PDP : ROUTAGE VERS TROU NOIR PILOTÉ À DISTANCE

25 janvier 2018

Université de Bordeaux

CHAUVEAU Pierre
BRISSET Rémi
MASSAMIRI Michel
PERUZZETTO Enzo

Table des matières

1 Présentation du projet

1.1 Intitulé

L'objectif de ce projet est de développer un outil permettant à un administrateur réseau de définir à distance à partir d'un client Web, des routes menant vers des trous noirs pour dévier des attaques réseaux. Ces routes seront envoyées à un serveur de route qui les diffusera auprès de tous les serveurs BGP du domaine. Le logiciel devra être implémenté en Javascript et du côté serveur il devra piloter le logiciel ExaBGP écrit en Python. L'application Web devra être de type RESTful et elle s'appuiera éventuellement sur un framework JS. Elle devra supporter le routage vers trou noir par la destination, par la source et par la communauté BGP.

1.2 Le routage vers trou noir [Sys05]

La déviation des routes vers un trou noir, aussi appelée "Remotely-Triggered Black Hole (RTBH)" en anglais, est une technique qui permet de faire tomber (suspendre) un trafic provenant d'une source étant indésirable, avant que ce dernier puisse entrer dans un réseau protégé.
Cette technique est appliquée sur un routeur BGP(Border Gateway Protocol)qui lui, utilise le protocole TCP afin d'échanger des informations de routage avec des autres routeurs BGP.

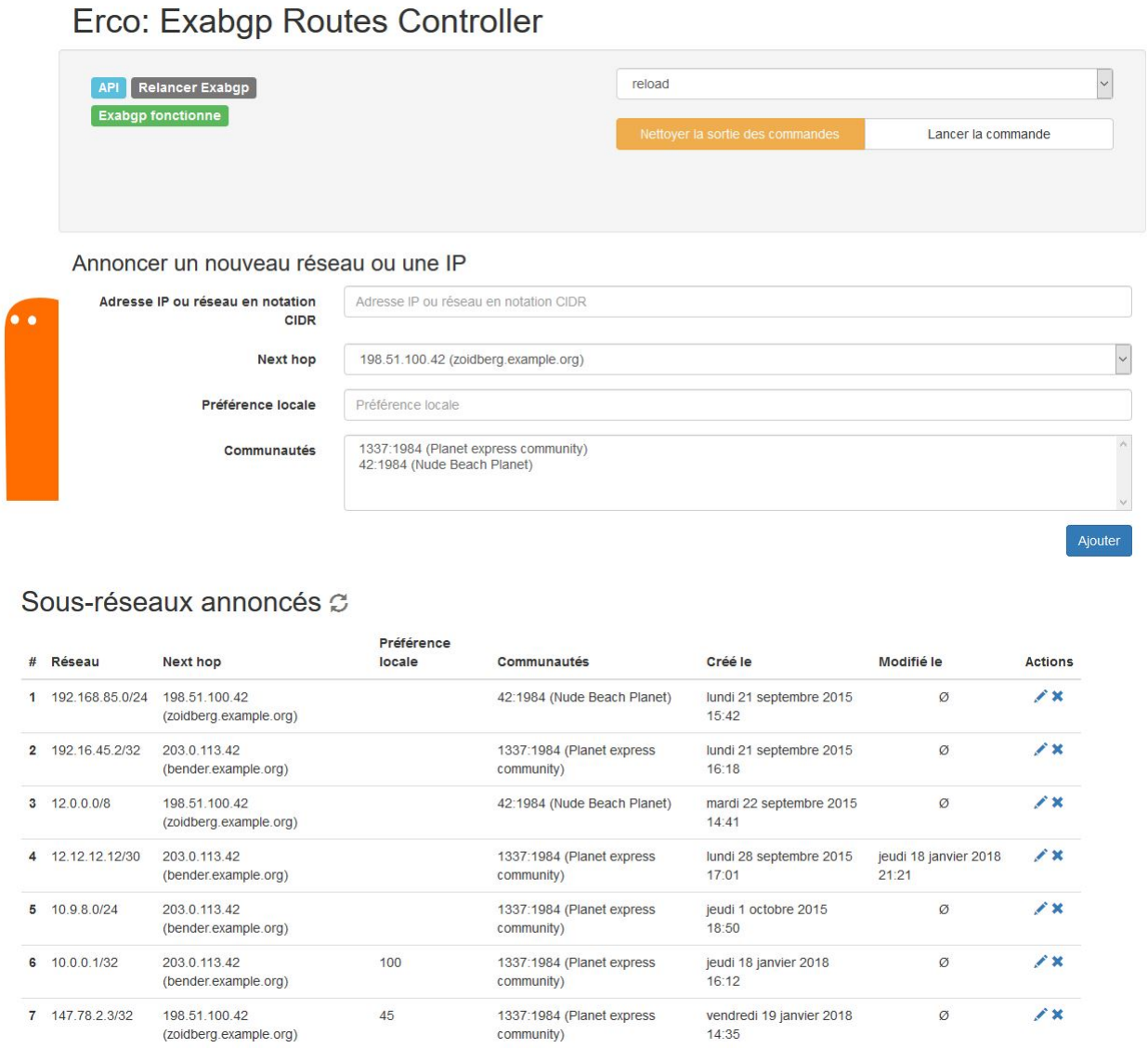
Le routage vers trou noir est essentiellement utilisé pour défendre ou proprement dit pour atténuer les attaques DDoS (distributed-denial-of-service). Les trous noirs sont placés principalement dans un réseau pour lequel, on peut dévier et/ou suspendre le trafic lorsque le système détecte une attaque.
Pour que le système puisse dévier des router, il se base sur l'adresse IP de la destination ou bien de l'adresse IP source. Donc, il existe deux méthodologies :

- **Destination-Based Remotely Triggered Black Hole Filtering** : On rend l'adresse IP de la destination inaccessible, en déviant toutes les routes allant à cet adresse vers le trou noir.
- **Source-Based Remotely Triggered Black Hole Filtering** : Dans ce scénario, si le trafic provenant d'une adresse IP est susceptible d'être une attaque, alors, tout trafic lié à cet adresse IP serait suspendu. Cela veut dire que selon l'adresse source IP, cette dernière ne peut pas avoir accès à sa destination. En outre, on fait tomber tous les chemins partants d'une adresse IP source précise.

2 Analyse de l'existant

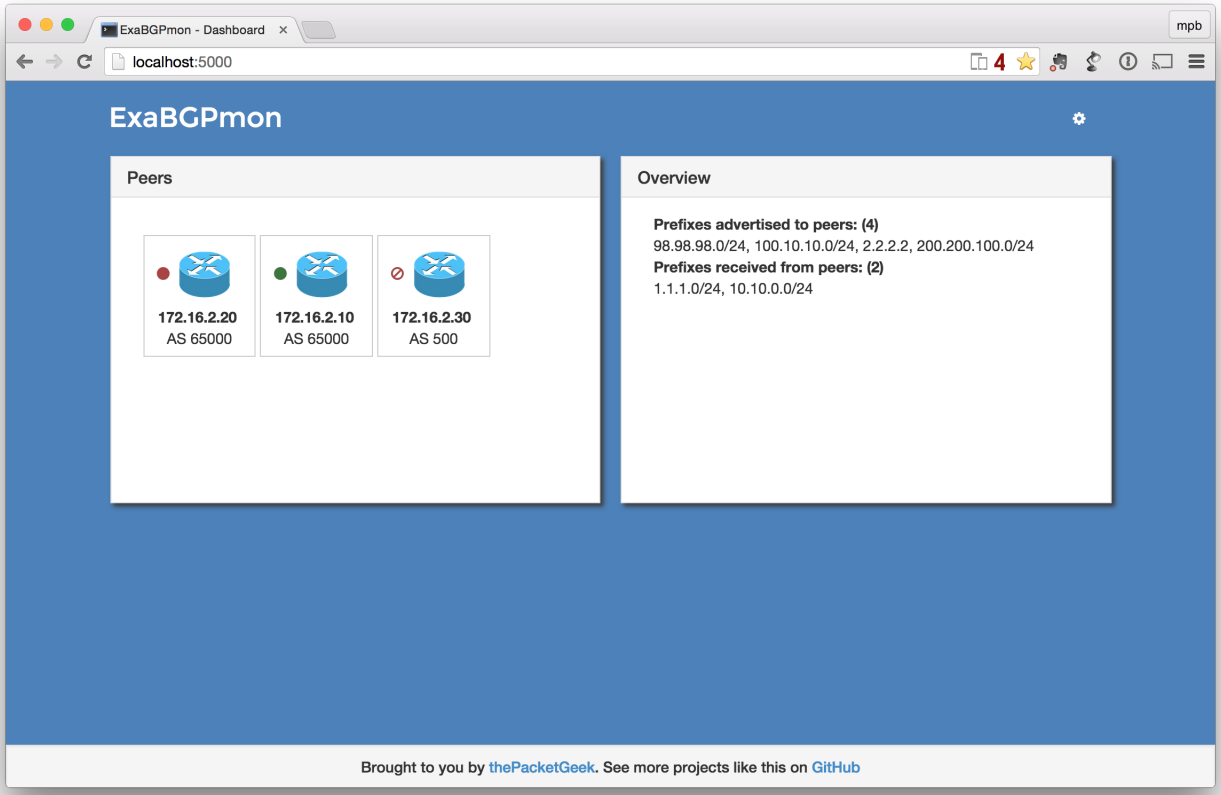
2.1 Erco.xyz [Did15]

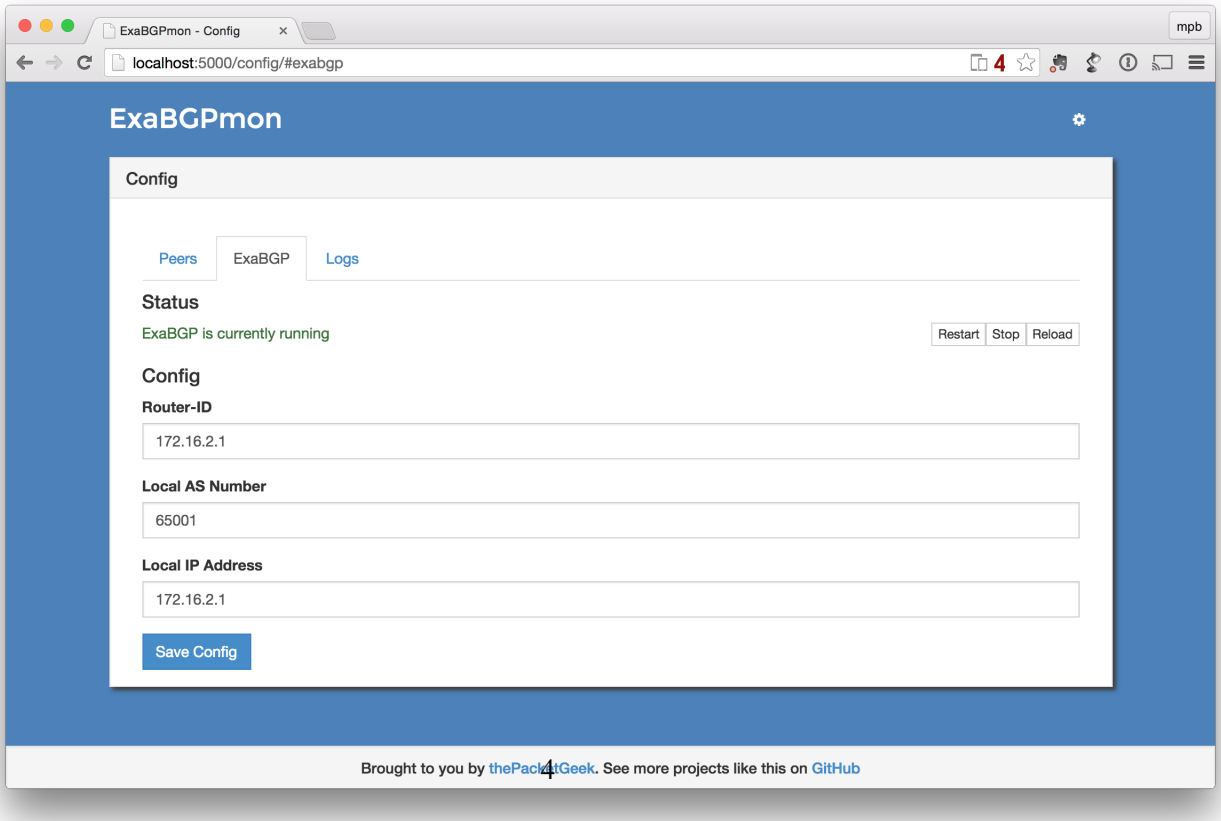
Erco est un outil initialement développé à l'Université de Lorraine facilitant la configuration des routes réseau avec Exabgp en réécrivant une partie du fichier de configuration d'Exabgp. Erco fournit une API RESTful et une interface web utilisateur. L'interface web permet de facilement : annoncer un nouveau réseau ou IP, modifier ou supprimer une route, envoyer des commandes à Exabgp(reload, show routes show neighbors et version)



#	Réseau	Next hop	Préférence locale	Communautés	Créé le	Modifié le	Actions
1	192.168.85.0/24	198.51.100.42 (zoidberg.example.org)		42:1984 (Nude Beach Planet)	lundi 21 septembre 2015 15:42	Ø	
2	192.16.45.2/32	203.0.113.42 (bender.example.org)		1337:1984 (Planet express community)	lundi 21 septembre 2015 16:18	Ø	
3	12.0.0.0/8	198.51.100.42 (zoidberg.example.org)		42:1984 (Nude Beach Planet)	mardi 22 septembre 2015 14:41	Ø	
4	12.12.12.12/30	203.0.113.42 (bender.example.org)		1337:1984 (Planet express community)	lundi 28 septembre 2015 17:01	jeudi 18 janvier 2018 21:21	
5	10.9.8.0/24	203.0.113.42 (bender.example.org)		1337:1984 (Planet express community)	jeudi 1 octobre 2015 18:50	Ø	
6	10.0.0.1/32	203.0.113.42 (bender.example.org)	100	1337:1984 (Planet express community)	jeudi 18 janvier 2018 16:12	Ø	
7	147.78.2.3/32	198.51.100.42 (zoidberg.example.org)	45	1337:1984 (Planet express community)	vendredi 19 janvier 2018 14:35	Ø	

2.2 ExaBGPmon





2.3 ExaBGP

ExaBGP est un outil open source écrit en Python qui permet d'interagir avec les réseaux BGP. Le logiciel peut injecter des routes annoncés dans les réseaux. ExaBGP offre un API contenant plusieurs commandes afin de manipuler les routeurs BGP. On peut aller voir la liste des commandes dans l'API d'ExaBGP :

`https://github.com/Exa-Networks/exabgp/wiki/Controlling-ExaBGP-:-interacting-from-the-API`

2.4 Meteor.JS [Met17]

Meteor.JS est un framework open-source javascript, Node.JS qui permet l'élaboration d'une application web de type RESTful. Elle permet de développer le client et le serveur de l'application web avec le même langage.

client javascript RESTfull, nous plus facile package, serveur cache client.

3 Cahier des Charges

Après avoir analysé les outils existants et aussi les besoins du client, on s'est rendu compte que le client aura besoin d'une application Web de type RESTful pour pouvoir interagir avec ExaBGP.
Par conséquent, notre application Web s'appuiera sur le framework Meteor JS.

3.1 Besoins fonctionnels

- Ajouter/Supprimer une route (admin) :
  - L'administrateur réseau peut annoncer un réseau ou une adresse IP.
  - L'administrateur réseau peut ainsi supprimer une adresse IP ou un réseau.
  - La possibilité d'attribuer une communauté à un router ou bien un réseau lors de l'ajout.
  - Les opérations de la suppression et de l'ajout seront réservées à l'administrateur de l'application.
- Vérifier le bon fonctionnement ExaBGP (admin) :
  - À l'aide d'un élément dynamique, l'administrateur peut observer l'état du ExaBGP avant de lancer des commandes.
  - Envoyer un message d'avertissement(popup)quand ExaBGP est en panne ou ne tourne pas.
- Exécuter les différentes commandes de l'API de ExaBGP
  - (Utiliser la technique du Black hole selon une source IP ou bien une destination) : expliquer ça à l'aide d'un UML de Séquence.
  - Les différentes commandes d'ExaBGP.
- Relancer ExaBGP (admin)
- Rechercher des routes selon leurs préfixes, (adresse IP, communauté, destination) :
  - Une page web dans l'application dédiée à effectuer la recherche des routes selon leurs préfixes.
- Lister les routes :
  - L'utilisateur peut voir toutes les routes qui existent dans la base de données.
  - Le résultat sera découpé en plusieurs pages web pour facilité la lisibilité.

3.2 Besoins non fonctionnels

- Une base de données stockant les informations des routes :
  - Utiliser une base de données NoSQL(MongoDB)
- Certains packages de meteor.js
- Synchronisation du serveur web avec ExaBGP
- Sécurité, fiabilité (https...)
- Interface différente pour l'admin et l'utilisateur anonyme

4 Schéma de structure

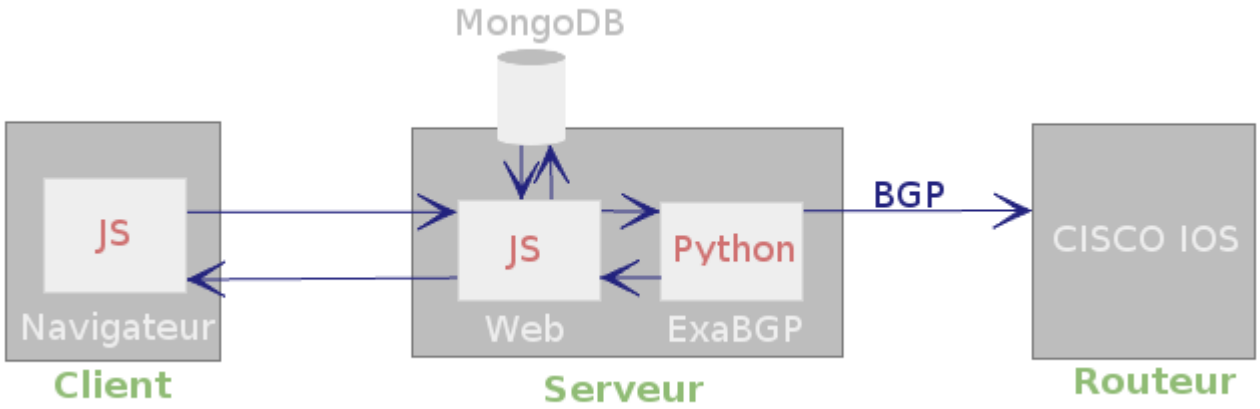


FIGURE 1: Schéma de structure

5 Diagramme de Gant

	semaine 5 : 5 fév / 9 fév	semaine 6 : 12 fév / 16 fé	semaine 7 : 19 fév / 23 fév	semaine 8 : 26 fév / 2 mars	semaine 9 : 27 fév / 3 mars	semaine 10 : 5 mars / 9 mars	semaine 11 : 12 mars / 16 mars	semaine 12 : 19 mars / 23 mars	semaine 13 : 26 mars / 30 mars	semaine 14 : 2 avr / 6 avr
ajouter/supprimer route					X					
supprimer adresse IP ou réseau				X						
attribution d'une communauté				X						
Lancer/Relancer ExaBGP		X								
état de ExaBGP		X								
Lister les route		X	X							
Executer les différentes commandes d'ExaBGP						X	X	X		
Recherche IP, Route par préfixe								X	X	X
connecter ExaBGP au serveur web		X								
Mise en place de machine virtuelle pour test	X	X	X							

Bibliographie

[Did15] Luc Didry. Erco : Exabgp routes controller. https://erco.xyz, 2015. [Accessed].

[Met17] Meteor.js. https://www.meteor.com/, 2017. [Accessed].

[Sys05] Cisco Systems. Remotely triggered black hole filtering— destination based and source based. https://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf, 2005. [Accessed].