PDP : ROUTAGE VERS TROU NOIR PILOTÉ À DISTANCE

30 janvier 2018

Université de Bordeaux

BRISSET Rémi
CHAUVEAU Pierre
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 [1] 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.

1.1.1 Définitions

Les **routes** sont définit par une adresse IP de destination, d'une adresse IP du prochain routeur (NextHop) puis une liste des Systèmes Autonomes traversé (AS).

Une **Communauté** est un système Autonomes :
"Un Système Autonomes est un ensemble cohérent de réseaux et de routeurs sous la responsabilité d'une autorité administrative [2]*."*

Un routeur BGP [3] est un routeur qui utilise le protocole BGP (Border Gateway Protocol). BGP s'appuie sur le protocole TCP, sur le port 179. Lorsque deux routeurs BGP forment une connexion TCP entre eux. Ces routeurs sont des routeurs homologues (voisins).

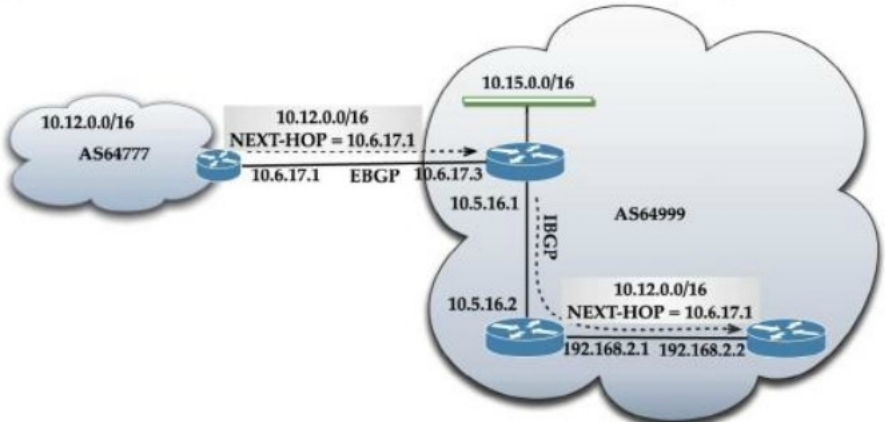
BGP est un protocole de type " Path Vector ". Les routeurs s'échangent des informations du type :

Adresse IP du réseau de destination	**Adresse IP du prochain routeur(next hop)**	**Liste des AS traversés pour atteindre le réseau**

Annoncer une route :
Les routeurs qui forment une connexion TCP afin d'échanger les données de routage BGP, sont des paires('peers') ou voisins('neighbors'). Les BGP 'peers' partagent alors les informations de routage BGP(Table de routage).
Normalement, BGP 'peers' mettent à jour leurs table de routage en utilisant la technique **UPDATE Message**, cela garantit que tous les BGPs aient la même version de la table de routage, et donc le numéro de version change pour tout changement effectué auprès n'importe quel 'peer'.

1. route BGP [BGP07]
2. Définition AS : `http://www.linux-france.org/prj/edu/archinet/systeme/ch65s02.html`
3. BGP `https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html`

Next-Hop[DM17] : Cette terme désigne l'adresse IP du prochain routeur auquel le paquet IP devrait être transmis afin que ce paquet IP puisse atteindre sa destination.
Afin d'illustrer le fonctionnement de l'attribut Next Hop, nous détaillons ce dernier sur un exemple :



Dans ce scénario, si la destination qu'on souhaite atteindre est le réseau : "10.12.0.0/16", donc, tout trafic allant à cette adresse, doit s'orienter vers le routeur "10.6.17.1". Cela veut dire que le prochain routeur (Next-Hop) du "10.12.0.0/16" est le "10.6.17.1".
L'adresse 10.12.0.0/16 est annoncé par le EBGP (External BGP) 10.6.17.1, et donc l'information est passé de la communauté "AS64777" à la "AS649999". Ensuite le UPDATE Message est passé aux voisins par le iBGP(internal BGP) afin que tous les BGP peers gardent la même version de la table de routage.

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.

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]

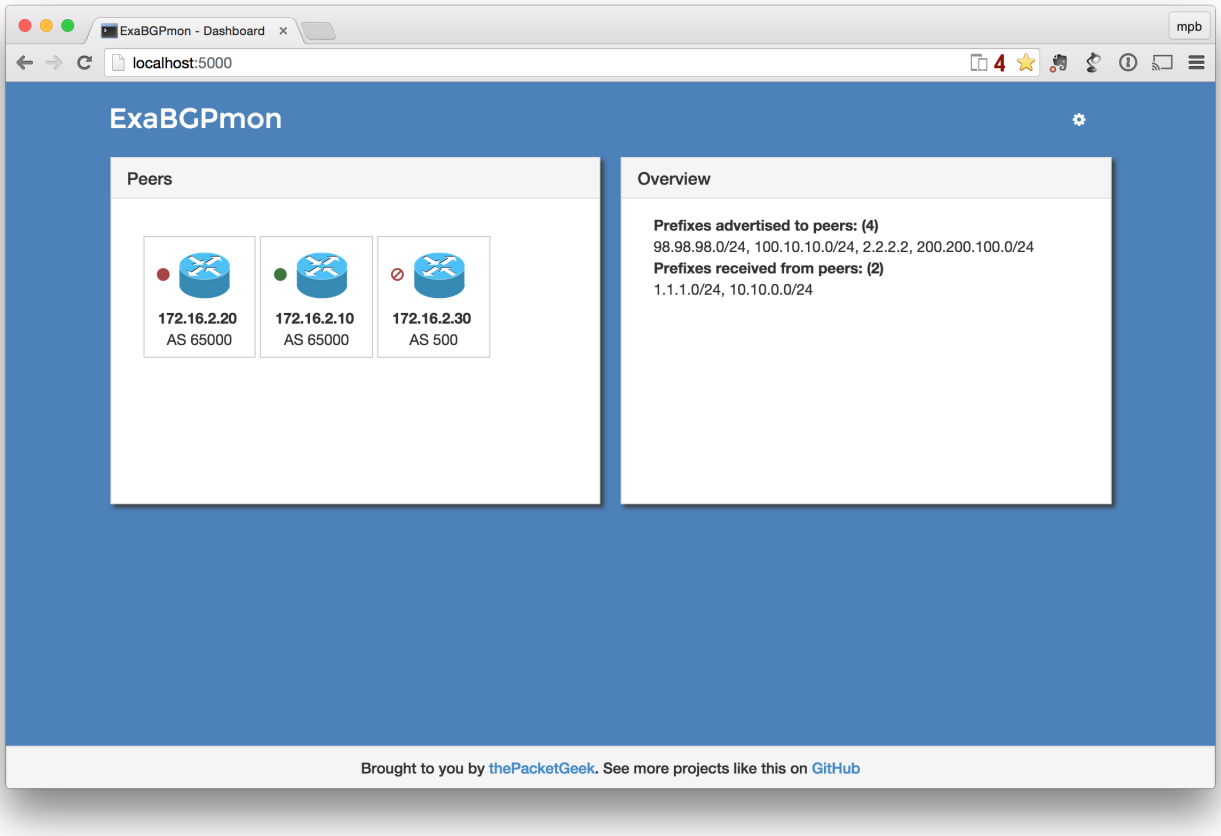
Erco est un outil initialement développé à l'Université de Lorraine facilitant la configuration des routes réseau avec Exabgp en réécrivant une partie du fichier de configuration d'Exabgp. Erco fournit une API RESTful et une interface web utilisateur. L'interface web permet de facilement : annoncer un nouveau réseau ou IP, modifier ou supprimer une route, envoyer des commandes à Exabgp(reload, show routes show neighbors et version).
L'esthéthique et les fonctionnalités de cette interfaces web sont utile pour notre projet. En effet, les bouttons "Relancer Exabgp" et "Exabgp fonctionne" sont exactement se que l'on a besoin. De plus notre section "lancer commande" ressemblera à celui de Erco mais avec plus de commande exécutable et un retour de message de Exabgp plus précis pour chaque commande. Nous prendrons aussi exemple sur Erco pour executer les commandes avec arguments sous forme de formulaire, et afficher les routes sous forme de tableaux, de liste.

Sous-réseaux annoncés

#	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

ExaBGPmon est une interface web sur le même principe que Erco.xyz, mais nous n'allons rien retenir de se site car il est moins intuitif et ergonomique que Erco et propose les mêmes fonctionnalités.



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`

Et apprendre à l'utiliser avec les tutos suivants :

`https://thepacketgeek.com/series/influence-routing-decisions-with-python-and-exabgp/`

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.
Notre client voulait une interface web développé en JavaScript de type Restful. Pour un déploiement et implémentation plus rapide de cette interface nous avons décidé d'utiliser le framework open-source Meteor.js qui réponds à ses besoins. De plus avec la possibilité d'utiliser des packages (extensions) de meteor.js nous pouvons implémenter certaines choses plus rapidement.

Les packages utilisés sont :

- twbs :bootstrap
- ian :accounts-ui-boostrap-3
- iron :router

Voici quelques liens pour pouvoir s'informer plus sur Meteor.js :

`http://meteortips.com/first-meteor-tutorial/`
`http://meteortips.com/second-meteor-tutorial/`
`http://www.meteor-tuts.com/`
`https://www.meteor.com/tutorials/react/creating-an-app`
Documentation : `http://docs.meteor.com/#/full/`

2.5 MongoDB

[Mon]

MongoDB est une base de données open source orientée documents qui fournit de hautes performances, une haute disponibilité, et mise à l'échelle automatique.

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

3.1.1 Administrateur

- Ajouter/Supprimer une route :
  - Annoncer un réseau ou une adresse IP.
  - Supprimer une adresse IP ou un réseau.
  - Attribuer une communauté à un router ou bien un réseau lors de l'ajout.
- Vérifier le bon fonctionnement ExaBGP :
  - À l'aide d'un élément dynamique, 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)

3.1.2 Administrateur et client

- 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

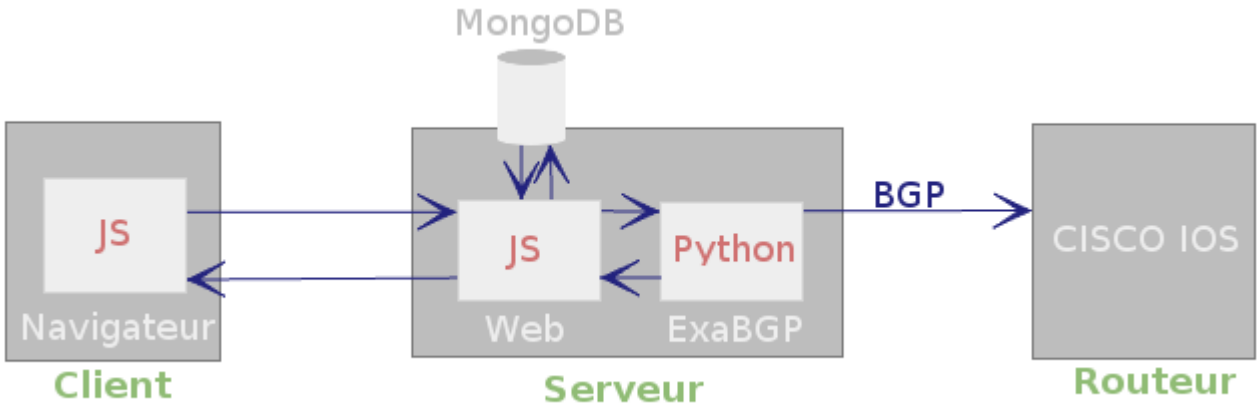
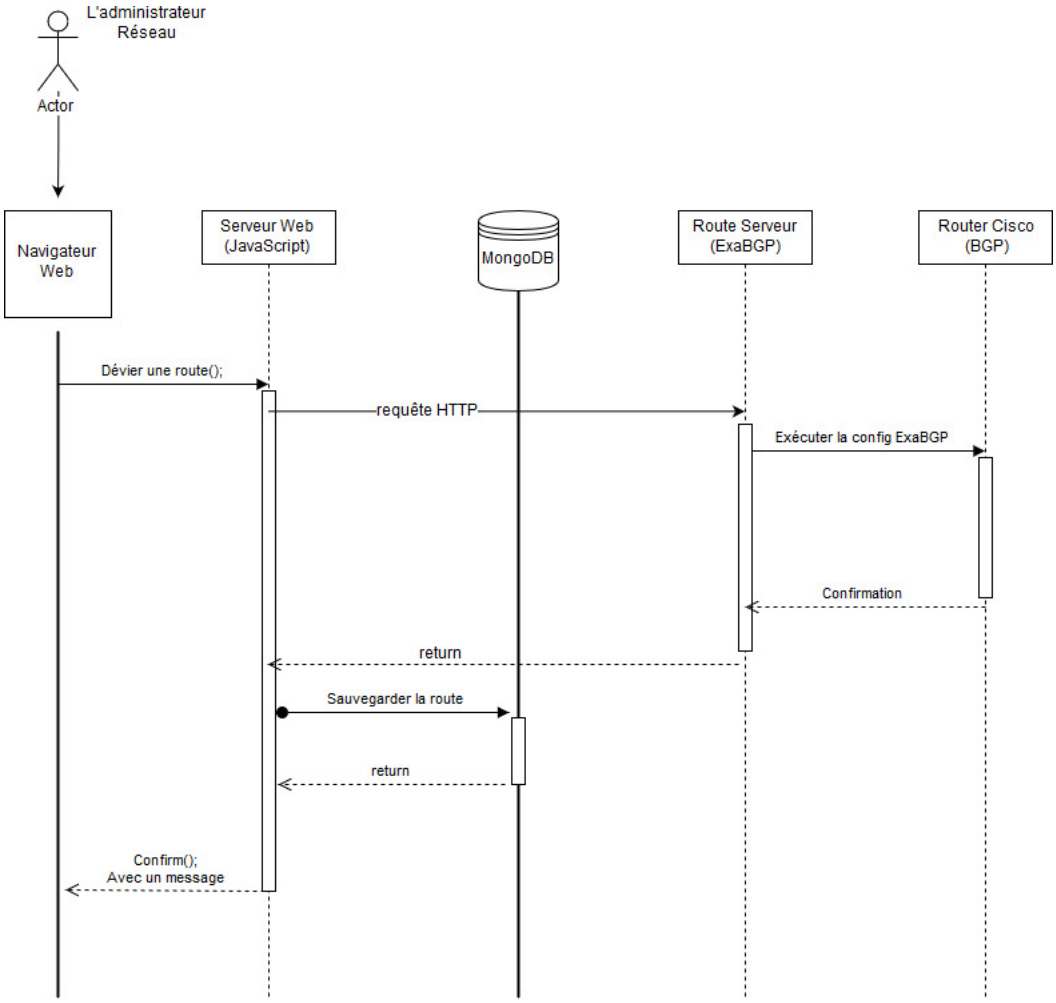


FIGURE 1: Schéma de structure

5 Scénario d’utilisation

6 Diagramme de séquence

Nous représentons le scénario de la déviation d'une route vers un trou noir en utilisant le diagramme de séquence.
L'utilisateur de l'application web dans cet exemple est l'administrateur réseaux. On suppose que l'administrateur réseaux veut dévier une route par son adresse IP source.
Lorsque l'opération est terminé, donc l'application web confirme que c'est fait, la route est ensuite serait stockée dans la base de données afin que le client puisse aller consulter les routes qui ne sont pas accessibles.



7 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

[BGP07] Le routage dynamique avec bgp. `http://www.linux-france.org/prj/edu/archinet/systeme/ch69.html`, 2007. [Accessed January].

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

[DM17] Karthik Ramasamy Deep Medhi. *Network Routing Algorithms, Protocols, and Architectures*. Morgan Kaufmann, 2017.

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

[Mon]

[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 January].