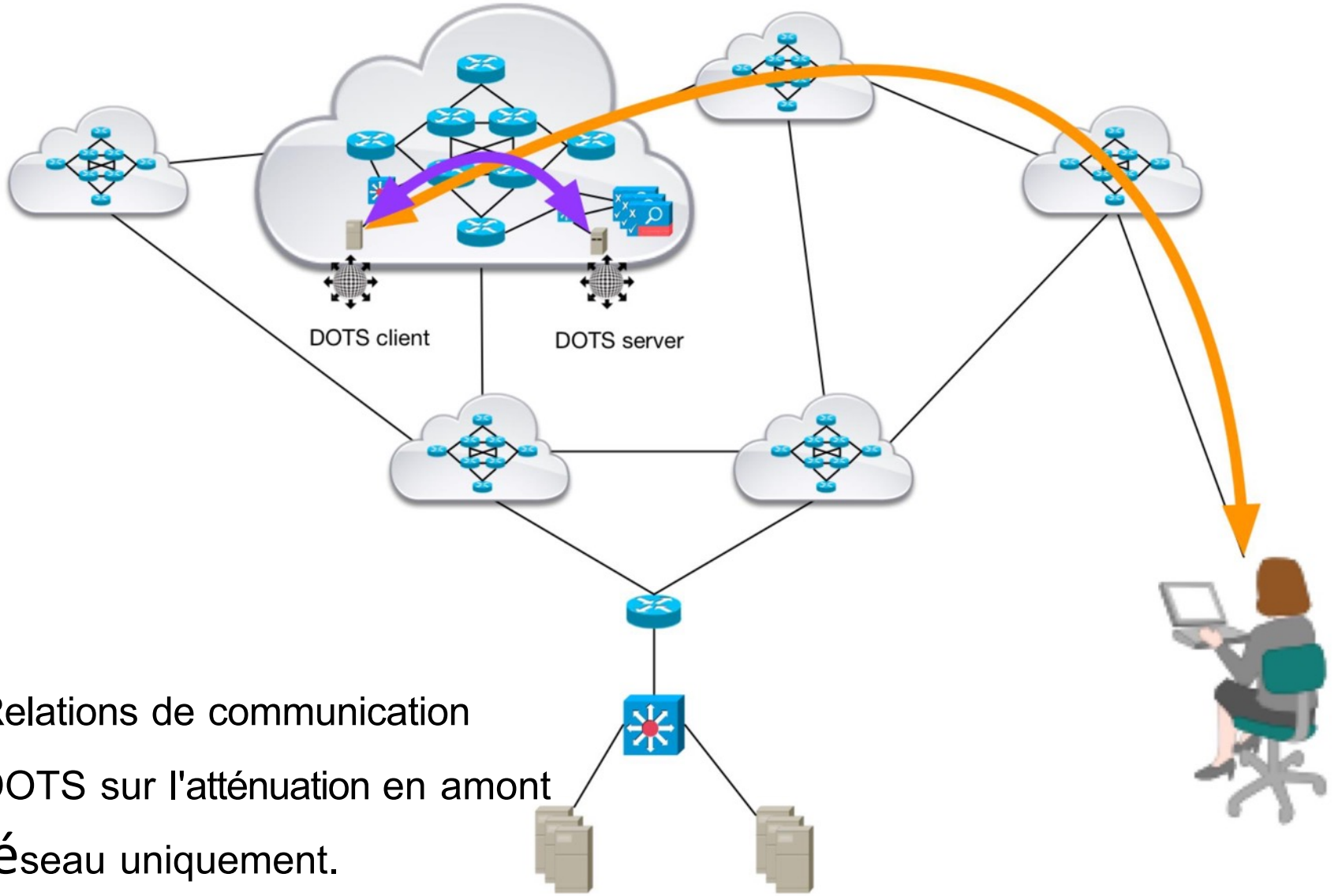
Atténuation en cours.

HTTP/S entre le Web navigateur et client DOTS sur le portail Web.



Atténuation en cours.

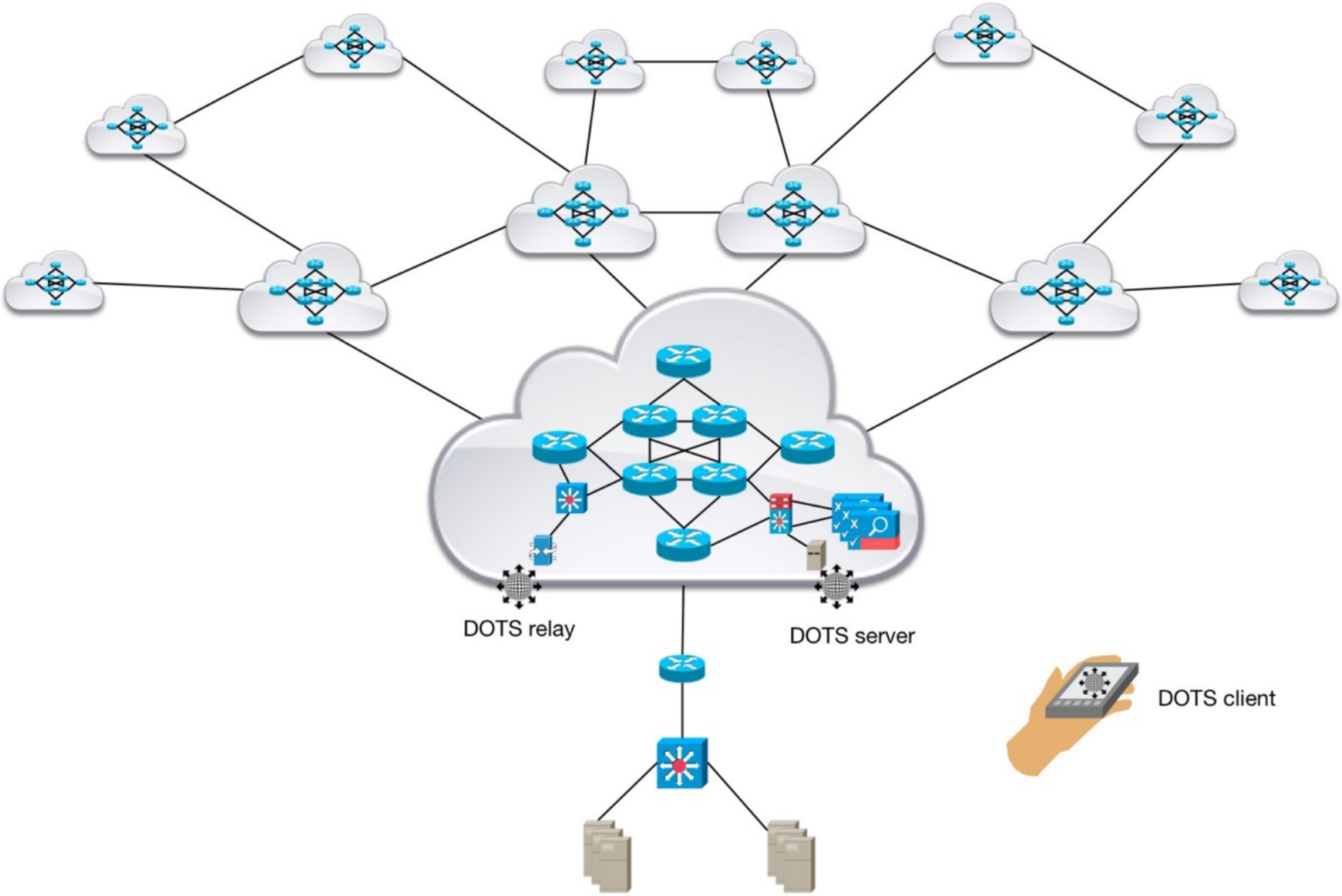
HTTP/S entre le Web navigateur et client DOTS sur le portail Web.

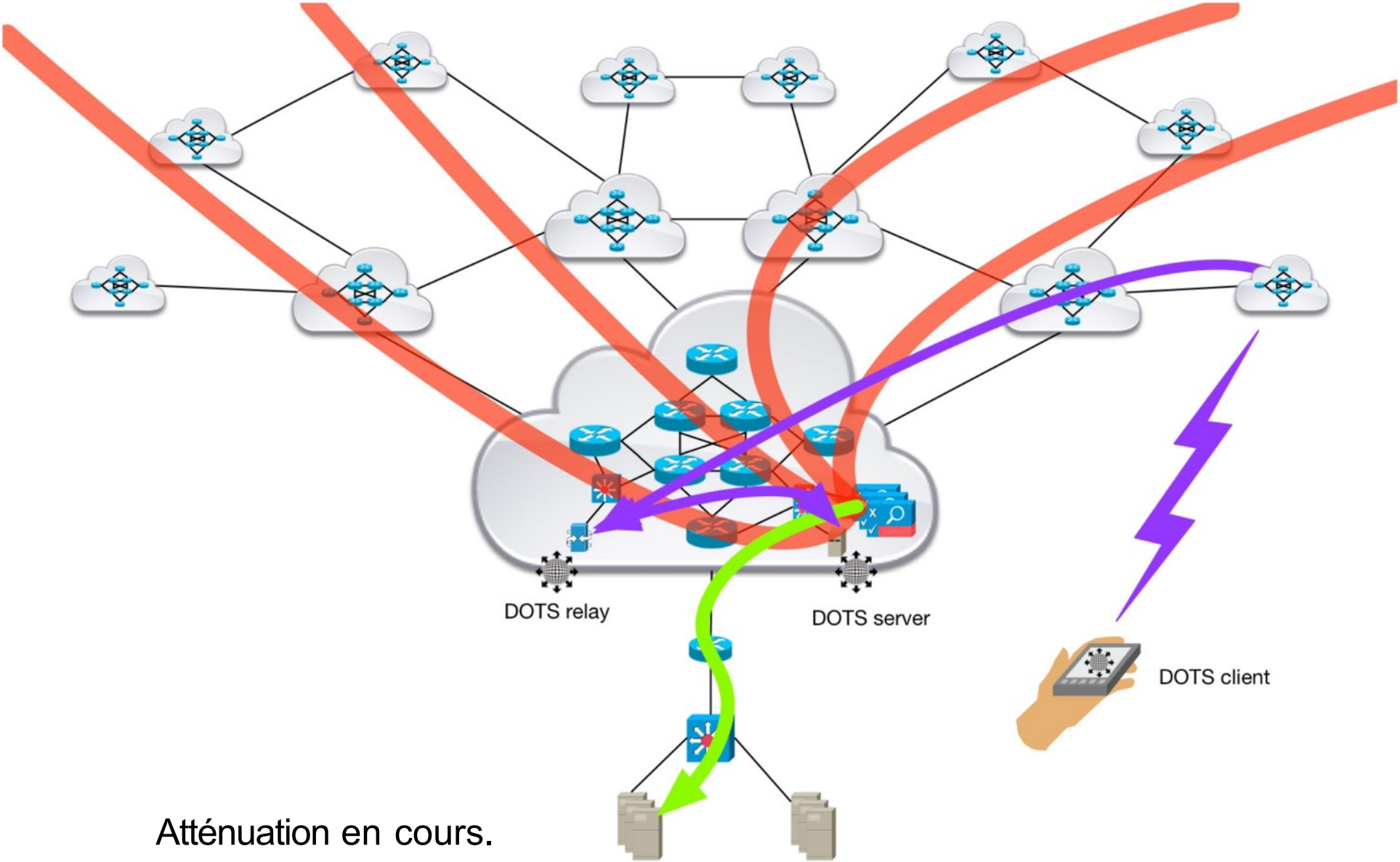


Relations de communication DOTS sur l'atténuation en amont réseau uniquement.

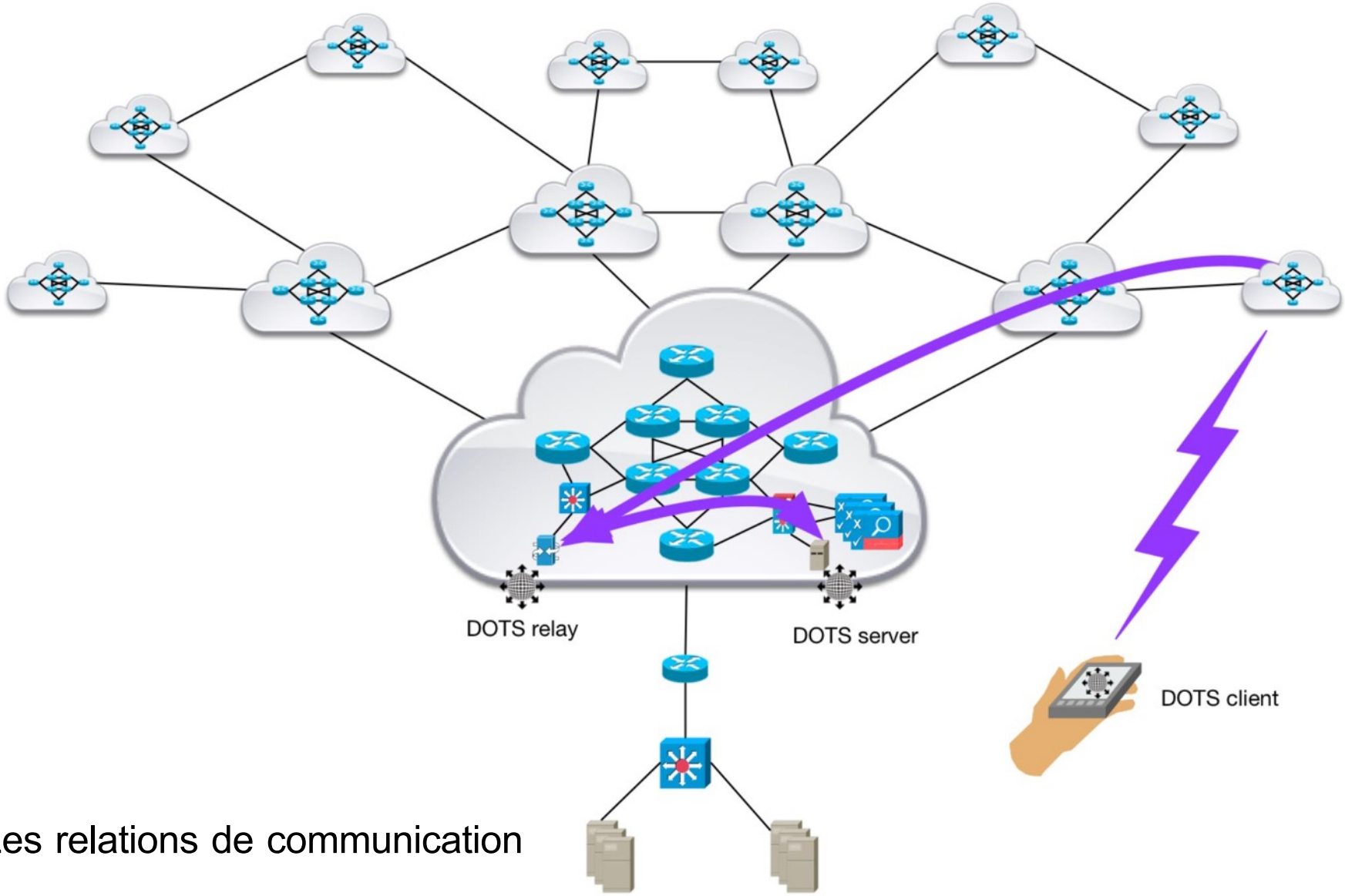
4.1.6 - Dispositif mobile manuel

Demande d'application en amont


DOTS relay
DOTS server
DOTS client



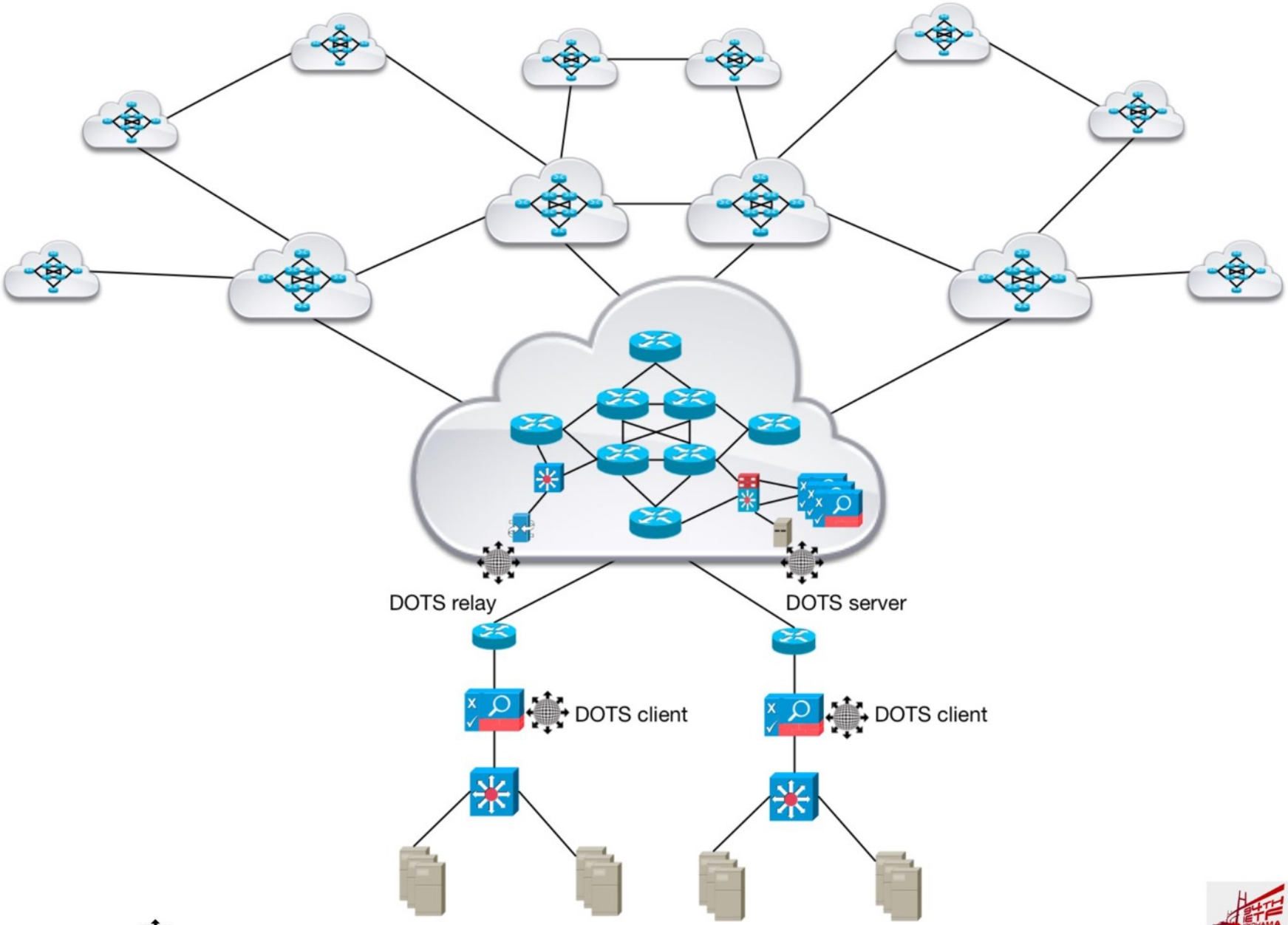
Atténuation en cours.

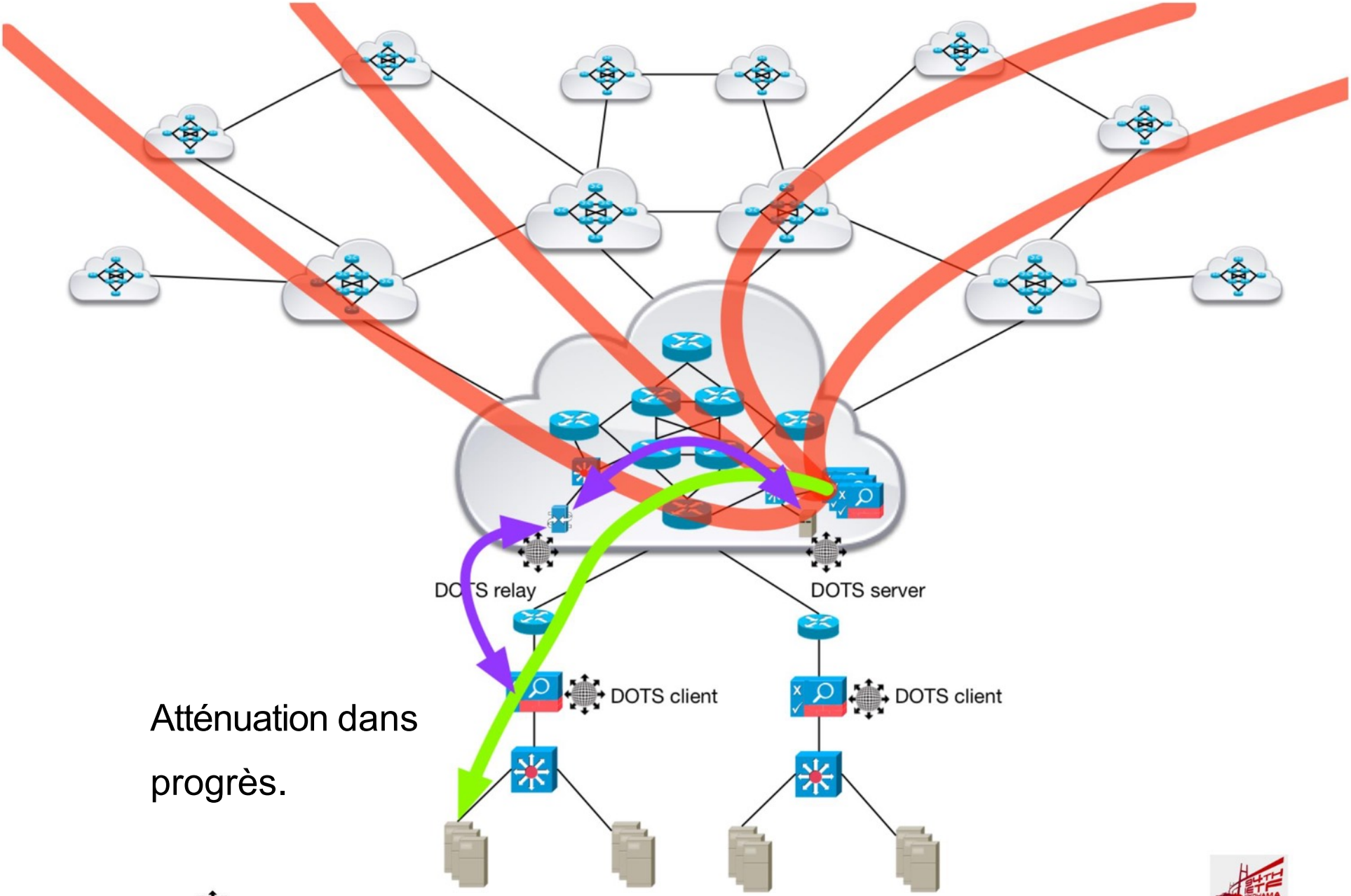


Les relations de communication du DOTS

4.1.7 - CPE ou PE non réussis

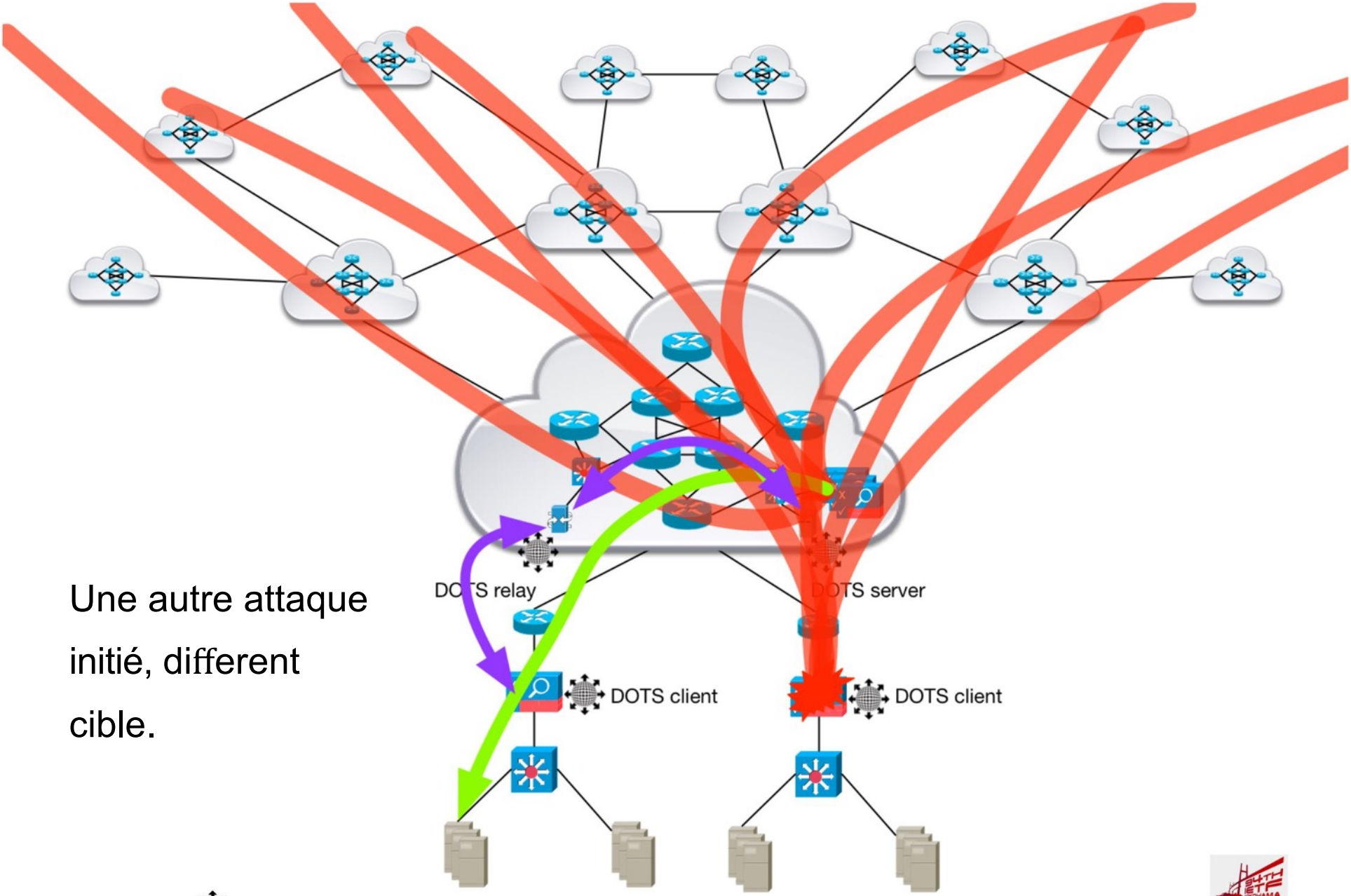
Demande d'atténuation pour l'amont


DOTS relay
DOTS server
DOTS client
DOTS client

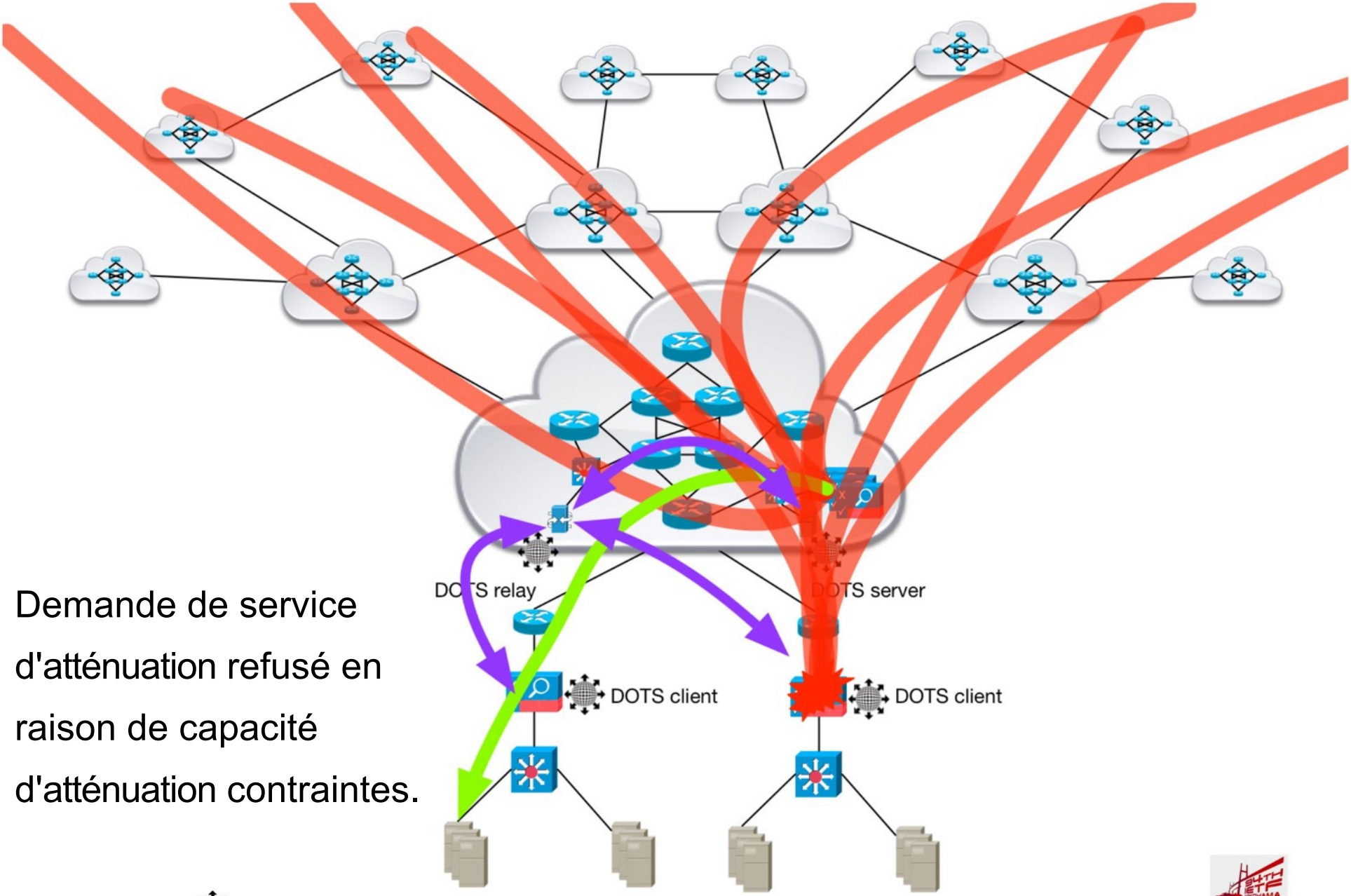


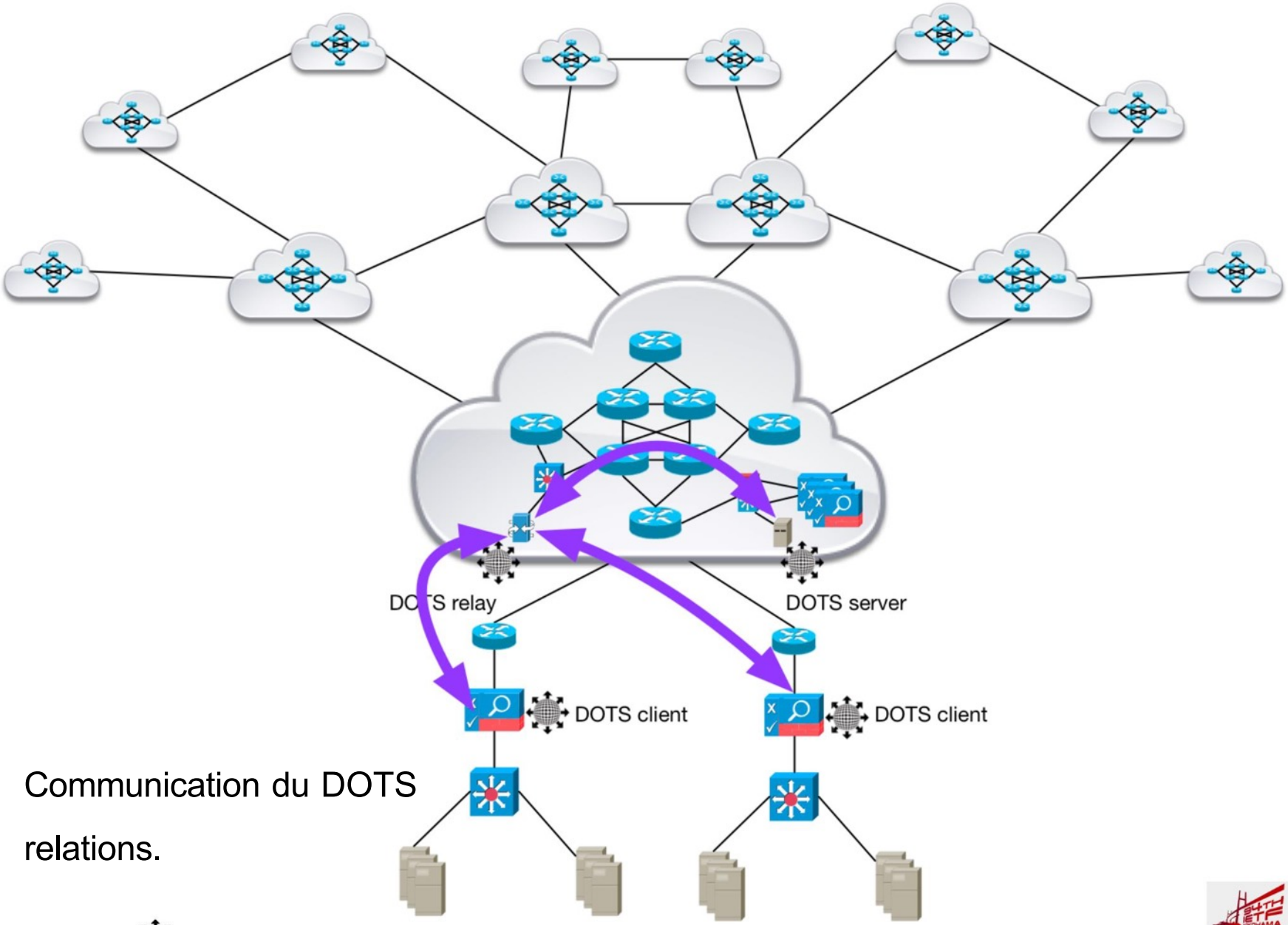
Atténuation dans progrès.

Une autre attaque initié, different cible.



Demande de service d'atténuation refusé en raison de capacité d'atténuation contraintes.





Communication du DOTS relations.

4.2 - Cas d'utilisation auxiliaires

4.2.1 - Auto-enregistrement

- Demandes d'atténuation des attaques, réponses et état d'avancement messages, le DOTS peut également être utile pour l'administration tâches.

- Les tâches administratives constituent un obstacle important à l'efficacité Atténuation des DDoS.

- Les clients du DOTS disposant des informations d'identification appropriées peuvent s'inscrire automatiquement avec les serveurs DOTS sur les réseaux d'atténuation en amont.

- Cela facilite l'intégration des services d'atténuation des attaques DDoS, déplacements/ajouts/modifications.

4.2.2 - Provisionnement automatique des contre-mesures DDoS

- Le provisionnement des contre-mesures DDoS est aujourd'hui une tâche largement processus manuel, les erreurs et l'inefficacité peuvent être problématiques.

- Cela peut conduire à des mesures d'atténuation DDoS inadéquates des services qui, souvent, ne sont pas optimisés pour les actifs sous protection contre les DDoS. La rapidité de l'atténuation, l'efficacité en souffre.

- L'intégration des organisations au cours d'une attaque - un problème trop souvent rencontré situation commune - peut être très difficile.

- La nature "autodescriptive" de l'enregistrement du système DOTS et les demandes de statut d'atténuation peuvent être exploitées pour automatiser le processus de sélection, d'approvisionnement et de réglage des contre-mesures.

- Retour d'information des clients du DOTS sur l'efficacité des mesures d'atténuation lors d'une attaque peut être exploitée en temps reel réglage et optimisation de l'atténuation.

4.2.3 - Notification informationnelle d'une attaque DDoS à des tiers

- En plus des demandes de service des organisations sous aux atténuateurs en amont, DOTS peut être utilisé pour envoyer notification des attaques DDoS et messages d'état aux intéressés et des tiers autorisés.

- Dans certaines circonstances, il peut être bénéfique d'automatiser fournir des notifications d'attaque et des messages d'état econdaire ou des fournisseurs d'atténuation de "secours" tertiaires, la sécurité les chercheurs, les vendeurs, les organismes d'application de la loi, les organismes de réglementation, agences, etc.

- Tout partage d'informations avec des tiers doit n'ont lieu que dans le respect de toutes les lois pertinentes, les règlements, les obligations contractuelles, le respect de la vie privée et les accords de confidentialité.

Prochaines étapes pour les cas d'utilisation