Bonnes pratiques de configuration de BGP

Document réalisé par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), en collaboration avec les opérateurs suivants :

- l'Association Kazar ;
- France-IX ;
- Jaguar Network ;
- Neo Telecoms ;
- Orange ;
- RENATER ;
- SFR.

Document mis en page à l'aide de LaTeX. Figures réalisées avec l'outil TikZ.

Vous pouvez adresser vos commentaires et remarques à l'adresse suivante :

guide.bgp@ssi.gouv.fr

Table des matières

Introduction

Ce document, réalisé avec la coopération d'opérateurs français, a pour objectif de présenter et de décrire des bonnes pratiques de configuration du protocole de routage BGP [1]. Il est avant tout destiné aux administrateurs de routeurs BGP, ainsi qu'aux personnes connaissant les architectures de déploiement de BGP. Le lecteur souhaitant obtenir des informations sur le protocole BGP peut se référer au rapport de l'observatoire de la résilience de l'Internet français [1].

Les éléments de configuration présentés dans ce document s'appliquent aux sessions EBGP [2], c'est-à-dire aux sessions établies entre des AS [3] distincts. Chaque bonne pratique est accompagnée d'exemples de configuration d'implémentations différentes. Le tableau suivant indique les routeurs et les versions des systèmes d'exploitation utilisés.

Système d'exploitation	Version utilisée
SR-OS (Alcatel-Lucent)	10.0r5
IOS (Cisco)	15.2(4)S
Junos (Juniper)	11.4R3.7
OpenBGPD (OpenBSD)	5.3

Routeurs et systèmes d'exploitation utilisés pour les exemples de configuration.

Les extraits de configuration donnés ont tous été testés sur les implémentations indiquées. Ces extraits ne sont donnés qu'à titre d'exemple : ils doivent être adaptés à l'environnement de déploiement. L'ANSSI [4] décline toute responsabilité quant aux conséquences de l'usage qui pourrait être fait de ces exemples.

1. Border Gateway Protocol.
2. External Border Gateway Protocol.
3. Autonomous System (Système autonome).
4. Agence nationale de la sécurité des systèmes d'information.

Chapitre 1

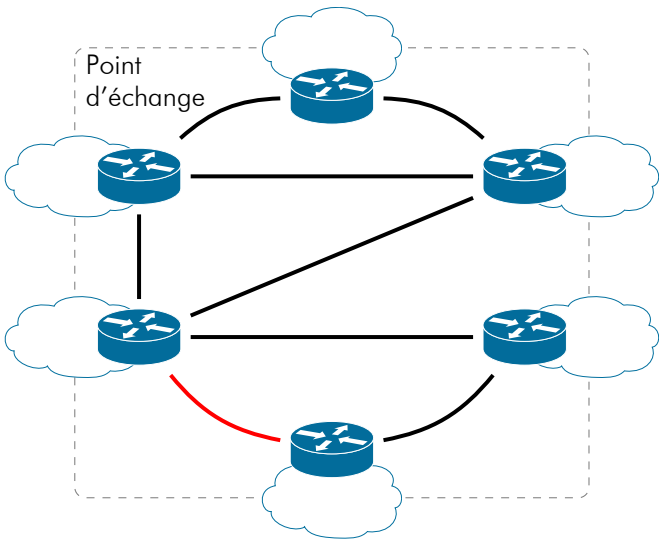
Recommandations de configuration

Ce chapitre rassemble différentes bonnes pratiques de configuration mentionnées dans ce document, et donne les niveaux de recommandations associés.

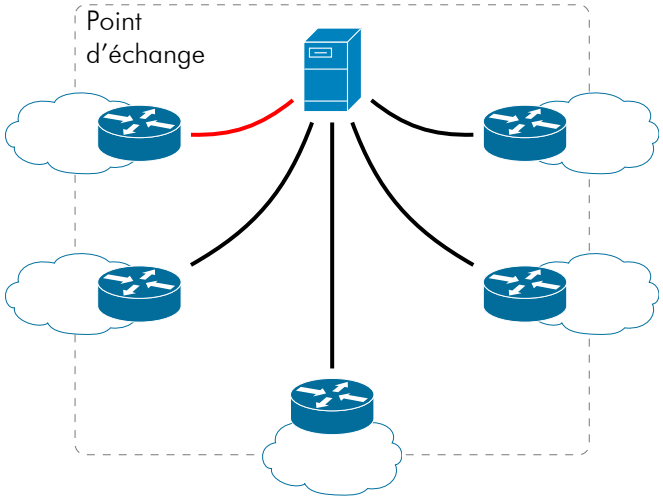
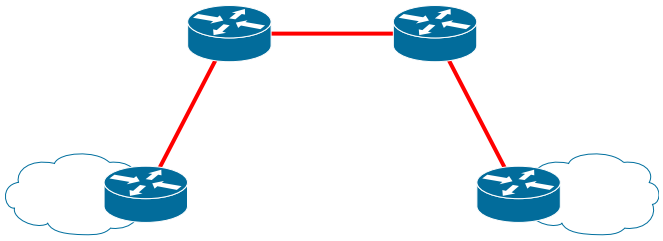
Les types d'interconnexions et de relations entre AS concernés par ces bonnes pratiques sont explicités dans les sections suivantes.

1.1 Types d'interconnexion

Le tableau suivant décrit les types d'interconnexion ciblés par les recommandations de configuration. Sur chaque figure, le lien rouge représente l'interconnexion décrite.

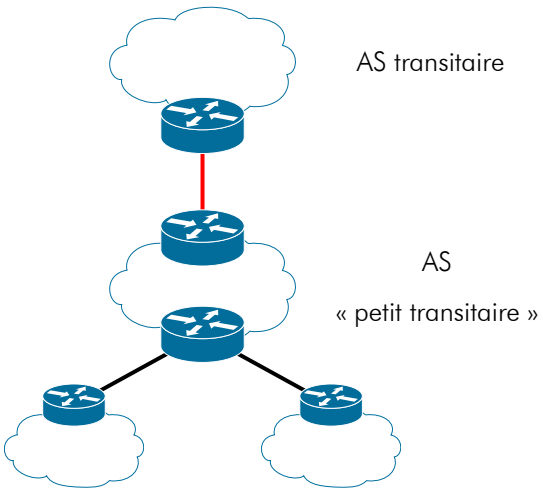
Description	Schéma
Interconnexion 1 : peering [1] bilatéral dans un point d'échange. Ce type d'interconnexion est établi au moyen d'un équipement géré par le point d'échange (non représenté sur le schéma). Chaque AS établit une ou plusieurs sessions avec un ou plusieurs autres AS.	

1. *Peering* ou appairage : accord entre pairs ou chacun annonce les préfixes qu'il gère.

Interconnexion 2 : peering à l'aide d'un serveur de routes dans un point d'échange. Ce type d'interconnexion permet aux pairs reliés à un serveur de routes de recevoir l'ensemble des routes annoncées par les autres pairs.	
Interconnexion 3 : peering privé entre deux AS dans un Network Access Point, ou interconnexion dans une « salle télécom ». Ce type d'interconnexion est effectué grâce à une liaison point-à-point entre deux pairs.	
Interconnexion 4 : session établie en « multi-hop ». L'interconnexion entre les routeurs BGP n'est pas directe.	

1.2 Types de relation entre AS

Le tableau suivant décrit les types de relation entre AS mentionnés dans la suite du document. Sur chaque figure, le lien rouge représente la relation décrite.

Description	Schéma
Relation 1 : transitaire / client « feuille ». Ce type de relation existe entre un AS transitaire et un AS « feuille », qui n'offre pas de service de transit.	
Relation 2 : transitaire / « petit transitaire ». Ce type de relation existe entre un transitaire et un AS client, ce dernier étant également fournisseur d'accès pour un ou plusieurs autres AS.	

Relation 3 : peering. Ce type de relation existe entre deux AS s'échangeant des préfixes, sans que l'un de ces AS ne fournisse à l'autre un service de transit.	

1.3 Recommandations

Les niveaux de recommandation s'appliquant à un élément de configuration donné sont définis sur une échelle à trois étoiles :

★☆☆ : souhaitable

★★☆ : recommandé

★★★ : fortement recommandé

1.3.1 Recommandations dépendant du type d'interconnexion

L'application des éléments de configuration suivants dépend des types d'interconnexions. Des renvois aux différentes sections de ce document sont donnés pour chaque bonne pratique (exemple : TCP-MD5 (2.1)).

Bonnes pratiques	Interconnexion	Niveau de recommandation	Remarques
TCP-MD5 (2.1)	Interconnexions 1 et 4	★★★	Le recours à ce mécanisme est fortement recommandé sur les interconnexions non dédiées.
	Interconnexion 2	★★☆	
	Interconnexion 3	★☆☆	
Filtrage sur le numéro d'AS du pair (3.7)	Interconnexions 1, 3 et 4	★★★	Filtrage systématique sur le numéro d'AS voisin.

1.3.2 Recommandations dépendantes du type de relation entre AS

L'application des éléments de configuration suivants dépend des relations entre les AS. La présence d'un tiret indique que la recommandation ne s'applique pas au pair.

<table>
<tr><th>Bonnes pratiques</th><th>Types de relation</th><th>Niveaux de recommandation</th><th>Remarques</th></tr>
<tr><td rowspan="5">Filtrage sur les préfixes attribués à un pair (3.2)</td><td rowspan="2">Relation 1</td><td>Côté transitaire : ★★★</td><td rowspan="5">Filtrage systématique pour des AS « feuilles ».</td></tr>
<tr><td>Côté client : –</td></tr>
<tr><td rowspan="2">Relation 2</td><td>Côté transitaire : ★★☆</td></tr>
<tr><td>Côté client : –</td></tr>
<tr><td>Relation 3</td><td>★★☆</td></tr>
<tr><td rowspan="2">Filtrage sur la limite du nombre maximum de préfixes reçus (3.6)</td><td rowspan="2">Relations 1 et 2</td><td>Côté transitaire : ★★★</td><td rowspan="2">Filtrage à mettre en œuvre côté transitaire.</td></tr>
<tr><td>Côté client : –</td></tr>
</table>

	Relation 3	★★★	Filtrage à mettre en œuvre par chacun des pairs.
Suppression des numéros d'AS privés (3.5)	Tous les types de relation	★★★	Les numéros d'AS privés doivent être systématiquement supprimés en bordure.

1.3.3 Recommandations générales

Les éléments de configuration suivants sont applicables quels que soient les types d'interconnexion et les relations entre AS.

Bonnes pratiques	Niveaux de recommandation	Remarques
Filtrage sur les *martians* (3.1)	★★★	Filtrage systématique.
Filtrage sur les préfixes trop spécifiques (3.3)	★★★	Plus spécifiques que /24 pour IPv4 (RIPE-399 [2]), /48 pour IPv6 (RIPE-532 [3]).
Filtrage des routes par défaut (3.4)	★★★	Filtrage systématique dès lors que la route par défaut ne doit pas être annoncée (sauf demande explicite d'un client).

Journalisation (4.1)		Journalisation des changements d'adjacence sur chaque routeur et remontée de ces événements pour la supervision.
Graceful Restart (4.2)		Ce mécanisme permet de renforcer la robustesse des interconnexions avec la conservation du transfert des paquets pendant le redémarrage du processus BGP.

Chapitre 2

La Sécurité des sessions

Les spécifications de la version actuelle de BGP (version 4) ne définissent pas de mécanisme permettant de protéger les sessions. Le protocole BGP s'appuyant sur TCP, il est possible de mettre fin aux sessions en envoyant des paquets TCP `RST`, ce qui peut permettre à un attaquant de réaliser un déni de service [4] [5] [6]. Bien que la mise en œuvre d'une telle attaque implique certains prérequis, TCP MD5 est un mécanisme complémentaire aux autres mesures de sécurité, et dont l'utilisation s'inscrit dans une démarche de défense en profondeur.

2.1 L'Authentification des messages

La RFC 4271 [7], publiée en janvier 2006, spécifie que les implémentations de BGP doivent permettre d'utiliser le mécanisme d'authentification fourni par l'option de TCP couramment appelé TCP MD5, et décrit dans la RFC 2385 [8]. Ce mécanisme est disponible dans la plupart des implémentations de BGP, et permet d'assurer l'intégrité et l'authenticité des messages TCP en incluant un MAC [1] calculé à l'aide de la fonction de hachage MD5.

La mise en place de ce mécanisme repose sur un secret partagé entre les deux routeurs. L'algorithme s'applique aux éléments suivants :

- un pseudo en-tête IP comprenant l'adresse IP source, l'adresse IP destination, le numéro de protocole et la longueur du segment ;
- l'en-tête TCP, hormis les options, avec une valeur nulle pour la somme de contrôle ;
- les données du segment TCP.

Le destinataire d'un segment calcule le MAC de la même façon et vérifie si le résultat est le même que la valeur contenue dans l'option TCP MD5. En cas d'échec, le segment est rejeté silencieusement. En cas de changement de secret au cours d'une session, les paquets émis par le pair ayant conservé l'ancien secret sont rejetés, et la session expire une fois que le *hold time* est dépassé.

1. Message Authentication Code.

TCP MD5 n'est pas un mécanisme cryptographique robuste. En particulier, ce mécanisme n'est pas conforme à l'annexe B1 du Référentiel Général de Sécurité de l'ANSSI [9]. Cependant, les implémentations existantes à la date d'écriture de ce document ne proposent pas l'*Authentication Option* de TCP, définie dans la RFC 5925 [10], qui doit permettre l'utilisation d'autres algorithmes. Malgré son obsolescence, TCP MD5 constitue un élément de sécurité supplémentaire aux autres bonnes pratiques de configuration. En l'absence de mécanisme plus robuste, TCP MD5 devrait être systématiquement utilisé lorsque l'interconnexion est effectuée en *multi-hop*, ou au moyen d'un équipement partagé (par exemple, un commutateur) au sein d'un point d'échange. Lorsque l'interconnexion est effectuée entre deux routeurs proposant un mécanisme cryptographique plus robuste, ce mécanisme doit être utilisé en lieu et place de TCP MD5.

Un secret différent doit être configuré pour chaque interconnexion. Le secret utilisé doit être fort, sans quoi le mécanisme fourni par TCP MD5 ne présente plus d'intérêt. La force d'un secret dépend de sa longueur et des classes de caractères qui le composent. L'ANSSI a publié une note technique, « Recommandations de sécurité relatives aux mots de passe » [11], qui donne des critères pour choisir judicieusement un mot de passe.

TCP MD5 - Routeurs Alcatel-Lucent

Extrait 2.1 – Commande permettant de configurer l'authentification MD5

```
neighbor <ip-address> authentication-key <secret>
```

Extrait 2.1 - Commentaires

Cet extrait montre comment configurer l'authentification TCP MD5 pour un pair (à l'adresse IP `ip-address`) sur un routeur Alcatel-Lucent à l'aide de la commande *authentication-key*. La clé demandée (`secret`) est la chaîne de caractères constituant le secret sur lequel les pairs se sont préalablement accordés.

Extrait 2.2 – Exemple de configuration de l'authentification MD5

```
neighbor 192.0.2.3 authentication-key ght8CD%E7am
```

TCP MD5 - Routeurs Cisco

Extrait 2.3 – Commande permettant de configurer l'authentification MD5

```
Cisco(config-router)#neighbor <ip-address> password <string>
```

Extrait 2.3 - Commentaires

L'authentification MD5 est configurable pour un pair à l'aide de son adresse IP (*ip-address*). Le secret entré est une chaîne de caractères (*string*).

Extrait 2.4 – Exemple de configuration de l'authentification MD5

```
Cisco(config)#router bgp 64506
Cisco(config-router)#neighbor 192.0.2.3 password ght8CD%E7am
```

TCP MD5 - Routeurs Juniper

Extrait 2.5 – Exemple de configuration de l'authentification MD5

```
[edit protocols bgp group session-to-AS64506 neighbor
   192.0.2.6]
root@Juniper# set authentication-key ght8CD%E7am
```

Extrait 2.5 - Commentaires

Cet extrait montre comment configurer l'authentification TCP MD5 sur un routeur Juniper à l'aide de la commande `set authentication-key`. La clé demandée est la chaîne de caractères constituant le secret sur lequel les pairs se sont préalablement accordés.

TCP MD5 - Routeurs OpenBGPD

Extrait 2.6 – Commande permettant de configurer l'authentification MD5

```
tcp md5sig {password | key} <secret>
```

Extrait 2.6 - Commentaire

Le secret entré peut être une chaîne de caractères ASCII (utilisation de `password` *secret*) ou fourni sous forme hexadécimale (utilisation de `key` *secret*).

Extrait 2.7 – Exemple de configuration de l'authentification MD5

```
tcp md5sig password "ght8CD%E7am"
```

Chapitre 3

Filtrage des annonces de préfixes

BGP ne fournit pas de mécanisme permettant de valider les annonces de préfixes. Ainsi, un AS peut annoncer n'importe quel préfixe. Il peut s'agir de préfixes non gérés par l'AS (c'est ce que l'on appelle une usurpation de préfixes), ou de préfixes ne devant pas être annoncés au sein de l'Internet. Cette section présente différentes règles et méthodes de filtrage visant à limiter la propagation d'annonces illégitimes.

3.1 Filtrage sur les préfixes réservés

Les *martians* sont des préfixes réservés à des fins spécifiques. Il peut s'agir, par exemple, des blocs d'adresses privées définis dans la RFC 1918 [12] et dans la RFC 6890 [13]. Les *martians* ne devraient pas être annoncés dans l'Internet, et constituent donc une première catégorie de préfixes devant être filtrés. Les filtres sur ces préfixes doivent être appliqués aussi bien sur les flux entrants que sur les flux sortants.

L'IANA [1] maintient une liste de préfixes IPv4 réservés [14], dont la version du 22 mai 2013 est donnée [2] dans le tableau 3.2. Ce tableau comporte également le préfixe `224.0.0.0/4`, réservé pour le *multicast*. Par ailleurs, l'IANA maintient une liste de préfixes IPv6 réservés [16]. Le tableau 3.3 présente la version du 1er mai 2013, avec en plus le préfixe `ff00::/8`, réservé pour le *multicast*. Parmi ceux-ci, on trouve `fc00::/7` (*unique local*), `fe80::/10` (*link-local*), les préfixes plus spécifiques que `2002::/16` (réservés pour le protocole *6to4*), ou encore `2001:db8::/32`, un préfixe réservé pour la documentation. Afin d'établir une liste de préfixes IPv6 devant être filtrés, il est possible de se référer aux documents suivants, disponibles en ligne :

- *IANA IPv6 Special Purpose Address Registry* [16] ;
- *Internet Protocol Version 6 Address Space* [17] ;
- *IPv6 Global Unicast Address Assignments* [18].

1. Internet Assigned Numbers Authority.

2. Le préfixe `192.0.0.0/29`, réservé pour le *Dual-Stack Lite* [15], ainsi que les préfixes `192.0.0.170/32` et `192.0.0.171/32`, réservés pour la découverte de NAT64/DNS64, n'apparaissent pas explicitement dans ce tableau : ils sont inclus dans le préfixe `192.0.0.0/24`. De plus, le préfixe réservé pour les relais *6to4* (`192.88.99.0/24`) n'est pas mentionné dans ce tableau.

L'IANA alloue des préfixes aux RIR [3] (registres régionaux) qui proviennent uniquement du préfixe 2000::/3, correspondant aux adresses dites *Global Unicast* [19]. À la date de rédaction du document, le bloc n'a pas été entièrement alloué. Les tableaux A.1 et A.2 de l'annexe A indiquent les préfixes réservés au 15 février 2013. Les listes de préfixes réservés évoluent au cours du temps. Par conséquent, si un filtrage des blocs non alloués du préfixe 2000::/3 est effectué, il est nécessaire de maintenir à jour les filtres basés sur ces listes.

Les exemples suivants indiquent comment configurer des filtres pour les *martians*. Par souci de concision, seul l'exemple de configuration sur les routeurs Alcatel-Lucent est exhaustif.

Préfixes IPv4 réservés	
0.0.0.0/8	réservé pour les adresses sources du réseau courant[20] [4]
127.0.0.0/8	réservé pour la boucle locale [20]
169.254.0.0/16	réservé pour le lien local [21]
198.18.0.0/15	réservé pour les tests de performance d'équipements réseau [22]
192.0.0.0/24	réservé pour l'IANA, pour des allocations futures dédiées à des protocoles de l'IETF [5] [13]
10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	réservés pour l'usage privé [12]
192.0.2.0/24 198.51.100.0/24 203.0.113.0/24	préfixes respectifs des TEST-NET-1, TEST-NET-2 et TEST-NET-3, réservés pour la documentation [23]
100.64.0.0/10	réservé pour les connexions entre fournisseurs et clients faisant usage du *Carrier-Grade NAT* [24]

3. Regional Internet Registry.
4. D'après la RFC 1122, ce préfixe ne doit pas être utilisé, sauf comme adresse source au cours d'une procédure d'initialisation pendant laquelle l'hôte apprend son adresse IP.
5. Internet Engineering Task Force.

Préfixes IPv4 réservés	
224.0.0.0/4	réservé pour le *multicast* [25]
240.0.0.0/4	réservé pour un « usage futur » [26]
255.255.255.255/32	« *limited broadcast* ». Les paquets à destination de cette adresse ne sont pas transférés par les routeurs [27]

Table 3.2 Préfixes IPv4 réservés.

Préfixes IPv6 réservés	
::1/128	réservé pour la boucle locale [19]
::/128	réservé pour l'adresse non spécifiée [19]
::ffff:0:0/96	réservé pour la correspondance IPv4 [19]
100::/64	réservé pour le *black-holing* [6] [28]
2001::/23	réservé par l'IANA pour des protocoles (TEREDO par exemple) [29]
2001::/32	réservé pour le service *TEREDO* [30]
2001:2::/48	réservé pour les tests de performance des équipements réseau [31]
2001:10::/28	réservé pour *ORCHID* [32]
2001:db8::/32	réservé pour la *documentation* [33]
2002::/16 (uniquement les préfixes plus spécifiques)	réservé pour le *6to4* [34]
fc00::/7	réservé pour les adresses *Unique-Local* [35]
fe80::/10	réservé pour les adresses *Link-Scoped Unicast* [19]
ff00::/8	réservé pour le *multicast* [19]

Table 3.3 Préfixes IPv6 réservés.

6. Le *black-holing* consiste à éliminer le trafic d'une destination ou d'une source donnée.

Filtrage sur des *martians* - Routeurs Alcatel-Lucent

Extrait 3.1 – Exemple de configuration de filtres statiques pour des martians IPv4

```
>config>router>policy-options#
            prefix-list "v4-martians"
                prefix 0.0.0.0/8 longer
                prefix 127.0.0.0/8 longer
                prefix 169.254.0.0/16 longer
                prefix 198.18.0.0/15 longer
                prefix 192.0.0.0/24 longer
                prefix 10.0.0.0/8 longer
                prefix 172.16.0.0/12 longer
                prefix 192.168.0.0/16 longer
                prefix 192.0.2.0/24 longer
                prefix 198.51.100.0/24 longer
                prefix 203.0.113.0/24 longer
                prefix 100.64.0.0/10 longer
                prefix 224.0.0.0/4 longer
                prefix 240.0.0.0/4 longer
                prefix 255.255.255.255/32 exact
            exit
            policy-statement "reject-martians"
                entry 10
                    from
                        prefix-list "v4-martians"
                    exit
                    action reject
                    exit
                exit
                default-action accept
            exit
```

Extrait 3.2 – Application du filtre créé dans l'extrait 3.1

```
>config>router>bgp#
    group "EBGP"
        import "reject-martians"
        export "reject-martians"
```

```
        neighbor 192.0.2.3
        exit
    exit
```

Extrait 3.3 – Exemple de configuration de filtres statiques pour des martians IPv6

```
>config>router>policy-options#
    prefix-list "v6-martians"
        prefix ::1/128 exact
        prefix ::/128 exact
        prefix ::ffff:0.0.0.0/96 longer
        prefix 100::/64 longer
        prefix 2001::/23 longer
        prefix 2001:db8::/32 longer
        prefix 2002::/16 prefix-length-range 17-128
        prefix fc00::/7 longer
        prefix fe80::/10 longer
        prefix ff00::/8 longer
        prefix 3ffe::/16 longer
        prefix 5f00::/8 longer
    exit
    prefix-list "v6-authorized"
        prefix 2000::/3 prefix-length-range 3-48
    exit
    policy-statement "reject-v6-martians"
        entry 10
            from
                prefix-list "v6-martians"
            exit
            action reject
            exit
        exit
        entry 20
            from
                prefix-list "v6-authorized"
            exit
            action accept
            exit
        exit
```

```
        default-action reject
    exit
```

Extraits 3.1, 3.2 et 3.3 - Commentaires

Les extraits 3.1 et 3.3 donnent des exemples de configuration de filtres statiques pour les préfixes réservés (IPv4 et IPv6). Ces filtres sont appliqués à un ou plusieurs pairs, comme indiqué dans l'extrait 3.2.

Filtrage sur des préfixes réservés - Routeurs Cisco

Extrait 3.4 – Commande permettant de créer une prefix-list

```
Cisco(config)#ip prefix-list <list-name> | <list-number> [seq
    number] {deny <network>/<length> | permit <network>/<
   length>} [ge ge-length] [le le-length]
```

Extrait 3.4 - Commentaires

Voici les paramètres et options disponibles pour cette commande :

- `list-name` et `list-number` permettent d'identifier la *prefix-list* par un nom ou un nombre ;
- `seq number` fixe un numéro de séquence, compris entre 1 et $2^{32} - 2$, indiquant l'ordre dans lequel sont traitées les entrées. Si aucun numéro de séquence n'est donné, un numéro par défaut est fixé. S'il s'agit d'une première entrée dans une *prefix-list*, la valeur 5 est fixée. Pour des entrées ultérieures, le numéro est incrémenté de 5 ;
- `deny` et `permit` permettent respectivement d'interdire ou d'autoriser un préfixe donné ;
- les paramètres optionnels `ge ge-length` et `le le-length` permettent d'indiquer une longueur de masque pour laquelle le test sera vrai. Le mot-clé `ge` permet d'effectuer un test de type « supérieur ou égal », `le` permet d'effectuer un test de type « inférieur ou égal ».

Extrait 3.5 – Exemple de configuration de filtres statiques pour des préfixes réservés (IPv4)

```
Cisco(config)#ip prefix-list ipv4-martians seq 5 deny
   0.0.0.0/8 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 10 deny
   127.0.0.0/8 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 15 deny
   169.254.0.0/16 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 20 deny
   198.18.0.0/15 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 25 deny
   192.0.0.0/24 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 30 deny
   10.0.0.0/8 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 35 deny
   172.16.0.0/12 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 40 deny
   192.168.0.0/16 le 32
Cisco(config)#ip prefix-list ipv4-martians seq 80 deny
   255.255.255.255/32
Cisco(config)#ip prefix-list ipv4-martians seq 500 permit
   0.0.0.0/0 le 24
```

Extrait 3.6 – Exemple d'application de la prefix-list de l'extrait 3.5 à un pair en entrée et en sortie

```
Cisco(config-router-af)#neighbor 192.0.2.3 prefix-list
   ipv4-martians in
Cisco(config-router-af)#neighbor 192.0.2.3 prefix-list
   ipv4-martians out
```

Extrait 3.6 - Commentaires

Une fois le filtre créé, celui-ci doit être appliqué sur un (ou plusieurs) pair(s). L'extrait 3.6 présente l'application de ces filtres pour un pair sur les flux entrants (*in*) et sortants (*out*).

Extrait 3.7 – Exemple de configuration de filtres statiques pour des préfixes réservés (IPv6)

```
Cisco(config)#ipv6 prefix-list ipv6-filter deny ::1/128
Cisco(config)#ipv6 prefix-list ipv6-filter deny ::/128
Cisco(config)#ipv6 prefix-list ipv6-filter permit 2002::/16
Cisco(config)#ipv6 prefix-list ipv6-filter deny 2002::/16 le
   128
Cisco(config)#ipv6 prefix-list ipv6-filter deny 3FFE::/16 le
   128
Cisco(config)#ipv6 prefix-list ipv6-filter deny 5F00::/8 le
   128
Cisco(config)#ipv6 prefix-list ipv6-filter permit 2000::/3 le
    48
Cisco(config)#ipv6 prefix-list ipv6-filter seq 500 deny ::/0
   le 128
```

Extrait 3.7 - Commentaire

Pour des préfixes IPv6, le filtrage s'effectue de manière analogue à celle présentée, à l'aide de la commande *ipv6 prefix-list*.

Filtrage sur des *martians* - Routeurs Juniper

Extrait 3.8 – Construction d'un filtre (`policy-statement`) pour les martians IPv4

```
[edit policy-options policy-statement ipv4-martians]
root@Juniper# set from route-filter 0.0.0.0/8 orlonger
```

Extrait 3.9 – Définition de l'action à effectuer pour le filtre ipv4-martians

```
[edit policy-options policy-statement ipv4-martians]
root@Juniper# set then reject
```

Extrait 3.10 – Filtre des martians IPv4

```
[edit policy-options]
root@Juniper# show policy-statement ipv4-martians
from {
    route-filter 0.0.0.0/8 orlonger;
    route-filter 127.0.0.0/8 orlonger;
    route-filter 169.254.0.0/16 orlonger;
    route-filter 192.168.0.0/16 orlonger;
    route-filter 192.0.2.0/24 orlonger;
    route-filter 240.0.0.0/4 orlonger;
    route-filter 255.255.255.255/32 exact;
}
then reject;
```

Extrait 3.11 – Application du filtre ipv4-martians

```
[edit protocols bgp]
root@Juniper# set group session-to-AS64502-v4 import
   ipv4-martians
root@Juniper# show group session-to-AS64502-v4
type external;
import ipv4-martians;
peer-as 64502;
neighbor 192.0.2.2;
```

Extrait 3.12 – Filtre des martians IPv6

```
[edit policy-options]
root@Juniper# show policy-statement ipv6-martians
from {
    family inet6;
    route-filter ::1/128 exact;
    route-filter ::/128 exact;
    route-filter 2001:0000::/23 orlonger;
    route-filter 2001:db8::/32 orlonger;
    route-filter 2002::/16 exact next policy;
    route-filter 2002::/16 longer;
```

```
}
then reject;
```

Extraits 3.8, 3.9, 3.10, 3.11, et 3.12 - Commentaires

Les extraits 3.8 et 3.9 montrent comment construire le `policy-statement` *ipv4-martians* : dans l'extrait 3.8, les règles du filtre (clause `from`) sont définies, tandis que l'extrait 3.9 indique l'action à effectuer. L'extrait 3.10 montre un filtre permettant de rejeter des *martians* IPv4. L'extrait 3.11 montre comment appliquer le filtre à un pair. De manière analogue, il est possible de filtrer les *martians* IPv6, comme le montre l'extrait 3.12.

Filtrage sur les *martians* - Routeurs OpenBGPD

Extrait 3.13 – Exemple de configuration de filtres statiques pour les martians IPv4 et IPv6

```
# Martians IPv4
deny from any prefix 0.0.0.0/8 prefixlen >= 8
deny from any prefix 127.0.0.0/8 prefixlen >= 8
deny from any prefix 169.254.0.0/16 prefixlen >= 16
deny from any prefix 198.18.0.0/15 prefixlen >= 15

# Martians IPv6
deny from any prefix ::1/128
deny from any prefix ::/128
deny from any prefix ::ffff:0:0/96 prefixlen >= 96
deny from any prefix 64:ff9b::/96 prefixlen >= 96
```

Extrait 3.13 - Commentaire

L'extrait 3.13 donne un exemple de configuration de filtres statiques pour des préfixes réservés (IPv4 et IPv6).

3.2 Filtrage sur les préfixes attribués à un pair

Dans le cas d'une session BGP entre un AS transitaire et un AS « feuille », il convient, côté transitaire, de filtrer les préfixes du client afin d'écarter tout préfixe que ce dernier ne devrait pas annoncer. Un tel filtrage peut être étendu à d'autres types d'interconnexion. En l'absence d'entente entre les AS sur les préfixes qu'ils s'annoncent entre eux, les IRR[7] doivent être consultés pour définir les filtres. Cependant, les IRR sont maintenus par les acteurs BGP eux-mêmes. Des observations montrent que les informations qu'ils renferment ne sont pas toujours à jour [1]. Un filtrage strict, c'est-à-dire qui écarte toute annonce n'étant pas conforme aux déclarations dans les registres, n'est donc pas toujours possible. Sur les implémentations testées, les filtres se configurent de manière analogue aux filtres présentés dans la section 3.1.

3.3 Filtrage sur les préfixes trop spécifiques

À la date de rédaction de ce document, la longueur des masques des préfixes annoncés ne doit pas excéder 24 bits en IPv4 [2] et 48 bits pour IPv6[8] [3]. Cette règle de filtrage permet de limiter la taille de la table de routage globale.

Filtrage des préfixes trop spécifiques - Routeurs Alcatel-Lucent

Extrait 3.14 – Filtrage des préfixes IPv4 plus spécifiques que /24

```
>config>router>policy-options#
    prefix-list "v4-too-specific"
        prefix 0.0.0.0/0 prefix-length-range 25-32
    exit
```

Extrait 3.15 – Filtrage des préfixes IPv6 plus spécifiques que /48

```
>config>router>policy-options#
    prefix-list "v6-too-specific"
        prefix ::/0 prefix-length-range 49-128
    exit
```

7. Internet Routing Registry.
8. Concernant IPv6, cette règle pourrait évoluer à l'avenir.

Extraits 3.14 et 3.15 - Commentaires

Les extraits 3.14 et 3.15 indiquent comment filtrer les préfixes trop spécifiques (IPv4 et IPv6) sur un routeur Alcatel-Lucent. La mise en œuvre de ces prefix-list est semblable à celle présentée dans les extraits 3.1 et 3.2.

Filtrage des préfixes trop spécifiques - Routeurs Cisco

Extrait 3.16 – Filtrage des préfixes IPv4 plus spécifiques que /24

```
Cisco(config)#ip prefix-list too-specific seq 5 permit
   0.0.0.0/0 le 24
```

Extrait 3.16 - Commentaires

La commande de l'extrait 3.16 peut être utilisée pour refuser des préfixes plus spécifiques que /24. La *prefix-list* est appliquée en entrée et en sortie pour un pair comme sur l'extrait 3.6.

Extrait 3.17 – Filtrage des préfixes IPv6 plus spécifiques que /48

```
Cisco(config)#ipv6 prefix-list v6-too-specific seq 5 permit
   ::/0 le 48
```

Extrait 3.17 - Commentaires

D'une manière analogue, la commande de l'extrait 3.17 permet de filtrer les préfixes IPv6 plus spécifiques que /48. La *prefix-list* est appliquée en entrée et sortie pour un pair, de manière similaire à l'exemple donné pour les préfixes IPv4 réservés (voir l'extrait 3.6).

Filtrage des préfixes trop spécifiques - Routeurs Juniper

Extrait 3.18 – Filtrage des préfixes IPv4 plus spécifiques que /24

```
[edit policy-options policy-statement v4-prefix-filter]
root@Juniper# set term accept-up-to-24 from route-filter
   0.0.0.0/0 upto /24
root@Juniper# set term accept-up-to-24 then next policy
root@Juniper# set then reject
root@Juniper# show
term accept-up-to-24 {
    from {
        route-filter 0.0.0.0/0 upto /24;
    }
    then next policy;
}
then reject;
```

Extrait 3.19 – Filtrage des préfixes IPv6 plus spécifiques que /48

```
[edit policy-options policy-statement v6-prefix-filter]
root@Juniper# set term accept-up-to-48 from route-filter ::/0
    upto /48
root@Juniper# set term accept-up-to-48 then next policy
root@Juniper# set then reject
root@Juniper# show
term accept-up-to-48 {
    from {
        route-filter ::/0 upto /48;
    }
    then next policy;
}
then reject;
```

Extraits 3.18 et 3.19 - Commentaires

L'extrait 3.18 indique comment rejeter les préfixes IPv4 trop spécifiques. En IPv6, le filtrage se fait de manière similaire, comme le montre l'extrait 3.19.

Filtrage des préfixes trop spécifiques - Routeurs OpenBGPD

Extrait 3.20 – Filtrage des préfixes IPv4 plus spécifiques que /24

```
deny from any inet prefixlen > 24
```

Extrait 3.21 – Filtrage des préfixes IPv6 plus spécifiques que /48

```
deny from any inet6 prefixlen > 48
```

3.4 Filtrage des routes par défaut

La route par défaut (`0.0.0.0/0` pour IPv4, `::/0` pour IPv6) ne doit pas être annoncée, sauf pour un client qui le demande. Cela permet d'éviter de devenir malencontreusement un AS de transit, ce qui pourrait conduire à une utilisation très importante de la bande passante, ainsi qu'à une surcharge au niveau des routeurs. D'autre part, la route par défaut doit seulement être acceptée par un client accédant à l'Internet via une route par défaut.

Filtrage des routes par défaut - Routeurs Alcatel-Lucent

Extrait 3.22 – Filtrage de la route par défaut (IPv4 et IPv6)

```
>config>router>policy-options#
    prefix-list "default-v4"
        prefix 0.0.0.0/0 exact
    exit
    prefix-list " default-v6"
        prefix ::/0 exact
    exit
    policy-statement "reject-default-v4"
        entry 10
        from
            prefix-list "default-v4"
        exit
        action reject
    exit
```

```
    policy-statement "reject-default-v6"
        entry 10
        from
            prefix-list "default-v6"
        exit
        action reject
    exit
```

Extrait 3.22 - Commentaires

L'extrait 3.22 indique comment filtrer les routes par défaut IPv4 et IPv6. Les filtres peuvent être appliqués à un ou plusieurs pairs (voir l'extrait 3.2).

Filtrage des routes par défaut - Routeurs Cisco

Extrait 3.23 – Filtrage de la route par défaut (IPv4 et IPv6)

```
Cisco(config)#ip prefix-list v4-default-route seq 5 deny
   0.0.0.0/0
Cisco(config)#ip prefix-list v4-default-route seq 10 permit
   0.0.0.0/0 le 24
Cisco(config)#ipv6 prefix-list v6-default-route seq 5 deny
   ::/0
Cisco(config)#ipv6 prefix-list v6-default-route seq 10 permit
    ::/0 le 48
```

Extrait 3.23 - Commentaires

Sur les routeurs Cisco, les *prefix-lists* permettent de filtrer les routes par défaut (IPv4 et IPv6). L'application à un pair s'effectue de manière similaire à l'extrait 3.6.

Filtrage des routes par défaut - Routeurs Juniper

Extrait 3.24 – Filtrage de la route par défaut (IPv4 et IPv6)

```
[edit policy-options policy-statement no-v4-default-route]
root@Juniper# set term default-route from route-filter
   0.0.0.0/0 exact
root@Juniper# set term default-route then reject

[edit policy-options policy-statement no-v6-default-route]
root@Juniper# set term default-route from route-filter ::/0
   exact
root@Juniper# set term default-route then reject

[edit policy-options]
root@Juniper# show policy-statement no-v4-default-route
term default-route {
    from {
        route-filter 0.0.0.0/0 exact;
    }
    then reject;
}
root@Juniper# show policy-statement no-v6-default-route
term default-route {
    from {
        route-filter ::/0 exact;
    }
    then reject;
}
```

Extrait 3.24 - Commentaire

Sur les routeurs Juniper, les routes par défaut peuvent être filtrées à l'aide de *policy-statements*.

Filtrage des routes par défaut - Routeurs OpenBGPD

Extrait 3.25 – Filtrage de la route par défaut (IPv4 et IPv6)

```
deny from any inet prefix 0.0.0.0/0 prefixlen = 0
deny from any inet6 prefix ::/0 prefixlen = 0
```

3.5 Suppression des numéros d'AS privés

Il n'est pas toujours nécessaire d'avoir un numéro d'AS unique. Par exemple, un AS client peut être connecté à un unique transitaire (par un ou plusieurs liens) qui lui permet d'accéder à l'ensemble de l'Internet. Le transitaire annonce alors les préfixes du client à la place de ce dernier. Dans ce cas, le transitaire attribue un numéro d'AS dit « privé » à cet AS. Les numéros d'AS privé s'étendent de 64512 à 65534 [36]. Afin de faire face à la croissance du nombre d'AS, des numéros d'AS sur 32 bits ont été introduits [37] : les numéros de 4200000000 à 4294967294 sont réservés pour l'usage privé.

Les numéros d'AS privés ne doivent pas être présents sur Internet dans les annonces puisqu'ils peuvent être utilisés simultanément par plusieurs AS. Un filtrage en sortie, permettant de supprimer les numéros d'AS privés, est donc nécessaire. Des exemples de configuration sont donnés pour toutes les implémentations testées à l'exception d'OpenBGPD. En effet, OpenBGPD ne permet pas de retirer les numéros d'AS privés.

Suppression des numéros d'AS privés - Routeurs Alcatel-Lucent

Extrait 3.26 – Commande permettant de supprimer les numéros d'AS privés

```
>config>router>bgp# remove-private [limited] [skip-peer-as]
```

Extrait 3.27 – Exemple de suppression de numéros d'AS privés dans les annonces à un pair

```
>config>router>bgp#
    group "EBGP"
        remove-private
```

```
        neighbor 192.0.2.3
        exit
    exit
```

Extrait 3.26 et 3.27 - Commentaires

L'option *limited* permet de supprimer les derniers numéros d'AS privés de l'`AS_PATH` jusqu'au premier numéro d'AS non privé. L'option *skip-peer-as* permet quant à elle de conserver un numéro d'AS privé s'il s'agit du numéro d'AS configuré pour le pair.

Suppression des numéros d'AS privés - Routeurs Cisco

Extrait 3.28 – Commande permettant de supprimer les numéros d'AS privés

```
Cisco(config-router)#neighbor <ip-address> | <group-name>
   remove-private-as [all [replace-as]]
```

Extrait 3.28 - Commentaires

Voici les paramètres et options disponibles pour cette commande :

- `ip-address` et `group-name` permettent d'indiquer l'adresse du pair, ou le groupe de pairs à qui la commande s'applique ;
- le mot-clé `all` permet de supprimer tous les numéros d'AS privés de l'`AS_PATH` pour les annonces ;
- `replace-as` permet de remplacer l'ensemble des numéros d'AS privés qui ont été supprimés par le numéro de l'AS local, c'est-à-dire l'AS dont le routeur fait partie.

Extrait 3.29 – Exemple d'utilisation de la commande remove-private-as

```
Cisco(config-router)#address-family ipv4
Cisco(config-router-af)#neighbor 192.0.2.3 remove-private-as
```

Extrait 3.29 - Commentaires

L'exemple 3.29 illustre l'utilisation de la commande. Dans ce cas, les annonces faites par l'AS local (AS 64506) vers l'AS du pair à l'adresse `192.0.2.3` ne contiendront pas de numéros d'AS privés. Le comportement peut être différent sur d'anciennes versions d'IOS. En particulier, dans les versions antérieures à la version 15.1(2)T [38], si l'`AS_PATH` contient des numéros d'AS publics, aucun numéro d'AS privé ne sera retiré.

Suppression des numéros d'AS privés - Routeurs Juniper

Extrait 3.30 – Exemple de suppression de numéros d'AS privés dans les annonces à un pair

```
[edit protocols bgp]
root@Juniper# set group session-to-AS64503 neighbor 2001:db8
   :0:3:fac0:100:22d3:ce80 remove-private
root@Juniper# show group session-to-AS64503
type external;
log-updown;
family inet6 {
    unicast;
}
peer-as 64503;
neighbor 2001:db8:0:3:fac0:100:22d3:ce80 {
    remove-private;
}
```

Extrait 3.30 - Commentaires

La commande `remove-private` permet d'effectuer la suppression des numéros d'AS privés sur les routeurs Juniper. L'extrait 3.30 donne un exemple d'utilisation permettant de supprimer les numéros d'AS privés des annonces à destination d'un pair.

3.6 Filtrage sur le nombre maximum de préfixes

Le filtrage sur le nombre maximal de préfixes annoncés par un pair a pour but de protéger les routeurs d'une surcharge, surtout dans le cas où ceux-ci ne sont pas dimensionnés pour effectuer un grand nombre de traitements. Cependant, ce type de filtre doit également être mis en place pour protéger la cohérence du routage. Par exemple, un AS client peut annoncer par erreur l'intégralité de la table de routage de l'Internet à son transitaire. Si ce dernier n'effectue aucun filtrage et accepte ces annonces, il est fort probable qu'il choisisse les routes associées aux préfixes annoncés et les réannonce par la suite à ses pairs. En effet, pour des raisons d'ordre économique, les valeurs des attributs `LOCAL_PREF` associés aux routes des clients sont en général plus élevées que celles des routes des autres pairs. Par conséquent, suite à l'annonce des préfixes du client, un certain nombre de pairs risquent à leur tour de choisir ces routes comme étant les meilleures, rendant ainsi les préfixes inaccessibles. Des incidents de ce type sont survenus à plusieurs reprises [39].

Afin de se prémunir d'une réannonce de la table de routage, il est fortement recommandé d'appliquer un filtre sur le nombre maximal de préfixes annoncés par un client ou un AS avec lequel une relation de *peering* est établie. En général, les équipements offrent une certaine flexibilité en permettant de configurer à partir de quel nombre de préfixes annoncés la session sera coupée, et de configurer un seuil pour générer des messages d'avertissement ou des *trap* SNMP[9], en fonction des implémentations. Par exemple, pour un pair annonçant 200 préfixes, il est possible de fixer une limite maximale à 1000 préfixes, et un seuil d'alerte de 400 préfixes.

Filtrage sur le nombre maximum de préfixes reçus - Routeurs Alcatel-Lucent

Extrait 3.31 – Commande permettant de configurer le nombre maximal de préfixes

```
>config>router>bgp>group#
# neighbor <address> prefix-limit <limit> [log-only] [
    threshold <percentage>]
```

Extrait 3.32 – Exemple de configuration du nombre maximal de préfixes

```
# neighbor 192.0.2.3 prefix-limit 1000 threshold 50
```

9. Simple Network Management Protocol.

Extrait 3.31 et 3.32 - Commentaires

Voici les paramètres disponibles pour la commande de l'extrait 3.31 :

- `prefix-limit` est la valeur maximale du nombre de préfixes autorisés pour le pair ;
- `threshold` est le pourcentage du nombre maximal de préfixes autorisés à partir duquel le routeur génère des messages d'avertissement. Lorsque le pourcentage est atteint, un *trap* SNMP est émis. Lorsque la limite est dépassée, la session BGP est coupée sauf si l'option `log-only` est configurée auquel cas seul un nouvel avertissement est émis.

L'exemple 3.32 donne un exemple de configuration d'un nombre maximal de 1000 préfixes, et d'un seuil d'alerte de 500 préfixes.

Filtrage sur le nombre maximum de préfixes reçus - Routeurs Cisco

Extrait 3.33 – Commande permettant de configurer le nombre maximal de préfixes

```
Cisco(config-router-af)#neighbor <ip-address> | <group-name>
   maximum-prefix <maximum> [threshold] [restart
   restart-interval] [warning-only]
```

Extrait 3.33 - Commentaires

Voici les paramètres et options disponibles pour cette commande :

- `maximum` est la valeur maximale du nombre de préfixes autorisés pour le pair ;
- `threshold` est le pourcentage du nombre maximal de préfixes autorisés à partir duquel le routeur génère des messages d'avertissement. Par défaut, des messages sont générés dès lors que le seuil de 75 % du nombre maximal est dépassé ;

- `restart-interval` est la durée en minutes avant que la session soit rétablie (de 1 à 65 535 minutes) ;
- `warning-only` permet d'indiquer que la session ne doit pas être terminée lorsque le nombre de préfixes annoncés dépasse le maximum fixé, mais que des messages d'avertissement doivent être générés.

Extrait 3.34 – Exemple de configuration du nombre maximal de préfixes

```
Cisco(config-router)#address-family ipv6
Cisco(config-router-af)#neighbor 2001:db8:0:3:fac0:100:22d3:
   d000 maximum-prefix 1000 50
```

Extrait 3.34 - Commentaire

Ici, le nombre maximal de préfixes autorisés est de 1000, et le routeur génère des messages d'avertissement lorsque 500 préfixes ou plus sont annoncés.

Filtrage sur le nombre maximum de préfixes reçus - Routeurs Juniper

Extrait 3.35 – Commande permettant de configurer le nombre maximal de préfixes

```
prefix-limit {
  maximum <number>;
  teardown <percentage> [idle-timeout {forever} | <minutes>];
}
```

Extrait 3.35 - Commentaires

Voici les paramètres et options disponibles pour cette commande :

- `maximum` est le nombre maximal de préfixes autorisés pour le voisin (de 1 à 2^{32} - 1) ;
- `teardown` indique que la session se termine si le nombre maximal de préfixes est atteint. Si `teardown` est suivi d'un pourcentage, les messages sont journalisés lorsque ce pourcentage est dépassé. Une fois la session terminée, elle est réinitialisée au bout d'une « courte durée » [40]. Si une durée est précisée via `idle-timeout`, alors la session ne sera réinitialisée qu'une fois cette durée écoulée. Si `forever` est précisé, alors la session ne sera pas réinitialisée.

Par souci de concision, les niveaux hiérarchiques de configuration ne sont pas présentés. Il est possible de configurer le nombre maximal de préfixes au niveau d'un voisin (la configuration est similaire au niveau des *routing-instances* et des *logical-systems*).

Extrait 3.36 – Exemple de configuration d'un nombre maximal de préfixes

```
[edit protocols bgp]
root@Juniper# set group session-to-AS64503 neighbor 2001:db8
   :0:3:fac0:100:22d3:ce80 family inet6 unicast prefix-limit
   maximum 1000 teardown 50
```

Filtrage sur le nombre maximum de préfixes reçus - Routeurs OpenBGPD

Extrait 3.37 – Commande permettant de configurer le nombre maximal de préfixes

```
max-prefix <number> [restart <minutes>]
```

Extrait 3.37 - Commentaires

Voici les paramètres et options disponibles pour cette commande :

- `number` est le nombre maximal de préfixes acceptable. Au-delà de ce seuil, la session se termine ;
- si `restart` est précisé, la session sera rétablie au bout de la durée spécifiée, en minutes.

3.7 Filtrage sur l'AS_PATH des routes annoncées par les pairs

D'une manière générale, il ne faut pas accepter les annonces pour lesquelles le premier numéro d'AS de l'`AS_PATH` (c'est-à-dire, le numéro d'AS le plus à gauche) n'est pas celui du pair. Par exemple, dans le cas d'une interconnexion entre un transitaire et un client « feuille », les annonces des clients devraient être filtrées afin d'éliminer les annonces dont l'`AS_PATH` ne contient pas uniquement le numéro d'AS du client.

Filtrage sur l'`AS_PATH` - Routeurs Alcatel-Lucent

Extrait 3.38 – Commande permettant de créer une règle de filtrage sur les `AS_PATH`

```
>config>router>policy-options#
    as-path <"name"> <"regular expression">
```

Extrait 3.39 – Exemple de configuration permettant de mettre en place un filtre sur le premier AS de l'`AS_PATH`

```
>config>router>policy-options#
    as-path "from-AS64506" "64506 .*"
    policy-statement "from-AS64506"
        entry 10
            from
                protocol bgp
                as-path "from-AS64506"
            exit
```

```
            action accept
            exit
        exit
        default-action reject
    exit
```

Extrait 3.38 et 3.39 - Commentaires

L'extrait 3.38 présente la commande `as-path` permettant de créer une règle de filtrage sur l'`AS_PATH`. Ce type de règle repose sur l'utilisation d'expressions rationnelles.

Le filtre présenté dans l'extrait 3.39 peut être appliqué à un pair comme indiqué dans l'extrait 3.2.

Filtrage sur l'`AS_PATH` - Routeurs Cisco

Extrait 3.40 – Commande permettant de mettre en place un filtre sur le premier AS de l'`AS_PATH`

```
Cisco(config-router)#bgp enforce-first-as
```

Extrait 3.40 - Commentaires

La commande `bgp enforce-first-as` permet de rejeter les routes dont le premier AS dans l'`AS_PATH` ne serait pas celui du pair annonçant cette route. Ce filtrage est activé par défaut [38].

L'extrait 3.40 montre comment faire apparaître explicitement cette fonctionnalité dans la configuration courante du routeur.

Filtrage sur l'AS_PATH - Routeurs Juniper

Extrait 3.41 – Configuration permettant de mettre en place un filtre sur le premier AS de l'AS_PATH

```
[edit policy-options]
root@Juniper# set as-path from-AS64506 "^64506 .*"

[edit policy-options policy-statement match-peer-AS64506]
root@Juniper# set term peer-AS64506 from as-path from-AS64506
root@Juniper# set term peer-AS64506 then accept
root@Juniper# set term reject-other-peers then reject
root@Juniper# show
term peer-AS64506 {
    from as-path from-AS64506;
    then accept;
}
term reject-other-peers {
    then reject;
}
```

Extrait 3.41 - Commentaires

Les règles, basées sur des expressions rationnelles, sont créées à l'aide de la commande as-path <*name*> <*regular-expression*>.

Dans cet exemple, une règle sur l'AS_PATH est créée en utilisant l'expression rationnelle ^64506 .*. Les AS_PATH correspondant à cette expression sont ceux dont le premier numéro d'AS est 64506. Dans la syntaxe Junos, le « . » correspond à un numéro d'AS.

Filtrage sur l'AS_PATH - Routeurs OpenBGPD

Extrait 3.42 – Exemple de configuration permettant de mettre en place un filtre sur le premier AS de l'AS_PATH

```
enforce neighbor-as {yes}
```

Extrait 3.42 - Commentaires

À l'instar de l'exemple de configuration donné pour les routeurs Cisco (3.40), la commande de l'extrait 3.42 permet de rejeter les routes annoncées par un AS dont le numéro n'est pas le dernier ajouté à l'`AS_PATH`. Il s'agit du comportement par défaut de l'implémentation [41].

Chapitre 4

Autres éléments de configuration de BGP

4.1 Utilisation de la journalisation

Les routeurs proposent de nombreuses fonctions de journalisation. La journalisation permet de déceler des problèmes de stabilité et peut s'avérer utile lors d'une intervention suite à un incident. Les enregistrements permettent ainsi d'identifier l'équipement à l'origine de l'entrée de journal, la session concernée, la cause et l'horodatage précis de l'incident. Pour le cas de BGP, et sur les routeurs Cisco et Juniper, les événements de changements d'adjacence ne sont pas journalisés par défaut. Ces événements correspondent aux changements d'état des sessions, ils doivent donc être journalisés. Par défaut, OpenBGPD journalise les changements d'état à l'aide de *syslog* [42]. Pour les routeurs Alcatel-Lucent, les événements BGP sont également journalisés par défaut.

Les routeurs offrent également des fonctions de journalisation plus poussées, permettant par exemple d'enregistrer le contenu des messages échangés. Ces fonctions peuvent s'avérer utiles à des fins de débogage.

Journalisation des événements BGP - Routeurs Alcatel-Lucent

Extrait 4.1 – Exemple d'entrées de journal générées par les routeurs Alcatel-Lucent

```
52915 2012/12/25 17:05:17.00 CET MINOR: BGP #2001 vprn300 Peer 12:
    198.51.100.50 "VR 12: Group CE-IPVPN300: Peer 198.51.100.50:
   moved into established state"

52914 2012/12/25 17:04:45.70 CET WARNING: BGP #2002 vprn300 Peer
   12: 198.51.100.50 "VR 12: Group CE-IPVPN300: Peer
   198.51.100.50: moved from higher state OPENSENT to lower state
   IDLE due to event TCP SOCKET ERROR"
```

```
52913 2012/12/25 17:04:45.70 CET WARNING: BGP #2011 vprn300 Peer
   12: 198.51.100.50 "VR 12: CE-IPVPN300: Peer 198.51.100.50:
   remote end closed connection"

52912 2012/12/25 17:04:45.66 CET WARNING: BGP #2005 vprn300 Peer
   12: 198.51.100.50 "VR 12: CE-IPVPN300: Peer 198.51.100.50:
   sending notification: code HOLDTIME subcode UNSPECIFIED"

52911 2012/12/25 17:04:45.66 CET WARNING: BGP #2002 vprn300 Peer
   12: 198.51.100.50 "VR 12: CE-IPVPN300: Peer 198.51.100.50:
   moved from higher state ESTABLISHED to lower state IDLE due to
   event HOLDTIME"
```

Extrait 4.1 - Commentaires

Par défaut, les événements BGP sont journalisés dans le *log 99* : changements d'état des sessions, réception de messages UPDATE malformés ou de NOTIFICATION. Il est possible de configurer une journalisation plus fine à l'instar des routeurs Cisco ou Juniper.

Journalisation des événements BGP - Routeurs Cisco

Extrait 4.2 – Configuration de la journalisation des changements d'adjacence pour tous les pairs

```
Router(config-router)#bgp log-neighbor-changes
```

Extrait 4.3 – Exemple d'entrées de journal relatives à BGP

```
Jun 25 11:19:28.111: %BGP-5-ADJCHANGE: neighbor 2001:DB8:0:3:
   FAC0:100:22D3:D000 Up
Jun 25 11:25:37.843: %BGP-4-MAXPFX: No. of prefix received
   from 2001:DB8:0:3:FAC0:100:22D3:D000 (afi 1) reaches 8,
   max 10
Jun 25 11:25:37.843: %BGP-3-MAXPFXEXCEED: No. of prefix
   received from 2001:DB8:0:3:FAC0:100:22D3:D000 (afi 1): 11
   exceed limit 10
```

```
Jun 25 11:25:37.843: %BGP-5-ADJCHANGE: neighbor 2001:DB8:0:3:
   FAC0:100:22D3:D000 Down BGP Notification sent
```

Extrait 4.3 - Commentaires

Cet extrait donne un exemple d'entrées de journal relatives aux changements d'adjacence et au nombre maximal de préfixes annonçables par un pair sur un routeur Cisco. Dans cet exemple, une session BGP est montée avec un pair à l'adresse 2001:db8:0:3:fac0:100:22d3:d000. La seconde entrée du journal est un message d'avertissement de dépassement d'un seuil d'alerte. La troisième entrée indique que la limite maximale a été dépassée (11 préfixes annoncés, soit 1 de plus que la limite fixée à 10). Enfin, la dernière entrée du journal indique qu'un message de type NOTIFICATION a été envoyé au pair, mettant fin à la session.

Journalisation des événements BGP - Routeurs Juniper

Extrait 4.4 – Configuration de la journalisation des changements d'adjacence pour tous les pairs

```
[edit protocols bgp]
root@Juniper# set log-updown
```

Extrait 4.5 – Exemple d'entrées de journal relatives à BGP

```
Jul 15 11:24:07 JUNIPER rpd[1176]: bgp_peer_mgmt_clear:5992:
   NOTIFICATION sent to 192.0.2.1 (External AS 64501): code 6
    (Cease) subcode 4 (Administratively Reset), Reason:
   Management session cleared BGP neighbor
Jul 15 11:24:07 JUNIPER rpd[1176]:
   RPD_BGP_NEIGHBOR_STATE_CHANGED: BGP peer 192.0.2.1 (
   External AS 64501) changed state from Established to Idle
   (event Stop)
Jul 15 11:24:39 JUNIPER rpd[1176]:
   RPD_BGP_NEIGHBOR_STATE_CHANGED: BGP peer 192.0.2.1 (
   External AS 64501) changed state from OpenConfirm to
```

```
Established (event RecvKeepAlive)
```

Extraits 4.4 et 4.5 - Commentaires

Sur les routeurs Juniper, la commande `log-updown` permet d'activer la journalisation des changements d'adjacence.

L'extrait 4.4 montre un exemple d'activation globale, c'est-à-dire pour tous les pairs BGP, et l'extrait 4.5 donne un exemple d'entrées de journal pour un redémarrage de session provoqué par un administrateur.

Journalisation des événements BGP - Routeurs OpenBGPD

Extrait 4.6 – Exemple d'entrées de journal générées par OpenBGPD

```
Apr 29 15:58:49 openbsd64-1 bgpd[13682]: neighbor 192.0.2.2: state
    change None -> Idle, reason: None
Apr 29 15:58:49 openbsd64-1 bgpd[13682]: neighbor 192.0.2.2: state
    change Idle -> Connect, reason: Start
Apr 29 15:58:49 openbsd64-1 bgpd[13682]: neighbor 192.0.2.2: state
    change Connect -> OpenSent, reason: Connection opened
Apr 29 15:58:49 openbsd64-1 bgpd[13682]: neighbor 192.0.2.2: state
    change OpenSent -> Active, reason: Connection closed
Apr 29 15:59:54 openbsd64-1 bgpd[13682]: neighbor 192.0.2.2: state
    change Active -> OpenSent, reason: Connection opened
Apr 29 15:59:54 openbsd64-1 bgpd[13682]: neighbor 192.0.2.2: state
    change OpenSent -> OpenConfirm, reason: OPEN message received
Apr 29 15:59:54 openbsd64-1 bgpd[13682]: neighbor 192.0.2.2: state
    change OpenConfirm -> Established, reason: KEEPALIVE message
   received
```

Extraits 4.6 - Commentaires

L'extrait 4.6 donne un exemple de journal généré par OpenBGPD lors de l'établissement d'une session. Les événements de changement d'adjacence sont journalisés par défaut dans le fichier `/var/log/daemon` (aucune commande spécifique à OpenBGPD n'est nécessaire pour activer cette journalisation).

4.2 Le Mécanisme de Graceful Restart

Le mécanisme de *Graceful Restart*, spécifié pour BGP dans la RFC 4724 [43], permet de limiter l'indisponibilité des préfixes dûe au redémarrage du processus BGP sur un routeur. Sur une interconnexion BGP entre deux pairs, l'annonce de la capacité dite de *Graceful Restart* permet de conserver le transfert des paquets pendant le redémarrage du processus BGP d'un des deux routeurs. Le transfert s'effectue pendant une durée limitée au-delà de laquelle les routes utilisées sont supprimées. Une fois le redémarrage effectué, le routeur sélectionne les meilleures routes parmi celles que ses pairs lui ont envoyées, et met à jour sa RIB [1] et sa FIB [2].

Graceful Restart - Routeurs Alcatel-Lucent

Extrait 4.7 – Commande permettant de configurer le mécanisme de Graceful Restart sur des routeurs Alcatel-Lucent

```
>config>router>bgp>group#
    group "EBGP"
        graceful-restart [stale-routes-time <time>]
```

Extrait 4.7 - Commentaires

Le paramètre `stale-routes-time` permet de fixer la durée maximale pendant laquelle le routeur conserve les routes marquées comme « périmées » avant de les supprimer. Cette durée peut prendre des valeurs de 1 à 3600 secondes. La valeur par défaut est de 360 secondes. Ce mécanisme se configure sur un voisin, un groupe ou dans le contexte BGP.

Graceful Restart - Routeurs Cisco

Extrait 4.8 – Configuration du mécanisme de Graceful Restart

```
Router(config-router)#bgp graceful-restart [restart-time
    <seconds> | stalepath-time <seconds>]
```

1. *Routing Information Base* ou table de routage.
2. *Forwarding Information Base* ou table de transfert.

Extrait 4.8 - Commentaires

Le *Graceful Restart* peut être configuré en mode de configuration `router` ou `address-family`. Voici les options disponibles pour cette commande :

- `restart-time` permet de fixer la durée maximale pendant laquelle le routeur va attendre qu'un pair rédémarre. Cette durée peut prendre des valeurs de 1 à 3600 secondes. La valeur par défaut est de 120 secondes ;

- `stalepath-time` permet de fixer la durée maximale pendant laquelle le routeur va conserver les routes marquées comme « périmées » avant de les supprimer. Cette durée peut prendre des valeurs de 1 à 3600 secondes. La valeur par défaut est de 360 secondes.

Extrait 4.9 – Exemple de configuration du mécanisme de Graceful Restart

```
Cisco(config)#router bgp 64506
Cisco(config-router)#bgp graceful-restart restart-time 120
Cisco(config-router)#bgp graceful-restart stalepath-time 360
```

Graceful Restart - Routeurs Juniper

Extrait 4.10 – Configuration du mécanisme de Graceful Restart

```
[edit protocols bgp]
graceful-restart {
  restart-time <seconds>;
  stale-routes-time <seconds>;
}
```

Extrait 4.10 - Commentaires

Voici les options disponibles pour cette commande :

- `restart-time` permet d'indiquer, en secondes, la durée prévue pour le redémarrage. La valeur peut être comprise entre 1 et 600 secondes. Par défaut, la durée est de 120 secondes ;
- `stale-routes-time` permet de fixer, en secondes, la durée pendant laquelle les routes marquées comme périmées seront conservées dans la FIB. La durée peut être comprise entre 1 et 600 secondes. Par défaut, la durée est de 300 secondes.

Extrait 4.11 – Exemple de configuration du mécanisme de Graceful Restart

```
[edit protocols bgp]
root@Juniper# set graceful-restart restart-time 120
root@Juniper# set graceful-restart stale-routes-time 360
root@Juniper# show graceful-restart
restart-time 120;
stale-routes-time 360;
```

Graceful Restart - Routeurs OpenBGPD

OpenBGPD et le *Graceful Restart*

La version testée d'OpenBGPD ne supporte pas le mécanisme de *Graceful Restart*. Cependant, OpenBGPD est capable de générer le marqueur de « fin de *Routing Information Base* » [43] après avoir réannoncé l'ensemble de ses routes au pair venant de redémarrer. L'annonce de ce marqueur autorise ce dernier à débuter le processus de sélection des routes, et favorise ainsi la convergence. En effet, en son absence, le pair venant de redémarrer doit attendre un certain délai avant de pouvoir commencer le processus de sélection.

Chapitre 5

Éléments de configuration générale des routeurs

Les mécanismes décrits dans cette section ne sont pas propres à la sécurité de BGP, mais peuvent contribuer à renforcer la robustesse des interconnexions.

5.1 Prévenir l'usurpation d'adresses IP

Les attaques de type déni de service impliquent souvent des adresses sources usurpées, afin de masquer l'origine de l'attaque et de rendre plus difficile la mise en place de filtres pour éliminer ce trafic. La technique dite de l'URPF [1] *Unicast Reverse Path Forwarding* a été créée dans le but de lutter contre l'usurpation d'adresses IP. Cette technique n'est pas liée à BGP, mais elle peut être utilisée pour limiter l'impact sur un routeur BGP en cas d'attaque par déni de service. Son principe de fonctionnement repose sur une vérification systématique de la correspondance entre les adresses source, l'interface sur laquelle les paquets arrivent et les entrées de la FIB pouvant permettre de joindre la source. Plus précisément, il existe trois principaux modes de fonctionnement, décrits dans la RFC 3704 [44] :

- le mode *strict*, qui permet de vérifier que l'adresse source d'un paquet arrivant sur une interface est joignable par une route présente dans la FIB et que l'interface qui serait utilisée pour la joindre est l'interface sur laquelle le paquet a été reçu ;

- le mode *feasible path* est une extension du mode strict. Dans ce mode, les routes alternatives, c'est-à-dire les routes qui ne sont pas utilisées par la FIB, sont également prises en compte pour le test ;

- le mode *loose*, qui vérifie uniquement que l'adresse source d'un paquet arrivant sur le routeur est joignable par une route présente dans la FIB. L'interface qui sera utilisée pour joindre la source n'est pas prise en compte pour ce mode. Le mode *loose* permet de rejeter les paquets dont l'adresse IP source n'est pas *routée* sur l'Internet.

1. Unicast Reverse Path Forwarding.

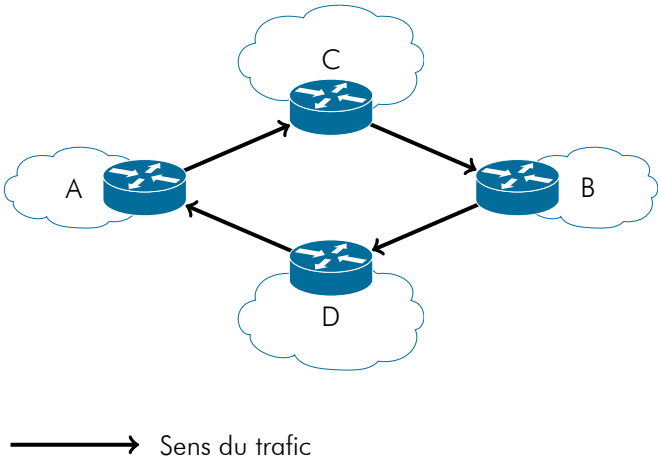


Figure 5.1 Routage asymétrique entre l'AS A et l'AS B.

Pour ces trois modes, si les conditions ne sont pas vérifiées, les paquets sont rejetés.

Le mode strict ne peut pas être employé en cas de routage asymétrique, comme l'illustre la figure 5.1, puisqu'il entraînerait l'élimination d'une partie du trafic légitime. Par exemple, sur la figure 5.1, si l'URPF est activé en mode strict au niveau du routeur de l'AS A, le trafic venant de l'AS B serait rejeté. En effet, la route empruntée (de l'AS B vers l'AS D, puis de l'AS D vers l'AS A) est différente de celle utilisée pour envoyer du trafic vers cet AS (de l'AS A vers l'AS C, puis de l'AS C vers l'AS B).

Dans ce cas de figure, il est possible de recourir au mode *feasible path*, qui prend en compte la route alternative passant par l'AS D. Cependant, le mode *feasible path* est implémenté sur les routeurs Juniper, mais pas sur les routeurs Alcatel-Lucent, Cisco ou OpenBGPD. Pour ces dernières implémentations, en cas de *multihoming*, seul le mode *loose* peut être utilisé.

Configuration de l'URPF - Routeurs Alcatel-Lucent

Extrait 5.1 – Commande permettant de configurer l'URPF

```
config
  router <router-name>
    interface <ip-int-name>
      urpf-check
        mode {strict | loose}
```

```
        no mode
      ipv6
        urpf-check
          mode {strict | loose}
          no mode
```

Extrait 5.7 - Commentaires

L'extrait 5.1 fournit la commande permettant de configurer l'URPF sur des routeurs Alcatel-Lucent. Par défaut, ce mécanisme n'est pas activé.

Voici les paramètres et options disponibles pour cette commande :

- `mode` permet de configurer le mode (*strict* ou *loose*) ;
- `no mode` permet de revenir au mode *strict*, qui est le mode par défaut.

Extrait 5.2 – Exemple de configuration de l'URPF en mode loose

```
>config>service#
  ies 200 customer 1 create
    interface "from_client" create
      urpf-check
        mode loose
      exit
      ipv6
        urpf-check
          mode loose
        exit
      exit
    exit
```

Extrait 5.7 - Commentaires

L'extrait 5.2 donne un exemple de configuration de l'URPF en mode *loose* sur des routeurs Alcatel-Lucent.

Si la route par défaut est présente dans la table de routage et que le mode

loose est configuré, alors le test réussit. Cependant, si l'adresse source d'un paquet correspond à une route utilisée pour du *black-holing*, alors le test de l'URPF échoue.

Par défaut, les paquets ne satisfaisant pas le test sont rejetés silencieusement.

Configuration de l'URPF - Routeurs Cisco

Extrait 5.3 – Commande permettant d'activer l'URPF sur une interface

```
Cisco(config-if)#ip verify unicast source reachable-via {rx |
    any} [allow-default] [allow-self-ping] [list]
```

Voici les paramètres et options disponibles pour cette commande :

- `rx` active le mode strict, tandis que `any` active le mode *loose* ;
- `allow-default` permet d'inclure la route par défaut dans le test ;
- `allow-self-ping` permet d'autoriser le routeur à *pinger* ses propres interfaces, ce qui impossible par défaut lorsque l'URPF est activé ;
- `list` est une *access-list* qui sera utilisée si le test de l'URPF échoue. Il est ainsi possible d'autoriser des sources pour lesquelles le test échouerait, ou de journaliser les paquets entrants avec des sources spécifiques, avant de les rejeter. Si aucune *access-list* précisant une journalisation n'est donnée en paramètre, les paquets sont rejetés mais non journalisés. En revanche, les compteurs de paquets rejetés associés à l'URPF sont mis à jour.

Extrait 5.4 – Exemple de configuration de l'URPF en mode loose

```
Cisco(config-if)#ip verify unicast source reachable-via any
```

Configuration de l'URPF - Routeurs Juniper

Extrait 5.5 – Commande permettant de configurer l'URPF

```
[edit logical-systems logical-system-name routing-options
    forwarding-table]
[edit routing-instances routing-instance-name instance-type name
    routing-options forwarding-table]
[edit routing-options forwarding-table]
root@Juniper# set unicast-reverse-path (active-paths |
    feasible-paths);
```

Extrait 5.6 – Commande permettant d'activer l'URPF sur une interface

```
[edit interfaces interface-name unit logical-unit-number family
    family]
[edit logical-systems logical-system-name interfaces
    interface-name unit logical-unit-number family family]
rpf-check {
  fail-filter <filter-name>;
  mode loose;
}
```

Extraits 5.5 et 5.6 - Commentaires

La commande `unicast-reverse-path` permet d'activer l'URPF. Si le paramètre `active-paths` est fourni, alors l'URPF examinera uniquement les routes actives de la FIB, c'est-à-dire les routes choisies pour le transfert des paquets. Si le paramètre `feasible-paths` est fourni, alors l'URPF examinera également les routes alternatives, c'est-à-dire qui ne sont pas nécessairement les routes actives de la FIB.

Une fois l'URPF configuré, il faut l'activer sur une interface à l'aide de la commande présentée dans l'extrait 5.6. À l'instar des routeurs Cisco, un filtre peut être configuré afin de définir des actions particulières, comme la journalisation, si le test échoue. Par défaut, les paquets sont rejetés silencieusement. L'URPF peut être configuré en mode *loose* en précisant `mode loose`.

Configuration de l'URPF - PF (routeurs OpenBGPD)

Extrait 5.7 – Commande permettant de configurer l'URPF

```
block in [quick] from urpf-failed [label <urpf>]
```

Extrait 5.7 - Commentaires

L'extrait 5.7 indique comment configurer l'URPF à l'aide de *Packet Filter*. Sur OpenBSD, seul le mode strict est disponible. De plus, si la route par défaut emprunte l'interface sur laquelle l'URPF est actif, la route n'est pas exclue lors du test : le mécanisme est donc inutile sur l'interface.

Afin de journaliser les paquets ayant fait échouer le test, il est possible d'ajouter le paramètre `log` à l'action `block`. La commande devient alors :
`block in [log] [quick] from urpf-failed [label <urpf>]`.

5.2 Durcissement de la configuration du routeur

La mise en œuvre des éléments de bonnes pratiques de configuration décrits dans ce document doit être accompagnée de mesures de protection du routeur. Plus généralement, les configurations des équipements et les moyens d'administration peuvent se baser sur les mesures d'hygiène informatique décrites dans le guide de l'ANSSI [45]. On pourra, entre autres :

- recourir à des protocoles sécurisés pour accéder au routeur (par exemple, SSH [46] avec authentification par clé publique) ;
- restreindre l'accès à l'équipement :
  - utilisation d'une interface d'administration dédiée ;
  - connexion depuis des adresses IP autorisées ;
  - définition de comptes utilisateurs dédiés à une utilisation spécifique …
- désactiver les services (processus ou protocoles) inutiles ;
- appliquer les bonnes pratiques de configuration des différents protocoles mis en œuvre par l'équipement ;
- utiliser des systèmes d'exploitation ou des *firmwares* à jour …

Les guides de configuration proposés par les équipementiers donnent les éléments de configuration permettant de durcir la configuration des équipements et implémentations.

5.2.1 Protection du plan de contrôle

Les tâches réalisées au niveau du plan de contrôle alimentent la FIB, c'est-à-dire les tables de transfert utilisées par le plan de transfert. Les processus des protocoles de routage comme BGP opèrent notamment au sein du plan de contrôle des routeurs. En conséquence, la protection du plan de contrôle est également un élément essentiel relatif à la sécurité de BGP. La nature variée des tâches réalisées au niveau du plan de contrôle explique que ce dernier soit implémenté avec des unités de calcul génériques. Le plan de transfert, en revanche, repose sur des ASIC[2] dédiés à des traitements spécifiques des paquets (opérations de transfert des paquets vers une interface appropriée ou vers le plan de contrôle). Ces composants matériels offrent une capacité de traitement de paquets très importante, et en particulier, bien supérieure à celle du plan de contrôle. En conséquence, ce dernier est plus susceptible d'être surchargé lors d'une attaque de type déni de service que le plan de transfert.

La protection du plan de contrôle a pour objectif principal de réduire sa surface d'attaque. Cela passe par la mise en place de filtres devant permettre d'éliminer la plus grande partie d'un trafic illégitime avant que ce dernier n'atteigne le plan de contrôle. La RFC 6192 [47] décrit le principe de filtrage permettant de protéger le plan de contrôle des routeurs et fournit des exemples de configuration permettant de mettre en œuvre les filtres décrits pour des routeurs Cisco et Juniper.

2. Application Specific Integrated Circuits.

Annexe A

Espace d'adressage IPv6

Les tableaux A.1 et A.2 donnent respectivement les préfixes réservés par l'IETF et les préfixes réservés appartenant au 2000::/3. La liste peut être obtenue par les registres de l'IANA : *Internet Protocol Version 6 Address Space* [17] et *IPv6 Global Unicast Address Assignments* [18]. La version du 15 février 2013 a été utilisée pour constituer ces tableaux.

Espace IPv6 réservé	
0000::/8 0100::/8 0400::/6 0800::/5 1000::/4 4000::/3 6000::/3 8000::/3 a000::/3 c000::/3 e000::/4 f000::/5 f800::/6 fe00::/9	réservé par l'IETF [19]
0200::/7	réservé par l'IETF [48].
fec0::/10	réservé par l'IETF [49].

Table A.1 Préfixes IPv6 réservés.

Espace IPv6 *Global Unicast*	
2001:3c00::/22 2d00:0000::/8 2e00:0000::/7 3000:0000::/4	réservé par l'IANA.
3ffe::/16 5f00::/8	préfixes qui étaient auparavant réservés pour le *6bone*, le réseau de test IPv6.

Table A.2 Espace *Global Unicast*.

Bibliographie

[1] AFNIC and ANSSI, « Observatoire de la Résilience de l'Internet français ». <http://www.ssi.gouv.fr/observatoire>, juillet 2013.

[2] RIPE-NCC, « RIPE Routing Working Group Recommendations on Route Aggregation ». <http://www.ripe.net/ripe/docs/ripe-399>, décembre 2006.

[3] RIPE-NCC, « RIPE Routing Working Group Recommendations on IPv6 Route Aggregation ». <http://www.ripe.net/ripe/docs/ripe-532>, novembre 2011.

[4] P. A. Watson, « Slipping in the Window : TCP Reset Attacks, CanSecWest », 2004.

[5] A. Ramaiah, R. Stewart et M. Dalal, « Improving TCP's Robustness to Blind In-Window Attacks ». RFC 5961 (Proposed Standard), août 2010.

[6] J. Touch, « Defending TCP Against Spoofing Attacks ». RFC 4953 (Informational), juil. 2007.

[7] Y. Rekhter, T. Li et S. Hares, « A Border Gateway Protocol 4 (BGP-4) ». RFC 4271 (Draft Standard), jan. 2006. Updated by RFCs 6286, 6608, 6793.

[8] A. Heffernan, « Protection of BGP Sessions via the TCP MD5 Signature Option ». RFC 2385 (Proposed Standard), août 1998. Obsoleted by RFC 5925, updated by RFC 6691.

[9] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Référentiel Général de Sécurité - version 1.0 ». <http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf>, janvier 2010.

[10] J. Touch, A. Mankin et R. Bonica, « The TCP Authentication Option ». RFC 5925 (Proposed Standard), juin 2010.

[11] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Recommandations de sécurité relatives aux mots de passe ». <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html>, mai 2012.

[12] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot et E. Lear, « Address Allocation for Private Internets ». RFC 1918 (Best Current Practice), fév. 1996. Updated by RFC 6761.

[13] M. Cotton, L. Vegoda, R. Bonica et B. Haberman, « Special-Purpose IP Address Registries ». RFC 6890 (Best Current Practice), avril 2013.

[14] IANA, « IPv4 Address Space Registry ». <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt>, mars 2013.

[15] A. Durand, R. Droms, J. Woodyatt et Y. Lee, « Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion ». RFC 6333 (Proposed Standard), août 2011.

[16] IANA, « IANA IPv6 Special Purpose Address Registry ». <http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.txt>, mai 2013.

[17] IANA, « Internet Protocol Version 6 Address Space ». <http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.txt>, février 2013.

[18] IANA, « IPv6 Global Unicast Address Assignments ». <http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.txt>, février 2013.

[19] R. Hinden et S. Deering, « IP Version 6 Addressing Architecture ». RFC 4291 (Draft Standard), fév. 2006. Updated by RFCs 5952, 6052.

[20] R. Braden, « Requirements for Internet Hosts - Communication Layers ». RFC 1122 (INTERNET STANDARD), oct. 1989. Updated by RFCs 1349, 4379, 5884, 6093, 6298, 6633, 6864.

[21] S. Cheshire, B. Aboba et E. Guttman, « Dynamic Configuration of IPv4 Link-Local Addresses ». RFC 3927 (Proposed Standard), mai 2005.

[22] S. Bradner et J. McQuaid, « Benchmarking Methodology for Network Interconnect Devices ». RFC 2544 (Informational), mars 1999. Updated by RFCs 6201, 6815.

[23] J. Arkko, M. Cotton et L. Vegoda, « IPv4 Address Blocks Reserved for Documentation ». RFC 5737 (Informational), jan. 2010.

[24] J. Weil, V. Kuarsingh, C. Donley, C. Liljenstolpe et M. Azinger, « IANA-Reserved IPv4 Prefix for Shared Address Space ». RFC 6598 (Best Current Practice), avril 2012.

[25] M. Cotton, L. Vegoda et D. Meyer, « IANA Guidelines for IPv4 Multicast Address Assignments ». RFC 5771 (Best Current Practice), mars 2010.

[26] S. Deering, « Host extensions for IP multicasting ». RFC 1112 (INTERNET STANDARD), août 1989. Updated by RFC 2236.

[27] J. Mogul, « Broadcasting Internet Datagrams ». RFC 919 (INTERNET STANDARD), oct. 1984.

[28] N. Hilliard et D. Freedman, « A Discard Prefix for IPv6 ». RFC 6666 (Informational), août 2012.

[29] R. Hinden, S. Deering, R. Fink et T. Hain, « Initial IPv6 Sub-TLA ID Assignments ». RFC 2928 (Informational), sept. 2000.

[30] C. Huitema, « Teredo : Tunneling IPv6 over UDP through Network Address Translations (NATs) ». RFC 4380 (Proposed Standard), fév. 2006. Updated by RFCs 5991, 6081.

[31] C. Popoviciu, A. Hamza, G. V. de Velde et D. Dugatkin, « IPv6 Benchmarking Methodology for Network Interconnect Devices ». RFC 5180 (Informational), mai 2008.

[32] P. Nikander, J. Laganier et F. Dupont, « An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID) ». RFC 4843 (Experimental), avril 2007.

[33] G. Huston, A. Lord et P. Smith, « IPv6 Address Prefix Reserved for Documentation ». RFC 3849 (Informational), juil. 2004.

[34] B. Carpenter et K. Moore, « Connection of IPv6 Domains via IPv4 Clouds ». RFC 3056 (Proposed Standard), fév. 2001.

[35] R. Hinden et B. Haberman, « Unique Local IPv6 Unicast Addresses ». RFC 4193 (Proposed Standard), oct. 2005.

[36] IANA, « Autonomous System (AS) Numbers ». <http://www.iana.org/assignments/as-numbers/as-numbers.txt>, avril 2013.

[37] J. Mitchell, « Autonomous System (AS) Reservation for Private Use ». RFC 6996 (Best Current Practice), juil. 2013.

[38] C. Systems, « Cisco IOS IP Routing : BGP Command Reference ». <http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html>, mars 2011.

[39] F. Contat, S. Nataf et G. Valadon, « Influence des bonnes pratiques sur les incidents BGP ». <https://www.sstic.org/2012/presentation/influence_des_bonnes_pratiques_sur_les_incidents_bgp/>, juin 2012.

[40] Juniper Networks, « Technical Documentation - prefix-limit ». <http://www.juniper.net/techpubs/en_US/junos11.4/topics/reference/configuration-statement/prefix-limit-edit-protocols-bgp.html>, octobre 2011.

[41] OpenBSD, « OpenBGPD : Manual pages ». <http://www.openbgpd.org/manual.html>, janvier 2013.

[42] R. Gerhards, « The Syslog Protocol ». RFC 5424 (Proposed Standard), mars 2009.

[43] S. Sangli, E. Chen, R. Fernando, J. Scudder et Y. Rekhter, « Graceful Restart Mechanism for BGP ». RFC 4724 (Proposed Standard), jan. 2007.

[44] F. Baker et P. Savola, « Ingress Filtering for Multihomed Networks ». RFC 3704 (Best Current Practice), mars 2004.

[45] Agence nationale de la sécurité des systèmes d'information (ANSSI), « Guide d'hygiène informatique ». <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html>, janvier 2013.

[46] T. Ylonen et C. Lonvick, « The Secure Shell (SSH) Protocol Architecture ». RFC 4251 (Proposed Standard), jan. 2006.

[47] D. Dugal, C. Pignataro et R. Dunn, « Protecting the Router Control Plane ». RFC 6192 (Informational), mars 2011.

[48] B. Carpenter, « RFC 1888 Is Obsolete ». RFC 4048 (Informational), avril 2005. Updated by RFC 4548.

[49] C. Huitema et B. Carpenter, « Deprecating Site Local Addresses ». RFC 3879 (Proposed Standard), sept. 2004.

Acronymes

ANSSI	Agence nationale de la sécurité des systèmes d'information
AS	Autonomous System (Système autonome)
ASIC	Application Specific Integrated Circuits
BGP	Border Gateway Protocol
EBGP	External Border Gateway Protocol
FIB	*Forwarding Information Base* ou table de transfert
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IRR	Internet Routing Registry
MAC	Message Authentication Code
RIB	*Routing Information Base* ou table de routage
RIR	Regional Internet Registry
SNMP	Simple Network Management Protocol
URPF	Unicast Reverse Path Forwarding

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Septembre 2013

Agence nationale de la sécurité des systèmes d'information
ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr