Contrôle des politiques BGP

SI-F

AfNOG 2014, Djibouti

Last updated 24 April 2013

Application d'une politique avec BGP

- Politiques basées sur l'AS-PATH, la communauté ou le préfixe
- Acceptation / refus de routes sélectionnées
- Assigne des valeurs aux attributs pour influencer la sélection de chemin
- Outils
  - Prefix-list (filtre sur les préfixes)
  - Filter-list (filtre sur les ASs)
  - Route-maps et communautés

Politiques de contrôle – Prefix List

- Filtre de préfixe par voisin
  - Configuration incrémentale
- En entrée ou en sortie (Inbound or Outbound)
- Basé sur l'identifiant des préfixes (notation adresse IPv4/masque, idem pour IPv6)
- L'utilisation des access-lists en Cisco IOS pour filtrer les préfixes est abandonnée depuis longtemps
  - **Fortement déconseillé!**

Syntaxe de la commande prefix-list

- Syntaxe:

  `[no] ip prefix-list list-name [seq seq-value] permit|deny network/len [ge ge-value] [le le-value]`

  `network/len:` Le préfixe et sa longueur

  `ge ge-value:` “supérieure ou égale à”

  `le le-value:` “inférieur ou égal à”

- “ge” and “le” tous deux optionnels
  - Utilisé pour spécifier la plage de la longueur de préfixe à mettre en correspondance les préfixes qui sont plus spécifiques que network/len
- Numéro de séquence est également facultative
  - **`no ip prefix-list sequence-number`** pour désactiver l'affichage des numéros de séquence

Exemples avec prefix-list

- Refuser la route par défaut

```
ip prefix-list EG deny 0.0.0.0/0
```

- Permettre le préfixe 35.0.0.0/8

```
ip prefix-list EG permit 35.0.0.0/8
```

- Rejeter le préfixe 172.16.0.0/12

```
ip prefix-list EG deny 172.16.0.0/12
```

- Dans 192/8 permettre jusqu'à /24

```
ip prefix-list EG permit 192.0.0.0/8 le 24
```

  - Cela permet à toutes les tailles de préfixe dans le bloc d'adresses 192.0.0.0/8, sauf 25, 26, 27, 28, 29, 30, 31 et 32.

Exemples avec prefix-list

- Dans 192/8 rejeter /25 et au dessus

  `ip prefix-list EG deny 192.0.0.0/8 ge 25`

  - Ceci rejete les tailles de prefixe /25, /26, /27, /28, /29, /30, /31 et /32 dans le bloc d'adresses 192.0.0.0/8.
  - Cela a le même effet que l'exemple précédent

- Dans 193/8 permettre les préfixes entre /12 et /20

  `ip prefix-list EG permit 193.0.0.0/8 ge 12 le 20`

  - Ceci rejette les préfixes de tailles /8, /9, /10, /11, /21, /22, … et plus dans le bloc d'adresses 193.0.0.0/8.

- Permet tous les préfixes

  `ip prefix-list EG permit 0.0.0.0/0 le 32`

  - 0.0.0.0 correspond à toutes adresses possibles, "0 le 32" correspond à toutes les longueurs de préfixes possible

Politiques de Contrôle – Prefix List

- Exemple de configuration

```
router bgp 100
 network 105.7.0.0 mask 255.255.0.0
 neighbor 102.10.1.1 remote-as 110
 neighbor 102.10.1.1 prefix-list AS110-IN in
 neighbor 102.10.1.1 prefix-list AS110-OUT out
!
ip prefix-list AS110-IN deny 218.10.0.0/16
ip prefix-list AS110-IN permit 0.0.0.0/0 le 32
ip prefix-list AS110-OUT permit 105.7.0.0/16
ip prefix-list AS110-OUT deny 0.0.0.0/0 le 32
```

Politiques de contrôle – Filter List

- Filtrage de routes basé sur l'attribut AS path
  - Trafic entrant ou sortant
- Exemple de configuration:

```
router bgp 100
 network 105.7.0.0 mask 255.255.0.0
 neighbor 102.10.1.1 filter-list 5 out
 neighbor 102.10.1.1 filter-list 6 in
!
ip as-path access-list 5 permit ^200$
ip as-path access-list 6 permit ^150$
```

Politiques de contrôle – Expressions Régulières

- Comme les expressions régulières Unix
  - . Correspond a un caractère
  - * N'importe quel nombre d'occurrences de l'expression précédente
  - + Au moins une occurrence de l'expression précédente
  - ^ Début de ligne
  - $ Fin de ligne
  - \ Echapper à une caractère d'expression régulière
  - _ Début, fin de ligne, espace, accolade
  - | Ou
  - () parenthèse pour contenir une expression
  - [] crochets pour contenir un intervalle (nombre d'occurrences)

Politique de contrôle
Expressions régulières

- Exemples simples

.*	correspond à n'importe quoi
.+	correspond à au moins un caractère
^$	correspond aux routes locales à cet AS
_1800$	routes générées par AS1800
^1800_	reçues de AS1800
_1800_	via AS1800
_790_1800_	via AS1800 et AS790
_(1800_)+	plusieurs AS1800 en séquence
(utilisé pour faire	correspondre les AS-PATH prepend)
_\(65530\)_	via AS65530 (confédérations)

Politiques de contrôle – Expressions Régulières

- Exemples plus compliqués

^[0-9]+$	Correspond à AS_PATH de longueur 1
^[0-9]+_[0-9]+$	Correspond à AS_PATH de longueur 2
^[0-9]*_[0-9]+$	Correspond à AS_PATH de longueur 1 ou 2
^[0-9]*_[0-9]*$	Correspond à AS_PATH de longueur 0, 1 ou 2
^[0-9]+_[0-9]+_[0-9]+$	Correspond à AS_PATH de longueur 3
_(701|1800)_	Correspond à tout ce qui est passé par AS701 ou AS1800
_1849(_.+_)12163$	Correspond à AS12163 comme origine et qui passe par AS1849

Politiques de contrôle – Route Maps

- Une route-map est comme un “programme” pour IOS
- Avec des numéros de ligne comme dans un programme
- Chaque ligne est un couple condition/action
- Le concept de base est:

  Si telle condition est vérifiée *alors faire telle action, puis sortir, (*if *condition* then do *expression* and exit)

  Sinon (else)

  Si telle autre condition est vérifiée *alors faire telle action, puis sortir (*if *condition* then do *expression* and exit)

  Sinon, etc (else etc)
- Le mot clé “continue” permet aux ISPs d’appliquer plusieurs couples conditions/actions dans une route map

Route Map – Mises en garde

- Les lignes peuvent avoir plusieurs instructions *set*
- Les lignes peuvent avoir plusieurs instructions de correspondance (*match*)
- Dans une ligne avec une seule instruction de correspondance "match"
  - Seuls les préfixes correspondant sont acceptés, le reste est rejeté
- Dans une ligne avec une seule instuction “set”
  - Tous les préfixes sont mis en correspondance et configurés
  - Toutes les lignes suivantes sont ignorées
- Ligne avec instruction match/set et aucune ligne suivante
  - Seuls les préfixes correspondant sont définis, le reste est supprimé

Route Map – Mise en garde

- Exemple
  - En omettant la troisième ligne ci-dessous, ceci signifie que les préfixes ne correspondant pas list-one ou list-two sont supprimés

```
route-map sample permit 10
 match ip address prefix-list list-one
 set local-preference 120
!
route-map sample permit 20
 match ip address prefix-list list-two
 set local-preference 80
!
route-map sample permit 30 ! Don't forget this
```

Route Map
préfixes correspondants

- Exemple de Configuration

```
router bgp 100
 neighbor 1.1.1.1 route-map infilter in
!
route-map infilter permit 10
 match ip address prefix-list HIGH-PREF
 set local-preference 120
!
route-map infilter permit 20
 match ip address prefix-list LOW-PREF
 set local-preference 80
!
ip prefix-list HIGH-PREF permit 10.0.0.0/8
ip prefix-list LOW-PREF permit 20.0.0.0/8
```

Route Map – filtrage AS-PATH

- Exemple de Configuration

```
router bgp 100
 neighbor 102.10.1.2 remote-as 200
 neighbor 102.10.1.2 route-map filter-on-as-path in
!
route-map filter-on-as-path permit 10
 match as-path 1
 set local-preference 80
!
route-map filter-on-as-path permit 20
 match as-path 2
 set local-preference 200
!
ip as-path access-list 1 permit _150$
ip as-path access-list 2 permit _210_
```

Route Map –AS-PATH prepend

- Exemple de configuration d' AS-PATH prepend

```
router bgp 300
 network 105.7.0.0 mask 255.255.0.0
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 route-map SETPATH out
!
route-map SETPATH permit 10
 set as-path prepend 300 300
```

- Utiliser votre propre numéro AS lors de l'AS-PATH prepend
  - Sinon la détection de boucle BGP peut causer une déconnection

Route Map – Communautés

- Exemple de Configuration

```
router bgp 100
 neighbor 102.10.1.2 remote-as 200
 neighbor 102.10.1.2 route-map filter-on-community in
!
route-map filter-on-community permit 10
 match community 1
 set local-preference 50
!
route-map filter-on-community permit 20
 match community 2 exact-match
 set local-preference 200
!
ip community-list 1 permit 150:3 200:5
ip community-list 2 permit 88:6
```

Communautés -Traitement de liste

- Note:
  - Lorsque plusieurs valeurs sont configurées dans la même instruction de la community-list, une condition ET logique est créée. Toutes les valeurs de la communauté doivent correspondre pour satisfaire une condition ET

```
ip community-list 1 permit 150:3 200:5
```

  - Lorsque plusieurs valeurs sont configurées dans des instructions distinctes de community-list, une condition OU logique est créée. La première liste qui correspond à une condition est traitée

```
ip community-list 1 permit 150:3
ip community-list 1 permit 200:5
```

Configuration des Communautés

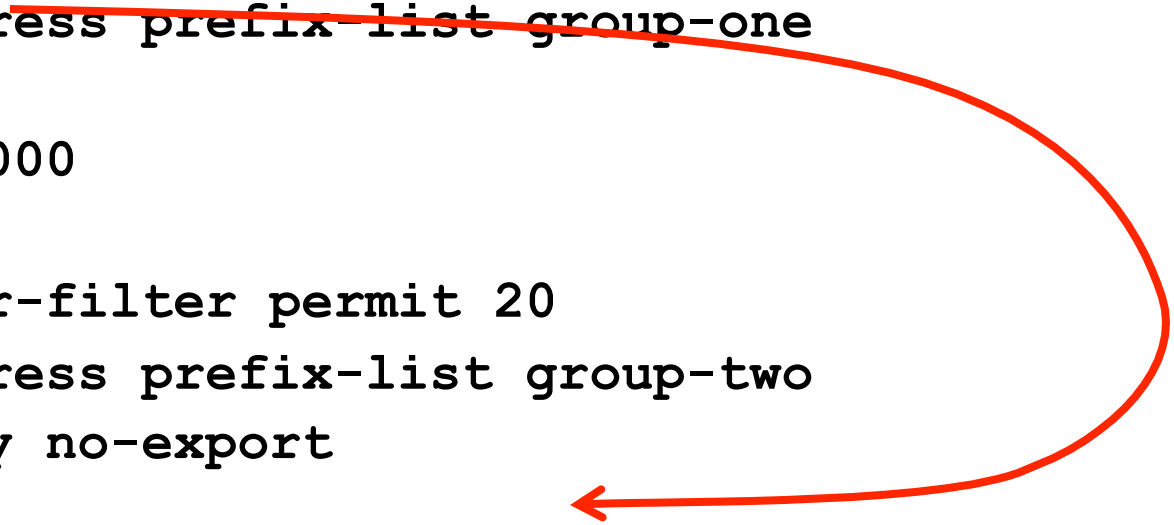
- Exemple de Configuration

```
router bgp 100
 network 105.7.0.0 mask 255.255.0.0
 neighbor 102.10.1.1 remote-as 200
 neighbor 102.10.1.1 send-community
 neighbor 102.10.1.1 route-map set-community out
!
route-map set-community permit 10
 match ip address prefix-list NO-ANNOUNCE
 set community no-export
!
route-map set-community permit 20
 match ip address prefix-list AGGREGATE
!
ip prefix-list NO-ANNOUNCE permit 105.7.0.0/16 ge 17
ip prefix-list AGGREGATE permit 105.7.0.0/16
```

Route Map avec l'option continue

- Manipulation de conditions et actions multiples dans une route-map (pour les relations de voisinage BGP uniquement)

```
route-map peer-filter permit 10
 match ip address prefix-list group-one
 continue 30
 set metric 2000
!
route-map peer-filter permit 20
 match ip address prefix-list group-two
 set community no-export
!
route-map peer-filter permit 30
 match ip address prefix-list group-three
 set as-path prepend 100 100
!
```



Ordre de traitement des politiques BGP

- Pour des politiques appliquées à un voisin BGP spécifique, la séquence suivante est exécutée :
  - Pour les mises à jour inbound, l'ordre est:
    - Route-map
    - Filter-list
    - Prefix-list
  - Pour les mises à jour outbound, l'ordre est :
    - Prefix-list
    - Filter-list
    - Route-map

Gestion des changements de politiques

- Les nouvelles politiques s'appliquent uniquement aux mises à jour allant à travers le routeur APRÈS que la politique ait été introduite ou modifiée
- Pour faciliter les changements de politiques sur l'ensemble de la table BGP gérée par le routeur, les pairs BGP doivent “rafraîchir” leurs relations
  - Ceci est fait un **clear** de la session BGP soit **in** ou **out**, par exemple:

```
clear ip bgp <neighbour-addr> in|out
```

- N'oubliez pas in ou out — à défaut une remise à l'état initial de la session de BGP (hard) sera fait

Gestion des changements de politiques

- Possibilité de relancer les sessions BGP par groupes de voisins configurés selon plusieurs critères
- **`clear ip bgp <addr> [in|out]`**

  `<addr>` peut être un des éléments suivants

`x.x.x.x`	L'adresse IP d'un pair
`*`	tous les pairs
`ASN`	tous les pairs dans AS
`external`	tous les pairs externes
`peer-group <name>`	tous les pairs dans un groupe de pairs

Contrôle des politiques BGP

SI-F

AfNOG 2014, Djibouti