La sécurité dans une transition vers IPv6

Gaël Beauquin
CNRS UREC
gael.beauquin@urec.cnrs.fr

Table des matières

Introduction

Lentement mais sûrement, l'IPv6 commence à se mettre en place. Il est aujourd'hui possible pour beaucoup de laboratoires de se connecter via ce protocole. Mais qu'en est-il de l'aspect sécurité ? Qu'est-ce qui va changer avec IPv6, qu'est-ce qui ne va pas changer avec IPv6, et quels nouveaux aspects de sécurité vont apparaître avec sa mise en place ? Ce document est là pour préparer et sensibiliser les administrateurs systèmes et réseaux à la facette sécurité de IPv6.

I. Les différents moyens d'implémenter IPv6

La problématique avec IPv6 n'est pas uniquement de mettre en place le protocole, mais de s'assurer qu'IPv4 et IPv6 puissent cohabiter ensemble. Pour cela, il y a différents moyens de permettre à votre réseau de communiquer en IPv6 avec le reste du monde. Ces moyens sont la double pile et le tunneling. Cette documentation ne s'étendra pas sur les tenants et aboutissants de chaque technique, mais se focalisera sur l'aspect sécurité en précisant les avantages et les inconvénients.

1) Double pile

La double pile consiste à implémenter IPv6 sur l'ensemble du réseau (routeur, firewalls, postes de travail) et à le faire tourner conjointement à IPv4. Chaque équipement possède une adresse IPv4 et une ou plusieurs adresses IPv6.

2) Tunneling

De la même façon que l'on peut établir un tunnel IPv4 pour relier 2 réseaux distants, il est possible d'établir un tunnel IPv4 pour faire passer de l'IPv6. Lorsque l'on souhaite communiquer en IPv6 avec le reste du monde, mais que le réseau que vous utilisez pour atteindre l'extérieur ne le permet pas, le tunnel est la bonne solution. Toutefois, le problème du tunnel est que par défaut, il est possible à n'importe qui d'établir un tunnel, ce qui rend inutile les filtrages mis en place au niveau du routeur et du firewall. Le problème existe déjà en IPv4, mais les tunnels IPv4 sont relativement peu répandus, alors que le tunnel IPv6 est une solution assez commune. A noter qu'il est possible d'établir un tunnel sur une passerelle pour l'ensemble du réseau, résultant en un mélange de double pile et de tunneling.

3) Quelle méthode choisir, et pourquoi ?

Renater offre gratuitement la connection en IPv6 à ceux qui sont reliés à son réseau, et fournit gracieusement un service de tunnel Broker pour les autres. La méthode préconisée est la double pile. Cette méthode est la seule solution qui permet d'avoir un réseau IPv6 natif de bout en bout, ce qui est tout de même le but à long terme. De plus, les tunnels rendent bien plus compliquée la mise en place de règles de sécurité. L'architecture IPv6 suivra a priori l'architecture IPv4 (à moins qu'une raison spécifique de faire autrement ne s'impose), donc les flux resteront les mêmes, ce seront les mêmes équipements réseaux qui traiteront IPv4 et IPv6. A noter qu'il faudra donc gérer deux protocoles sur le même réseau, le plus important étant les pare-feu qui auront deux ensembles de règles indépendants.

II.Les changements apportés par IPv6

Cette partie va parler des choses nécessaires de connaitre au sujet d'IPv6, étant une évolution d'IPv4, certaines caractéristiques seront inchangées tandis que d'autres sont modifiés et que de nouvelles fonctionnalités sont introduites.

1) Ce qui ne change pas

Fondamentalement, IPv4 et IPv6 sont très similaires, et reposent sur les mêmes principes pour un grand nombre de points. Même si l'en-tête des paquets sont différents, on y retrouve à peu de choses près les mêmes informations. Par conséquent, certaines attaques existantes en IPv4 sont toujours appliquables en IPv6. La sécurité physique est donc toujours aussi importante, car une personne mal intentionnée qui peut connecter sa machine directement sur le réseau aura toujours autant de possibilités d'attaques (voire même plus comme nous le verrons un peu plus loin).

De même, il est tout aussi simple de renifler des paquets IPv6 que des paquets IPv4, avec toutes les conséquences que cela peut entraîner. Les attaques basées sur l'envoi massif de paquets sont tout autant possibles, avec cependant une légère modification: IPv6 n'a plus la notion de broadcast.

En IPv4, une technique courante pour dissimuler des attaques aux yeux des Intrusion Detection System est d'utiliser des paquets fragmentés. Cette méthode est toujours possible en IPv6 malgré le changement de la gestion de la fragmentation (voir partie II.3). L'IP spoofing (envoyer des paquets avec une adresse source modifiée) est également possible en IPv6.

Les protocoles de routage ont été aménagés pour pouvoir gérer IPv6, mais aucune mesure de sécurité spéciale n'a été ajoutée.

2) Les changements dus à la multiplication d'adresses

Un des changements apportés avec IPv6 est l'augmentation de l'espace d'adressage, afin de palier à la carence d'adresses dont fait l'objet IPv4. Du point de vue sécurité, cette caractéristique est intéressante puisqu'il devient plus fastidieux de scanner des plages d'adresses.

Cependant, il ne faut pas négliger le fait que pour des questions de facilité mnémoniques, l'administrateur a tendance à donner des adresses faciles à retenir et donc faciles à découvrir pour les machines primordiales qui hébergent des services. C'est d'autant plus facile pour les machines dont le nom DNS est du type webmail.domaine.pays.

Les postes clients ne seront pas totalement dissimulés non plus. Les adresses IPv6 attribuées via autoconfiguration ou DHCP sur une large réserve s'apparentent à 2001:200:0:8002:203:47ff:fea5:3085 et sont impossibles à mémoriser. Il leur faudra donc un nom DNS attribué d'une façon ou d'une autre, et ce sera également un moyen de remonter jusqu'à l'adresse. Et même sans celà, l'autoconfiguration utilise l'adresse MAC de l'interface réseau pour déterminer une adresse IPv6. Si on a quelques informations sur le parc informatique, il est possible de deviner une partie des adresses d'autoconfiguration en utilisant le préfixe constructeur de

l'adresse MAC, et par conséquent, de réduire le champ de recherche. Enfin, dans le cade d'une double pile, les machines auront également une connectivité IPv4, et seront donc toujours accessible par ce bias.

Une autre possibilité de découverte de machine est envisageable : celle où un pirate réussit à prendre le contrôle d'une machine en interne. Dans ce cas il pourra lancer un renifleur de paquets qui lui permettra de découvrir, en fonction de la configuration du commutateur, les adresses qui sont actives.

Un domaine dans lequel la multiplication d'adresses pourra apporter un plus non négligeable sont les vers. En effet, pour pouvoir se propager aussi vite que possible, ils tentent d'infecter un maximum d'adresses IP en prenant des adresses au hasard et/ou en attaquant des blocs d'adresses. Ils auront donc possiblement beaucoup de mal à trouver des cibles, et cela pourrait ralentir considérablement leur expansion. Bien sûr, le déploiement d'IPv6 n'en est encore qu'à ses débuts, et aucune version IPv6 de ver n'a encore fait son apparition, donc il est difficile de juger de l'impact réel.

3) Les nouvelles fonctionnalités qu'il faut connaitre

L'augmentation de l'espace d'adressage n'est pas le seul changement apporté par IPv6, bien entendu. Il apporte également de nouvelles fonctionnalités, qui sont à prendre en compte dans le cadre de la sécurité : les multiples adresses IPv6, les multicast, la privacy extension, la mobilité IPv6, la fragmentation, et l'autoconfiguration du réseau.

- Multiples adresses
Une interface réseau IPv6 aura plusieurs adresses IPv6, tandis que cette même interface sur réseau IPv4 n'a généralement qu'une seule adresse. La raison à cela est qu'il existe plusieurs types d'adresse IPv6, “link-local”, “site-local”, et “global”. La notion de site-local est très peu utilisée, et la RFC 3879 les déclare même obsolète, décision contestée aujourd'hui. Voici un article qui parle de ce sujet : http://people.redhat.com/drepper/linux-rfc3484.html. En attendant que le sujet s'éclaircisse, je continuerai à parler des adresses site-local.

- Les multicasts

  Comme dit précédemment, la notion de broadcast n'existe plus en IPv6. En revanche, de nouveaux multicasts font leur apparition, et ils peuvent être utilisés pour trouver ou communiquer avec des machines spécifiques. Pour mieux cerner les multicasts, voici une liste concrète :
- * Multicast en link-local
  - All nodes FF02::1
    All routers FF02::2
    All DHCP-agents FF02::1:2
  * Multicast en site-local
    All routers FF05::2
    All DHCP servers FF05::1:3
-

Les adresses link-local commencent par la valeur FE80, et ne doivent pas être routées. Elles servent uniquement à communiquer sur le brin réseau. Les adresses site local commencent par la valeur FCE0, et ne doivent être routées qu'au sein d'un même site. Les adresses globales sont l'équivalent des adresses publiques IPv4, adresses qui peuvent être routées partout. Une machine aura toujours une adresse link-local, elle obtiendra une adresse global via DHCP ou autoconfiguration selon le réseau, l'adresse site-local est optionelle. La liste des adresses global attribuées est disponible sur le site de l'IANA : http://www.iana.org/assignments/ipv6-unicast-address-assignments

- Privacy extension
Le DHCP offre la possibilité d'avoir une adresse qui change au cours du temps, ce qui peut être un avantage pour les postes clients, qui deviennent plus difficile à tracer. L'option privacy extension est une fonction ajoutée à l'autoconfiguration sans état qui permet aux machines de faire varier leur adresse globale. La privacy extension n'apporte pas de risques de sécurité supplémentaires à l'autoconfiguration sans état, mais il faut garder en mémoire que des adresses qui varient peuvent compliquer la tâche de l'administrateur quand il s'agit de tracer un problème ou d'établir la source d'un trafic donné.

– Mobilité IPv6
IPv6 permet de gérer la mobilité, de telle sorte qu'une machine puisse changer de réseau physique et même d'adresse IP sans que les connexions réseaux ne soient coupées. Pour celà, quand un périphérique mobile change de réseau et d'adresse IP, il en informe un “Home agent” sur son réseau natif, en lui donnant sa nouvelle adresse IP (appellée “care of address”). Le home agent va faire le lien en relayant les paquets destinés à l'ancienne adresse vers la nouvelle. Une paquet Binding Update permet d'informer les correspondants de la nouvelle adresse afin d'éviter au home agent d'avoir à relayer trop de trafic.

- Fragmentation
La gestion de la fragmentation des paquets a été changée. En IPv4, chaque routeur pouvait fragmenter un paquet si celui-ci avait une taille supérieure à la MTU (Maximum Transmission Unit) du lien vers lequel le paquet devait être routé. En IPv6, les routeurs ne sont pas autorisés à fragmenter les paquets. Dans le cas où ils reçoivent un paquet trop gros, ils doivent prévenir l'émetteur du problème avec un message ICMP.

- Autoconfiguration du réseau
Avec l'autoconfiguration, une machine peut obtenir elle-même une adresse routable, mais elle peut également obtenir l'adresse d'un routeur à utiliser. Cette fonctionnalité se base sur les routeurs s'annoncent d'eux-même en envoyant des messages sur le réseau. Malheureusement, il n'y a aucune mesure de sécurité intégrée au protocole de base, ce qui signifie que n'importe qui peut envoyer des paquets ICMP de type 134 (Router Advertisement) et essayer de se faire passer pour un routeur. Cette attaque est très similaire aux attaques de DHCP Poisoning. En cas de succès, le pirate aurait un contrôle total sur l'ensemble des communications entre le LAN et le reste du monde. Il lui faudra néanmoins avoir établi au préalable un avant-post sur notre LAN, de part les filtrages mis en place et le fonctionnement du protocole ICMP. Les actions à entreprendre pour se prémunir de ce danger seront abordés dans la troisième partie.

4) ICMPv6

IPv6, de par les changements qu'il apporte, requiert une nouvelle version de ICMP pour pouvoir

gérer les nouvelles fonctionnalités. Nous allons ici nous intéresser à l'ICMPv6, et décrire les différences par rapport à ICMPv4.

Tout d'abord, des paquets ICMPv6 importants sont dérivés de paquets ICMPv4, mais leur type/code a été changé :

Description du paquet	ICMPv4	ICMPv6
Destination unreachable	Type 3	Type 1
Time Exceeded	Type 11	Type 3
Parameter problem	Type 12	Type 4
Echo request et Echo reply	Type 8 et 0	Type 128 et 129

Les trois premiers messages permettent aux équipements communiquant sur le réseau de s'informer quand il y a un problème. Echo request et Echo reply sont utilisés par le programme très connu “ping”.

Les nouveaux paquets dans ICMPv6 soutiennent les fonctionnalités de IPv6. Quels sont-ils ?

- ICMPv6 type 2 : Packet too big. Comme nous l'avons vu dans la partie précédente, la fragmentation est gérée par les 2 extrémités d'une connection. Un routeur devra donc refuser un paquets trop gros et utilisera ce message pour notifier l'expéditeur.
- ICMPv6 type 130-132, 143, et 151-153 : Ce sont des messages destinés au multicast IPv6 sur un lien local
- ICMP v6 type 133-136 et 141-142 : Ces messages sont utilisés pour l'autoconfiguration des machines, les annonces des routeurs, et la bonne marche de la communication entre couche liaison et couche réseau.
- ICMPv6 type 137 : Ces messages sont utilisés par les routeur pour informer les stations de travail quand un autre routeur est plus approprié pour atteindre la destination demandée.
- ICMPv6 type 138 : Ces messages peuvent servir à redéfinir les préfixes réseaux au niveau routeur
- ICMPv6 type 139 et 140 : Ces messages sont utilisées pour demander le nom attribué à une machine en s'adressant directement à la machine (et en ne passant pas par le DNS donc)
- ICMPv6 type 144-147 : Ces messages sont utilisés pour la mobilité physique au sein du réseau IPv6
- ICMPv6 type 148-149 : Ces messages servent au protocole SEND (Secure Neighbor Discovery)
- ICMPv6 type 154-199 et 202-254 sont des messages d'erreurs non définis par l'IANA. Ils peuvent éventuellement être utilisés par des applications spécifiques, mais également être utilisés pour encapsuler des données.

–

III.Action à entreprendre

1) Les filtres de base

La plupart des équipements réseaux et logiciels gère l'IPv6 à présent, mettre en place un filtrage IPv6 ne sera pas plus compliqué qu'un filtrage IPv4. Etant donné qu'en double pile, les flux restent identiques entre les deux protocoles, les règles de filtrage IPv6 suivront les mêmes lignes que pour le filtrage IPv4. Il faut juste tenir compte des nouveautés déjà présentées dans ce document.

Rappellons néenmoins quelques règles de base pour le filtrage IP :

- ingress filtering : filtrer les paquets qui ont une adresse source correspondant à notre propre réseau, mais qui arrivent sur l'interface extérieure du routeur (tentative d'IP Spoofing)
- rejeter les paquets dont l'adresse source n'est ni unicast, ni attribuée (une adresse source ne correspondant à ces critères est très suspecte)
- En IPv4, il est plus simple de rejeter les adresses non valides, et d'accepter le reste “par défaut”. Vu le nombre d'adresses IPv6, il est plus simple d'accepter les adresses reconnues valides, et de refuser les autres. Une liste est disponible à l'adresse http://www.iana.org/assignments/ipv6-unicast-address-assignments, attention au préfixe 2001:db8::/32 qui est réservé à des fins de documentation.

2) Décider du filtrage des ICMP

La politique de filtrage des ICMPv6 suivra la politique des ICMPv4 pour les paquets équivalents. Pour les nouveaux paquets, il faut savoir que certains ICMP sont supposés ne jamais quitter le LAN.

Type ICMP	Politique de filtrage recommandée	Commentaires
1	Autorisé partout	
2	Autorisé partout	Ce paquet est nécessaire à la gestion de la fragmentation
3	Autorisé partout	
4	Autorisé partout	
128 et 129	Autorisé sauf si bloqué en IPv4	Le risque de scan avec ces paquets est bien plus réduits qu'en IPv4
130-132, 143, et 151-153	Autorisé sur le LAN uniquement	
133-136	Autorisé sur le LAN uniquement	

138	A bloquer sauf si besoin spécifique	
139-140	A bloquer sauf si besoin spécifique	
141-142	Autorisé sur le LAN uniquement	
144-147	Autorisé si besoin mobilité IPv6	
148-149	Autorisé sur le LAN uniquement	
154-199 202-254	A bloquer sauf cas spécifique	Vous n'en n'avez probablement pas besoin.
Par défaut	Bloquer	

3) Contrôler le type d'implémentation d'IPv6.

Comme la solution retenue pour implémenter IPv6 est celle de la double pile, il est donc indispensable de bloquer les tunnels, afin de pouvoir garder le contrôle sur les flux réseaux. Pour celà :

- Bloquer dans les deux sens tous les paquets IPv4 qui contiennent la valeur « 41 » dans le champ *Protocole* de l'en-tête (http://tools.ietf.org/html/rfc791#page-11). Cela bloquera les tunnels basés sur le protocole 6to4, ISATAP, et 6over4.

Exemple avec une ACL Cisco (à appliquer en in et out) : IPv6 access-list X deny 41 any any [log]

- Bloquer dans les deux sens le port UDP 3544. Cela bloquera les tunnels basés sur Teredo. Teredo est dangereux, si le source routing est activé sur le client (il est généralement désactivé sur les routeurs), un client Teredo pourra être amené à relayer des paquets. Un rapport plus détaillé est disponible à http://www.securiteam.com/securityreviews/6C00O2KHFK.html

Exemple avec une ACL Cisco (à appliquer en in et out) : IPv6 access-list X deny UDP any any eq 3544 [log]

4) Sécuriser le LAN contre les "rogues devices"

Comme vu dans la partie II, l'IPv6 introduit la possibilité d'obtenir une adresse de routeur automatiquement, ce qui induit des possibilités de détournement. Le déploiement pratique de l'IPv6 n'étant pas encore développé, il y a peu de solutions concrètement utilisables aujourd'hui. Nous allons vous en citer 4 :

- La solution la plus évidente, et la moins pratique à mettre en place : donner en statique à chaque machine l'adresse du ou des routeurs à utiliser. Le risque d'un routeur clandestin devient alors nul, mais on perds l'intérêt de l'autoconfiguration. De plus, c'est une perte de temps importante dans le cadre de grands parcs de machines.
- Utiliser un filtrage au niveau machines pour bloquer les ICMPv6 type 134 (Router Advertisement)à qui ne proviennent pas des routeurs connus. Elle a le même inconvénient que la même ci-dessus, à savoir la nécessité de configurer individuellement chaque machine.

L'avantage est qu'un changement de préfixe est toujours possible, mais est un peu plus compliqué à mettre en place.

- Utiliser SEND (Secure Neighbor Discovery), qui est une version améliorée du Neighbor Discovery et qui a été pensée avec la sécurité en tête. Elle est protégée contre ce genre d'attaques, mais n'a pas fait l'objet de beaucoup d'implémentations pour le moment.
- Utiliser une solution de contrôle d'accès à la couche liaison, tel que IEEE 802.1x. Ainsi, un pirate devra passer une couche de sécurité supplémentaire avant de pouvoir attaquer.
- Surveiller le réseau avec des outils comme NDPMon pour détecter les attaques.

D'autres solutions seraient plus élégantes, mais ne sont pas encore mises en oeuvre pour le moment. Par exemple une fonctionnalité “RA Snooping” dans les équipements réseaux qui filtrerait les annonces de routeurs provenant d'une source inconnue, similaire au “DHCP Snooping” qui existe déjà chez Cisco.

En attendant d'avoir une solution solide à ce problème, il est possible de surveiller le réseau avec NDPMon afin de détecter une éventuelle attaque.

5) Isoler des machines spécifiques du réseau

Dans le cadre d'une migration progressive vers l'IPv6, on peut être amené à vouloir isoler certaines machines spécifiques du réseau IPv6. Ainsi, à l'UREC, le VLAN DMZ a été basculée en IPv6, le serveur DNS était prêt à gérer l'IPv6 tandis que le serveur de listes de messagerie demandait des tests supplémentaires. J'ai donc isolé spécifiquement le serveur de listes du réseau IPv6, afin de permettre au DNS d'être opérationnel en double-pile aussi vite que possible.

Il est bien évidemment possible de mettre en place des filtres sur les équipements réseaux, mais il est plus simple d'effectuer des filtrages au niveau de la machine. Il faut prendre en compte le fait que Linux et Windows fonctionnent de façon légèrement différente quand à la gestion des filtrages. Par exemple, pour bloquer le trafic avec ip6tables, on utilisera les commandes suivantes :

```
ip6tables -A INPUT -j DROP
ip6tables -A OUTPUT -j DROP
ip6tables -A FORWARD -j DROP
```

Si vous désirez utiliser un filtrage local pour bloquer certains services uniquement, c'est possible aussi. Toutefois, il faut faire attention à la façon de procéder.

Linux dispose de deux outils totalement indépendants pour effectuer le filtrage, iptables et ip6tables. Il revient donc à l'administrateur de réécrire l'ensemble des filtres IPv4 pour IPv6, en vérifiant la cohésion entre les deux filtres, ce qui peut s'avérer fastidieux.

Windows n'est pas tellement mieux lotis, son garde-barrière intégré ne fait pas la différence entre IPv4 et IPv6 puisqu'il fait un traitement au niveau des ports. Un port 80 autorisé en IPv4 sera donc systématiquement autorisé en IPv6, ce qui n'est pas forcément le but recherché.

5) Se munir de logiciels appropriés

De nombreux outils de sécurité gèrent maintenant l'IPv6, il est impossible de faire une liste exhaustive, mais voici quelques noms qui permettront de commencer votre boite à outil v6 :

NDPmon : Ce logiciel permet de surveiller le protocole Neighbour Discovery, afin de détecter les attaques contre ce protocole dont nous avons déjà parlé.

Ntop : Non spécifique à IPv6, il le supporte et permet de surveiller l'état du réseau en reniflant les paquets.

TCPDump : similairement à Ntop, ce programme (et tous les autres qui se basent dessus) supporte l'IPv6 et permet de renifler les paquets.

Netcat6 : version IPv6 de netcat, indispensable outil d'un administrateur système-réseau.

IP6Sic : Version IPv6 de ISIC, il permet d'éprouver une pile réseau en envoyant une multitude de paquet.

Nmap : Célébrissime outil de scan, il supporte bien évidemment l'IPv6.

Conclusion.

Beaucoup de théories existent sur la sécurité d'IPv6, mais c'est seulement avec sa mise en production massive que sa sécurité sera vraiment éprouvée. En effet, en informatique, plus un logiciel ou un produit est utilisé, plus il sera la cible des pirates. Il ne faut donc absolument pas négliger la sécurité de l'IPv6, qui est tout aussi critique que la sécurité IPv4 dans la sécurité d'un système d'information.

Des articles tels que http://www.usipv6.com/6sense/2007/jan/article01.htm décrivent comment des vers pourraient envahir l'espace IPv6, et des fonctionnalités tels que la mobilité IPv6 ou le multicast doivent encore montrer en pratique qu'ils se soient pas facilement exploitables par une personne mal attentionnée.

La sécurisation d'IPv6 ne fait que commencer.

Références :

Différences entre en-tête IPv4 et IPv6
http://www.luv.asn.au/overheads/IPv6/IPv6_headers.html

RFC 4890 : Recommendations for filtering ICMPv6 Messages in Firewalls
http://www.ietf.org/rfc/rfc4890.txt

CERTA : Migration IPv6 : enjeux de sécurité
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/CERTA-2006-INF-004.html

IPv6 and IPv4 Thread Comparison and Best-Practice Evalutaion, March 2004, S. Convery, D. Miller
http://www.seanconvery.com/v6-v4-threats.pdf

Rogue IPv6 Router Advertisement Problem Statement
http://tools.ietf.org/html/draft-chown-v6ops-rogue-ra-00

Adresses IPv6 global assignées
http://www.iana.org/assignments/IPv6-unicast-address-assignments