

Travail de Bachelor 2012

Publication de services web IPv4 sur Internet IPv6

Proposé par : Service Informatique de l'Entité Neuchâteloise (SIEN)

heig-vd, filière Télécommunication, orientation réseaux et services

Simon Dunand

Professeur responsable: Dr. Stephan Robert, heig-vd

Mandant: Jérôme Vernez, SIEN

Cette page est laissée blanche intentionnellement.

Table des matières

1	Résumé	- 7 -
2	Cahier des charges.....	- 8 -
2.1	Résumé du problème	- 8 -
2.2	Cahier des charges.....	- 8 -
3	Introduction	- 9 -
4	IPv6.....	- 11 -
4.1	Pourquoi ?.....	- 11 -
4.2	Adresse	- 13 -
4.2.1	Syntaxe	- 14 -
4.2.2	Préfixe	- 14 -
4.2.3	Types d'adresse	- 15 -
4.2.4	Portée des adresses	- 15 -
4.3	En-tête	- 18 -
4.4	ICMPv6	- 19 -
4.4.1	Découverte de voisins.....	- 20 -
4.5	IPv4 vs IPv6	- 20 -
5	Mécanismes de transition IPv4-IPv6	- 21 -
5.1	Dual-Stack.....	- 21 -
5.2	Techniques de tunneling.....	- 22 -
5.2.1	IPv6 over IPv4 GRE tunnel.....	- 23 -
5.2.2	Tunnel broker	- 23 -
5.2.3	6to4 tunnel	- 24 -
5.2.4	ISATAP (Intra-Site Automatic Tunnel Addressing Protocol).....	- 25 -
5.2.5	Teredo.....	- 25 -
5.2.6	IPv6 Rapid Deployment (6rd)	- 26 -
5.2.7	Dual-stack Lite (DS-Lite).....	- 27 -
5.3	Techniques de translation.....	- 27 -
5.3.1	NAT-PT.....	- 27 -

5.3.2	NAT64.....	- 28 -
5.3.3	Bump in the Host (BIH)	- 29 -
5.3.4	Application Level Gateway (ALG).....	- 29 -
5.3.5	Reverse proxy.....	- 29 -
6	Prototypes.....	- 31 -
6.1	IPv6 only	- 31 -
6.1.1	Configuration du routeur	- 32 -
6.1.2	Configuration du firewall	- 33 -
6.1.3	Configuration du serveur web IIS	- 39 -
6.1.4	Configuration du DNS.....	- 40 -
6.2	Reverse proxy.....	- 42 -
6.2.1	Configuration du routeur	- 45 -
6.2.2	Configuration du firewall	- 45 -
6.2.3	Configuration du DNS.....	- 45 -
6.2.4	Configuration du proxy TCP générique	- 45 -
6.2.5	Configuration du TMG.....	- 46 -
6.2.6	Configuration du serveur Web IIS	- 46 -
6.3	Dual Stack	- 47 -
6.3.1	Configuration du routeur	- 49 -
6.3.2	Configuration du firewall	- 50 -
6.3.3	Configuration du DNS.....	- 52 -
6.3.4	Configuration du proxy TCP générique	- 52 -
6.3.5	Configuration du TMG.....	- 53 -
6.3.6	Configuration du serveur web IIS	- 53 -
7	Performances observées.....	- 53 -
8	Discussion des résultats.....	- 55 -
9	Développements futurs.....	- 56 -
10	Conclusion.....	- 56 -
11	Remerciements.....	- 57 -

12	Références	- 58 -
12.1	Bibliographie	- 58 -
12.2	Webographie	- 58 -
12.2.1	Spécificités du protocole IPv6.....	- 58 -
12.2.2	RFC	- 59 -
13	Liste des symboles et abréviations	- 59 -
13.1	Symboles	- 59 -
13.2	Abréviation.....	- 60 -
14	Liste des figures	- 61 -
15	Annexes.....	- 65 -
15.1	Configuration du prototype IPv6 only.....	- 65 -
15.1.1	Routeur accessa-ipv6.....	- 65 -
15.1.2	Firewall.....	- 66 -
15.2	Configuration du prototype reverse proxy.....	- 70 -
15.2.1	Routeur accessa-ipv6.....	- 70 -
15.2.2	Firewall.....	- 70 -
15.2.3	Proxy TCP générique	- 70 -
15.2.4	Installation de Microsoft Forefront Threat Management Gateway 2010 (TMG).....	- 70 -
15.2.5	Configuration TMG.....	- 91 -
15.3	Configuration du prototype dual stack	- 103 -
15.3.1	Routeur accessa-ipv6.....	- 103 -
15.3.2	Firewall.....	- 105 -
15.3.3	Proxy TCP générique	- 108 -
15.3.4	TMG	- 108 -

1 Résumé

Le but de ce travail est d'étudier la migration de services web existant en IPv4, vers l'IPv6. Mandaté par le Service Informatique de l'Entité Neuchâteloise (SIEN), il est réalisé comme travail de Bachelor pour l'orientation réseaux et services de la filière télécommunication de la Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud (heig-vd). Ce travail peut facilement être décomposé en trois parties principales :

- Introduction et description théorique de l'IPv6
- Mécanismes de transition IPv4-IPv6
- Prototypes

Tout d'abord, un tour d'horizon de l'adressage, et des diverses possibilités de l'IPv6 permettra au lecteur de se plonger dans cette version du protocole internet. Même si les différences peuvent paraître triviales, le changement est important pour chaque personne habituée à travailler avec un réseau IPv4, vu notamment le nombre d'adresses disponibles en IPv6.

Ensuite, une présentation des différents moyens de transition IPv4-IPv6 permettra d'y voir un peu plus clair dans la multitude des normes et des techniques existantes, à savoir le dual-stack, le tunneling et la translation.

Puis, un chapitre sera consacré aux divers prototypes qui ont été déployés et testés en condition de laboratoire. La complexité de ceux-ci évolue crescendo, d'un premier prototype très académique, au troisième qui reproduit à quelques détails matériels près l'environnement de production du SIEN.

Finalement, les derniers chapitres présenteront respectivement les résultats obtenus à la fin du projet, une discussion de ceux-ci, et les développements futurs de ce projet.

Pour terminer, une citation de M. Shannon McFarland, expert de l'IPv6 pour l'entreprise Cisco, qui permet de se faire une idée de quel outil employé lorsqu'on veut migrer un réseau IPv4 vers l'IPv6 :

“Dual stack where you can –Tunnel where you must –Translate when you have a gun to your head.”¹

¹ <http://www.interop.com/lasvegas/2011/presentations/free/174-shannon-mcfarland.pdf>, dernière diapositive

2 Cahier des charges

2.1 Résumé du problème

Le SIEN exploite plusieurs réseaux informatiques pour l'administration neuchâteloise, pour les écoles obligatoires, les hôpitaux, la police, etc... Un grand nombre de services sont donc proposés sur internet, mais actuellement seulement accessibles en IPv4.

Le SIEN désire donc participer au décollage d'IPv6 en proposant ses services IPv4 au monde IPv6. Une première phase avant un dual-stack complet au niveau du réseau d'entrée est de faire l'inventaire des solutions disponibles, afin de publier un service web sur l'internet IPv6, puis de choisir et de déployer la mieux adaptée. L'environnement de travail sera exclusivement Microsoft & Cisco.

2.2 Cahier des charges

- Étudier les solutions de publication de services web IPv4 vers IPv6
- Valider la solution choisie
- Créer une nouvelle zone publique IPv6 (DMZ) pour l'Etat de Neuchâtel (FW: ASA 5510)
- Configurer un serveur Web IIS basique (IPv6 et IPv4)
- Interagir avec un serveur DNS AAAA externe
- Configurer la solution choisie sur un serveur Windows Server
- Étudier les aspects sécurité du système
- Étudier les aspects de migration vers les serveurs de production du SIEN

3 Introduction

Cela devait arriver un jour, et ce fut le 31 janvier 2012. Mais que s'est-il passé ? Aucune catastrophe annoncée par le calendrier maya, mais un événement prédit il y a une dizaine d'années, et qui était inévitable : l'allocation par l'Internet Assigned Numbers Authority (IANA) des derniers espaces d'adressage public IPv4 disponibles². Cet événement fut annoncé publiquement lors de la conférence de presse, donnée le 3 février 2012. Même s'il reste un stock d'adresses disponibles à chaque Regional Internet Registry (RIR), cela ne durera qu'un temps, comme on peut le voir dans la Figure 1. C'est pourquoi il est l'heure de passer à l'IPv6 !

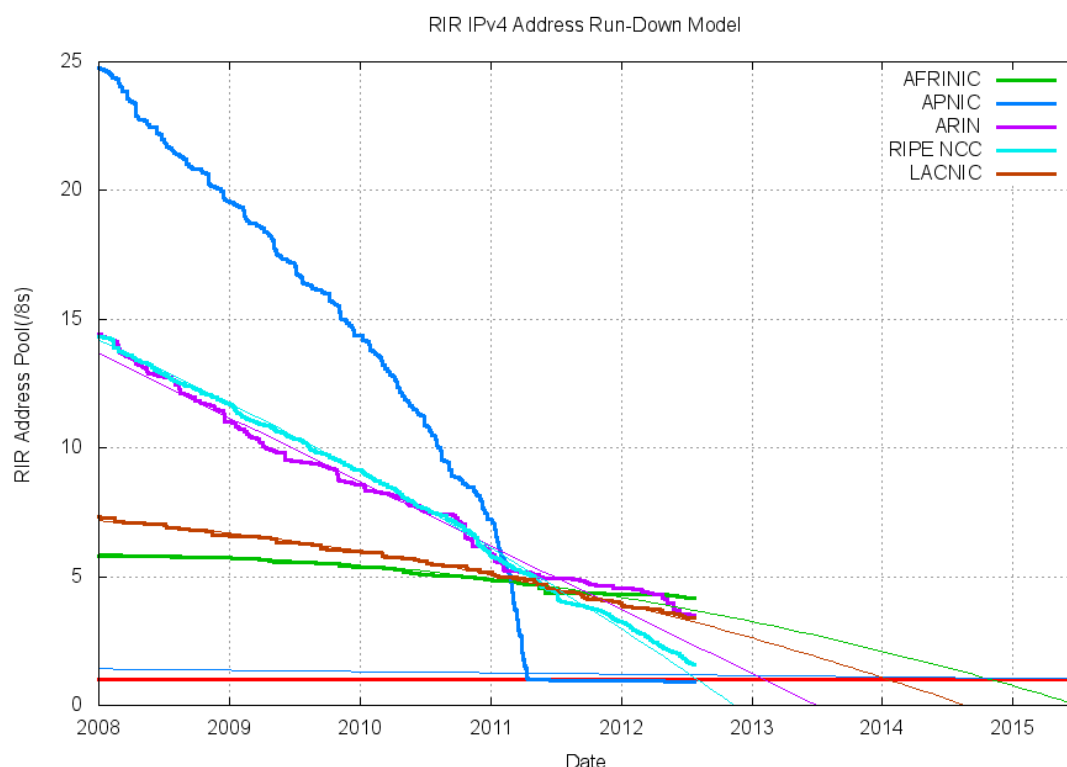


Figure 1 : projection de l'épuisement d'adresse IPv4 chez les différents RIR³

Mais l'IPv6 : c'est quoi ? C'est le protocole internet version 6, remplaçant IPv4, dont la longueur d'adresse est de 128 bits, contre 32 bits pour l'IPv4. Il permet ainsi de disposer de 2^{96} ($\approx 2.9 \cdot 10^{27}$) fois plus d'adresses que l'IPv4, et de nombreux autres avantages qui seront détaillés dans le chapitre lui étant consacré. Il est difficile de se représenter le gigantisme du nombre précédemment mentionné. Si l'on répartissait l'ensemble des adresses IPv6 sur la surface de la terre, cela en ferait encore $6.7 \cdot 10^{17}$ adresses par millimètre carré ! Prenons une autre comparaison : si toutes les adresses IPv4 étaient représentées par un atome,



Figure 2: logo du lancement mondial de l'IPv6

² <http://www.nro.net/news/ipv4-free-pool-depleted>

³ <http://www.potaroo.net/tools/ipv4/index.html>

l'espace d'adressage IPv6 serait représenté par 80 tonnes de cet atome, c'est-à-dire le poids de deux camions semi-remorques de gravier chargés au maximum.

Mais ce protocole est-il adopté par les acteurs majeurs d'internet ? La réponse est oui ! En effet, le lancement mondial de l'IPv6⁴ a eu lieu le 6 juin 2012. Deux des plus importants vendeurs d'équipement réseau domestique, une cinquantaine d'opérateurs réseaux, et plus de 1600 sites internet, parmi lesquels Google, Facebook et Youtube, ont participé à ce lancement, certifiant ainsi que leurs services seraient disponibles en permanence en IPv6 à compter de ce jour.

⁴ <http://www.worldipv6launch.org/>

4 IPv6

4.1 Pourquoi ?

Mais pourquoi adopter l'IPv6, alors que tout fonctionne en IPv4 ? Les raisons sont diverses, et la plus évidente d'entre elles est l'épuisement des adresses IPv4 disponibles. Evidemment, des mécanismes ont été mis en place pour contourner le problème, en traduisant une multitude d'adresses IPv4 internes et privée, en une adresse IPv4 routable. Il s'agit de la traduction d'adresse réseau, plus connue sous le nom de NAT. Bien que le NAT ait repoussé le délai d'épuisement des adresses IPv4, cela a fortement compliqué la communication d'un bout à un autre du réseau (end to end).

Une autre raison est d'être disponible pour les personnes n'ayant pas accès à l'IPv4. Mais qui est-ce ? Ce sont les utilisateurs des pays émergents tel la Chine ou l'Inde, dont les gouvernements encouragent fortement, ou ont rendu obligatoire l'IPv6. L'Asie au sens large regroupe plus de la moitié de la population mondiale, avec environ 3,8 milliards d'habitants (état au 31 décembre 2011). Le taux de pénétration d'internet en Asie est de 26%. Un pour cent d'augmentation, ce qui va forcément arriver au vu du nombre croissant de téléphones portables et de tablettes connectés au réseau IP, représente 39 millions d'utilisateurs en plus. Un tel nombre d'adresses n'est plus disponible en IPv4 ! Il est utile de préciser qu'avec un taux de pénétration de 26% seulement, cela représente aujourd'hui 44.8% des utilisateurs d'internet au monde, comme on peut le voir à la Figure 3, pour un total de 2.2 milliards. A titre de comparaison, et pour estimer l'accroissement futur d'internet en Asie, le taux de pénétration d'internet en Europe et aux Etats-Unis est supérieur à 50%.

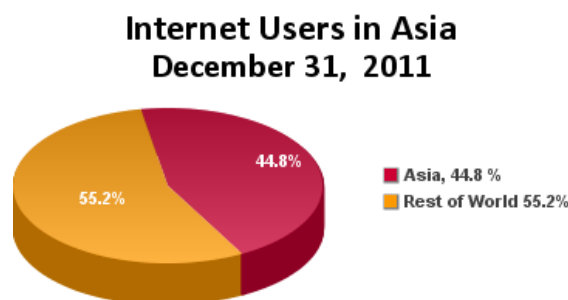


Figure 3: proportion d'utilisateurs asiatiques d'internet par rapport au nombre mondial d'utilisateurs (état au 31.12.2011)⁵

Mais avec 2.2 milliards d'utilisateurs mondiaux d'internet, les 4 milliards d'adresses IPv4 devraient suffire. Comment se fait-il qu'elles soient toutes attribuées par l'IANA, et que les RIR n'en possèdent pratiquement plus ? La réponse est simple : ce n'est pas parce qu'une adresse est allouée qu'elle est utilisée. En effet, les premières sociétés ayant acheté des adresses IPv4 dans les années nonante, ont pu en acquérir un nombre excédant largement leurs besoins. Mais il est clair que ces sociétés ne vont pas rendre ces adresses aux RIR, alors même qu'elles se font rares.

⁵ <http://www.internetworldstats.com/stats3.htm>

Un autre facteur est le nombre d'appareils connectés aux réseaux IP que chaque personne utilise. On parle de la société à 5 adresses par personne. Un smartphone, une tablette, un ordinateur portable, un ordinateur fixe à la maison, une imprimante réseau, et le compte est bon ! Voici pourquoi les 4 milliards d'adresses IPv4 ne suffisent pas !

Mais l'IPv6 ne fait pas qu'augmenter sensiblement le nombre d'adresses IP disponibles. En effet, depuis la création de l'IPv6 en décembre 1998⁶, les améliorations ont pu se succéder, afin de créer un protocole satisfaisant aux contraintes de l'internet actuel, et palliant aux nombreuses erreurs de jeunesse de son illustre prédécesseur. Ces avantages sont listés dans le Tableau 1 ci-dessous :

Résolution du manque d'adresse IP	Bénéfice principal de l'IPv6, avec son format d'adresse de 128 bits de longueur, cela augmente considérablement le nombre d'adresses disponibles, pour un total de $340 \cdot 10^{36}$ adresses.
Déploiement d'adresse plus simple	Chaque appareil voulant communiquer sur internet a besoin d'une adresse IP, qui peut être assignée manuellement ou via DHCP. En plus des deux méthodes précitées, l'IPv6 accepte l'auto-configuration des adresses en utilisant SLAAC. Ceci permet le déploiement rapide d'un réseau dont les périphériques ne sont pas configurés directement par un utilisateur, comme un réseau de milliers de capteurs d'une voiture par exemple.
Retour de la connectivité end-to-end	Avec le NAT, une adresse IP publique masquait un nombre important d'adresses IP privées, privant les utilisateurs et les administrateurs réseaux d'une connectivité end-to-end. Avec IPv6, le besoin du NAT est définitivement supprimé, grâce au nombre important d'adresses disponibles.
Support natif d'IPsec requis	Le support natif de l'en-tête IPsec est requis par le protocole IPv6. Cela permet d'avoir une solution standard pour les besoins de protection du réseau, et cela assure une compatibilité entre les différentes implémentations d'IPv6. Cependant, le support natif d'IPsec ne rend pas IPv6 plus sécurisé intrinsèquement. En effet, cela ne veut pas dire que son utilisation est obligatoire, ni requise pour déployer l'IPv6.

⁶ <http://tools.ietf.org/html/rfc2460>

Amélioration de l'extension de l'en-tête de paquet pour la sécurité, la QoS et l'encryption L'extension de l'en-tête de paquet présente dans l'IPv6 permet d'améliorer le chiffrement, la mobilité, d'optimiser le routage, et d'améliorer la qualité de service. Lorsque c'est nécessaire, cet en-tête additionnel est inséré entre l'en-tête standard du paquet IPv6 et ses données. Le champ *Next Header* permet de savoir si cet en-tête optionnel est présent.

Amélioration de la mobilité Le protocole Mobile IP permet à un utilisateur mobile de se déplacer d'un réseau à un autre, tout en gardant une connexion active. Cependant, l'implémentation IPv4 de ce protocole fonctionne en utilisant un routage triangulaire, qui n'est pas efficace. L'implémentation IPv6 de Mobile IP utilise un processus appelé routage direct, qui permet de réduire les coûts, et surtout de grandement améliorer les performances.

Tableau 1: Avantages de l'IPv6

4.2 Adresse

L'adresse IPv6 est formée de 128 bits, soit quatre fois plus longue que l'adresse IPv4. Mais pourquoi avoir choisi 128 bits ? Est-ce afin d'avoir un nombre d'adresses tellement énorme, que l'on peine à se le représenter ? La raison est bien évidemment ailleurs : ces 128 bits ont été choisis afin d'assurer de multiples niveaux de hiérarchie et de flexibilité dans la conception d'un plan de routage et d'adressage. Le routage et l'attribution d'adresse IPv6 est strictement hiérarchique, comme on peut le voir à la Figure 4, ceci afin de pouvoir au mieux agréger les routes, pour limiter au maximum la taille des tables de routage.

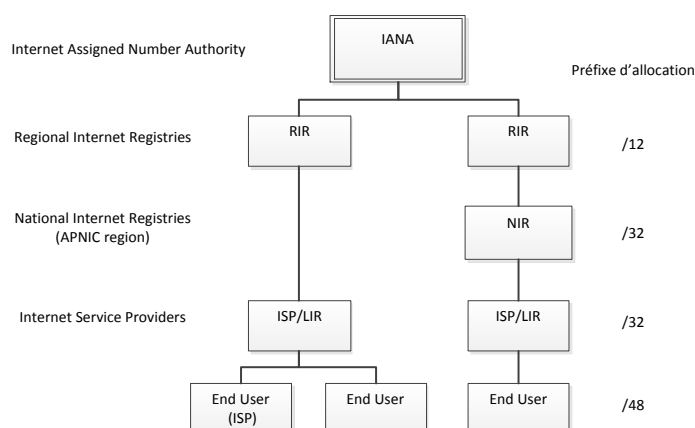


Figure 4: hiérarchie d'allocation d'adresse IPv6⁷

⁷ Basé sur le graphique disponible à l'adresse <http://www.ripe.net/ripe/docs/ripe-552>

Il est facile de se perdre dans l'immensité de l'espace d'adresse IPv6. Mais commençons par le commencement : la syntaxe d'une adresse.

4.2.1 Syntaxe

On peut tout d'abord représenter une adresse IPv6 sous sa forme binaire :

```
001000000000000100001101101110000000000000000000010111100111011
0000001010101010100000000111111111111110001010001001110001011010
```

On peut ensuite regrouper cette forme binaire en groupe de 16 bits :

```
0010000000000001    0000110110111000    0000000000000000    0000000000000000
0000001010101010    0000000011111111    1111111000101000    1001110001011010
```

Chaque block de 16 bits peut-être converti en notation hexadécimale, séparée par deux points :

```
2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A
```

Une simplification peut encore être opérée, en supprimant les zéros consécutifs au début de chaque bloc de 16 bits. Cependant, il doit toujours y avoir au moins un chiffre par bloc. Voici le résultat :

```
2001:DB8:0:0:2AA:FF:FE28:9C5A
```

Si une adresse IPv6 contient de longues séquences de zéros, il est possible de simplifier une dernière fois la représentation, en remplaçant au maximum une fois une séquence de zéros consécutifs, multiple de 16, par la répétition de deux signes deux-points :

```
2001:DB8::2AA:FF:FE28:9C5A
```

Il est utile de remarquer que la notation hexadécimale n'est pas sensible à la case. Pour pouvoir utiliser une adresse IPv6 dans la barre d'adresse d'un navigateur, l'URL s'écrit comme suit :

```
http://[2001:DB8::2AA:FF:FE28:9C5A]:80/index.html
```

L'adresse *localhost* quant à elle s'écrit 0:0:0:0:0:0:0:1 ou plus simplement ::1.

4.2.2 Préfixe

Le préfixe est la partie de l'adresse dont les bits ont une valeur fixe, définissent une route ou un sous-réseau. Un préfixe pour les sous-réseaux ou les routes agrégées se note de la même manière qu'en notation CIDR en IPv4, avec une valeur de préfixe de 128 au maximum :

adresse ipv6/longueur du préfixe.

Exemple : 2001:4DA0:C01 ::/48 pour une route

2001:4DA0:C01:0030::/64 pour un sous-réseau.

2001:4DA0:C01:0030::1/128 pour une adresse loopback ou un noeud.

Il est important de préciser qu'il n'existe pas de masque de sous-réseau à longueur variable (VLSM) en IPv6. Chaque sous-réseau individuel est formé d'un préfixe de 64 bits, puis de l'adresse de l'interface de 64 bits de longueur ou d'une adresse choisie par l'administrateur réseau. Des exceptions sont acceptées pour les adresses loopback (/128) et les adresses de liens point à point (/126).

4.2.3 Types d'adresse

Il existe trois types d'adresse IPv6 :

- **Unicast** : une adresse unicast identifie une seule interface. Elle sert à transmettre des messages d'un hôte à un autre hôte (one-to-one).
- **Anycast** : Une adresse anycast identifie plusieurs interfaces. Un paquet envoyé à une adresse anycast sera délivré à une seule interface : la plus proche de l'adresse source en termes de métrique de routage (one-to-one-of-many).
- **Multicast** : une adresse multicast identifie zéro ou plus interfaces sur le même, ou sur différents hôtes. Cela sert à délivrer les messages d'une machine, vers toutes les interfaces identifiées par l'adresse multicast (one-to-many).

Il est important de noter l'absence d'adresse de broadcast. En effet, le broadcast existant en IPv4 est remplacé par des adresses de multicast en IPv6.

4.2.4 Portée des adresses

Chaque adresse IPv6 a une portée. Chaque interface physique peut par conséquent posséder plusieurs adresses, ayant chacune une portée différente. La notion de portée équivaut à la notion de validité géographique, comme on peut le voir à la Figure 5. Les cinq portées existantes sont expliquées ci-dessous :

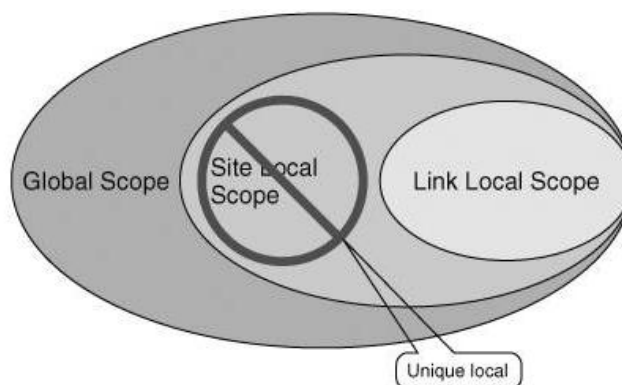


Figure 5: domaine de validité de la portée des adresses⁸

⁸ http://www.realccielab.org/wp-content/uploads/2012/05/image_thumb3.png

4.2.4.1 Nœud-local

Une adresse de nœud-local est utilisée pour envoyer des paquets au même nœud. C'est par exemple l'adresse localhost ::1, ou l'adresse non spécifiée : : .

4.2.4.2 Lien-local

Une adresse de liaison locale est utilisée pour communiquer entre des hôtes sur le même lien, donc elle ne traverse aucun routeur. Les adresses de liaison locale sont toujours configurées automatiquement, mais ce n'est pas de l'auto-configuration via SLAAC. Cette adresse est utilisée par exemple pour découvrir les routeurs, grâce au *Neighbor Discovery Protocol*, qui sera étudié plus en détail dans le chapitre consacré à l'ICMPv6. La création de cette adresse se déroule en ajoutant le préfixe fe80 ::/64 à l'adresse de format EUI-64 identifiant l'interface. On crée l'adresse EUI-64 en prenant l'adresse MAC de l'interface, de 48 bits de longueur. On insère fffe, soit 16 bits, entre le 24^{ème} et le 25^{ème} bit, comme illustré à la Figure 6. Enfin on change la valeur du 7^{ème} bit du premier octet à 1 si l'adresse est unique, et à 0 sinon.

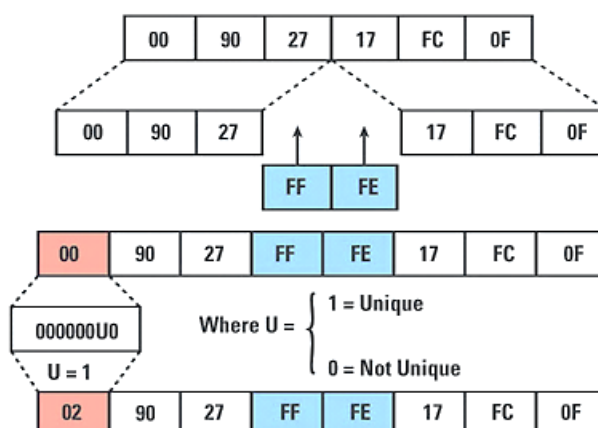


Figure 6: création d'une adresse EUI-64⁹

L'adresse de liaison locale créée avec l'exemple de la Figure 6 sera alors fe80::290:27ff:fe17:fc0f

Il faut encore noter que Cisco et Microsoft Windows 5 (2003 & XP) utilisent le format EUI-64 pour la création d'adresses de liaison locale. Dès Microsoft Windows 6 (2008 & Vista) et plus récent, les adresses de liaison locale sont formées de manière aléatoire, afin d'éviter le scan d'adresse et la localisation, due à l'utilisation perpétuelle de la même adresse de liaison locale. On peut forcer Windows 6 et plus récent à former les adresses de liaison locale avec le format EUI-64 en tapant la commande suivante :

```
Netsh interface ipv6 set global randomize-identifiers=disabled10
```

⁹ <http://www.zid.tuwien.ac.at/zidline/zl15/ipv6.html>

4.2.4.3 *Site-local deprecated par RFC 3879*

Une adresse de site-local était prévue à la base pour être utilisée selon le même principe que les adresses privées en IPv4, à savoir à l'intérieur d'un intranet n'ayant pas de connexion à internet. Le préfixe des adresses de site-local pouvant être réutilisé dans plusieurs sites différents d'une même organisation, cela augmenta la complexité et la difficulté autant pour les administrateurs réseau que pour les routeurs. C'est pour cela que ce n'est plus utilisé, mais les implémentations existantes peuvent perdurer. Le préfixe d'une adresse site-local est `fec0 ::/10`.

4.2.4.4 *Unique-local*

L'adresse unique-local (ULA) a été créée pour remplacer l'adresse de site local, qui pouvait ne pas être unique. Elle doit seulement être utilisée à l'intérieur d'un site, bien qu'elle ait une portée globale. C'est donc la topologie de routage et les filtres mis en place sur les routeurs connectés à internet qui devront veiller à respecter cette règle. Le préfixe d'une adresse unique-local est `fc00 ::/7`.

4.2.4.5 *Global*

Une adresse globale est équivalente à une adresse IPv4 publique. Elle est donc routable et atteignable sur le réseau internet IPv6. Contrairement au réseau IPv4, qui est un mélange de routage hiérarchique et plat, le routage hiérarchique est une des composantes de base du réseau IPv6. Une adresse globale se compose du préfixe `2001 ::/3`, puis de 45 bits de préfixe de routage global, de 16 bits d'identification de sous-réseau, et enfin de 64 bits d'identification de l'interface.

4.2.4.6 *Récapitulatif des préfixes*

Type d'adresse	Préfixe binaire	Notation IPv6
Non-spécifié	00...0 (128 bits)	::/128
Localhost	00...1 (128 bits)	::1/128
IPv4-compatible (<i>deprecated</i>)	00...0 (96 bits)	::IPv4/128
IPv4-mapped	00..0 1111 1111 1111 1111	::ffff:IPv4/128
Global Unicast	001	2001::/3
Unique Local Unicast (ULA)	1111 110	fc00::/7
Lien-local Unicast	1111 1110 10	fe80::/10
Site-local Unicast (<i>deprecated</i>)	1111 1110 11	fec0::/10
Multicast	1111 1111	ff00/8
Réservé	Tout le reste	

Tableau 2: Récapitulatif des préfixes d'adresse

¹⁰ <http://technet.microsoft.com/en-us/magazine/2007.08.cableguy.aspx>

4.3 En-tête

Un paquet de données IPv6 consiste en un en-tête, des extensions d'en-tête (*extension headers*), et des données d'un protocole de couche supérieure. L'en-tête IPv6, d'une taille fixe de 40 octets, est toujours présent. Il contient différents champs, dont les noms sont explicites, comme on peut le voir à la Figure 7, avec :

- En jaune les champs du header IPv4 gardé en IPv6
- En rouge les champs n'ayant pas été conservés dans le header IPv6
- En bleu les champs ayant changé de nom et de position
- En vert le nouveau champ de l'en-tête IPv6

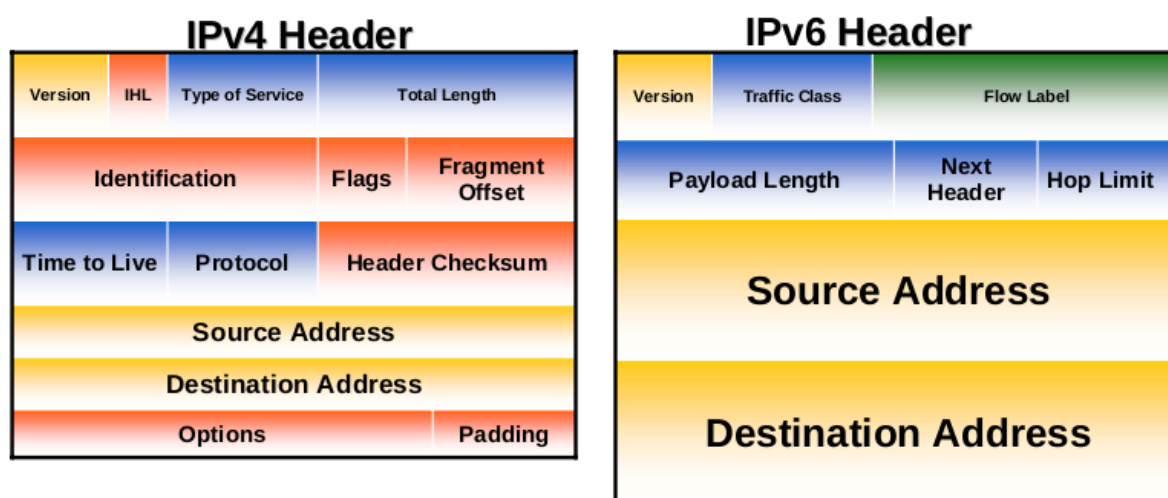


Figure 7: comparaison de l'en-tête IPv4 et IPv6¹¹

On peut noter la présence du nouveau champ *Flow Label*, d'une longueur de 20 bits. Il indique si le paquet en question fait partie d'une séquence spécifique de paquets entre l'adresse source et l'adresse de destination, demandant un traitement particulier par les routeurs à travers lesquels il transitera. Conjugué au champ *Traffic Class*, qui est complètement similaire au champ IPv4 *Type of Service*, un routeur peut traiter en priorité un paquet, afin de le délivrer à temps pour les applications temps-réel, comme la vidéo-conférence.

Les extensions d'en-tête peuvent être présentes après l'en-tête IPv6, mais ne sont nullement obligatoires. Si une ou plusieurs extensions sont présentes, le champ *Next Header* indiquera l'adresse du début de la première extension. Puis, dans chaque extension d'en-tête, un champ *Next Header* indiquera la présence ou non d'une extension supplémentaire, comme on peut le voir à la Figure 8.

L'ordre des extensions d'en-tête n'est pas arbitraire, et est fixé dans la RFC 2460.

¹¹ https://www.ridgerun.com/developer/wiki/index.php/RidgeRun_SDK_IPv6_guide

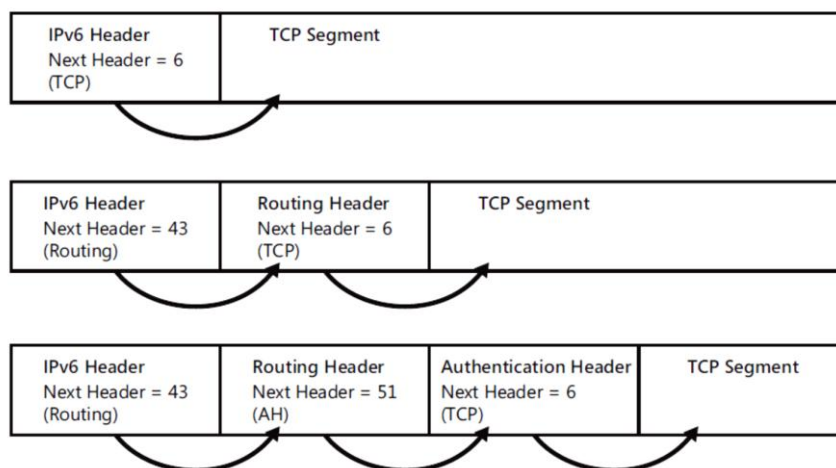


Figure 8: le fonctionnement récursif du champ *Next Header*¹²

4.4 ICMPv6

Le protocole ICMPv6 est une mise à jour du protocole ICMP pour l'IPv6, défini dans la RFC 4443. Comme le protocole ICMP, ICMPv6 fournit un service de report d'erreur de transfert et de livraison, ainsi qu'un service d'écho (ping) aidant à la détection de problèmes. Mais ICMPv6 fournit en plus un cadre pour :

- La découverte de voisins (*Neighbor Discovery - ND*)
- La découverte des auditeurs multicast (*Multicast Listener Discovery- MLD*)
- La découverte sécurisée de voisins (*Secured Neighbor Discovery – SEND*) : pas utilisé par Windows

Les deux types de messages ICMPv6 sont :

- Messages d'erreurs : le premier bit du champ *Type* de l'en-tête est égal à 0
 - Destination inatteignable (*ICMPv6 Type 1*)
 - Paquet trop grand (*ICMPv6 Type 2*)
 - Temps dépassé (*ICMPv6 Type 3*)
 - Problème de paramètre (*ICMPv6 Type 4*)
- Messages d'information : le premier bit du champ *Type* de l'en-tête est égal à 1
 - Requête écho (*ICMPv6 Type 128*)
 - Réponse écho (*ICMPv6 Type 129*)
 - etc

¹² Understanding IPv6, §4 p.92, second edition, Joseph Davies, Microsoft Press

4.4.1 Découverte de voisins

La découverte de voisins s'effectue à l'aide de paquets ICMPv6 de type information. Cela remplace le protocole ARP d'IPv4, les ICMPv4 *Router Discovery* et *Redirect*. Pour ce faire, on utilise les messages :

- Router Solicitation (*ICMPv6 Type 133*)
- Router Advertisement (*ICMPv6 Type 134*)
- Neighbor Solicitation (*ICMPv6 Type 135*)
- Neighbor Advertisement (*ICMPv6 Type 136*)
- Redirect (*ICMPv6 Type 137*)

Afin d'obtenir une vision détaillée du fonctionnement de la découverte de voisins, le lecteur voudra bien se référer au travail de Bachelor de M. Julien Tissot, disponible à l'adresse suivante :

<http://stephan-robert.ch/attachments/File/Travaux-etudiants/RapportFinalJulienTissot.pdf>

4.5 IPv4 vs IPv6

Les principales différences entre IPv4 et l'IPv6 sont décrites dans le Tableau 3 ci-dessous.

Caractéristique	IPv4	IPv6
Longueur d'adresse	32 bits	128 bits
Support d'IPsec	En option	Natif fortement conseillé ¹³
Support de la QoS	Existant	Amélioré
Fragmentation	Par l'émetteur et les routeurs	Par l'émetteur seulement
Taille du paquet	576 octets	1280 octets
Checksum dans l'en-tête	Oui	Non
Option dans l'en-tête	Oui	Non
Résolution d'adresse	ARP en broadcast	Multicast Neighbor Discovery
Multicast membership	IGMP	Multicast Listener Discovery
Découverte de routeur	En option	Requise
Utilisation du broadcast	Oui	Non
Configuration d'IP	Manuelle ou DHCP	Manuelle, automatique, DHCP
Requête de nom DNS	A records	AAAA records
Requête DNS inverse	IN-ADDR.ARPA DNS	IP6.ARPA

Tableau 3: Différences entre IPv4 et IPv6

¹³ <http://tools.ietf.org/html/rfc6434>, page 17, 4^{ème} paragraphe :

« Previously, IPv6 mandated implementation of IPsec and recommended the key management approach of IKE. This document updates that recommendation by making support of the IPsec Architecture [RFC4301] a SHOULD for all IPv6 nodes. »

5 Mécanismes de transition IPv4-IPv6

Une fois le protocole IPv6 créé, il ne reste plus qu'à le déployer, afin de remplacer le vieil IPv4, et de bénéficier de tous les avantages précités. C'est alors qu'un autre problème se présente : la transition d'un protocole à l'autre. En effet, les transitions ne sont jamais faciles, et celle-ci n'est pas une exception. D'autant plus que la dimension mondiale d'internet rend une transition rapide impossible.

Les créateurs d'IPv6 ont maintenant reconnu que la transition prendrait des années, et qu'il est probable que certains hôtes à l'intérieur d'entreprise utiliseront IPv4 indéfiniment. Et même si la migration de tout le réseau reste le but à long terme, la coexistence des deux protocoles est le but à court terme. Pour cela, il faut se rendre compte que le réseau est panaché, et que des hôtes IPv4 ou IPv6 devront communiquer en utilisant un réseau IPv4, un réseau IPv6, ou un réseau mixte. Il existe de nombreuses techniques de transition pour migrer de l'IPv4 à l'IPv6, que l'on peut regrouper en trois catégories :

1. Dual-Stack
2. Techniques de tunneling
3. Techniques de translation.

Chacune de ces catégories fait l'objet d'une description détaillée dans les sous-chapitres qui suivent.

5.1 Dual-Stack

Le dual-stack est la préférée des techniques de transition, car elle ne fait intervenir aucun mécanisme de tunneling ou de translation d'adresse. Cela signifie que les deux protocoles IPv4 et IPv6 fonctionnent côte-à-côte sur la même infrastructure et sur tous les équipements connectés au réseau : ordinateur, routeur, switch, firewall, serveur, etc. comme on peut le voir à la Figure 9.

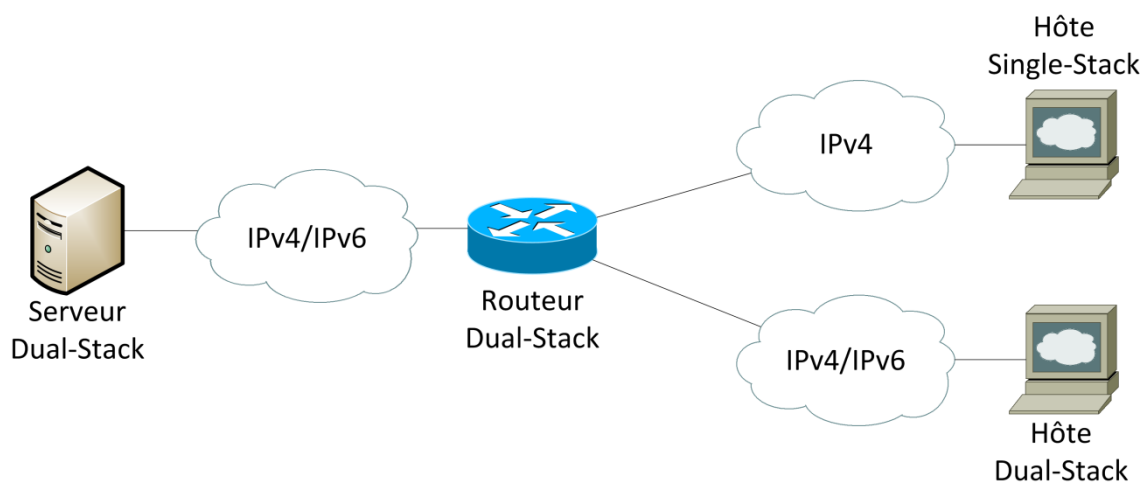


Figure 9: réseau dual-stack¹⁴

¹⁴ IPv6 for Enterprise Networks §3 p.49, McFarland, Sambhi, Sharma & Hooda, Cisco Press

L'avantage principal de cette méthode est de pouvoir se connecter aux applications IPv4 existantes via IPv4, tout en ayant accès aux applications IPv6 via le réseau IPv6. Cependant, comme les deux protocoles fonctionnent simultanément sur une machine, cela peut-être coûteux en termes de performance et d'utilisation CPU.

5.2 Techniques de tunneling

Alors que les portions du réseau internet où l'IPv6 est actif augmentent, une large majorité reste IPv4. Le besoin d'interconnecter ces îles IPv6 à travers le réseau IPv4 s'est donc rapidement fait sentir. C'est pour cela que les techniques de tunneling ont été mises en place. Cela consiste en l'ajout d'un en-tête IPv4 à un paquet IPv6, afin que ce dernier puisse circuler dans le réseau IPv4 à travers un tunnel, comme illustré à la Figure 10.

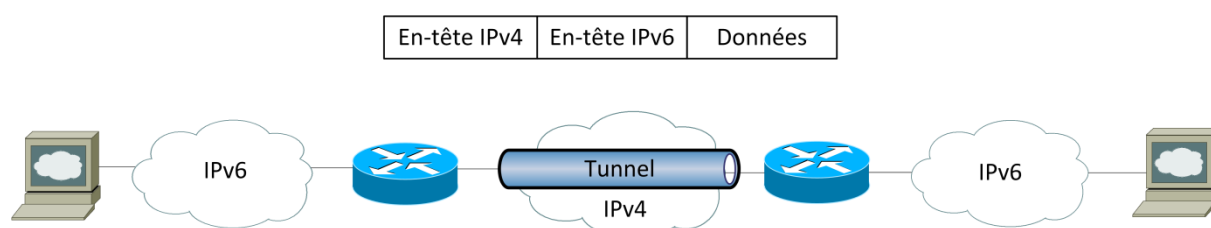


Figure 10: tunnel d'un paquet IPv6 à l'intérieur d'IPv4¹⁵

Il existe de nombreux types de tunnels différents, et différentes topologies sont possibles, notamment au niveau du processus d'encapsulation. Il faut distinguer les tunnels :

- **Routeur à routeur** : deux routeurs interconnectés via le réseau IPv4 et ayant une connexion au réseau IPv6 peuvent transporter des paquets IPv6 en les encapsulant. C'est la situation de la Figure 10.
- **Hôte à routeur** : l'hôte peut créer un tunnel jusque vers un routeur ayant une connectivité IPv6. Le paquet sera envoyé en IPv6 natif depuis le routeur jusqu'à la destination, comme illustré à la Figure 11.

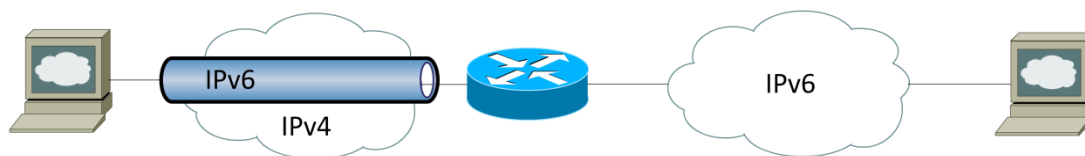


Figure 11: tunnel hôte à routeur

- **Hôte à Hôte** : un hôte source effectue l'encapsulation, et le tunnel se termine chez l'hôte de destination, comme on peut le voir à la Figure 12.

¹⁵ IPv6 for Enterprise Networks §3 p.51, McFarland, Sambhi, Sharma & Hooda, Cisco Press

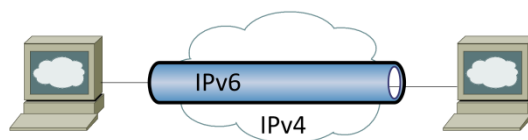


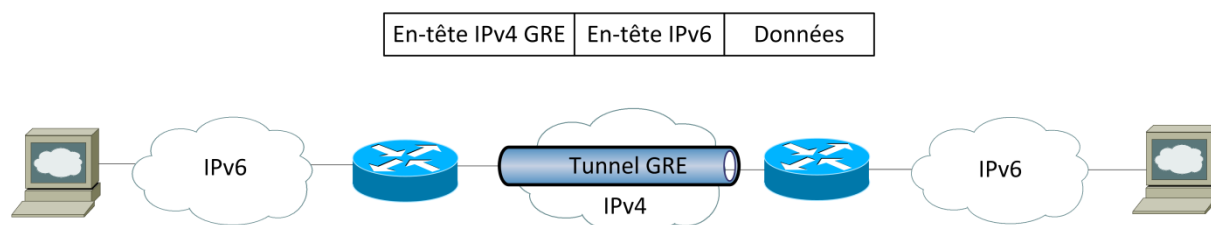
Figure 12: tunnel hôte à hôte

La complexité de configuration est aussi un critère de classement. On peut distinguer :

- Les tunnels configurés manuellement (GRE)
- Les tunnels configurés semi-automatiquement (Tunnel broker)
- Les tunnels configurés automatiquement (6to4, ISATAP, Teredo, etc.)

5.2.1 IPv6 over IPv4 GRE tunnel

Utilisé traditionnellement pour encapsuler des données IPv4 contenant une adresse privée de destination, le tunnel GRE a aussi été utilisé pour encapsuler du trafic d'autres protocoles comme *AppleTalk* sur le réseau IPv4. L'adresse de destination encapsulée n'était donc pas routable. Dans l'utilisation nous intéressant, les données IPv6 sont encapsulées à l'intérieur d'un tunnel fournissant une connexion point-à-point entre deux routeurs. Ceci est illustré à la Figure 13. Afin que ce mécanisme fonctionne, les deux routeurs doivent être dual-stack, afin que l'IPv6 et l'IPv4 puissent être traités et routés avant, pendant, et après l'encapsulation. Ce tunnel peut être perçu comme configuré manuellement, car le tunnel GRE n'existe qu'entre une paire de routeurs. Cette solution n'est donc pas évolutive (*scalable*), si le nombre de sites augmente. Cela entraînera des difficultés de configuration et de recherche de problème (*troubleshooting*).

Figure 13: tunnel IPv6 sur IPv4 GRE¹⁶

5.2.2 Tunnel broker

Le système du tunnel broker, décrit dans la RFC 3053 éponyme, permet la configuration semi-automatique d'un tunnel, afin de pouvoir connecter des ordinateurs épars ou des sites de petites entreprises interconnectés en IPv4 à l'IPv6. Le tunnel broker est une société tierce fournissant un service de tunnel. Pour ce faire, il faut généralement s'inscrire chez le tunnel broker, puis demander l'ouverture d'un tunnel. Alors, le tunnel broker va configurer un de ses routeurs afin de mettre en place le tunnel. Enfin, il enverra un script à exécuter sur la machine souhaitant utiliser le tunnel, pour configurer correctement les paramètres réseaux. La machine est alors connectée à l'IPv6 via le service du tunnel broker. Les étapes énumérées ci-avant sont illustrées à la Figure 14.

¹⁶ IPv6 for Enterprise Networks §3 p.53, McFarland, Sambhi, Sharma & Hooda, Cisco Press

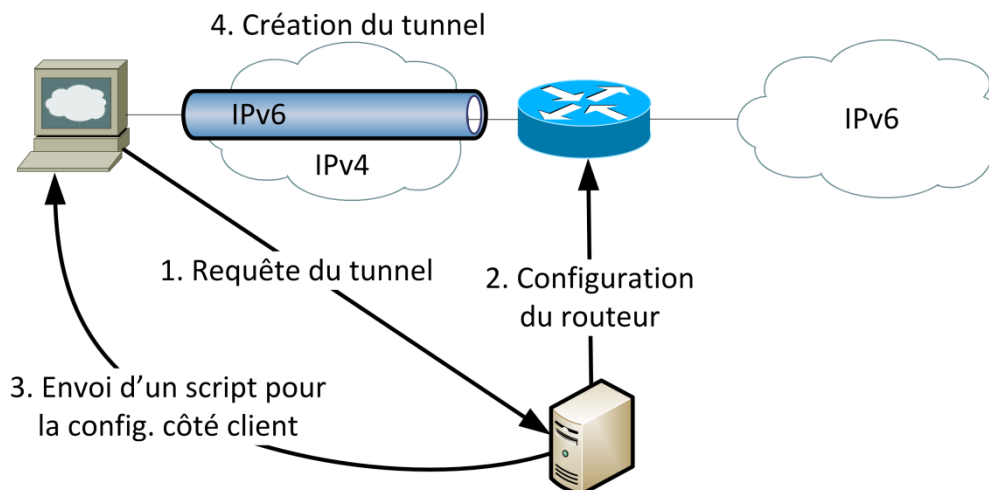


Figure 14: mise en place automatique d'un tunnel à l'aide d'un tunnel broker

Les limitations principales de ce système sont d'une part les performances, l'emplacement géographique du routeur du tunnel broker jouant un rôle important ; et d'autre part la sécurité, car le routeur du tunnel broker doit accepter des modifications de configuration depuis un serveur distant. Mais ceci est du ressort du tunnel broker.

5.2.3 6to4 tunnel

Le tunnel 6to4, décrit dans la RFC 3056, est un mécanisme de tunnel automatique permettant à des domaines IPv6 isolés de s'interconnecter via le réseau IPv4. Contrairement aux mécanismes évoqués précédemment, les tunnels 6to4 sont multipoints, et non point-à-point. Une autre particularité est que ce n'est pas un tunnel à proprement parlé. En effet, cela fonctionne en utilisant le préfixe réservé $2002::/16$ directement suivi de l'adresse IPv4 du routeur 6to4 auquel l'hôte est connecté, comme on peut le voir à la Figure 15. Les 16 bits suivants sont utilisé pour désigner un sous-réseau, et les 64 derniers pour déterminer l'identifiant de l'interface de l'hôte (adresse MAC). Les routeurs 6to4 sont ensuite responsables d'extraire l'adresse IPv4 du routeur de destination à partir de l'adresse IPv6 de destination, et enfin d'encapsuler le paquet IPv6.

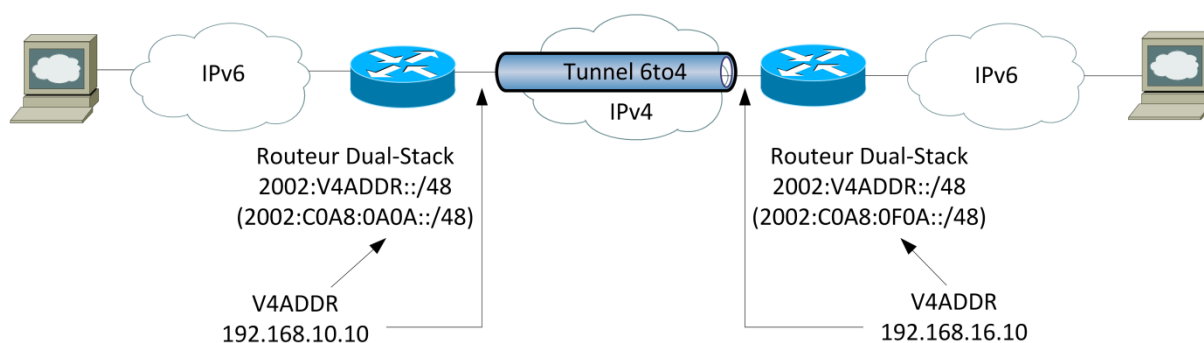


Figure 15: interconnexion de domaines 6to4¹⁷

¹⁷ IPv6 for Enterprise Networks §3 p.56, McFarland, Sambhi, Sharma & Hooda, Cisco Press

Il existe cependant les différents problèmes suivants liés à cette technique :

- Elle est limitée par le nombre d'adresses IPv4 publiques, puisqu'il est obligatoire pour un routeur d'en posséder une.
- Elle ne supporte pas qu'un NAT soit sur le chemin.
- Elle ne supporte pas l'utilisation du multicast.

5.2.4 ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

ISATAP est un mécanisme automatique de tunneling défini dans la RFC 5214, permettant la communication entre hôtes IPv6 à l'intérieur d'un même site, en utilisant l'infrastructure IPv4 existante. Ceci est illustré à la Figure 16. L'adresse ISATAP est formée d'un préfixe IPv6 global ou lien-local d'une longueur de 64 bits, de l'identificateur propre `0000:5efe` et enfin des 32 bits de l'adresse IPv4 identifiant l'interface. Il faut toutefois noter qu'ISATAP ne supporte pas le NAT, ni le multicast.

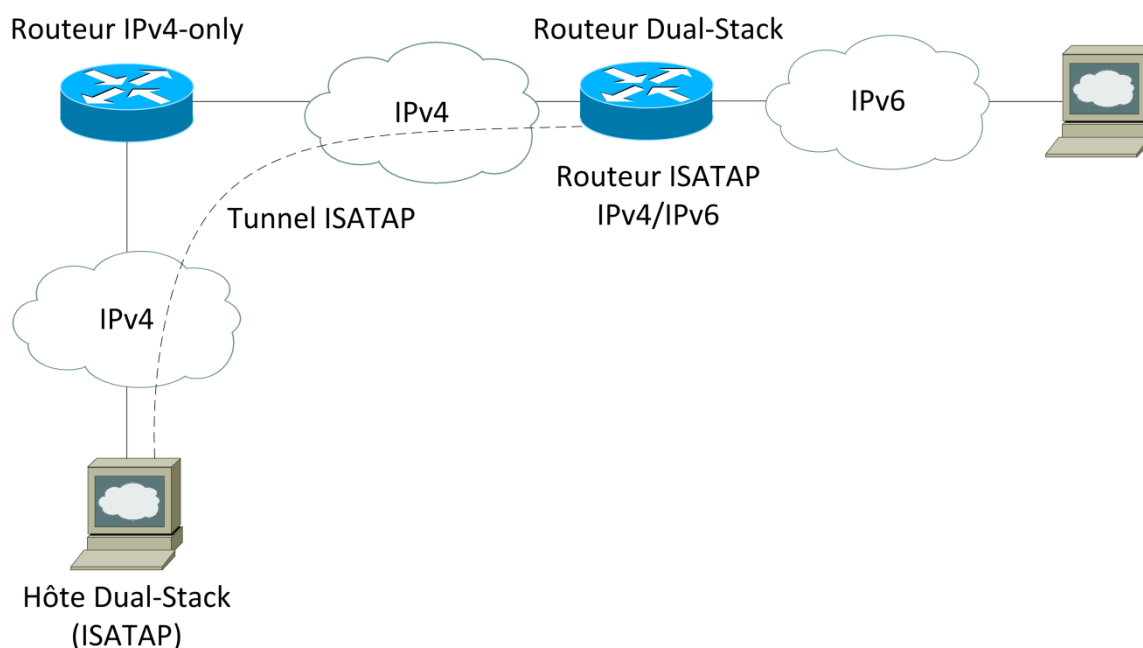


Figure 16: création d'un tunnel ISATAP¹⁸

5.2.5 Teredo

Teredo est une technologie d'adressage et de tunneling automatique définie dans la RFC 4380, établissant une connexion IPv6 au moyen du réseau IPv4. Son point fort est sa capacité de traverser la plupart des NAT sur un ou plusieurs niveaux, en encapsulant le paquet IPv6 dans un paquet UDP IPv4. Ce paquet sera donc constitué d'un en-tête IPv4, suivi d'un en-tête UDP, puis d'un en-tête IPv6, et enfin des données IPv6. Une adresse Teredo commence toujours par le préfixe `2001::/32`. Il faut noter que ce protocole développé par Microsoft s'adapte automatiquement au type de Nat qu'il doit traverser.

¹⁸ IPv6 for Enterprise Networks §3 p.58, McFarland, Sambhi, Sharma & Hooda, Cisco Press

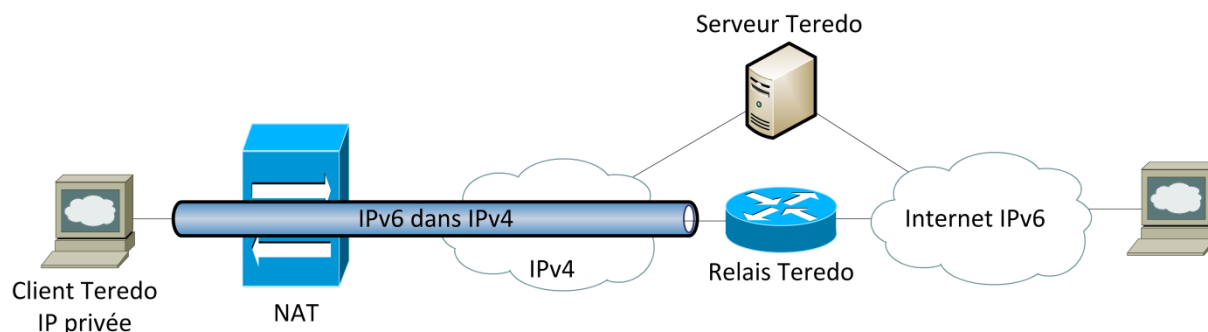


Figure 17: infrastructure Teredo

L'infrastructure Teredo est composée d'un client, d'un relais et d'un serveur Teredo, comme illustré à la Figure 17. Le serveur Teredo assiste un client dans sa configuration d'adresse en découvrant son adresse et son port, et facilite la communication entre clients Teredo. Le relais Teredo transmet les paquets à un hôte IPv6. Il existe encore un relais *host-specific* dual-stack, qui peut communiquer directement avec les clients Teredo.

5.2.6 IPv6 Rapid Deployment (6rd)

Le protocole 6rd permet de faciliter le déploiement de l'IPv6 dans l'infrastructure IPv4 d'un fournisseur d'accès à internet (FAI). Il est décrit pour la première fois par son créateur Rémi Després dans la RFC 5569 en janvier 2010, comme RFC d'information. Puis elle est proposée comme standard par l'IETF en août 2010, sous le nom RFC 5969.

Le protocole 6rd reprend les principes de fonctionnement du protocole 6to4, tout en corrigeant ses défauts. A la place d'utiliser un seul et unique préfixe (2002::/16 pour 6to4), 6rd utilise un préfixe différent pour chaque FAI. Ceci supprime donc le problème des relais hors de contrôle et d'anonymisation du trafic. C'est la technique que Swisscom a choisi d'utiliser pour déployer IPv6 sur son réseau, comme l'a expliqué M. Martin Gysi lors de la conférence du *Swiss IPv6 Council* du 10 mai 2012 à Lausanne. La Figure 18 présente le schéma de fonctionnement du protocole 6rd.

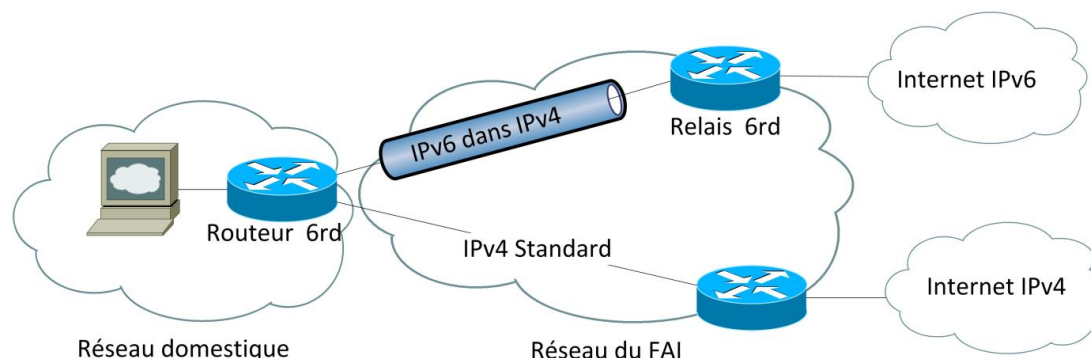


Figure 18: schéma de fonctionnement de 6rd

5.2.7 Dual-stack Lite (DS-Lite)

Dual-stack Lite, décrit dans la RFC 6333, peut être considéré comme l'opposé de 6rd. Si 6rd facilite le déploiement d'IPv6 sur une infrastructure IPv4 existante, alors DS-Lite facilite le déploiement de l'IPv4 sur une infrastructure IPv6 existante. Ceci est donc destiné aux nouveaux FAI - asiatiques particulièrement pour le moment, car le stock d'adresses IPv4 de l'APNIC est épuisé, voir Figure 1 - n'ayant pas pu avoir d'adresses IPv4 en quantité, et dont le réseau interne est IPv6. Mais comme la majorité de l'internet est encore en IPv4, le FAI en question se doit de pouvoir connecter ses clients.

Pour ce faire, il combine deux technologies bien connues, à savoir le NAT et le tunneling, comme illustré à la Figure 19. Il est utile d'introduire deux éléments nécessaires au bon fonctionnement de DS-Lite :

- **B4** (*Basic Bridging Broadband element*) : élément servant à créer un tunnel vers un AFTR.
- **AFTR** (*Address Family Transition Router*) : combinaison d'une fin de tunnel IPv4-dans-IPv6 et d'un NAT IPv4-IPv4

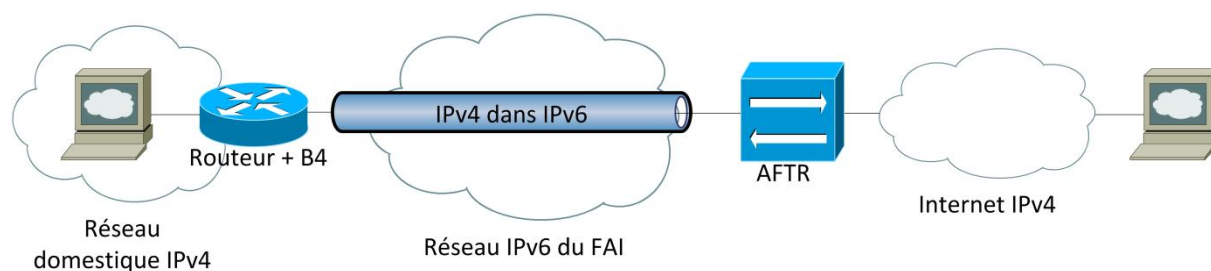


Figure 19: topologie d'utilisation de DS-Lite

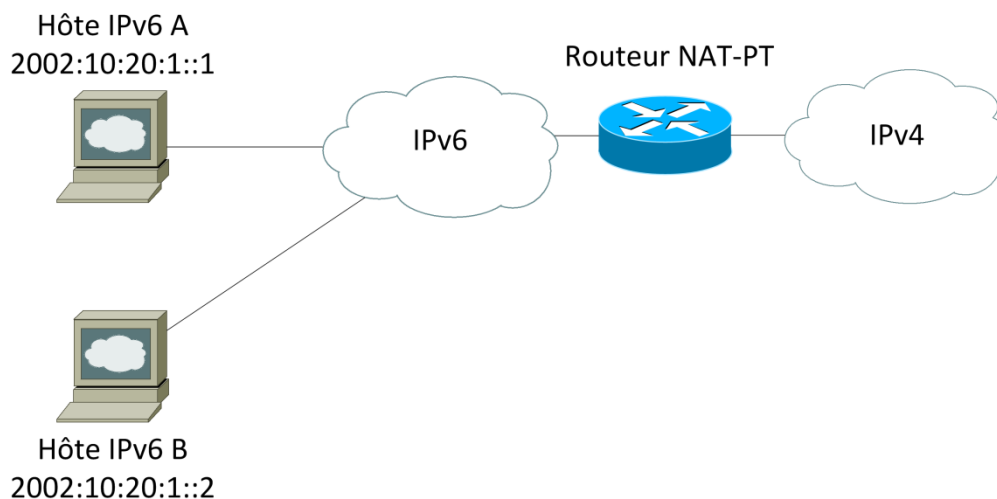
5.3 Techniques de traduction

Certains cas d'utilisation imposent la traduction, ou l'utilisation d'un proxy entre l'IPv6 et l'IPv4. C'est le cas notamment lorsque des hôtes du réseau d'entreprise sont en IPv6, mais que les serveurs du *data center* sont IPv4-only.

Ce sous-chapitre décrit donc les différents mécanismes utilisés pour faire de la traduction d'adresse, c'est-à-dire traduire une adresse IPv4 en IPv6, et inversement. Les techniques utilisées sont aussi variées que différentes, comme vous pouvez le lire ci-après.

5.3.1 NAT-PT

Cette technique est officiellement déclarée comme **historique** par la RFC 4966, en raison de nombreux problèmes décrits en détail dans cette même RFC. **Il ne faut donc plus l'utiliser**. Elle consiste en une traduction d'adresse réseau (couche 3 du modèle OSI) IPv4 en adresse IPv6, et vice-versa. Ceci est illustré à la Figure 20. Ce mécanisme de fonctionnement est similaire au NAT présent dans le réseau IPv4.



Avant Traduction		Après Traduction	
Source	Destination	Source	Destination
2002:10:20:1::1	2002:CA:F0:1::1	192.168.1.1	10.12.1.1
2002:10:20:1::2	2002:CA:F0:1::2	192.168.1.2	10.12.1.2

Figure 20: fonctionnement du NAT PT¹⁹

5.3.2 NAT64

Le NAT64, décrit dans la RFC 6146, est le successeur du NAT-PT. Il permet à des clients IPv6-only de contacter un serveur IPv4, comme on peut le voir à la Figure 21. Il faut noter que la communication ne peut s'initier que dans ce sens. En complétant le NAT64 avec un DNS 64, aucun changement de configuration n'est nécessaire, ni du côté de l'hôte IPv6, ni du côté du serveur IPv4.

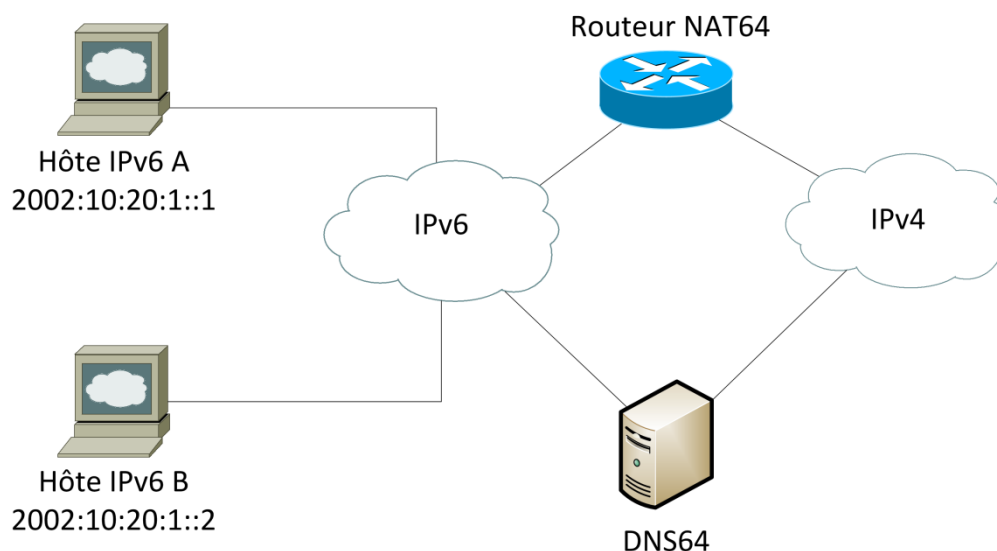


Figure 21: NAT64 et DNS 64²⁰

¹⁹ IPv6 for Enterprise Networks §3 p.63, McFarland, Sambi, Sharma & Hooda, Cisco Press

²⁰ IPv6 for Enterprise Networks §3 p.64, McFarland, Sambi, Sharma & Hooda, Cisco Press

5.3.3 Bump in the Host (BIH)

Bump-in-the-Host, décrit dans la RFC 6535, est un mécanisme de translation côté hôte, permettant à une application IPv4-only fonctionnant derrière un NAT de communiquer avec un serveur IPv6-only. C'est à la fois le successeur et une combinaison de Bump-in-the-stack (RFC 2767) et Bump-in-the-API (RFC 3338). BIH peut être implémenté au niveau de l'API de la socket, en traduisant les appels aux fonctions, ou au niveau de la couche réseau, en convertissant les paquets IPv4 en IPv6 en utilisant le *Stateless IP/ICMP Translation Algorithm* (RFC 6145).

5.3.4 Application Level Gateway (ALG)

Comme son nom l'indique, un ALG est actif à la couche applicative du modèle OSI, et inspecte en détail le contenu des paquets lui étant adressés. Cette machine est placée en général entre le serveur application interne et le lien à internet. Pour l'utilisateur se connectant depuis internet, il est vu comme le but des paquets, mais en réalité, l'ALG inspecte, interprète et traduit si nécessaire chaque requête, avant de la transmettre au serveur applicatif concerné. Le même processus se déroule lorsqu'il reçoit la réponse du serveur applicatif.

Comme système de translation, un ALG peut être utilisé pour effectuer la traduction entre IPv6 et IPv4. Pour ce faire, il inspecte les paquets, et s'ils sont conformes aux règles établies, l'ALG remplace les adresses et numéros de port IPv4 par de l'IPv6, et inversement.

5.3.5 Reverse proxy

Afin de faciliter la communication entre hôtes ou entre applications utilisant une version différente du protocole internet, il est possible d'utiliser un *reverse proxy*. Cela permet donc à un utilisateur de se connecter en IPv6 au proxy, qui lui va chercher la page demandée sur le serveur web en IPv4, et la retourne en IPv6 au client, comme on peut le voir à la Figure 22. Bon nombre d'entreprises ont déjà cet équipement, sous la forme d'un répartiteur de charge (*load balancer*).

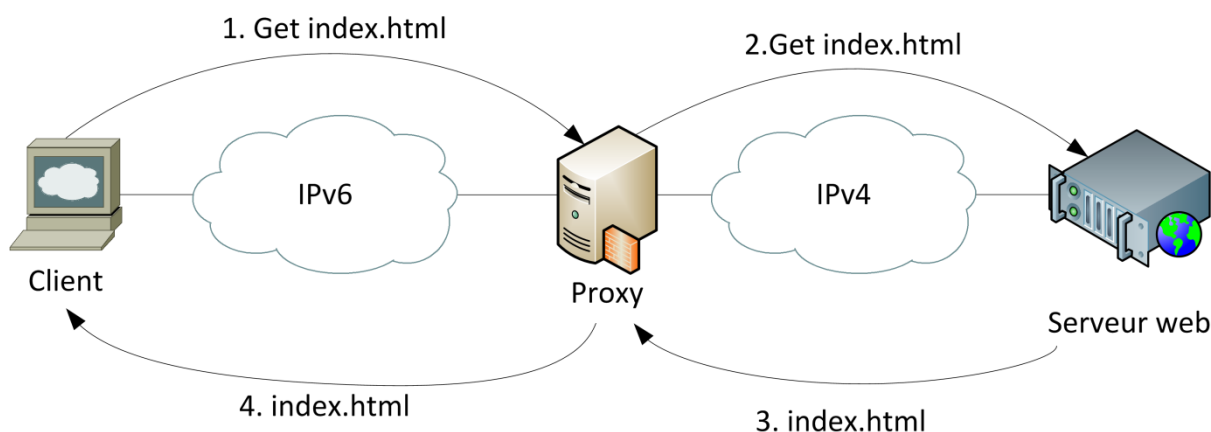


Figure 22: fonctionnement d'un proxy

Cela reste la méthode la plus simple, la moins coûteuse, et la plus performante afin de pouvoir activer IPv6 sur les services web, comme l'a expliqué Fabien Broillet, consultant chez eb-Qual SA, lors de la

conférence du *Swiss IPv6 Council* du 10 mai 2012 à Lausanne²¹. Elle possède l'énorme avantage de ne devoir effectuer aucun changement à l'intérieur même de la DMZ IPv4 existante, si ce n'est l'ajout d'un DNS avec une connectivité IPv6, ou plus simplement l'ajout d'une connexion IPv6 au DNS existant, et des *AAAA records* nécessaires.

Cette intuition fut confirmée par M. François Buntschu, professeur à l'Ecole d'Ingénieurs et d'Architectes de Fribourg (EIA-FR), lors de sa présentation pour le *Swiss IPv6 Council* du 25 juin 2012 à Fribourg. En effet, afin de publier le site internet de l'EIA-FR, M. Buntschu a utilisé leur répartiteur de charge de marque F5 comme reverse proxy.

²¹ http://www.swissipv6council.ch/sites/default/files/images/eb-qual_load_balancing_lasolution.pdf

6 Prototypes

6.1 IPv6 only

Ce premier prototype consiste à mettre en place un routeur Cisco 1921, un firewall Cisco ASA 5510, avec derrière lui une DMZ IPv6, contenant un serveur web Microsoft IIS 2008 R2, ainsi qu'un autre serveur Microsoft 2008 R2 configuré avec le rôle de DNS. Ceci est illustré à la Figure 23.

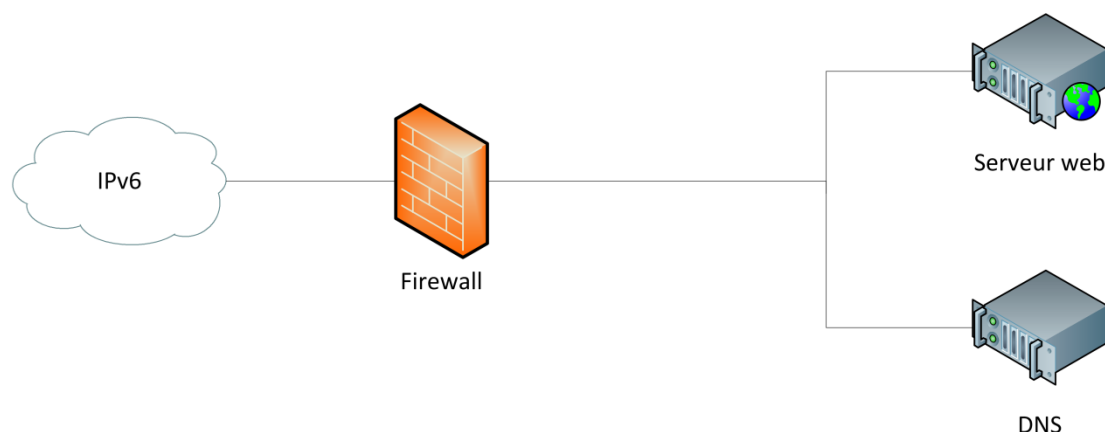


Figure 23: Schéma logique du prototype 1

Dans la topologie détaillée de la Figure 24, on peut voir tout d'abord l'accès IPv6 arrivant vers le routeur *accessa-ipv6* depuis le switch L2-L3 *accessa-ncn*. Derrière le routeur *accessa-ipv6* se trouve le firewall *fw-ipv6*, porte d'entrée de la DMZ contenant le serveur web et le DNS.

Après une phase de configuration de base du routeur, en mettant notamment les mots de passe nécessaires à sa sécurisation, la configuration spécifique a pu commencer. Pour des raisons évidentes de lisibilité, les configurations entières des équipements se trouvent en annexe, à la fin de ce travail. Afin de ne pas perturber le fonctionnement du domaine de production *www.ne.ch*, le domaine *www.ipv6-ne.ch* a été utilisé tout au long de ce travail.

Il n'y a pas eu de difficulté majeure dans la mise en place de ce prototype, mais plutôt un long chemin de recherche, car les commandes du routeur changent quelque peu de l'IPv4. La prise en main de l'interface graphique de configuration du firewall *Cisco ASDM-IDM Launcher, version 1.5(55)* a quant à elle nécessité un investissement notable, puisqu'elle est relativement complexe, et qu'elle m'était inconnue.

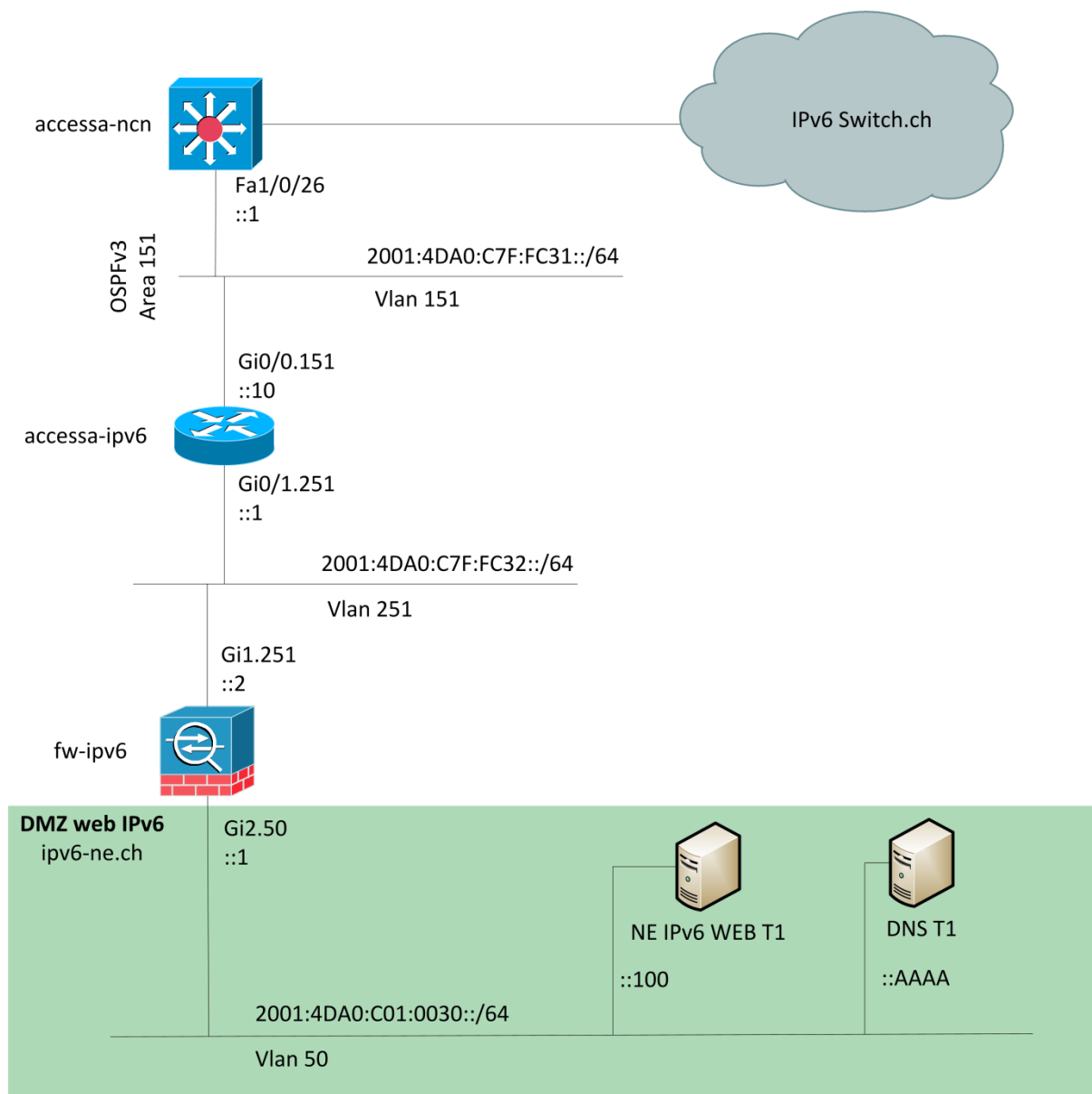


Figure 24: topologie détaillée du prototype IPv6 only

6.1.1 Configuration du routeur

Pour la configuration du routeur, il a tout d'abord fallu mettre à jour OS du routeur à la version 15.2. Ensuite, il a fallu configurer la sous-interface Gigabit Ethernet 0/0 dans le vlan 151, activer l'ipv6, et configurer OSPFv3 area 151. Les commandes sont les suivantes :

```
enable
conf t
interface GigabitEthernet0/0.151
 encapsulation dot1Q 151
 ipv6 address 2001:4DA0:C7F:FC31::10/64
 ipv6 enable
 ipv6 ospf 151 area 151
```

Il faut ensuite répéter le même processus pour l'interface Gigabit Ethernet 0/1, mais dans le vlan 251. De plus, il faut créer une route statique vers l'interface externe du firewall, et la redistribuer dans OSPF. Les commandes sont donc les suivantes :

```
enable
conf t
interface GigabitEthernet0/1.251
  encapsulation dot1Q 251
  ipv6 address 2001:4DA0:C7F:FC32::1/64
  ipv6 enable
end

enable
conf t
ipv6 route 2001:4DA0:C00::/40 2001:4DA0:C7F:FC32::2
ipv6 router ospf 151
  router-id 1.1.31.2
  redistribute static
```

6.1.2 Configuration du firewall

La configuration du firewall s'effectue via l'interface graphique Java du programme *Cisco ASDM-IDM Launcher, version 1.5(55)*. Afin de pouvoir utiliser ce programme, il faut se connecter à l'interface de management du firewall, puis indiquer l'adresse IP de ce dernier. On peut aussi indiquer le nom d'utilisateur et le mot de passe, si ceux-ci ont été configurés, comme on peut le voir à la Figure 25.

6.1.2.1 Configuration des interfaces

Une fois le programme lancé, la première tâche est de configurer les interfaces de notre firewall. La Figure 26 illustre les manipulations :

1. Configuration
2. Device Setup
3. Interfaces

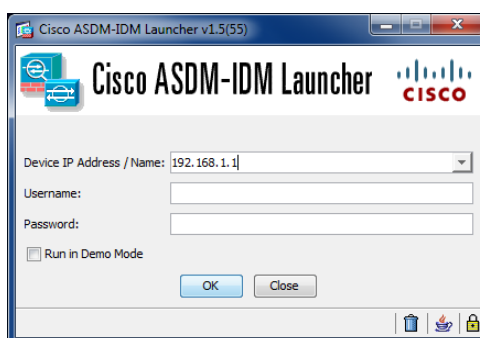


Figure 25: lancement de l'interface graphique du firewall

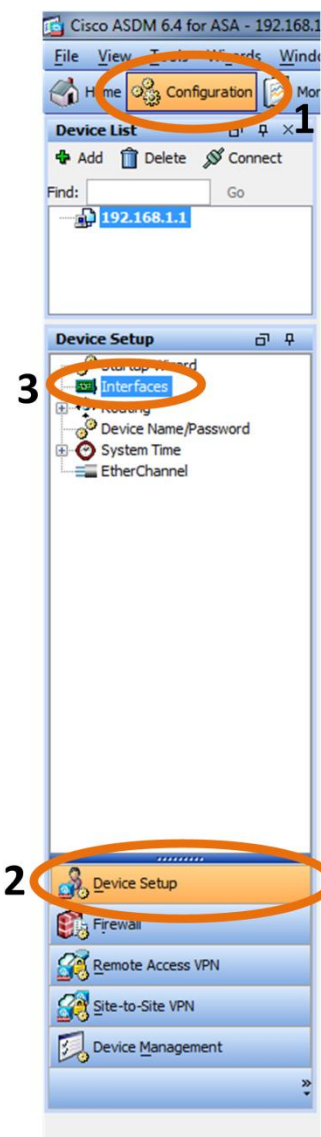


Figure 26: accéder au menu de configuration des interfaces du firewall

Il faut alors sélectionner une interface, et cliquer sur *Edit*. La fenêtre s'étant ouverte, il faut ensuite sélectionner l'onglet IPv6, puis cocher *enable IPv6* et enfin cliquer sur *Add*, afin d'ajouter une adresse IPv6, comme on peut le voir à la Figure 27. Ensuite, on entre l'adresse IPv6 de l'interface dans le champ de la fenêtre représentée à la Figure 28. On confirme en cliquant sur OK. L'adresse est alors ajoutée dans le champ du milieu de la Figure 27. On clique sur OK, et on revient à la fenêtre de configuration des interfaces (Figure 26).

Il ne reste plus qu'à recommencer l'opération pour configurer la deuxième interface.

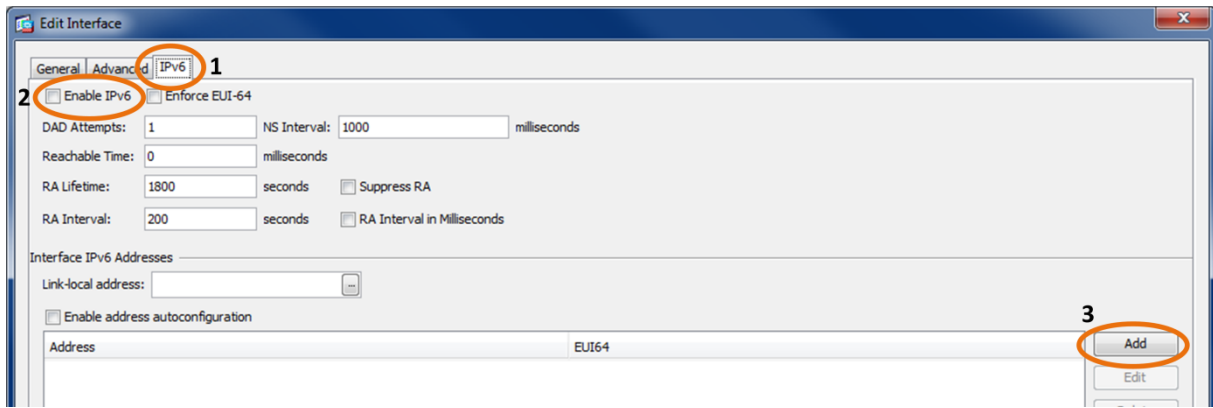


Figure 27: la fenêtre *Edit interface* de l'interface graphique du firewall

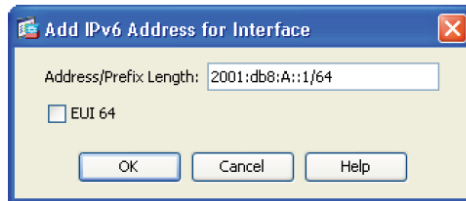


Figure 28: ajout de l'adresse IPv6 de l'interface

6.1.2.2 Configuration de la route statique

Afin que le trafic sortant de la DMZ vers le firewall puisse (s'il en a le droit) ressortir de ce dernier vers l'internet, il est nécessaire de configurer une route statique. Pour cela, il faut tout d'abord se rendre sur (Figure 29) :

1. Configuration
2. Device Setup
3. Routing
4. Static Routes et sélectionné IPv6 Only

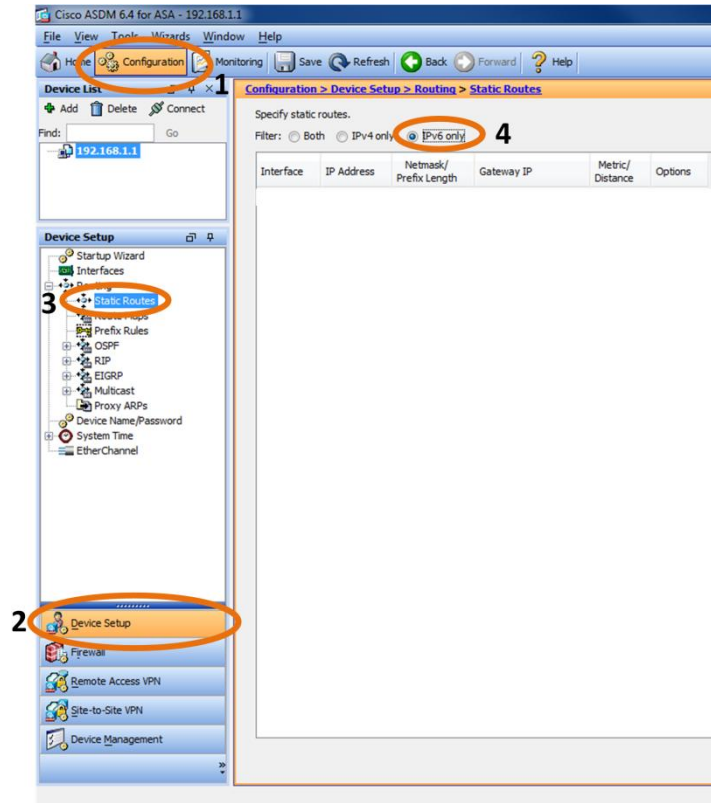


Figure 29: onglet de configuration des routes statiques de l'interface graphique du firewall

Il faut alors cliquer sur *Add*. La fenêtre d'ajout de route statique s'ouvre alors. Il faut remplir les options comme suit (Figure 30) :

- **Interface** : outside
- **IP Address** : ::
- **Gateway IP** : 2001:4da0:c7f:fc32::1 (l'interface du routeur avec laquelle est connecté le firewall)

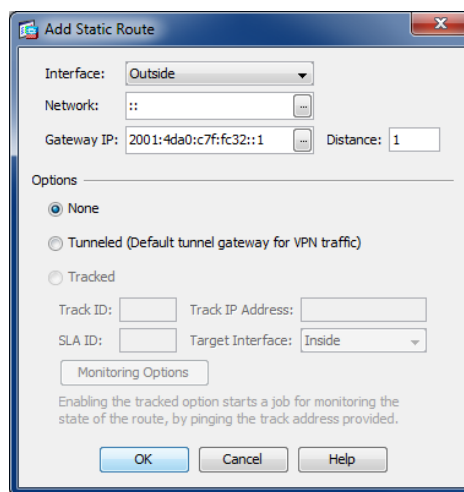


Figure 30: onglet d'ajout d'une route statique

Pour finir, il suffit de cliquer sur OK, et la route est installée.

6.1.2.3 Ajout d'un objet réseau

Afin de simplifier l'ajout de règle du firewall, il est bon de créer des objets réseaux. Pour ce faire, il faut se rendre sur (Figure 31) :

1. Configuration
2. Firewall
3. Objects > Network Objects/Groups
4. Sélectionner IPv6 Network Object
5. Cliquer sur Add – Network Object

La fenêtre d'ajout d'objet réseau s'ouvre alors. Il faut remplir les options comme suit :

- **Name** : dmz-web-ipv6
- **Type** : Network
- **IP Address** : 2001:4DA0:C01:0030::
- **Prefix Length** : 64

Pour finir, il suffit de cliquer sur OK.

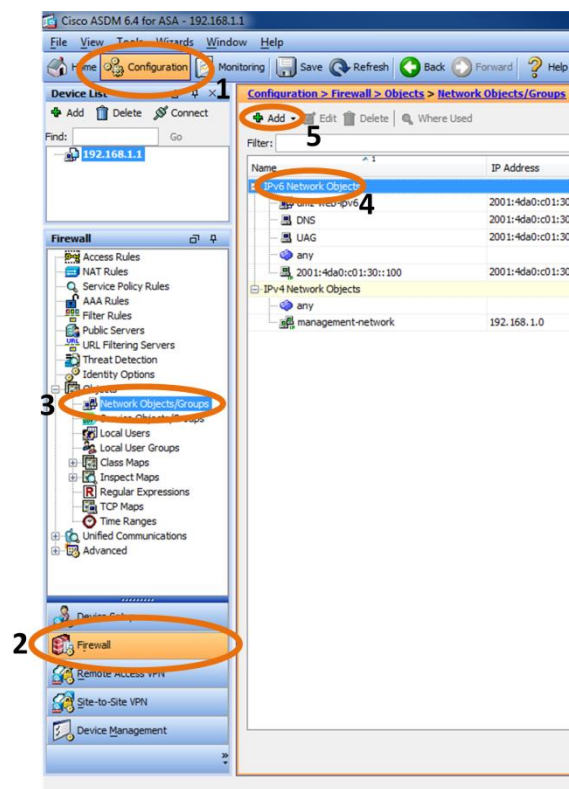


Figure 31: configuration d'un objet réseau

6.1.2.4 Ajout de règles IPv6 pour le Firewall

Afin de sécuriser notre DMZ, nous n'allons laisser passer que le trafic désiré, à savoir l'HTTP/HTTPS vers le serveur web, et les requêtes DNS vers le DNS. Dans un premier temps, à des fins de debugge, nous allons aussi autoriser les paquets ICMPv6 vers le serveur web. Pour ce faire, il faut se rendre :

1. Configuration
2. Firewall
3. Access rules

Ensuite, sélectionner les options suivantes dans la fenêtre (Figure 32) :

1. IPv6 Only
2. Global IPv6
3. Cliquer sur *Add* afin d'ouvrir une fenêtre de configuration de liste d'accès

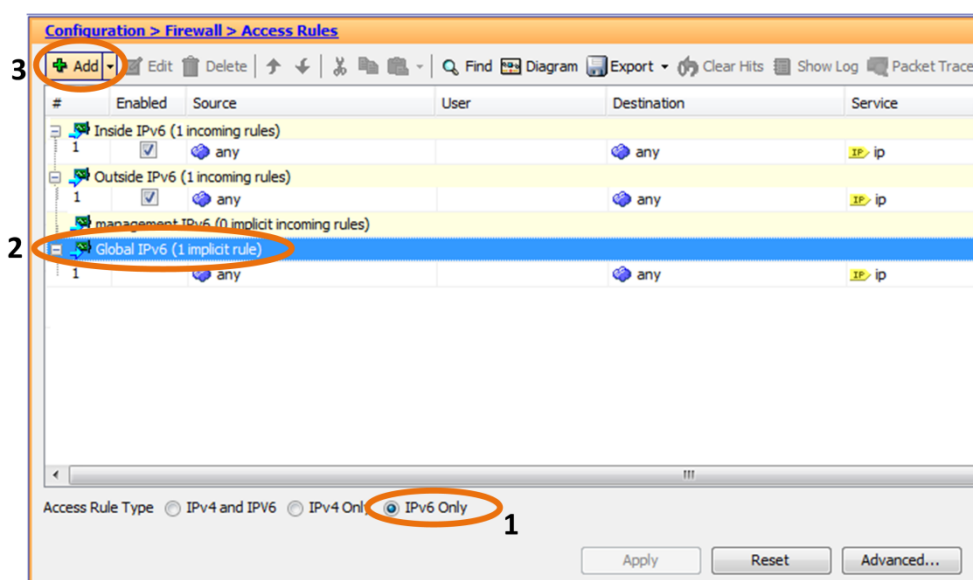


Figure 32: configuration d'une nouvelle règle de firewall

La fenêtre s'étant ouverte, remplissez les options comme suit (Figure 33) :

- **Interface** : any
- **Source** : any
- **Destination** : cliquer sur (...) et sélectionnez dmz-web-ipv6 et cliquer *Add* puis OK
- **Service** : cliquer sur (...) et choisir HTTP et HTTPS

Cliquer sur OK, et la première règle est ajoutée ! Il en va de même pour les règles suivantes. La configuration finale du Firewall peut se voir à la Figure 34.

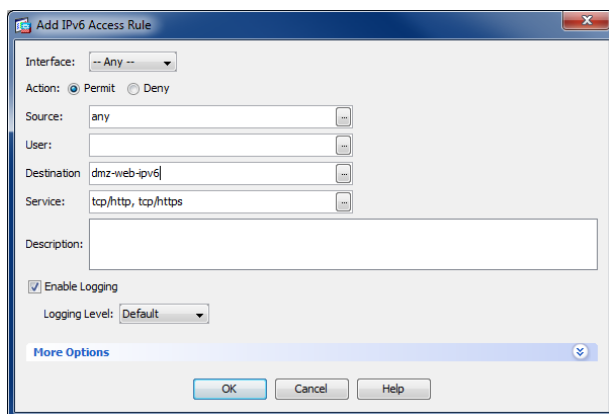


Figure 33: création d'une nouvelle règle du firewall

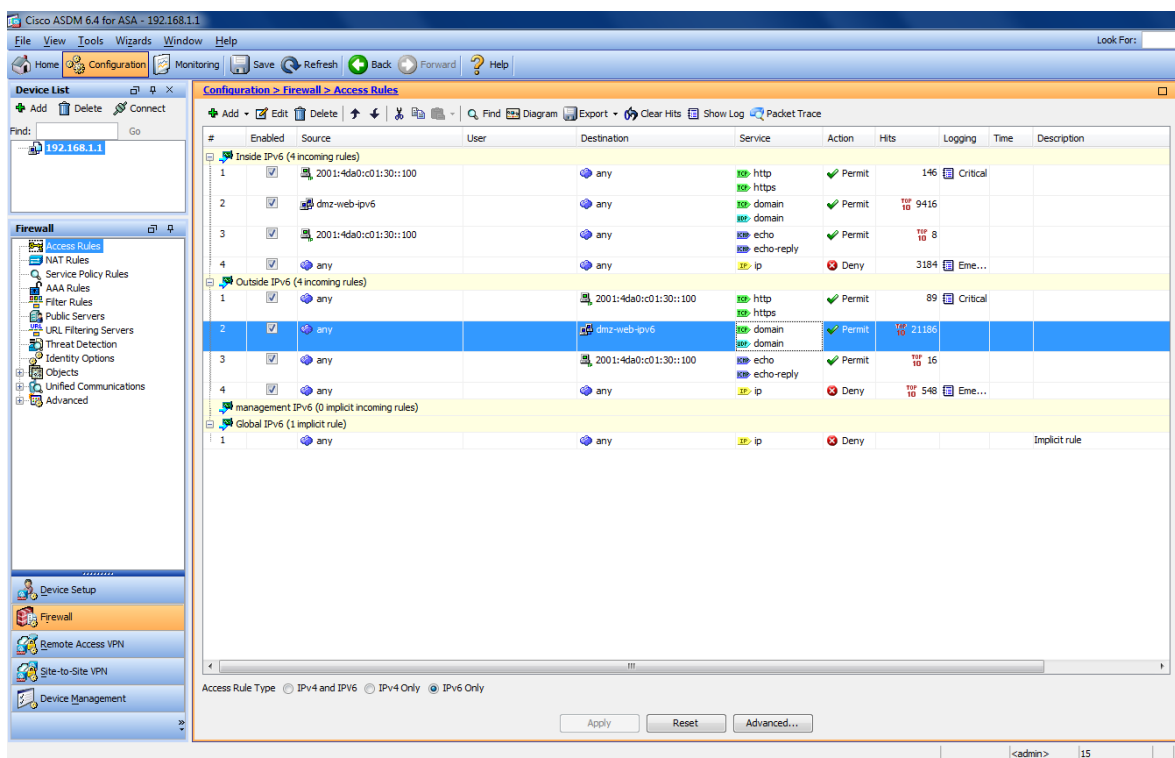


Figure 34: règles finales du firewall pour le prototype 1

6.1.3 Configuration du serveur web IIS

La configuration du serveur web IIS est complètement standard. Après avoir configuré l'interface réseau, ajouté le rôle IIS à un serveur Microsoft Windows 2008 r2, la page index.html par défaut a été remplacée par une page personnalisée, dont le rendu dans un navigateur peut se voir à la Figure 35.



Figure 35: rendu du site dans le navigateur Internet Explorer

6.1.4 Configuration du DNS

La configuration du DNS est complètement standard. Après avoir ajouté le rôle DNS à un serveur Microsoft Windows 2008 r2, il ne reste plus qu'à créer une nouvelle zone et à configurer les *AAAA record* reliant l'adresse IPv6 du serveur web (2001:4da0:c01:30::100) à notre nom de domaine, comme on peut le voir à la Figure 36. Les *pointer records* se configurent automatiquement, en fonction des *AAAA record*, comme on peut le voir à la Figure 37. Il a bien entendu fallu annoncer l'adresse IPv6 du DNS chez switch.ch. La configuration détaillée d'un DNS est documentée en détail dans l'annexe B du travail de Bachelor de M. Steve Lienhard, disponible à l'adresse suivante :

http://www.stephan-robert.ch/attachments/File/Travaux-etudiants/PDB_Steve_Lienhard.pdf

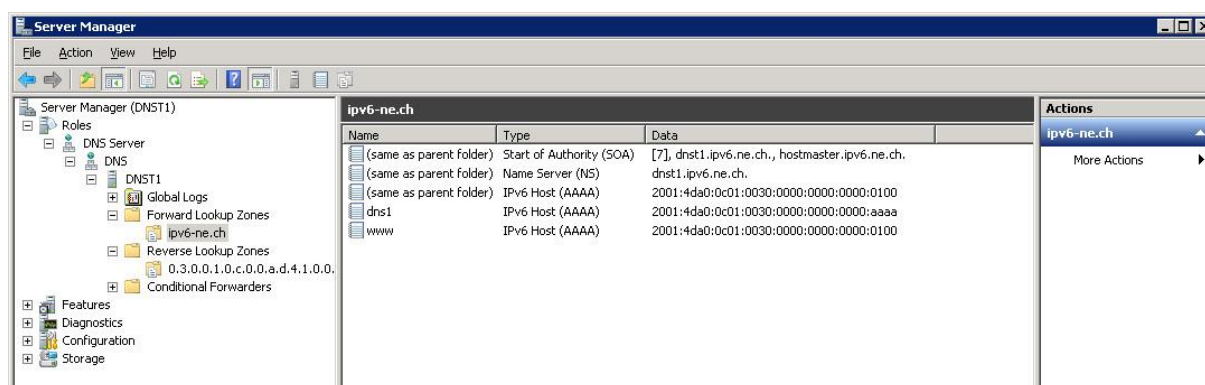


Figure 36: forward lookup zones du DNS

Afin de pouvoir tester les différentes configurations de ce prototype, une connexion internet fournie par Bluewin a été utilisée. IPv6 étant en phase de test chez Bluewin, il était nécessaire pour l'utilisateur désirant obtenir une adresse IPv6, d'activer manuellement une option sur l'interface web de configuration du routeur (manière de faire propre à Swisscom). Il faut noter que le serveur DNS T1

mis en place était seulement connecté au réseau IPv6. En conséquence, la résolution du nom `www.ipv6-ne.ch` ne se faisait pas du tout en utilisant la connexion Bluewin. On peut donc en conclure que le DNS de Bluewin ne dispose pas de connexion au réseau IPv6. Ce problème fut rapidement réglé, en configurant l'adresse IPv6 du DNS public de Google dans les paramètres DNS de la carte réseau. L'adresse de ce dernier se trouve facilement sur internet²², et est : `2001:4860:4860::8888`

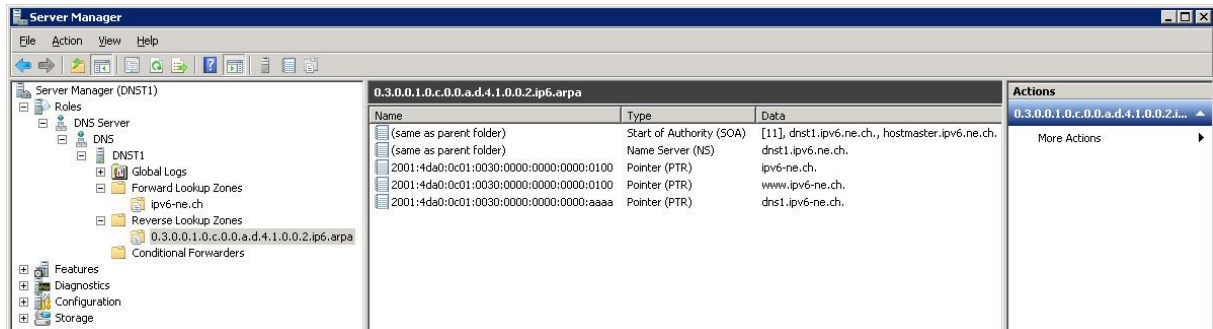


Figure 37: reverse lookup zones du DNS

²² <https://developers.google.com/speed/public-dns/docs/using>

6.2 Reverse proxy

Ce deuxième prototype consiste en une évolution du prototype *IPv6 only*. Son but est de rendre disponible aux internautes se connectant avec IPv6 les ressources internet existant sur un serveur web IPv4. Pour ce faire, la solution du reverse proxy (cf. § 5.3.5) a été retenue, pour des raisons évidentes de simplicité et de coût. Il s'agit donc de connecter la DMZ IPv6 d'un côté du proxy, et une zone privée IPv4 contenant le serveur web de l'autre, comme on peut le voir à la Figure 38. Bien que la solution du NAT64 ait été envisagée de prime abord, elle n'est pas implémentée sous Windows, sauf pour les clients se connectant via Direct Access, le VPN IPv6 de Windows, et désirant accéder à un serveur IPv4 du réseau interne de l'entreprise.

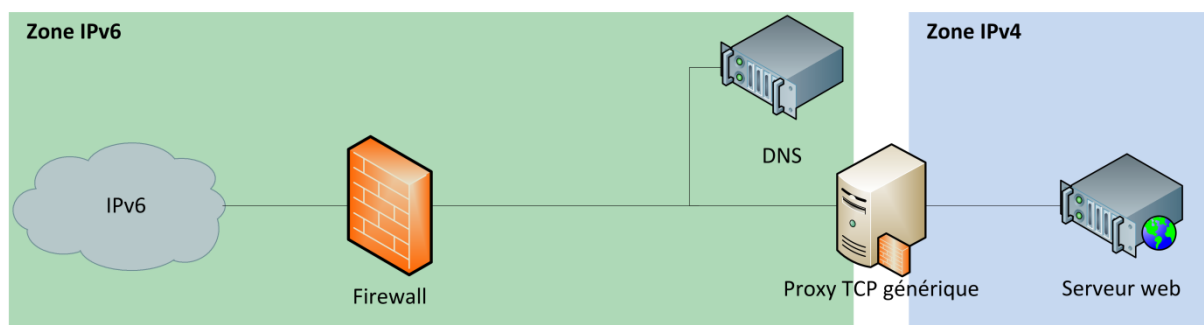


Figure 38: schéma logique du prototype 2

La route jusqu'au prototype fonctionnel fut longue et semée d'embûches. Le paragraphe suivant est donc consacré à l'explication des différentes solutions testées.

Travaillant dans un environnement exclusivement Microsoft, le déploiement du proxy de cette entreprise, appelé *Microsoft Forefront Threat Management Gateway 2010 (TMG)* était la première option choisie. Après l'installation comme serveur virtuel et un test de prise en main, force était de constater que ce produit ne supportait pas l'IPv6. Ceci est confirmé par le site officiel de Microsoft²³. L'étape d'après était l'installation du « grand frère » de TMG, à savoir *Microsoft Forefront Unified Access Gateway 2010 (UAG)*, car il supporte l'IPv6, et contient TMG. Mais là encore, impossible de paramétrer le TMG intégré comme proxy IPv6. Microsoft ayant informé Gartner, leader mondial de la recherche et du conseil sur les technologies de l'information, qu'il n'y aurait pas de nouvelle version de TMG prévue²⁴, il était donc possible que TMG soit intégré dans le dernier né des produits Microsoft : *Windows Server 2012 Release Candidate*. Une fois encore, la désillusion fut totale.

C'est alors que la description de la commande `PortProxy`, trouvée à la page 271 du livre *Understanding IPv6, second edition, Microsoft Press* attira mon attention. Cette commande, disponible depuis Windows Vista / Serveur 2008, permet de configurer une machine Windows comme proxy TCP générique pour les trafics suivant s :

²³ <http://technet.microsoft.com/en-us/library/ee796231.aspx#bvd45dsf45>

²⁴ <http://blog.konab.com/2011/05/what-will-happen-with-tmg/>

- **IPv4 à IPv4** : le trafic TCP arrivant à une adresse IPv4 est redirigé vers une autre adresse IPv4.
- **IPv4 à IPv6**: le trafic TCP arrivant à une adresse IPv4 est redirigé vers une adresse IPv6.
- **IPv6 à IPv6**: le trafic TCP arrivant à une adresse IPv6 est redirigé vers une autre adresse IPv6.
- **IPv6 à IPv4**: le trafic TCP arrivant à une adresse IPv6 est redirigé vers une adresse IPv4.

Dans notre cas, c'est la fonction de proxy du trafic TCP IPv6 à du trafic TCP IPv4 qui nous intéresse, car elle permet à un hôte IPv6 d'accéder à un service IPv4.

Comme on peut le remarquer sur la topologie détaillée de la Figure 39, l'architecture jusqu'au DNS situé derrière le firewall est la même que pour le prototype *IPv6 only*. Le changement principal est qu'un serveur Windows configuré comme proxy TCP générique (NE IPv6 T1) est connecté à la place du serveur web, sur le même segment réseau que le DNS. Derrière ce proxy TCP générique, qui interface le réseau IPv6 avec le réseau IPv4, se trouve un TMG (NE TMG T1), servant de passerelle web sécurisée pour la publication des pages du serveur web. Nous avons derrière le TMG un contrôleur de domaine (NE IPv6 DC T1), nécessaire à l'installation du TMG, et le serveur web (NE IPv6 WEB T1). Cette infrastructure est semblable à celle utilisée en production par le SIEN.

Le lecteur averti remarquera que l'espace d'adressage choisi derrière le proxy TCP générique est un espace d'adressage publique, mais qu'il n'appartient pas au SIEN. Ceci a été imposé par l'administrateur système lors de la configuration des serveurs virtuels. Vu la configuration du firewall, il n'était pas possible que des paquets contenant une adresse de cet espace sorte sur internet.

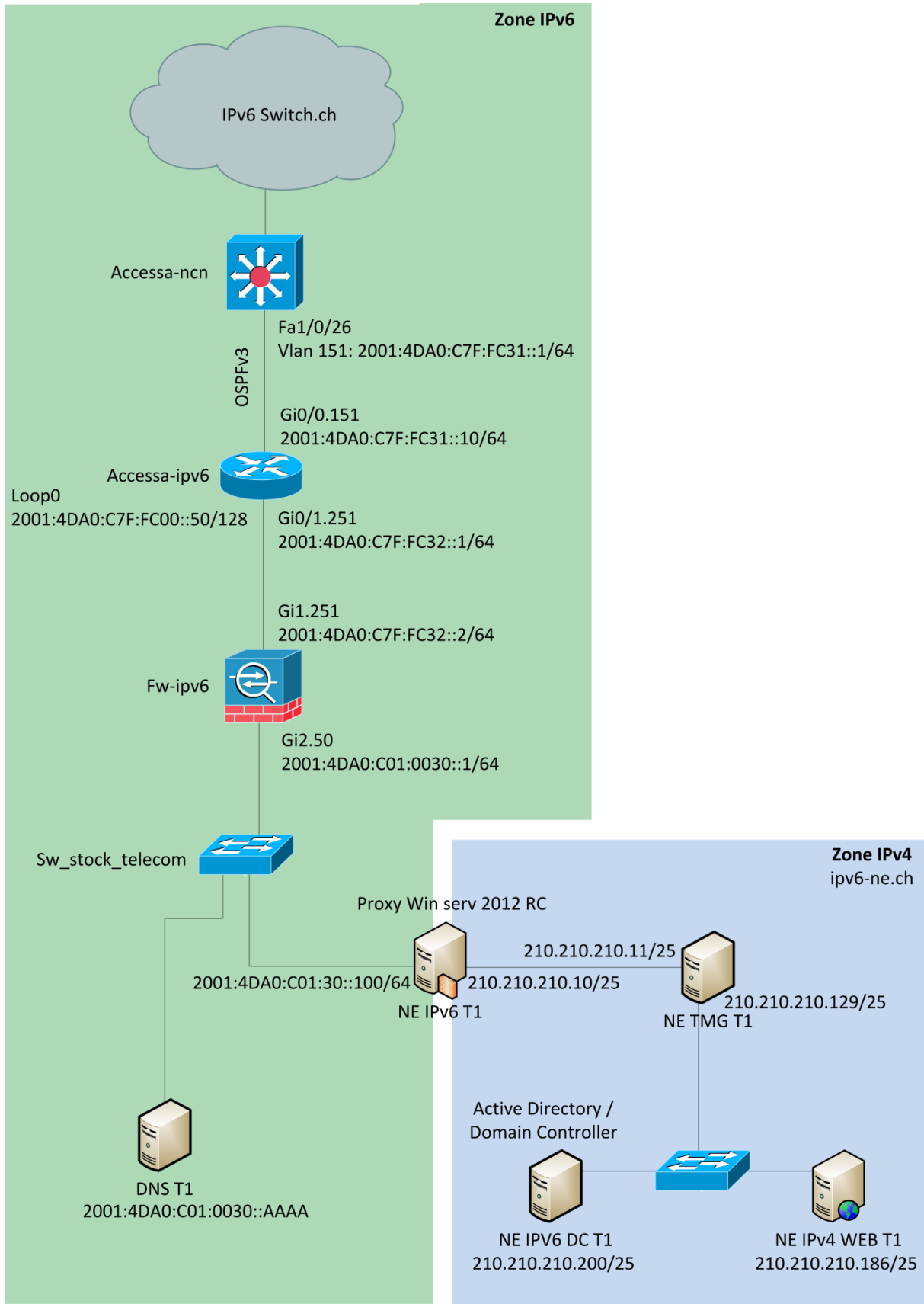


Figure 39: topologie détaillée du prototype reverse proxy

6.2.1 Configuration du routeur

La configuration du routeur `accessa-ipv6` est identique au prototype *IPv6 only*.

6.2.2 Configuration du firewall

La configuration du firewall `fw-ipv6` est identique au prototype *IPv6 only*.

6.2.3 Configuration du DNS

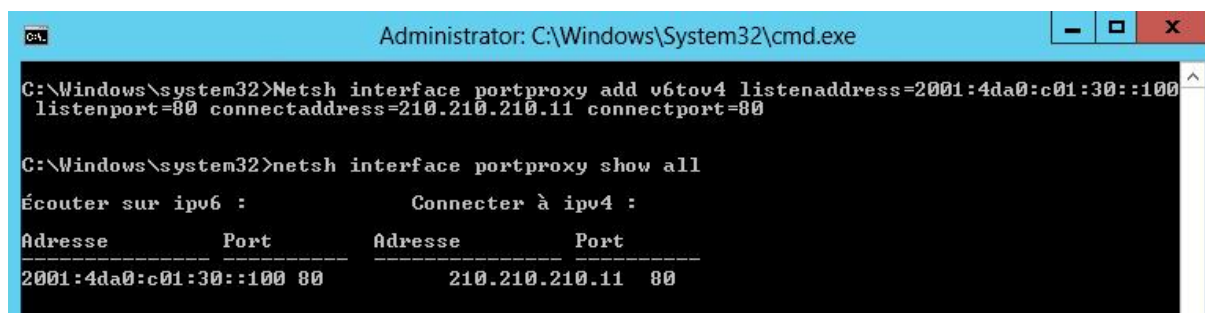
La configuration du DNS est identique au prototype *IPv6 only*, car l'adresse qui était utilisée pour le serveur web dans le précédent prototype est utilisée par la proxy TCP générique.

6.2.4 Configuration du proxy TCP générique

La configuration du proxy TCP générique fut le morceau de choix, après avoir choisi quel produit utiliser pour réaliser ce dernier, comme expliqué au début de ce chapitre. Pour ce faire, il a tout d'abord fallu ouvrir une invite de commande en tant qu'administrateur. Puis, il a fallu taper la commande de configuration, comme on peut le voir à la Figure 40. Elle s'énonce comme ceci :

```
Netsh interface portproxy add v6tov4 listenaddress=2001:4da0:c01:30::100  
listenport=80 connectaddress=210.210.210.11 connectport=80
```

Listenaddress et *listenport* sont respectivement l'adresse IPv6 et le port d'écoute du proxy TCP générique ; et *connectaddress* et *connectport*, l'adresse IPv4 et le port sur lesquels le proxy TCP générique va se connecter. *Listenaddress* est donc l'adresse du *AAAA record* du DNS, et *connectaddress* l'adresse d'écoute du TMG.



```
Administrator: C:\Windows\System32\cmd.exe  
C:\Windows\system32>netsh interface portproxy add v6tov4 listenaddress=2001:4da0:c01:30::100  
listenport=80 connectaddress=210.210.210.11 connectport=80  
  
C:\Windows\system32>netsh interface portproxy show all  
Écouter sur ipv6 :          Connecter à ipv4 :  
-----  
Adresse      Port      Adresse      Port  
-----  
2001:4da0:c01:30::100 80          210.210.210.11 80
```

Figure 40: commande de configuration du proxy TCP générique et affichage de la configuration

Avant d'arriver à la topologie décrite à la Figure 39, différents essais ont été réalisés. Tout d'abord, simplement en connectant le proxy TCP générique directement au serveur web. Ce premier test fut concluant en tout point. Ensuite, afin de se rapprocher de la topologie de production du SIEN, la machine NE IPv6 T1 faisant office de proxy TCP a été remplacée par la machine NE TMG T1, étant le TMG, avec le serveur web connecté derrière elle. L'idée était d'utiliser la même machine pour le proxy TCP et le TMG. Après configuration de la commande `netsh interface portproxy add v6tov4` sur le TMG, force fut de constater qu'il était impossible d'accéder à la page hébergée sur le serveur web. Le firewall intégré au TMG bloquait les paquets, avant même d'arriver sur le proxy TCP et de pouvoir être redirigés. C'est pourquoi l'ajout d'une machine dédiée à la fonction de proxy TCP fut nécessaire, pour arriver finalement à la topologie de la Figure 39.

6.2.5 Configuration du TMG

Bien que ne rentrant pas exactement dans le cadre de la migration de service web en IPv6, l'installation et la configuration d'un TMG fut nécessaire, afin de pouvoir l'utiliser dans ce prototype et le suivant. En effet, le SIEN utilise un TMG comme proxy web sécurisé en production, et il fallait se rapprocher au maximum de l'infrastructure de production lors des tests. L'installation et la configuration du TMG se sont avérées longues, mais peu ardues. Elles sont documentées en annexe, au chapitre 15.2.4 et 15.2.5 respectivement.

6.2.6 Configuration du serveur Web IIS

Le changement d'adresse IP de la carte réseau pour se conformer à la topologie de la Figure 39 mis à part, la configuration du serveur web est identique au prototype *IPv6 only*.

6.3 Dual Stack

Le dernier des trois prototypes mis en place dans le cadre de ce travail consiste en une évolution du prototype *reverse proxy*. Il en reprend intégralement la topologie, mais en étant dual-stack (c.f § 5.1), comme on peut le voir à la Figure 41. Ceci est le but du SIEN pour la publication de leur service web en IPv4 et en IPv6.

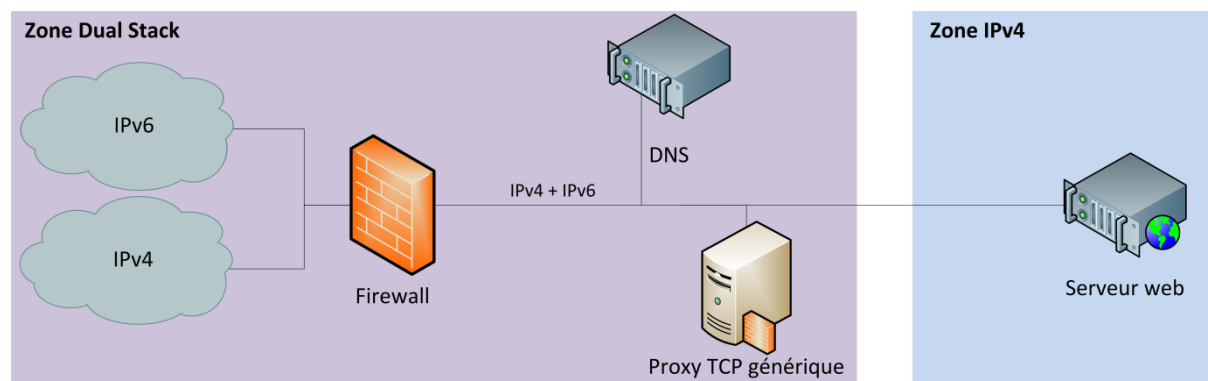


Figure 41: schéma logique du prototype dual stack

L'ajout de l'IPv4 sur l'infrastructure n'a pas été d'une grande difficulté, puisque tout est connu et extrêmement bien documenté. Il a aussi été question dans ce prototype d'être le plus strict possible au niveau du filtrage des paquets, mais sans perdre de fonctionnalités. C'est pourquoi la recherche a aussi été poussée en ce sens, que ça soit au niveau des *access-lists* du routeur *accessa-ipv6* situées en amont du firewall, ou au niveau des règles du firewall elles-mêmes.

A la Figure 42, on peut remarquer l'ajout d'adresses IPv4 publiques au switch *accessa-ncn*, au routeur *accessa-ipv6*, aux deux interfaces du firewall, ainsi qu'au DNS. Concernant le proxy TCP générique, qui possédait deux interfaces réseau lors du précédent prototype, il a été décidé avec le mandant de regrouper les adresses IPv4 et IPv6 sur une seule et même interface. Ceci fonctionnerait bien évidemment en conservant les deux interfaces réseaux avec l'adresse IPv4 sur une, et l'adresse IPv6 sur l'autre. L'interface réseau externe du TMG reçoit elle aussi une adresse IPv4 publique. Pour l'interne cependant, comme pour le serveur web, et le contrôleur de domaine, l'espace d'adressage publique n'appartenant pas au SIEN a été conservé, selon la volonté de l'administrateur système. Ces adresses ne se retrouveront jamais du côté externe du TMG.

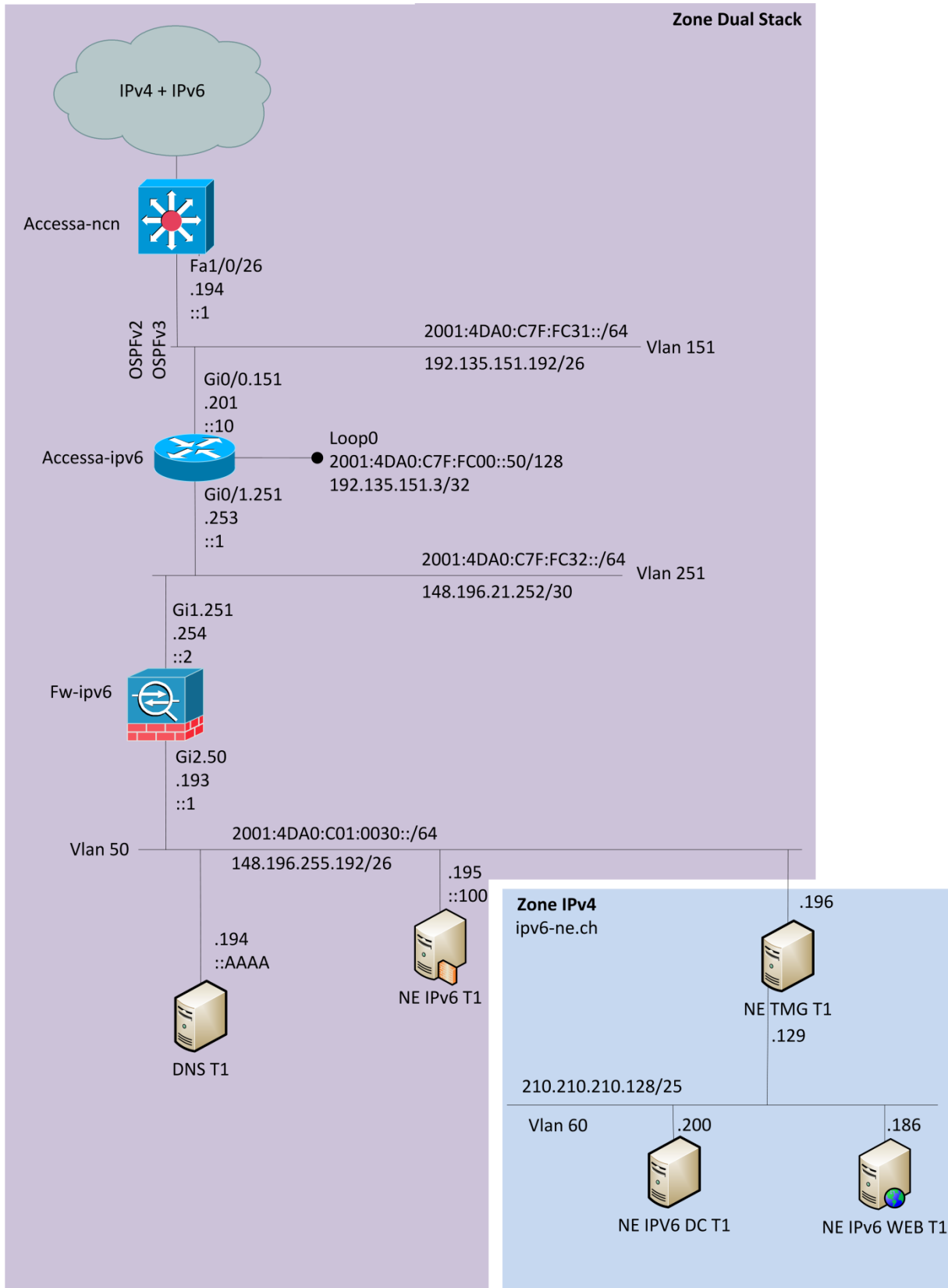


Figure 42: topologie détaillée du prototype dual stack

6.3.1 Configuration du routeur

Pour la configuration du routeur, il a tout d'abord fallu ajouter une adresse IPv4 aux deux interfaces, ainsi qu'à l'interface loopback. Les commandes pour ceci sont les suivantes :

```
enable
conf t
interface GigabitEthernet0/0.151
 ip address 192.135.151.201 255.255.255.192

interface GigabitEthernet0/1.251
 ip address 148.196.21.253 255.255.255.252

interface Loopback0
 ip address 192.135.151.3 255.255.255.255
```

Ensuite, il a fallu configurer OSPF, en précisant de redistribuer les réseaux directement connectés :

```
router ospf 40
 redistribute static subnets
 network 148.196.21.252 0.0.0.3 area 1
 network 192.135.151.192 0.0.0.63 area 1
```

Puis, il a fallu créer une route statique vers l'interface externe du firewall :

```
enable
conf t
ip route 148.196.255.192 255.255.255.192 148.196.21.254
```

Pour continuer, il faut créer une *access-list* IPv4 afin de filtrer les adresses privées et une *access-list* IPv6 afin de n'autoriser que les adresses publiques, et le multicast servant aux échanges de LSA entre routeurs, afin de maintenir le peering OSPF. Il faut noter les autorisations implicites des *access-list* IPv6, ajoutées en vert à la suite de la liste GlobalUnicastOnly, avant l'interdiction par défaut. Elles sont ajoutées automatiquement à la fin de chaque *access-list* IPv6, et permettent aux paquets ICPMv6 servant à la découverte de voisins de transiter par le routeur. En IPv4, il n'y a que l'interdiction par défaut qui est implicite.

```
enable
conf t
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 deny 172.16.0.0 0.15.255.255
access-list 10 deny 192.168.0.0 0.0.255.255
access-list 10 permit any

ipv6 access-list GlobalUnicastOnly
 permit ipv6 2000::/3 any
 permit ipv6 FE80::/10 any
 permit icmp any any nd-na
 permit icmp any any nd-ns
 deny ipv6 any any
```

Enfin, il faut activer les *access-lists* sur la bonne interface, et choisir si c'est pour le trafic entrant dans le routeur, ou le trafic sortant du routeur. Dans notre cas, on les applique les deux pour le trafic entrant sur l'interface connectée au switch *accessa-ncn* :

```
enable
conf t
interface GigabitEthernet0/0.151
 ip access-group 10 in
 ipv6 traffic-filter GlobalUnicastOnly in
```

6.3.2 Configuration du firewall

La configuration du firewall en IPv4 à l'aide de l'interface graphique Java du programme *Cisco ASDM-IDM Launcher, version 1.5(55)* est bien connue, c'est pourquoi seul les éléments remarquables seront soulevés.

6.3.2.1 Configuration des interfaces

Les interfaces ont été configurées sans problème particulier.

6.3.2.2 Configuration de la route statique

La configuration de la route statique redirigeant le trafic de l'interface *outside* du firewall vers le routeur *accessa-ipv6* n'a posé aucun problème.

6.3.2.3 Ajout d'un objet réseau

L'essai de création d'un objet réseau IPv4 portant le même nom qu'un objet réseau IPv6 s'est soldé par une erreur, illustré à la Figure 43. Il n'est donc pas possible pour le même objet réseau d'avoir une adresse IPv4 et une adresse IPv6 dans cette version du programme, qui était la dernière au moment d'effectuer ce travail.

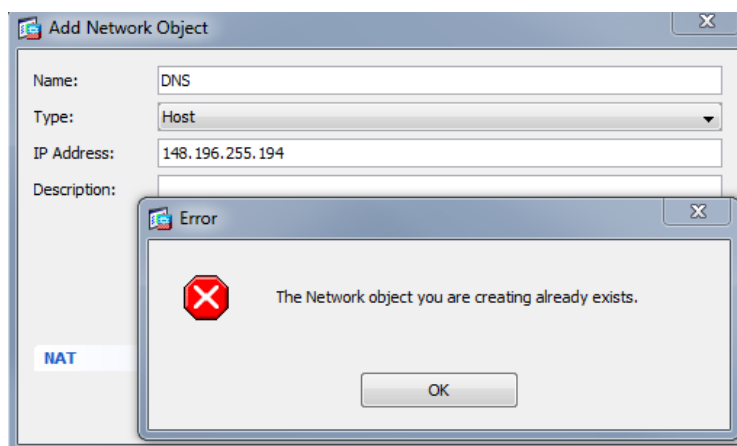


Figure 43: erreur lors de la création d'un objet réseau IPv4 portant le même nom qu'un objet IPv6 existant

6.3.2.4 Ajout de règles IPv4 pour le firewall

Concernant les règles IPv4 du firewall, elles sont standards, comme on peut le voir à la Figure 44. On autorise toutes les adresses de l'extérieur à se connecter en http et https au serveur web, et à faire des requêtes DNS (TCP et UDP 53) vers le DNS, et on autorise le DNS à envoyer ces mêmes requêtes depuis l'intérieur.

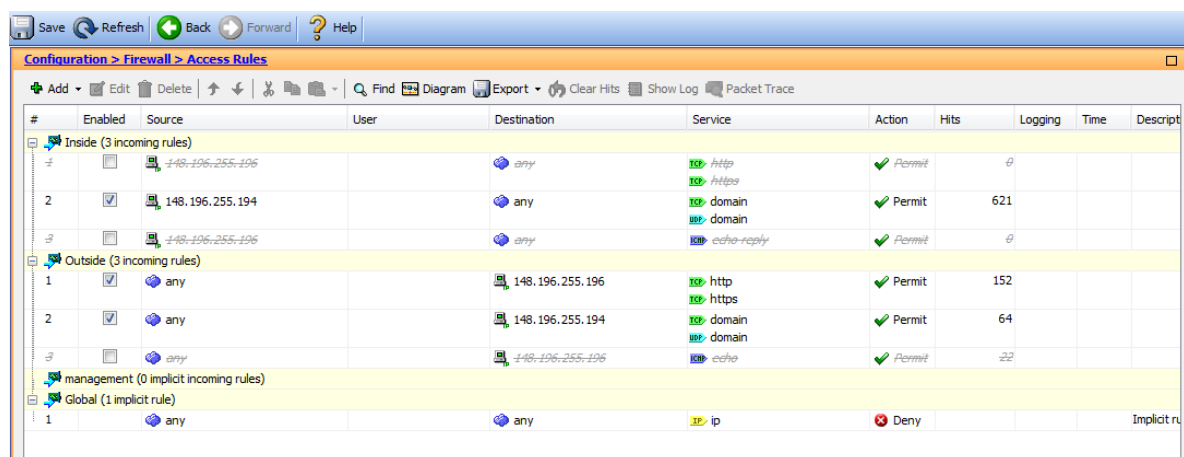


Figure 44: règles IPv4 du firewall

Concernant les règles IPv6, elles sont les mêmes que pour le prototype *IPv6 only*, sauf que le filtrage des paquets ICMPv6 a été affiné. En effet, simplement interdire tous les paquets ICMPv6 après la phase de debugge est une erreur, comme le suggère la RFC 4890, intitulée « *Recommendations for Filtering ICMPv6 Messages in Firewalls* ». Après réflexion, et en suivant les recommandations du chapitre 4.3 de la RFC, les messages ICMPv6 suivant sont autorisés :

Type	Nom
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
135	Neighbor Solicitation
136	Neighbor Advertisement

Tableau 4: messages ICMPv6 autorisés

On peut voir les règles IPv6 du firewall à la Figure 45.

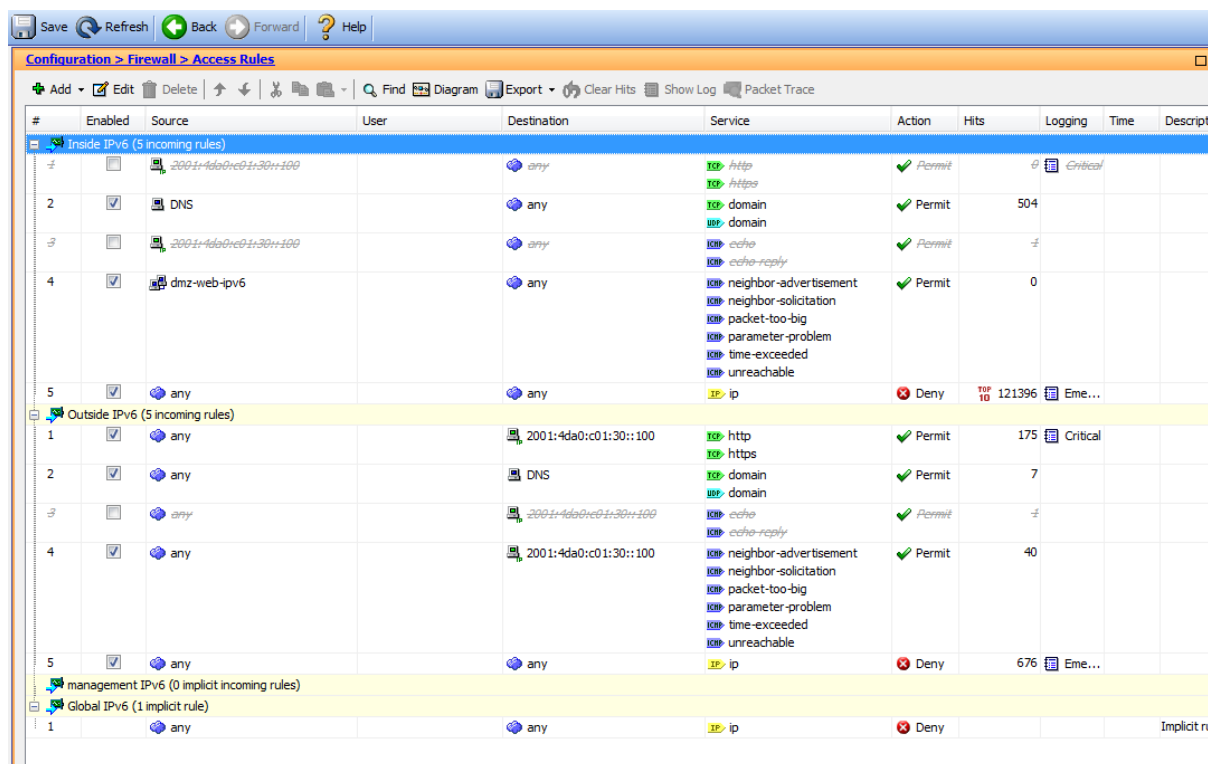


Figure 45: règles IPv6 du firewall

6.3.3 Configuration du DNS

La configuration du DNS est identique au prototype précédent, à deux exceptions près :

- l'ajout d'un *A record* pointant sur l'adresse IPv4 de l'interface réseau externe du TMG : 148.196.255.196.
- l'ajout d'une adresse IPv4 à l'interface réseau, et l'annonce de celle-ci chez switch.ch.

6.3.4 Configuration du proxy TCP générique

La configuration du proxy TCP générique est identique au prototype précédent, à l'exception de l'adresse sur laquelle la connexion est redirigée. En effet, c'est sur l'adresse IPv4 publique de l'interface réseau externe du TMG, à savoir 148.196.255.196, comme on peut le voir à la Figure 46.

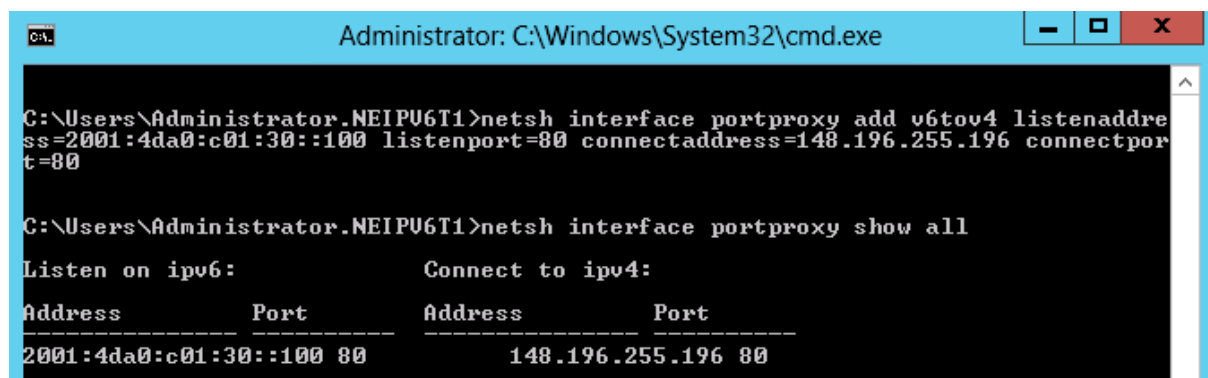


Figure 46 : commande de configuration du proxy TCP générique et affichage de la configuration

On peut clairement voir à la Figure 47 le fonctionnement du proxy TCP lors de la connexion d'un client en IPv6, essayant de charger la page `www.ipv6-ne.ch`. Cette capture de paquet est effectuée sur le proxy TCP générique, à l'aide du logiciel *Wireshark v. 1.8.0*²⁵ avec le filtre `http` activé.

Le paquet 524 représente la connexion depuis l'hôte vers l'adresse contenue dans le *AAAA record* du DNS, à savoir l'interface réseau du proxy TCP. Le paquet 529 représente la même requête que le paquet 524, mais avec l'adresse source IPv4 de l'interface réseau du proxy TCP, et l'adresse de destination de l'interface réseau externe du TMG. C'est cela même qui est configuré à l'aide de la commande `netsh interface portproxy`. On peut ensuite voir au paquet 557 la réponse du TMG vers l'adresse IPv4 de l'interface réseau du proxy TCP. Enfin, au paquet 558, la réponse du proxy TCP avec comme source l'adresse IPv6 de son interface réseau, et comme destination l'adresse IPv6 du client. Pour des raisons de nombres de paquets, le fonctionnement n'est expliqué qu'avec la connexion, et non le chargement complet de la page. Cependant, le principe est analogue.

No.	Time	Source	Destination	Protocol	Length	Info
524	65.069298000	2a02:120b:2c0c:4530:84cd:7608:e3c0:123c	2001:4da0:c01:30::100	HTTP	389	GET / HTTP/1.1
529	65.069542000	148.196.255.195	148.196.255.196	HTTP	369	GET / HTTP/1.1
557	77.439648000	148.196.255.196	148.196.255.195	HTTP	929	HTTP/1.1 200 OK (text/html)
558	77.439729000	2001:4da0:c01:30::100	2a02:120b:2c0c:4530:84cd:7608:e3c0:123c	HTTP	949	HTTP/1.1 200 OK (text/html)

Figure 47: capture de paquets sur le proxy TCP lors d'une connexion en IPv6

6.3.5 Configuration du TMG

Le changement de l'adresse IPv4 de l'interface réseau externe du TMG est la seule différence de configuration par rapport au prototype *reverse proxy*.

6.3.6 Configuration du serveur web IIS

La configuration du serveur web n'a pas changé par rapport au prototype précédent.

7 Performances observées

Les performances des prototypes mis en place ont été testées à l'aide du programme *Apache Jmeter*²⁶, sous la forme d'un test de charge. L'intérêt d'un tel test ne se justifie par sur le prototype *IPv6 only* ou *reverse proxy*, car ils ne sont pas prévus pour être utilisés en production. Ils étaient la construction logique du prototype *dual-stack*. Sur ce dernier par contre, il est intéressant de voir comment il supporte une charge de trafic conséquente.

La bande passante de la connexion fournie par l'entreprise Swisscom afin de réaliser le test de charge est de 10'000 kbits/s en download et 1'000 kbits/s en upload. Les résultats du test de charge en IPv4 sont bons, comme on peut le voir à la Figure 48. En effet, lors de mille connexions successives générées aussi rapidement qu'un ordinateur le peut, la moyenne du temps de réponse (bleu) se situe à 59 ms, et la médiane (violet) à 50 ms. Ce délai est tout à fait respectable.

²⁵ <http://www.wireshark.org/>

²⁶ <http://jmeter.apache.org/>

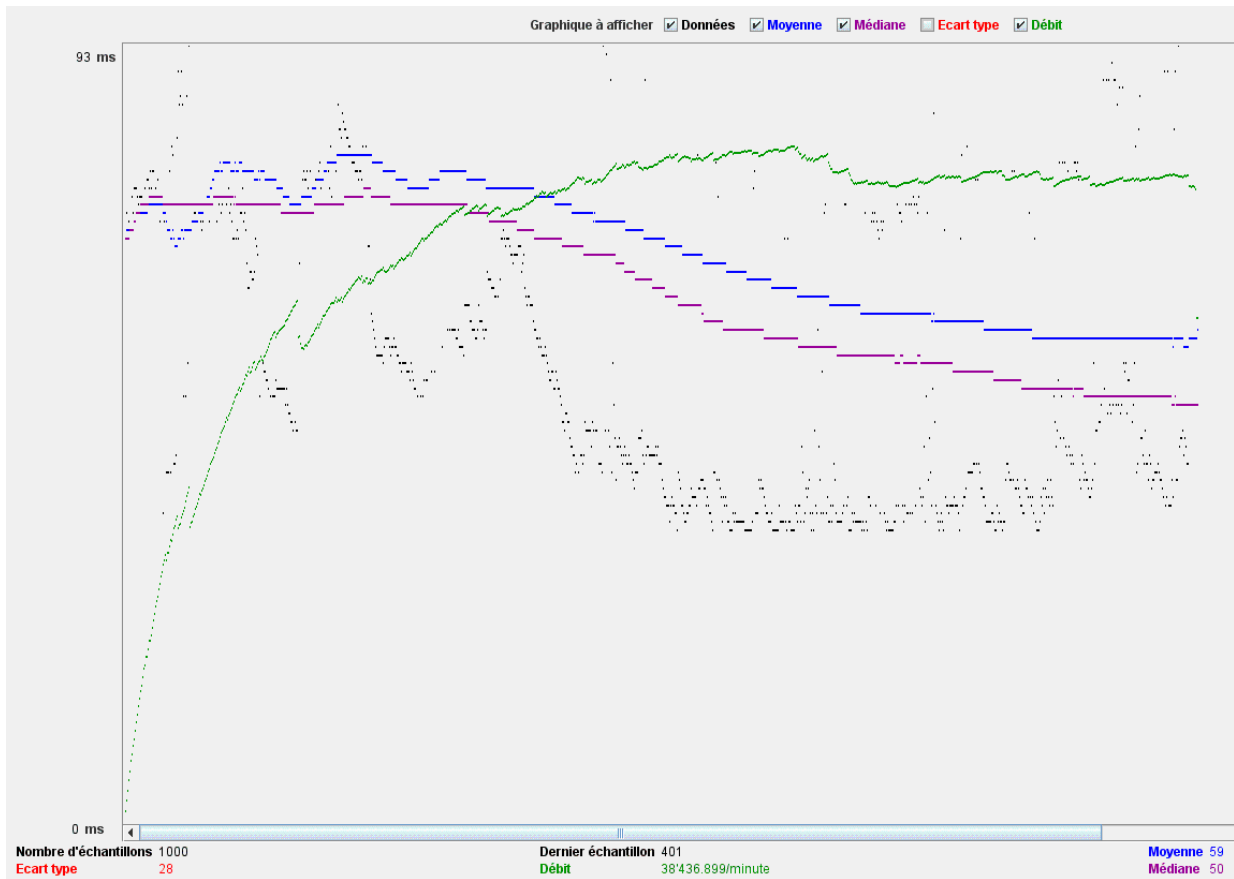


Figure 48: graphique de résultat pour un test de charge IPv4 de mille connexions

Afin de pouvoir faire le même test de charge en IPv6, il a tout d'abord fallu supprimer le *A record* du DNS reliant le nom `www.ipv6-ne.ch` à l'adresse de l'interface réseau externe du TMG. En effet, en présence d'un *A record* et d'un *AAAA record*, le programme *Apache Jmeter* préfère utiliser l'adresse IPv4 afin de se connecter au serveur web. On peut voir à la Figure 49 les résultats du test de charge en IPv6, et ils sont presque semblables à la connexion en IPv4, et ce malgré l'ajout du proxy TCP générique. La moyenne du temps de réponse se situe à 72 ms, et la médiane à 54 ms.

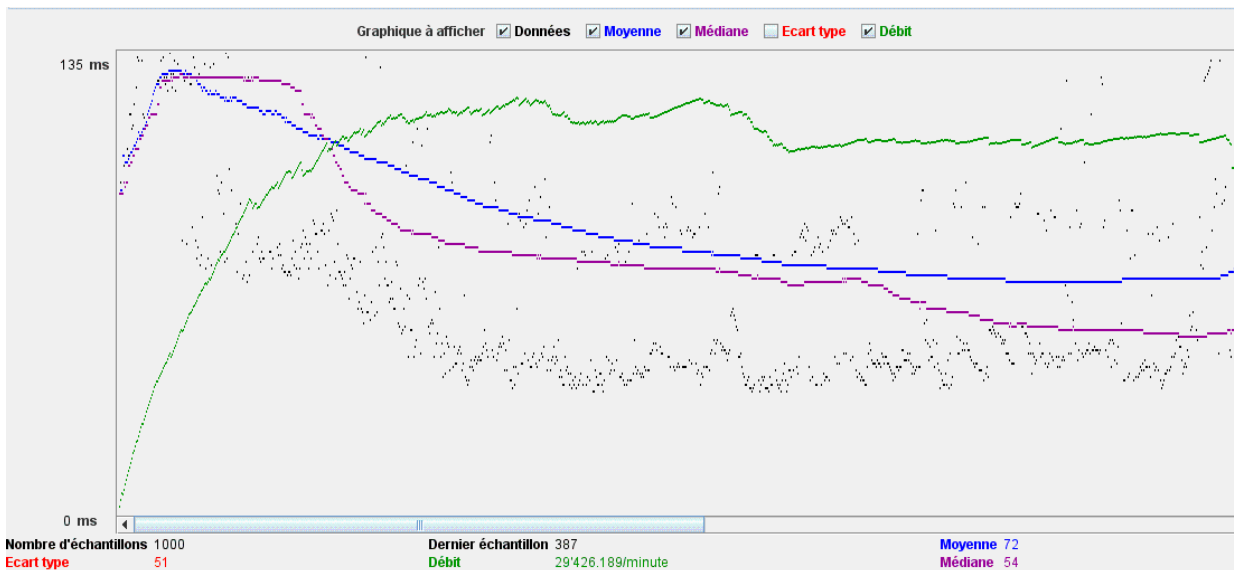


Figure 49: graphique de résultat pour un test de charge IPv6 de mille connexions

Ces tests nous montrent donc que l'infrastructure mise en place supporte convenablement une montée en charge.

8 Discussion des résultats

Les résultats obtenus dans les tests de charge sont bons. Ils nous ont montré que l'infrastructure supportait une montée en charge. La topologie du prototype *dual-stack* est aussi proche que possible de l'environnement de production du SIEN, à quelques exceptions hardware près (modèle du firewall par exemple). Ceci laisse donc raisonnablement penser que cette topologie est viable en production.

Toutefois, il faut être attentif aux différentes limitations du prototype *dual-stack*. Elles se situent essentiellement au niveau du proxy TCP générique, qui constitue un composant critique pour les hôtes se connectant en IPv6. Tout d'abord, celui-ci doit posséder une capacité de traitement suffisante, et il doit être redondant, comme expliqué au dernier paragraphe de la page 7 du white paper d'Akamai²⁷, intitulé « *IPv6: What the Transition Means for Content and Application Delivery* ».

Ensuite, il faut être conscient que le proxy TCP générique crée une perte d'information pour les statistiques web IPv6. En effet, toutes les requêtes arrivant depuis l'IPv6 sur le proxy TCP générique se transformeront en requête IPv4, avec comme adresse source l'adresse IPv4 du proxy TCP lorsqu'elles arriveront sur le TMG. Le SIEN effectue actuellement ses statistiques web sur le TMG, et non sur les serveurs web situés derrière lui. Ceci pourrait être corrigé en utilisant un proxy commercial (de la marque F5 comme à l'EIA-FR) ou un proxy utilisant un autre OS que Windows. Les deux solutions précitées utilisent le champ *X-forwarded-for*, qui permet de garder la trace de l'adresse source lors du passage à travers un proxy. Ce champ n'est pas implémenté par Windows, car il n'est défini dans aucune RFC, mais est un standard issu de l'industrie. L'IETF a cependant commencé le processus de standardisation.

Puis, il faut être attentif au nombre de connections par seconde sur le proxy TCP générique. En effet, l'épuisement des ports TCP peut engendrer l'indisponibilité du service, alors même que l'utilisation du CPU, de la RAM, et de la connexion réseau du proxy TCP sont des plus raisonnables. Lors d'une connexion, un serveur Microsoft 2008 R2 va utiliser par défaut les ports de 49'152 à 65'535, ce qui fait un total de 16'383 ports. Un port utilisé pour une connexion reste réservé pendant 4 minutes. On peut facilement augmenter le nombre de ports utilisés par Windows, et diminuer le temps pendant lequel un

27

http://www.akamai.com/dl/whitepapers/IPv6_whitepaper.pdf?curl=/dl/whitepapers/IPv6_whitepaper.pdf&solche so=1&, p. 7, dernier paragraphe

port reste réservé à 30 secondes. Ceci est expliqué en détail dans l'article « *How to tune the TCP/IP stack for high volume of web requests* » rédigé par M. Miguel Simões João²⁸.

Enfin, il faut être attentif à la charge de trafic subie par le firewall. Bien qu'il n'ait jamais souffert d'une quelconque surcharge, le firewall Cisco ASA 5510 inspecte l'IPv6 en software, et non en hardware.

9 Développements futurs

La migration des services web est une première étape dans le processus de migration d'un réseau. Le prototype dual-stack réalisé a pu servir d'étude pour une migration de l'environnement de production. Il ne reste qu'à mettre en place les éléments mentionnés dans ce travail, afin que les services web soient disponibles en IPv6 comme en IPv4, avec un minimum de changements à l'infrastructure existante.

Pour la suite, une migration du service mail est la prochaine étape. Pour ce faire, il faut configurer le serveur Microsoft Exchange 2010 (ou plus récent) en IPv6. Bien entendu, ceci doit obligatoirement passer par une phase de test en laboratoire.

La migration d'un réseau multi-VRF en IPv6 n'étant pas encore possible à cause des limitations matérielles, il faut surveiller quand cette fonctionnalité sera implémentée sur les équipements réseau. Dès lors, il devrait être possible de migrer une grande partie, voir la totalité du réseau du SIEN en IPv6.

10 Conclusion

Ne connaissant l'IPv6 que de nom avant le début de ce travail, j'ai pu approfondir mes connaissances dans ce domaine. Les changements par rapport au protocole IPv4 sont multiples et permettent assurément une optimisation. Cependant, l'adoption d'IPv6 n'a pas été et n'est toujours pas aussi rapide qu'il le faudrait. En effet, le phénomène du serpent qui se mord la queue a pendant longtemps joué le rôle de frein : les entreprises disent qu'elles ne veulent pas migrer, car les fournisseurs d'accès ne sont pas prêts, et les fournisseurs d'accès disent qu'il n'y a pas de demande de la part des clients, c'est pourquoi ils ne migrent pas. Mais ceci a heureusement changé depuis le lancement mondial de l'IPv6, car les poids lourds de l'industrie ont définitivement adopté ce protocole.

La grande révélation de ce travail est le retard des fournisseurs de matériels réseaux dans l'implémentation de fonctions clés qu'utilisent les administrateurs réseaux. Si une grande partie des

²⁸ <http://www.outsystems.com/NetworkForums/ViewTopic.aspx?TopicId=6956&Topic=How-to-tune-the-TCP%2FIP-stack-for-high-volume-of-web-requests>

fonctionnalités de base existent, les outils de monitoring et de log de réseau n'existent pas, ou ne sont pas suffisamment au point en IPv6. Mais heureusement, le retard se comble rapidement.

Enfin, travailler sur un projet aussi concret, et ayant une portée aussi grande a été une véritable source de motivation. Intégrer un environnement de production de la taille de celui du SIEN, en comprendre une partie de la topologie, et pouvoir relier les compétences théoriques aux appareils physiques présents dans le datacenter fut un réel plaisir, et m'a conforté dans mon choix de formation.

11 Remerciements

Je tiens ici à remercier M. Jérôme Vernez et M. Joaquim Silva pour leur disponibilité et leurs conseils durant chaque phase de ce projet.

Un grand merci également à M. Fabien Bruchez, qui éclaira de ses compétences techniques les passages obscures, et à M. Stephan Robert qui m'a fait confiance et m'a suivi tout au long de ce projet.

Ensuite, merci à M. Yann Müller pour son aide logistique et sa bonne humeur.

Enfin, merci à Elisabeth, ma mère, pour son soutien, son écoute et ses attentives relectures.

Renens, le 27 juillet 2012

Simon Dunand

12 Références

12.1 Bibliographie

- IPv6 for Enterprise Networks, McFarland, Sami, Sharma & Hooda, Cisco Press
- Understanding IPv6, second edition, Joseph Davies, Microsoft Press
- Demain: IPv6 êtes-vous prêts?, Fabien Bruchez, LANexpert SA
- 6net, An IPv6 Deployment Guide, The 6NET Consortium, September 2005
- Prototype dual-stack IPv4/6 sur un backbone MPLS-VPN, Steve Lienhard, Projet de Bachelor heig-vd
- Prototype dual-stack IPv4/6 sur un backbone MPLS-VPN, Julien Tissot, Projet de Bachelor heig-vd

12.2 Webographie

12.2.1 Spécificités du protocole IPv6

- Bienvenue | Swiss IPv6 Council : <http://www.swissipv6council.ch/fr>
- Test your IPv6 : <http://test-ipv6.com/>
- IPv6 – Wikipédia : <http://fr.wikipedia.org/wiki/Ipv6>
- IPv6 – Wikipédia : <http://en.wikipedia.org/wiki/IPv6>
- MPLS | V6 World Congress 2012 :
<http://www.uppersideconferences.net/mplsworld2012/index.html>
- Teredo Overview: <http://technet.microsoft.com/en-us/library/bb457011.aspx>
- IPv6 address types : [http://technet.microsoft.com/en-us/library/cc757359\(v=ws.10\)](http://technet.microsoft.com/en-us/library/cc757359(v=ws.10))
- Portée des adresses : <http://www.linux-france.org/prj/edu/archinet/systeme/ch07s06.html>
- IPv6 address - Wikipedia : http://en.wikipedia.org/wiki/IPv6_address#IPv6_address_scopes
- IPv6 addressing : <http://msdn.microsoft.com/en-us/library/aa917150.aspx>
- Application-level Gateway - Wikipedia : http://en.wikipedia.org/wiki/Application-level_gateway
- Internet World Statistics : <http://www.internetworldstats.com/>
- Results of a Security Assessment of the IPv6, Fernando Gont, SI6 Networks, Hack.lu 2011 conference : <http://archive.hack.lu/2011/fgont-hacklu2011-ip-security.pdf>
- How to tune the TCP/IP stack for high volume of web requests :
<http://www.outsystems.com/NetworkForums/ViewTopic.aspx?TopicId=6956&Topic=How-to-tune-the-TCP%2FIP-stack-for-high-volume-of-web-requests>
- Securing IPv6 : <http://blogs.cisco.com/security/securing-ipv6/>

12.2.2 RFC

- Internet Protocol, Version 6 (IPv6) specification : <http://tools.ietf.org/html/rfc2460>
- Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS) :
<http://tools.ietf.org/html/rfc2767>
- IPv6 Tunnel Broker: <http://tools.ietf.org/html/rfc3053>
- Connection of IPv6 Domains via IPv4 Clouds: <http://tools.ietf.org/html/rfc3056>
- Dual Stack Hosts Using "Bump-in-the-API" (BIA) : <http://tools.ietf.org/html/rfc3338>
- Deprecating Site Local Addresses : <http://tools.ietf.org/html/rfc3879>
- Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs) :
<http://tools.ietf.org/html/rfc4380>
- Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification : <http://tools.ietf.org/html/rfc4443>
- Recommendations for Filtering ICMPv6 Messages in Firewalls :
<http://www.ietf.org/rfc/rfc4890.txt>
- Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status : <http://tools.ietf.org/html/rfc4966>
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) :
<http://tools.ietf.org/html/rfc5214>
- IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) : <http://tools.ietf.org/html/rfc5569>
- IP/ICMP Translation Algorithm : <http://tools.ietf.org/html/rfc6145>
- Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers : <http://tools.ietf.org/html/rfc6146>
- Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion :
<http://tools.ietf.org/html/rfc6333>
- IPv6 Node Requirements : <http://tools.ietf.org/html/rfc6434>
- Dual-Stack Hosts Using "Bump-in-the-Host": <http://tools.ietf.org/html/rfc6535>

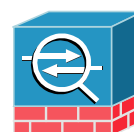
13 Liste des symboles et abréviations

13.1 Symboles

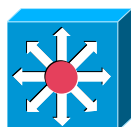
Routeur Cisco 1921



Firewall Cisco ASA 5510



Switch L2/L3



NAT



13.2 Abréviation

6rd	IPv6 rapid deployment
AFRINIC	African Network Information Center
ALG	Application Level Gateway
APNIC	Asia Pacific Network Information Center
ARIN	American Registry for Internet Numbers
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EIA-FR	Ecole d'ingénieurs et d'architectes de Fribourg
EUI-64	Extended Unique Identifier 64
FAI	Fournisseur d'accès Internet
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
ICMPv6	Internet Control Message Protocol Version 6
IETF	Internet Engineering Task Force
Ipsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Internet Service Providers
LACNIC	Latin American and Caribbean IP address Regional Registry
LSA	Link State Advertisement
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NAT64	Network Address Translation IPv6 to IPv4
NAT-PT	Network Address Translation - Protocol Translation
NIC	Network Interface Card
OSI	Open Systems Interconnection
QoS	Quality of Service
RAM	Random Access Memory
RFC	Request for Comments
RIPE-NCC	Réseau IP Européens - Network Coordination Center
RIR	Regional Internet Registry
SIEN	Service Informatique de l'Entité Neuchâteloise
SLAAC	Stateless Address Autoconfiguration
TCP	Transmission Control Protocol
TEREDO	Microsoft address assignment and automatic tunneling technology
TMG	Microsoft Forefront Threat Management Gateway
UAG	Microsoft Forefront Unified Access Gateway
UDP	User Datagram Protocol
ULA	Unique-local Address
VLSM	Variable Length Subnet mask

VPN	Virtual Private Network
-----	-------------------------

14 Liste des figures

Figure 1 : projection de l'épuisement d'adresse IPv4 chez les différents RIR.....	- 9 -
Figure 2: logo du lancement mondial de l'IPv6.....	- 9 -
Figure 3: proportion d'utilisateurs asiatiques d'internet par rapport au nombre mondial d'utilisateurs (état au 31.12.2011) `	- 11 -
Figure 4: hiérarchie d'allocation d'adresse IPv6	- 13 -
Figure 5: domaine de validité de la portée des adresses.....	- 15 -
Figure 6: création d'une adresse EUI-64	- 16 -
Figure 7: comparaison de l'en-tête IPv4 et IPv6.....	- 18 -
Figure 8: le fonctionnement récursif du champ <i>Next Header</i>	- 19 -
Figure 9: réseau dual-stack.....	- 21 -
Figure 10: tunnel d'un paquet IPv6 à l'intérieur d'IPv4	- 22 -
Figure 11: tunnel hôte à routeur	- 22 -
Figure 12: tunnel hôte à hôte	- 23 -
Figure 13: tunnel IPv6 sur IPv4 GRE.....	- 23 -
Figure 14: mise en place automatique d'un tunnel à l'aide d'un tunnel broker	- 24 -
Figure 15: interconnexion de domaines 6to4	- 24 -
Figure 16: création d'un tunnel ISATAP	- 25 -
Figure 17: infrastructure Teredo.....	- 26 -
Figure 18: schéma de fonctionnement de 6rd.....	- 26 -
Figure 19: topologie d'utilisation de DS-Lite	- 27 -
Figure 20: fonctionnement du NAT PT.....	- 28 -
Figure 21: NAT64 et DNS 64	- 28 -
Figure 22: fonctionnement d'un proxy	- 29 -
Figure 23: Schéma logique du prototype 1.....	- 31 -
Figure 24: topologie détaillée du prototype IPv6 only	- 32 -
Figure 25: lancement de l'interface graphique du firewall	- 33 -
Figure 26: accéder au menu de configuration des interfaces du firewall	- 34 -
Figure 27: la fenêtre <i>Edit interface</i> de l'interface graphique du firewall.....	- 35 -
Figure 28: ajout de l'adresse IPv6 de l'interface	- 35 -
Figure 29: onglet de configuration des routes statiques de l'interface graphique du firewall	- 36 -
Figure 30: onglet d'ajout d'une route statique.....	- 36 -
Figure 31: configuration d'un objet réseau	- 37 -

Figure 32: configuration d'une nouvelle règle de firewall.....	- 38 -
Figure 33: création d'une nouvelle règle du firewall.....	- 39 -
Figure 34: règles finales du firewall pour le prototype 1	- 39 -
Figure 35: rendu du site dans le navigateur Internet Explorer	- 40 -
Figure 36: forward lookup zones du DNS.....	- 40 -
Figure 37: reverse lookup zones du DNS.....	- 41 -
Figure 38: schéma logique du prototype 2	- 42 -
Figure 39: topologie détaillée du prototype reverse proxy.....	- 44 -
Figure 40: commande de configuration du proxy TCP générique et affichage de la configuration..	- 45 -
Figure 41: schéma logique du prototype dual stack	- 47 -
Figure 42: topologie détaillée du prototype dual stack.....	- 48 -
Figure 43: erreur lors de la création d'un objet réseau IPv4 portant le même nom qu'un objet IPv6 existant	- 50 -
Figure 44: règles IPv4 du firewall.....	- 51 -
Figure 45: règles IPv6 du firewall.....	- 52 -
Figure 46 : commande de configuration du proxy TCP générique et affichage de la configuration.-	- 52 -
Figure 47: capture de paquets sur le proxy TCP lors d'une connexion en IPv6	- 53 -
Figure 48: graphique de résultat pour un test de charge IPv4 de mille connexions	- 54 -
Figure 49: graphique de résultat pour un test de charge IPv6 de mille connexions	- 54 -
Figure 50:écran d'accueil de l'installation de TMG, choisir <i>Run Preparation Tool</i>	- 70 -
Figure 51: écran de démarrage de l'outil de préparation.....	- 71 -
Figure 52: acceptation des termes du contrat de licence	- 72 -
Figure 53: choix du type de l'installation	- 72 -
Figure 54: fin l'outil de préparation	- 73 -
Figure 55: écran d'accueil de l'installation de TMG, choisir <i>Run Installation Wizard</i>	- 74 -
Figure 56: assistant d'installation de TMG	- 75 -
Figure 57: acceptation des termes du contrat de licence	- 75 -
Figure 58: information concernant le client	- 76 -
Figure 59: choix du scénario d'installation	- 76 -
Figure 60: choix du chemin d'installation.....	- 77 -
Figure 61: ajout de l'espace d'adressage utilisé	- 77 -
Figure 62: définition du réseau interne (i.e. derrière le TMG).....	- 78 -
Figure 63: avertissement concernant les services qui seront redémarrés ou désactivés.....	- 78 -
Figure 64:configuration de la politique d'accès à distance	- 79 -
Figure 65: l'assistant est prêt à commencer l'installation	- 79 -
Figure 66: l'assistant d'installation s'est terminé avec succès	- 80 -
Figure 67: lancement de l'assistant de démarrage de TMG, configuration des paramètres réseaux.-	- 80 -

Figure 68: assistant de configuration des paramètres réseaux.....	- 81 -
Figure 69: choix du modèle de réseau.....	- 81 -
Figure 70: paramètres LAN du réseau interne.....	- 82 -
Figure 71: paramètres LAN du réseau externe.....	- 83 -
Figure 72: fin de l'assistant de configuration des paramètres réseaux.....	- 84 -
Figure 73: avertissement : les changements des paramètres réseau peuvent déconnecter la session distante.....	- 84 -
Figure 74: assistant de démarrage de TMG, configuration des paramètres du système.....	- 85 -
Figure 75: assistant de configuration du système.....	- 85 -
Figure 76: entrer les détails d'identification de l'hôte.....	- 86 -
Figure 77: fin de l'assistant de configuration du système.....	- 86 -
Figure 78: assistant de démarrage de TMG, configuration des options de déploiement.....	- 87 -
Figure 79: assistant de déploiement.....	- 87 -
Figure 80: paramètre de mise à jour Microsoft.....	- 88 -
Figure 81: avertissement, car les mise-à-jour automatique ne sont pas activées.....	- 88 -
Figure 82: paramètres des fonctions de protection du TMG.....	- 89 -
Figure 83: participation à l'amélioration du produit.....	- 89 -
Figure 84: participation au rapport d'attaque et de virus.....	- 90 -
Figure 85: fin de l'assistant de déploiement.....	- 90 -
Figure 86: fin de l'assistant de démarrage de TMG.....	- 91 -
Figure 87: console d'administration du TMG, rubrique <i>Firewall Policy</i>	- 91 -
Figure 88: assistant de création d'une nouvelle règle de publication web.....	- 92 -
Figure 89: sélection de l'action de la règle de publication web.....	- 92 -
Figure 90: sélection du type de publication.....	- 93 -
Figure 91: sélection de la sécurisation de la connexion au serveur.....	- 93 -
Figure 92: sélection des détails de publication interne, nom et adresse IP.....	- 94 -
Figure 93: sélection des détails de publication interne, chemin et options.....	- 94 -
Figure 94: choix du nom public du site web.....	- 95 -
Figure 95: assistant de définition d'un nouveau <i>web listener</i>	- 95 -
Figure 96: sélection de la sécurisation de la connexion du client.....	- 96 -
Figure 97: sélection des IP d'écoute du <i>web listener</i>	- 96 -
Figure 98: sélections des paramètres d'authentification des clients.....	- 97 -
Figure 99: sélection du <i>single sign on</i>	- 97 -
Figure 100: fin de l'assistant de définition d'un nouveau <i>web listener</i>	- 98 -
Figure 101: Sélection du <i>web listener</i> pour la nouvelle règle de publication web.....	- 98 -
Figure 102: sélection de la délégation de l'authentification.....	- 99 -
Figure 103: sélection du groupe d'utilisateur.....	- 99 -

Figure 104: fin de l'assistant de création d'une nouvelle règle de publication web.....- 100 -

Figure 105: cliquer sur *Apply* pour valider les changements.....- 100 -

Figure 106: ajout d'une description du changement de configuration du TMG- 101 -

Figure 107: fenêtre de propriété de la règle de publication.....- 101 -

Figure 108: résultat du test de la règle.....- 102 -

15 Annexes

15.1 Configuration du prototype IPv6 only

15.1.1 Routeur accessa-ipv6

```
accessa-ipv6#sh run
Building configuration...

Current configuration : 1890 bytes
!
! No configuration change since last restart
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname accessa-ipv6
!
boot-start-marker
boot system flash c1900-universalk9-mz.SPA.152-2.T1.bin
boot-end-marker
!
!
enable secret 5 $1$N1gI$YkOW2t1.YbLYcFA9f7V1S.
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
!
!
!
!
ip cef
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO1921/K9 sn FCZ154391RC
!
!
!
!
!
!
interface Loopback0
 no ip address
 ipv6 address 2001:4DA0:C7F:FC00::50/128
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description connection to accessa-ncn
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.151
 encapsulation dot1Q 151
```

```

ipv6 address 2001:4DA0:C7F:FC31::10/64
ipv6 enable
ipv6 ospf 151 area 151
!
interface GigabitEthernet0/1
description connection to Firewall
no ip address
duplex auto
speed auto
ipv6 enable
!
interface GigabitEthernet0/1.251
encapsulation dot1Q 251
ipv6 address 2001:4DA0:C7F:FC32::1/64
ipv6 enable
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ipv6 route 2001:4DA0:C00::/40 2001:4DA0:C7F:FC32::2
ipv6 router ospf 151
router-id 1.1.31.2
redistribute static
!
!
!
!
ipv6 access-list ACL-Console
permit ipv6 2001:4DA0:C00::/40 any
!
control-plane
!
!
banner login ^CBachelor Work S.DUNAND, contact SIEN Jerome VERNEZ ^C
!
line con 0
password 7 05080F1C2243
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 13061E010803
ipv6 access-class ACL-Console in
login
transport input all
!
scheduler allocate 20000 1000
!
end

```

15.1.2 Firewall

```

fw-ipv6# sh run
: Saved
:
ASA Version 8.4(3)
!
hostname fw-ipv6
enable password QvrPT0vWp6lvjvUD encrypted

```

```
passwd QvrPTOvWp6lvjvUD encrypted
names
!
interface Ethernet0/0
  no nameif
  security-level 0
  no ip address
  ipv6 enable
!
interface Ethernet0/0.251
  vlan 251
  nameif Outside
  security-level 0
  no ip address
  ipv6 address 2001:4da0:c7f:fc32::2/64
  ipv6 enable
!
interface Ethernet0/1
  no nameif
  security-level 0
  no ip address
  ipv6 enable
!
interface Ethernet0/1.50
  vlan 50
  nameif Inside
  security-level 100
  no ip address
  ipv6 address 2001:4da0:c01:30::1/64
  ipv6 enable
!
interface Ethernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  management-only
!
banner login Coucou
banner login #SIEN, authorised people only#
boot system disk0:/asa843-k8.bin
boot system disk0:/asa821-k8.bin
ftp mode passive
clock timezone CEST 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
object network dmz-web-ipv6
  subnet 2001:4da0:c01:30::/64
object-group service DM_INLINE_TCP_2 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_3
  service-object tcp destination eq domain
  service-object udp destination eq domain
object-group service DM_INLINE_TCP_1 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_4
```

```
service-object tcp destination eq domain
service-object udp destination eq domain
object-group service DM_INLINE_SERVICE_1
service-object icmp6 echo
service-object icmp6 echo-reply
object-group service DM_INLINE_SERVICE_2
service-object icmp6 echo
service-object icmp6 echo-reply
pager lines 24
logging enable
logging asdm-buffer-size 512
logging asdm informational
mtu Outside 1500
mtu management 1500
mtu Inside 1500
ipv6 icmp permit any Outside
ipv6 route Outside ::/0 2001:4da0:c7f:fc32::1
ipv6 access-list Outside_access_ipv6_in permit tcp any host 2001:4da0:c01:30::100
object-group DM_INLINE_TCP_2 log critical
ipv6 access-list Outside_access_ipv6_in permit object-group DM_INLINE_SERVICE_3 any
object dmz-web-ipv6
ipv6 access-list Outside_access_ipv6_in permit object-group DM_INLINE_SERVICE_2 any
host 2001:4da0:c01:30::100
ipv6 access-list Outside_access_ipv6_in deny ip any any log emergencies
ipv6 access-list Inside_access_ipv6_in permit tcp host 2001:4da0:c01:30::100 any
object-group DM_INLINE_TCP_1 log critical
ipv6 access-list Inside_access_ipv6_in permit object-group DM_INLINE_SERVICE_4
object dmz-web-ipv6 any
ipv6 access-list Inside_access_ipv6_in permit object-group DM_INLINE_SERVICE_1 host
2001:4da0:c01:30::100 any
ipv6 access-list Inside_access_ipv6_in deny ip any any log emergencies
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-647.bin
no asdm history enable
arp timeout 14400
access-group Outside_access_ipv6_in in interface Outside
access-group Inside_access_ipv6_in in interface Inside
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 management
http 2001:4da0:c01:30::/64 Inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 2001:4da0:c01:30::/64 Inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics host
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
```

```
!  
class-map inspection_default  
  match default-inspection-traffic  
!  
!  
policy-map type inspect dns preset_dns_map  
  parameters  
    message-length maximum 512  
policy-map global_policy  
  class inspection_default  
    inspect dns preset_dns_map  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect rsh  
    inspect rtsp  
    inspect esmtp  
    inspect sqlnet  
    inspect skinny  
    inspect sunrpc  
    inspect xdmcp  
    inspect sip  
    inspect netbios  
    inspect tftp  
    inspect ip-options  
!  
service-policy global_policy global  
prompt hostname context  
no call-home reporting anonymous  
call-home  
  profile CiscoTAC-1  
    no active  
    destination address http  
https://tools.cisco.com/its/service/oddce/services/DDCEService  
  destination address email callhome@cisco.com  
  destination transport-method http  
  subscribe-to-alert-group diagnostic  
  subscribe-to-alert-group environment  
  subscribe-to-alert-group inventory periodic monthly  
  subscribe-to-alert-group configuration periodic monthly  
  subscribe-to-alert-group telemetry periodic daily  
Cryptochecksum:84a6deb293b2d5262f75c5bae46ca220  
: end
```

15.2 Configuration du prototype reverse proxy

15.2.1 Routeur accessa-ipv6

Idem au prototype *IPv6 only*.

15.2.2 Firewall

Idem au prototype *IPv6 only*.

15.2.3 Proxy TCP générique

Dans un terminal, taper la commande suivante :

```
netsh interface portproxy add v6tov4 connectaddress=210.210.210.11  
connectport=80 listenaddress=2001:4da0:c01:30::100 listenport=80
```

15.2.4 Installation de Microsoft Forefront Threat Management Gateway 2010 (TMG)

TMG est un composant ajouté à un serveur Microsoft 2008 R2.



Figure 50:écran d'accueil de l'installation de TMG, choisir *Run Preparation Tool*

Il faut tout d'abord exécuter la préparation à l'installation : *Run Preparation Tool*.

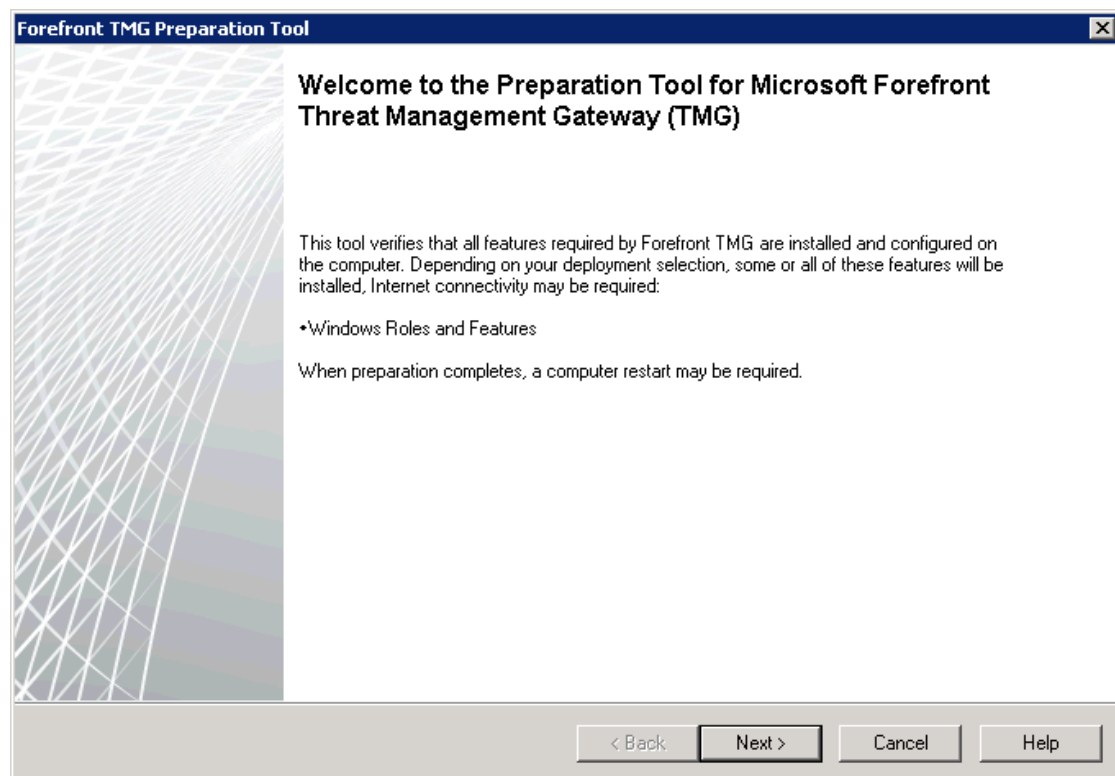


Figure 51: écran de démarrage de l'outil de préparation

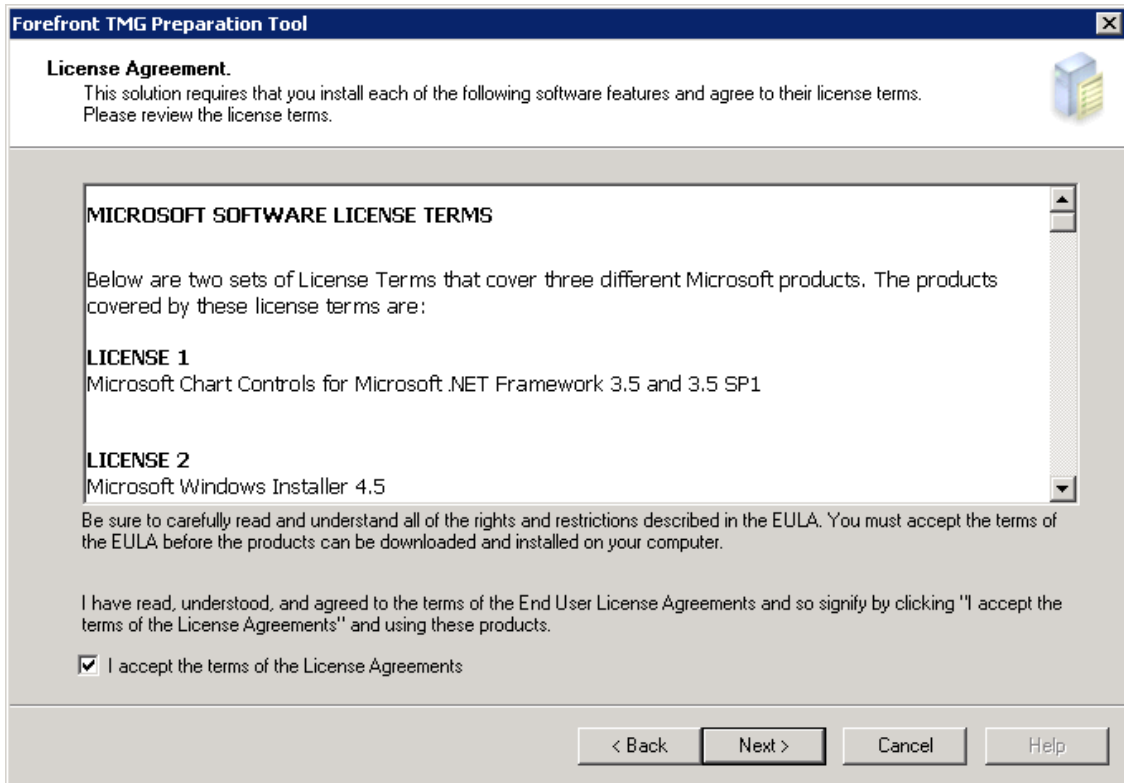


Figure 52: acceptation des termes du contrat de licence

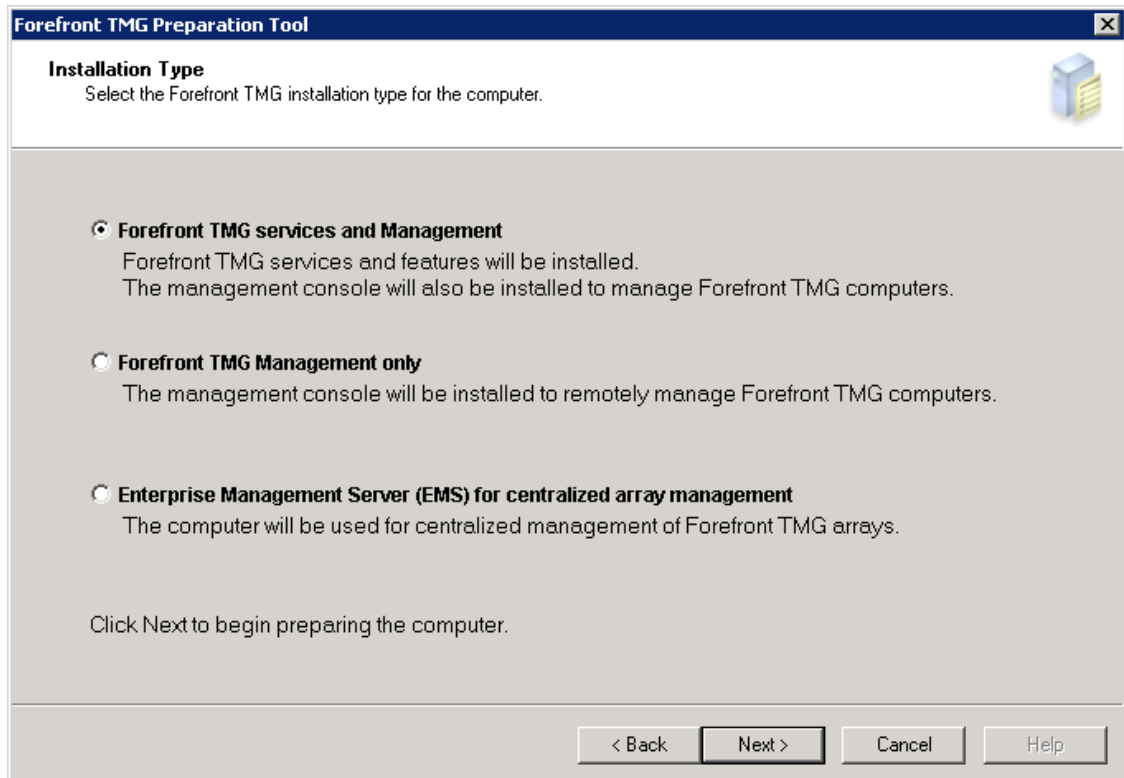


Figure 53: choix du type de l'installation

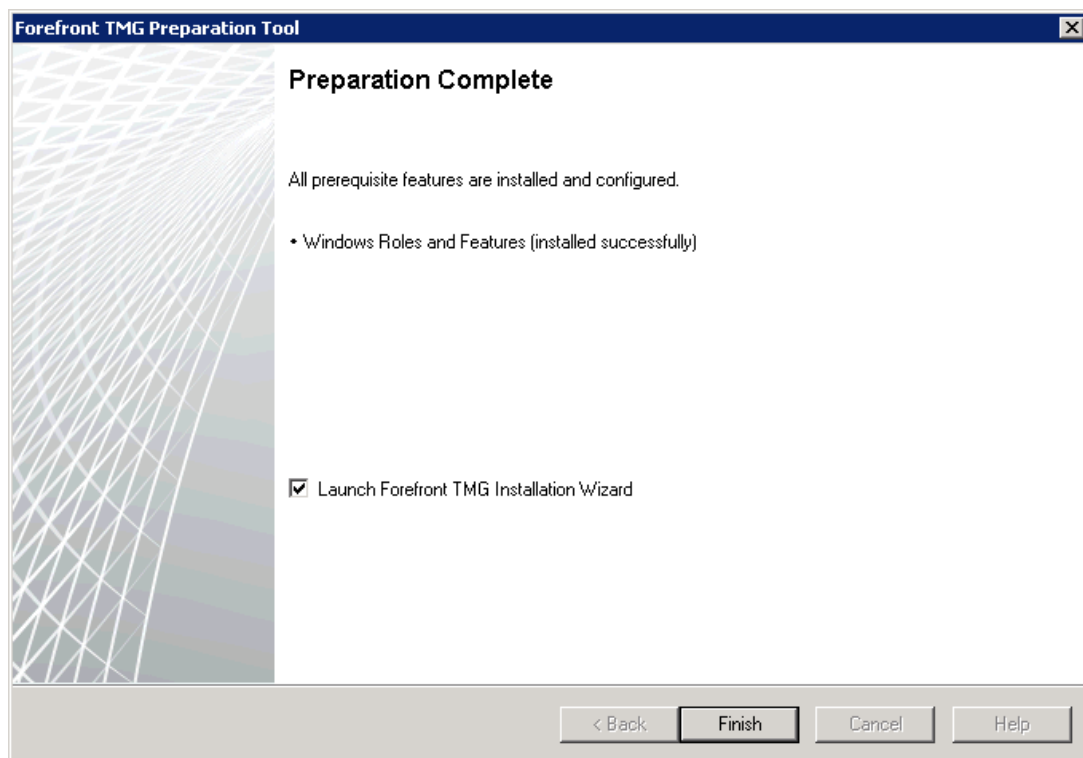


Figure 54: fin l'outil de préparation

Fin de l'outil de préparation, retour à l'écran d'accueil.

Il faut maintenant passer à l'installation : *Run Installation Wizard*.



Figure 55: écran d'accueil de l'installation de TMG, choisir *Run Installation Wizard*

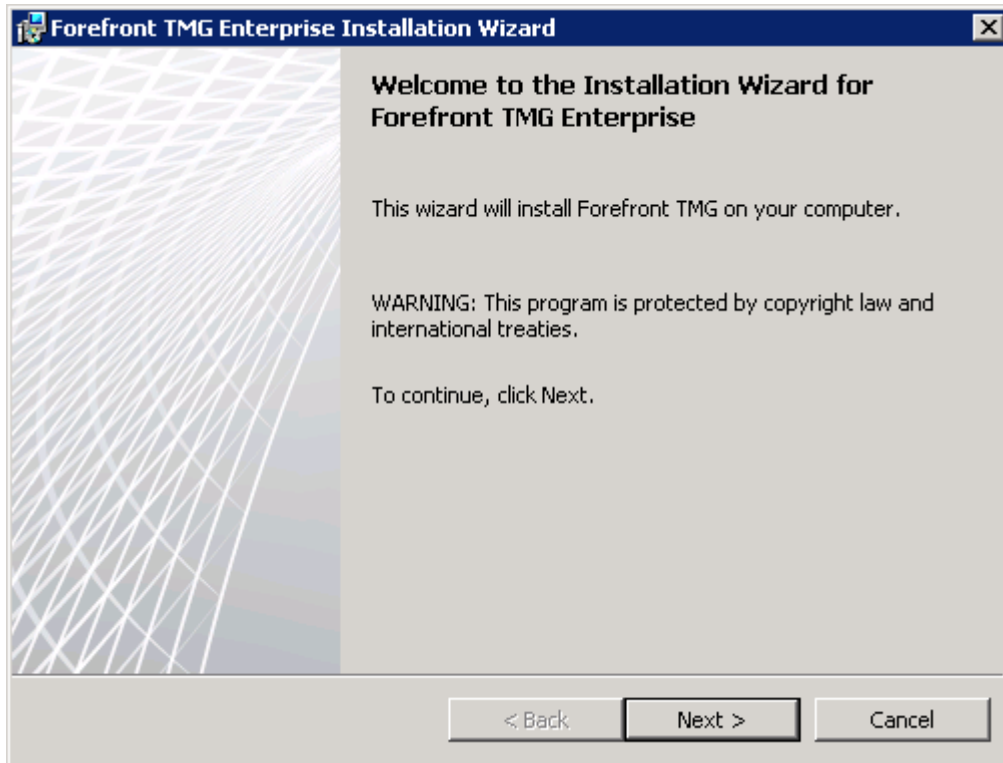


Figure 56: assistant d'installation de TMG

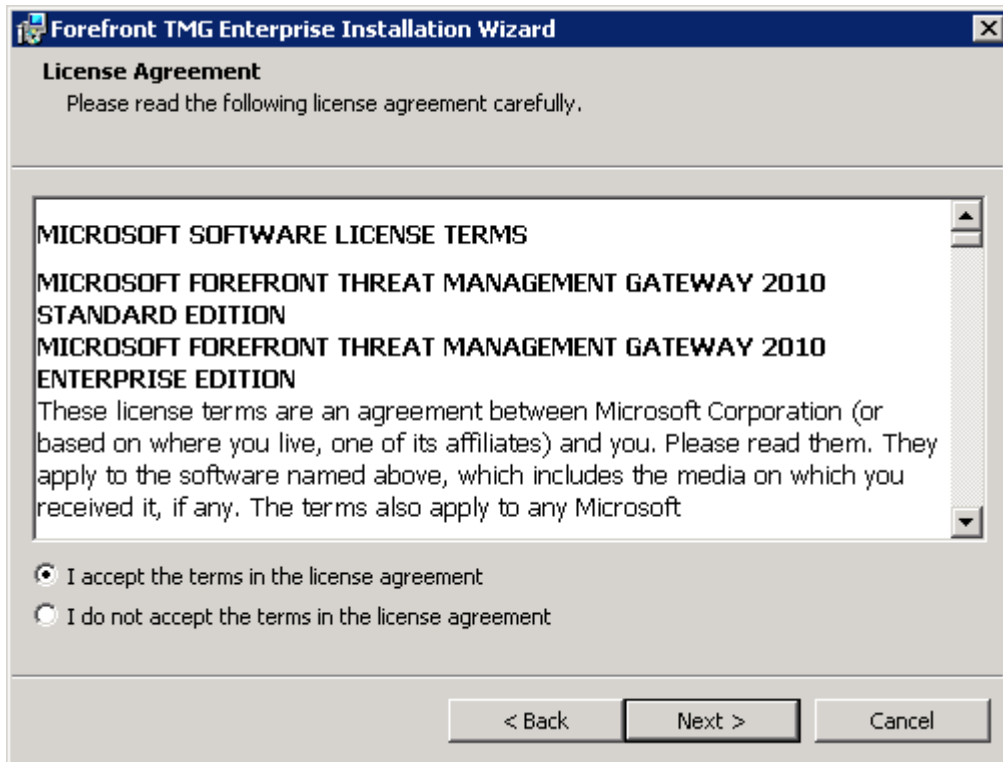


Figure 57: acceptation des termes du contrat de licence

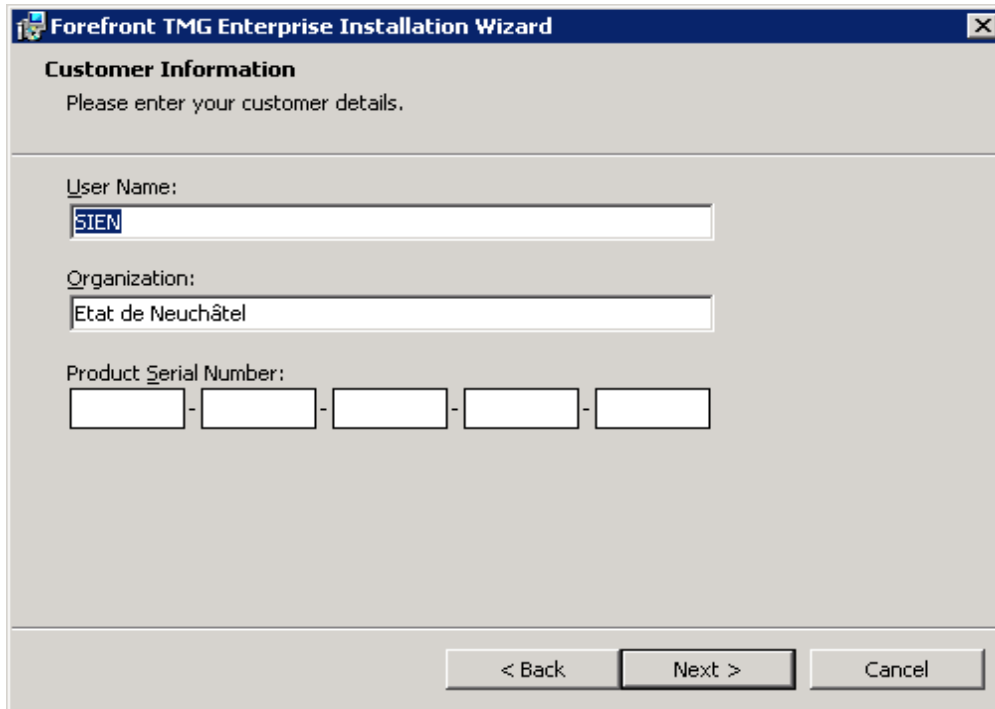


Figure 58: information concernant le client

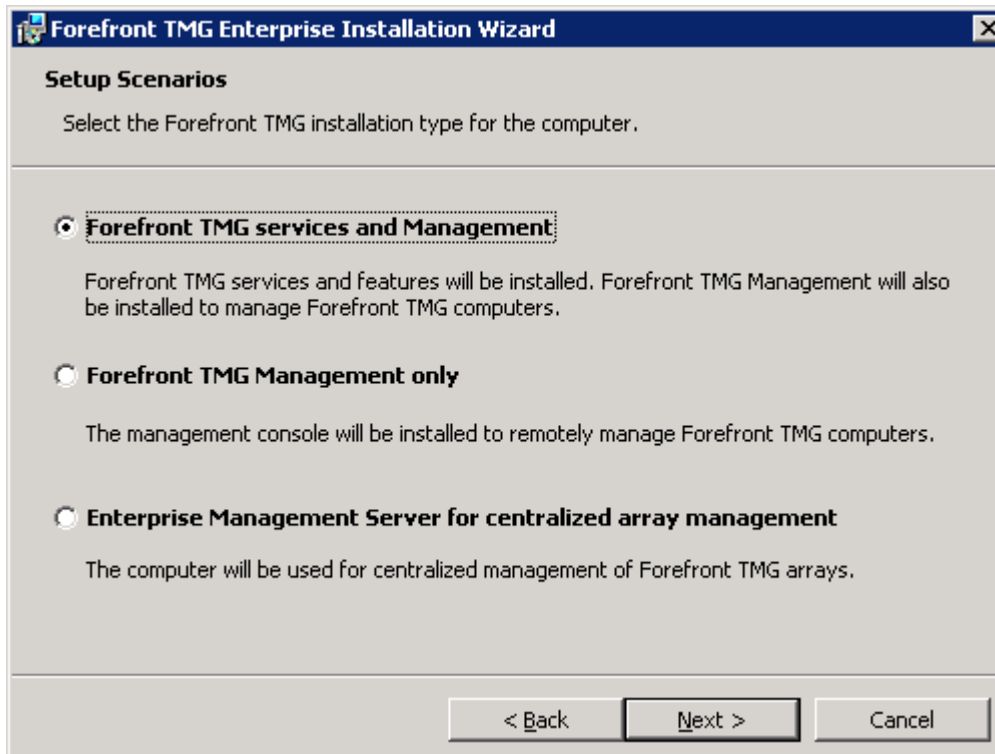


Figure 59: choix du scénario d'installation

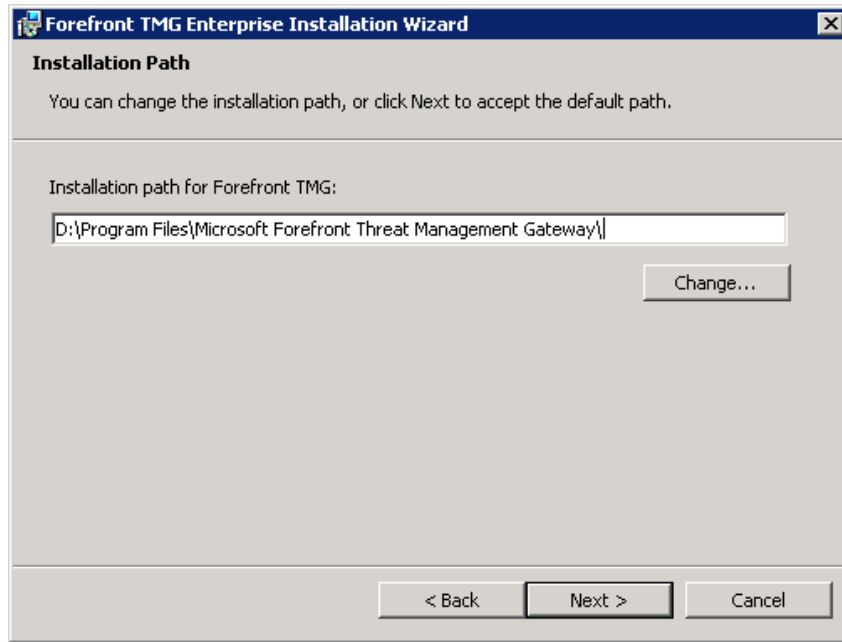


Figure 60: choix du chemin d'installation

L'espace d'adressage 210.210.210.0/24 utilisé à la Figure 61 a été imposé par l'administrateur système, bien qu'il s'agisse d'adresses publiques n'appartenant pas au SIEN.

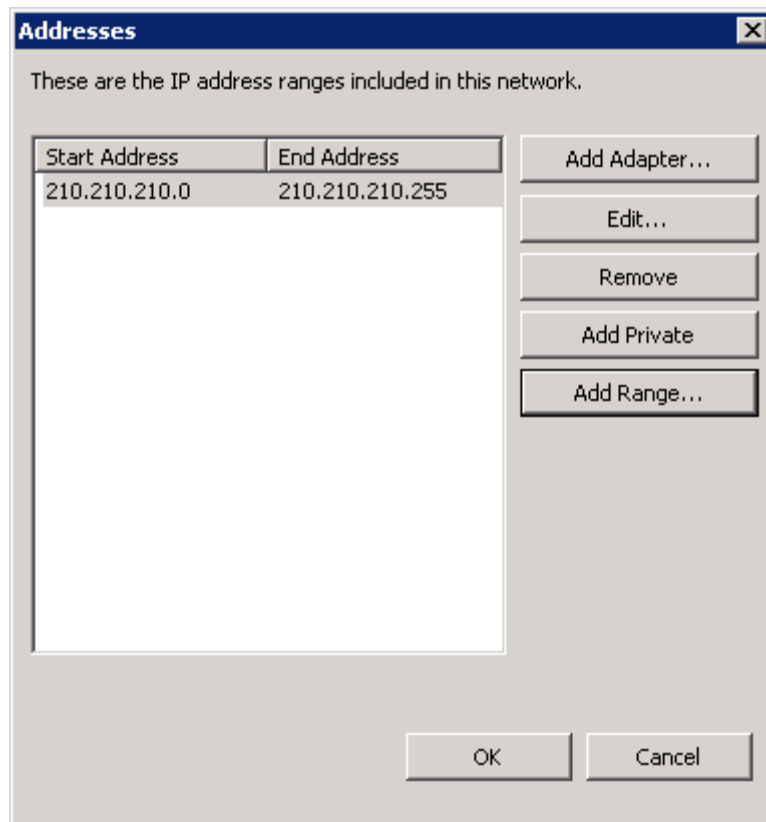


Figure 61: ajout de l'espace d'adressage utilisé

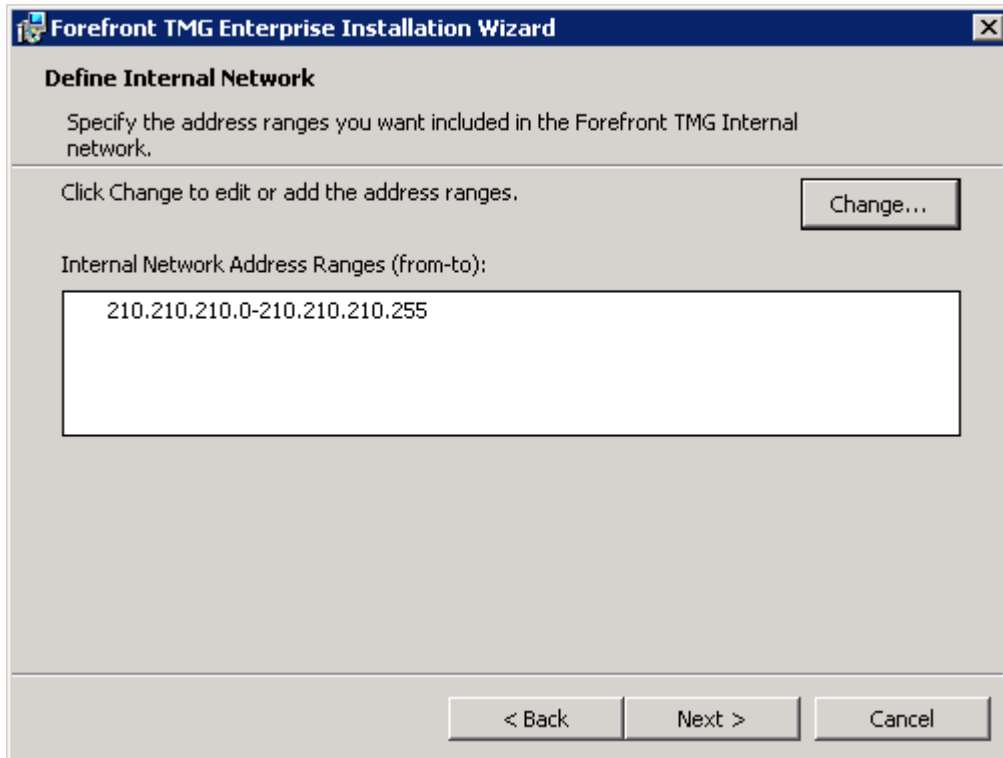


Figure 62: définition du réseau interne (i.e. derrière le TMG)

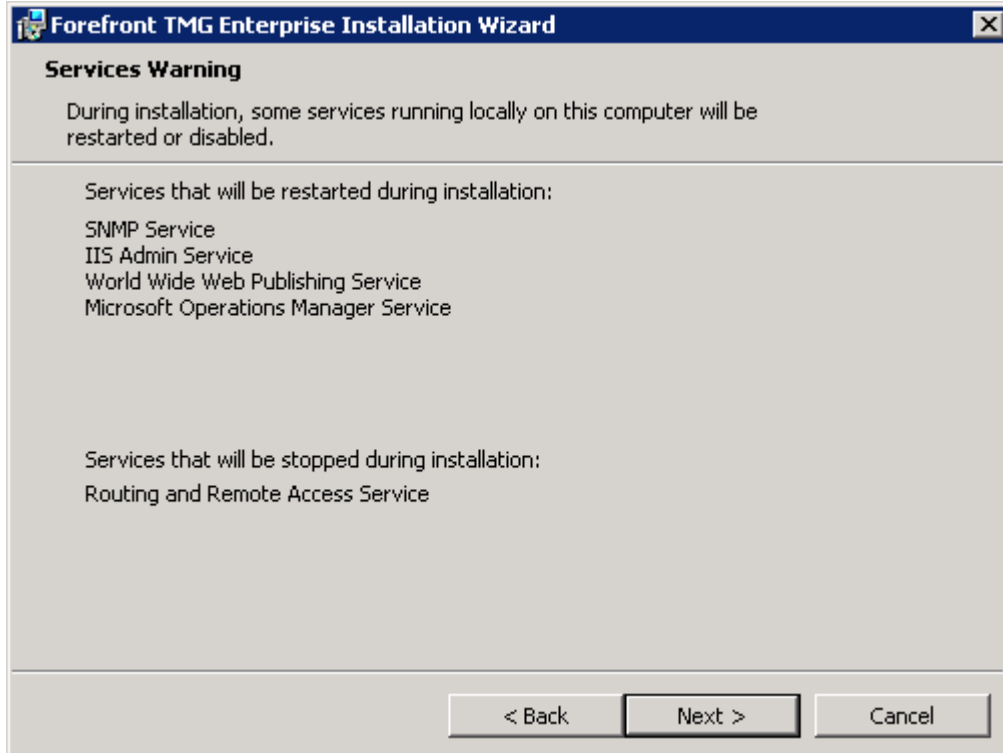


Figure 63: avertissement concernant les services qui seront redémarrés ou désactivés

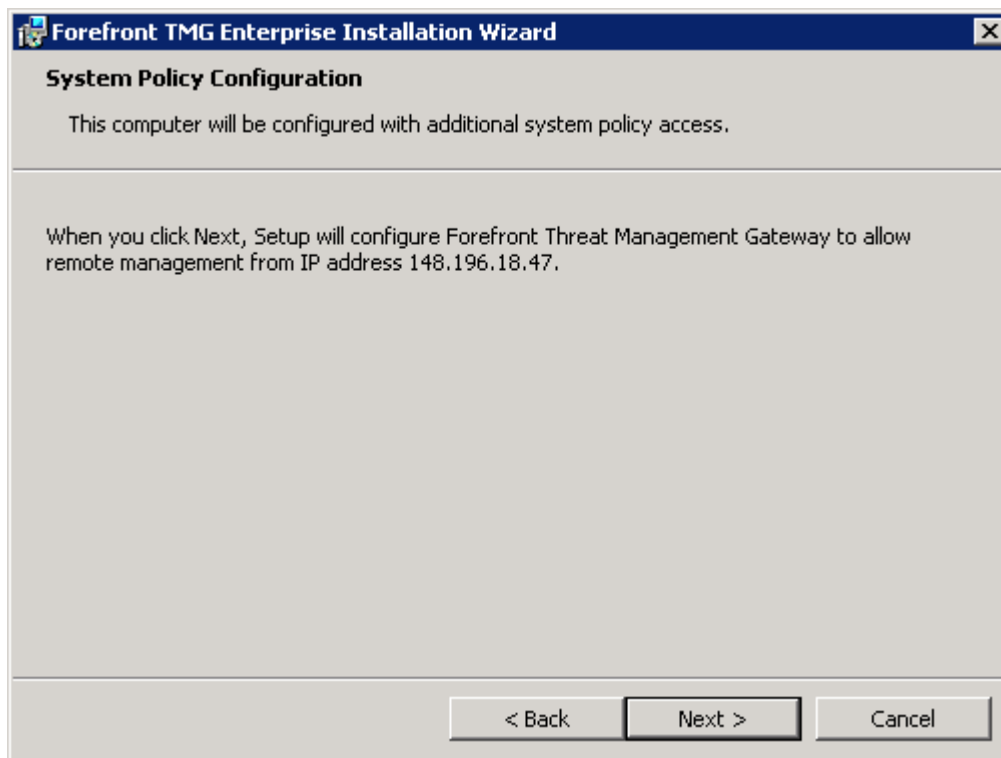


Figure 64: configuration de la politique d'accès à distance

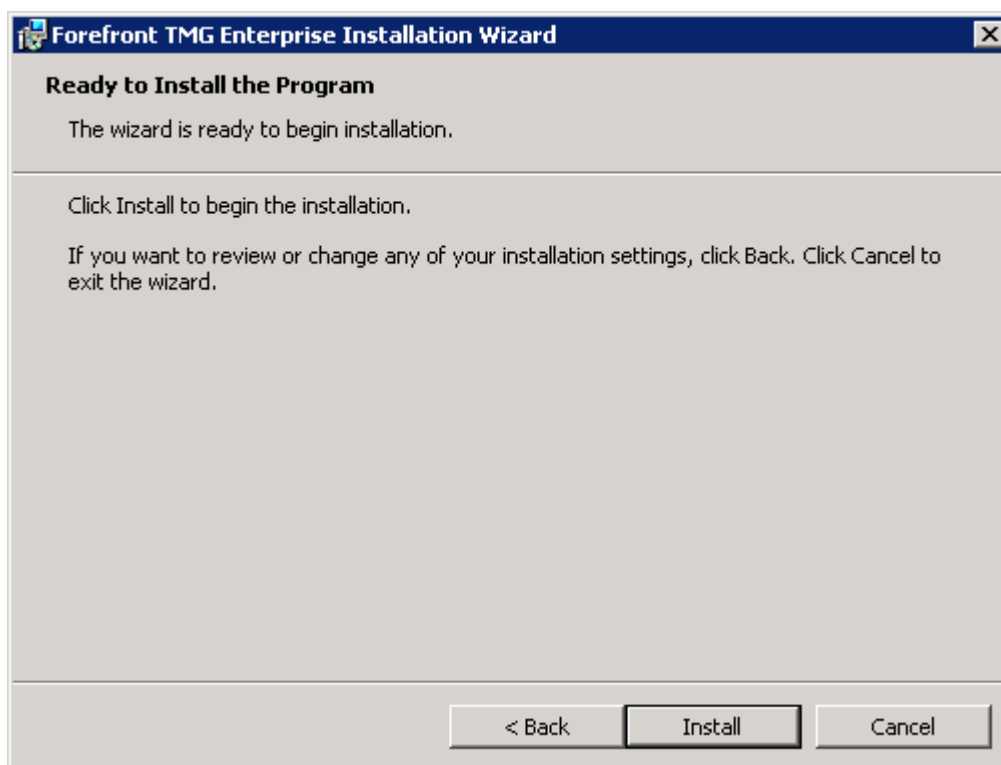


Figure 65: l'assistant est prêt à commencer l'installation

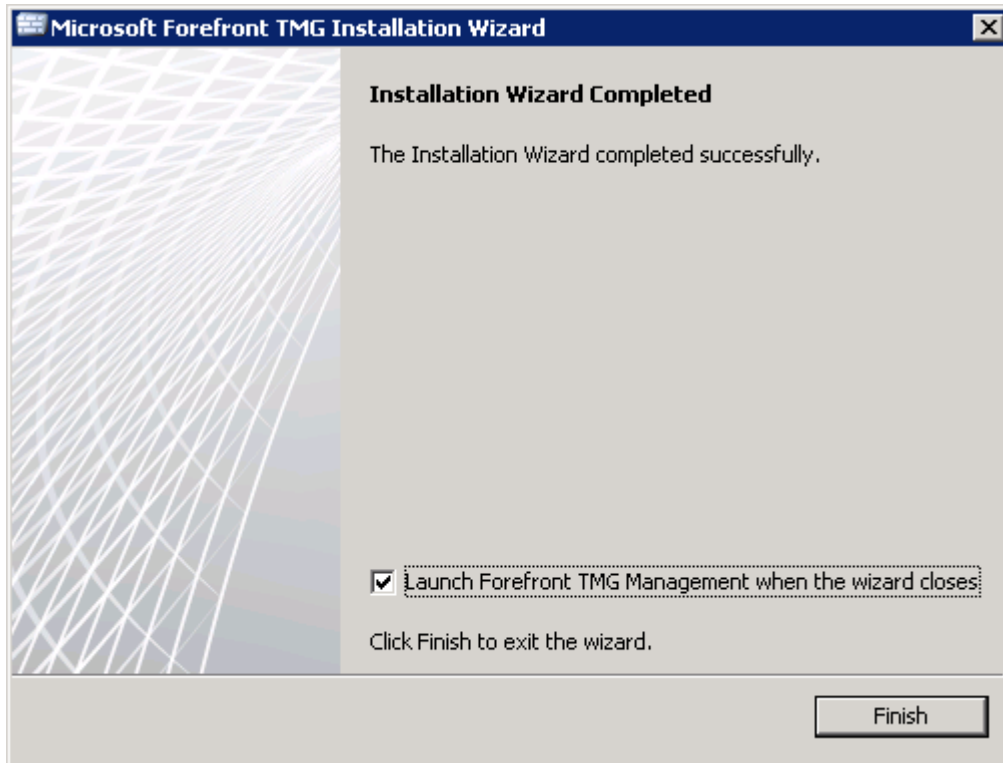


Figure 66: l'assistant d'installation s'est terminé avec succès

La Figure 66 montre la fin de l'assistant d'installation. On continue avec l'assistant de démarrage, comme on peut le voir à la Figure 67.

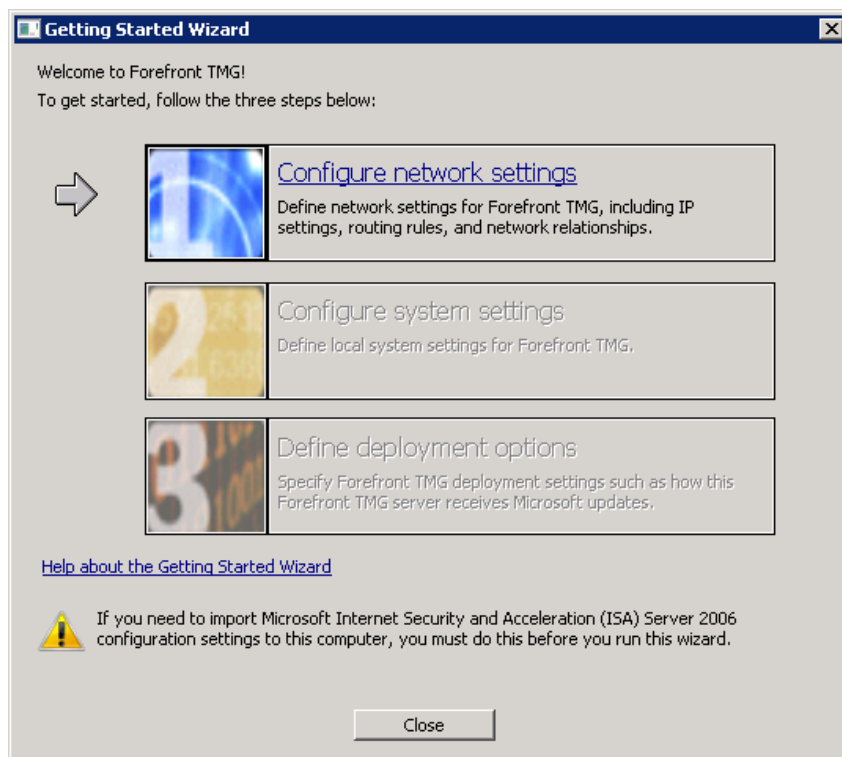


Figure 67: lancement de l'assistant de démarrage de TMG, configuration des paramètres réseaux

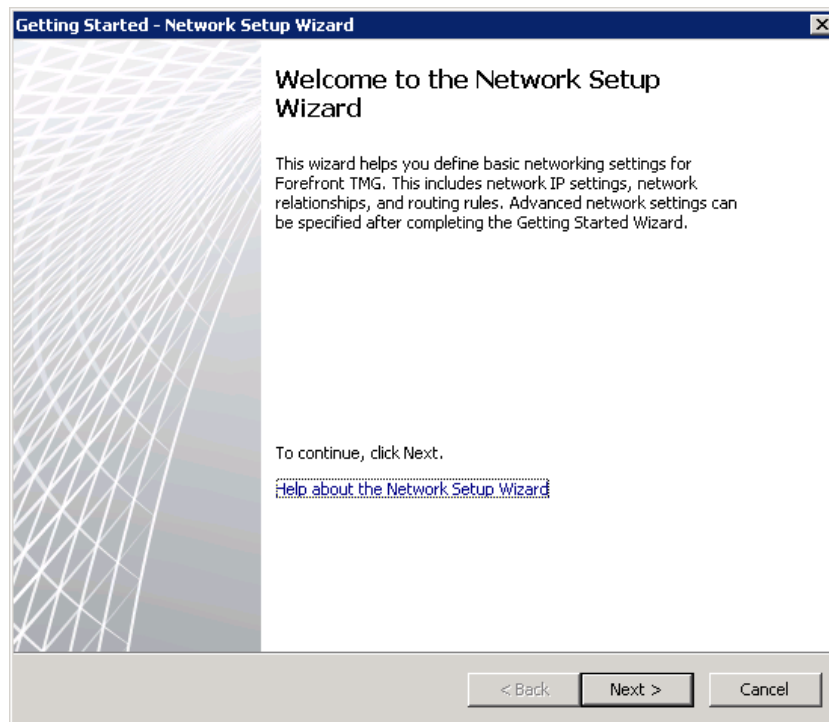


Figure 68: assistant de configuration des paramètres réseaux

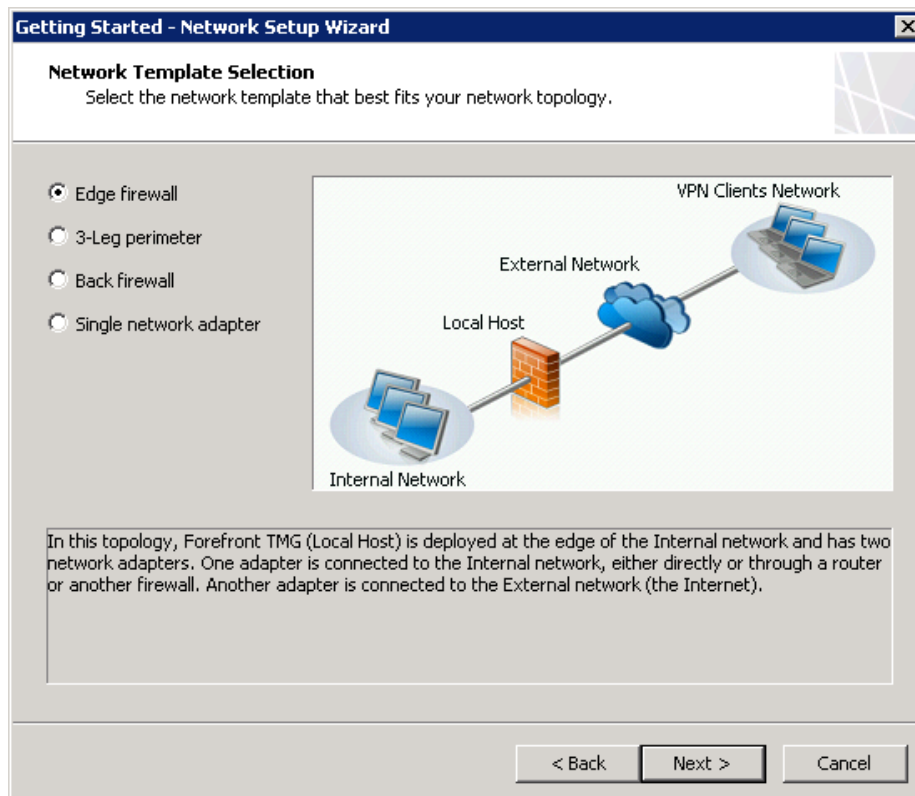


Figure 69: choix du modèle de réseau

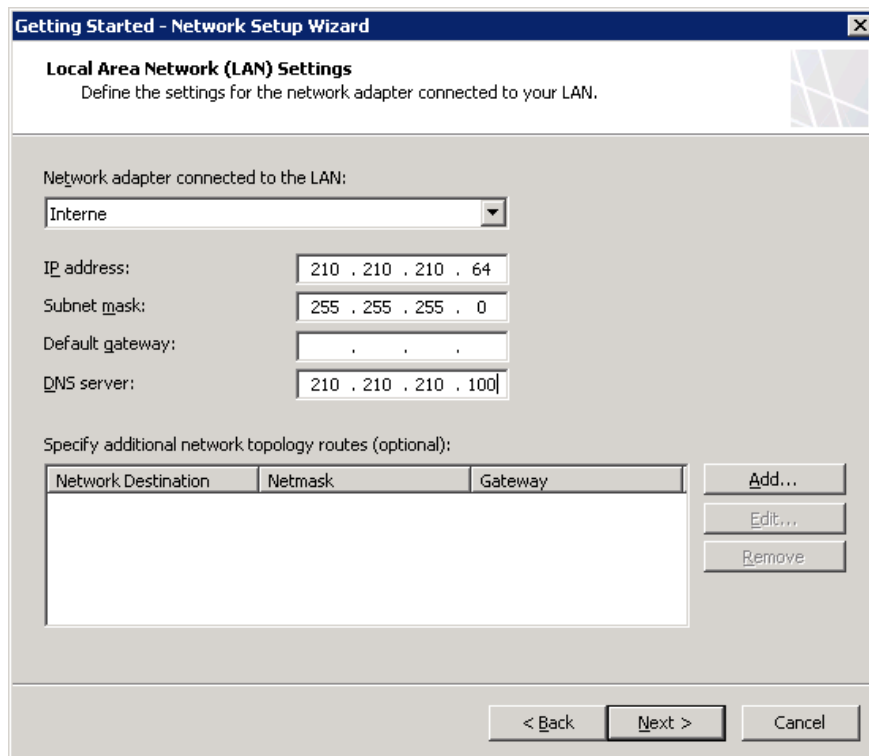


Figure 70: paramètres LAN du réseau interne

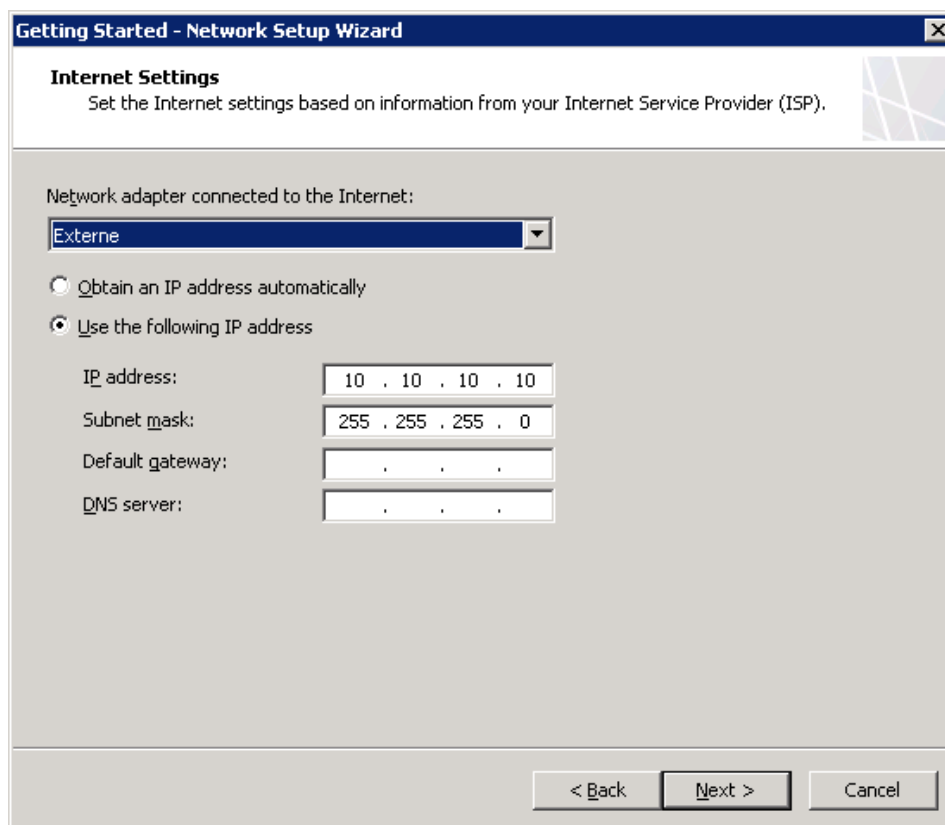


Figure 71: paramètres LAN du réseau externe

Il faut noter que l'adresse de l'interface du réseau externe visible à la Figure 71 ne correspond pas à celle mentionnée dans le plan d'adressage de la Figure 39. En effet, elle a changé quelques fois, après l'installation. De plus, il est nécessaire de mettre une passerelle par défaut, sinon certains paquets qui devraient être acceptés par le TMG seront refusés, car le TMG ne pourra contacter l'hôte, et son adresse sera alors considérée comme de l'IP spoofing²⁹.

²⁹ <http://blogs.technet.com/b/isablog/archive/2010/08/18/understanding-a-scenario-where-tmg-drops-the-packet-as-spoofed-even-when-the-source-ip-doesn-t-belong-to-the-internal-network.aspx>

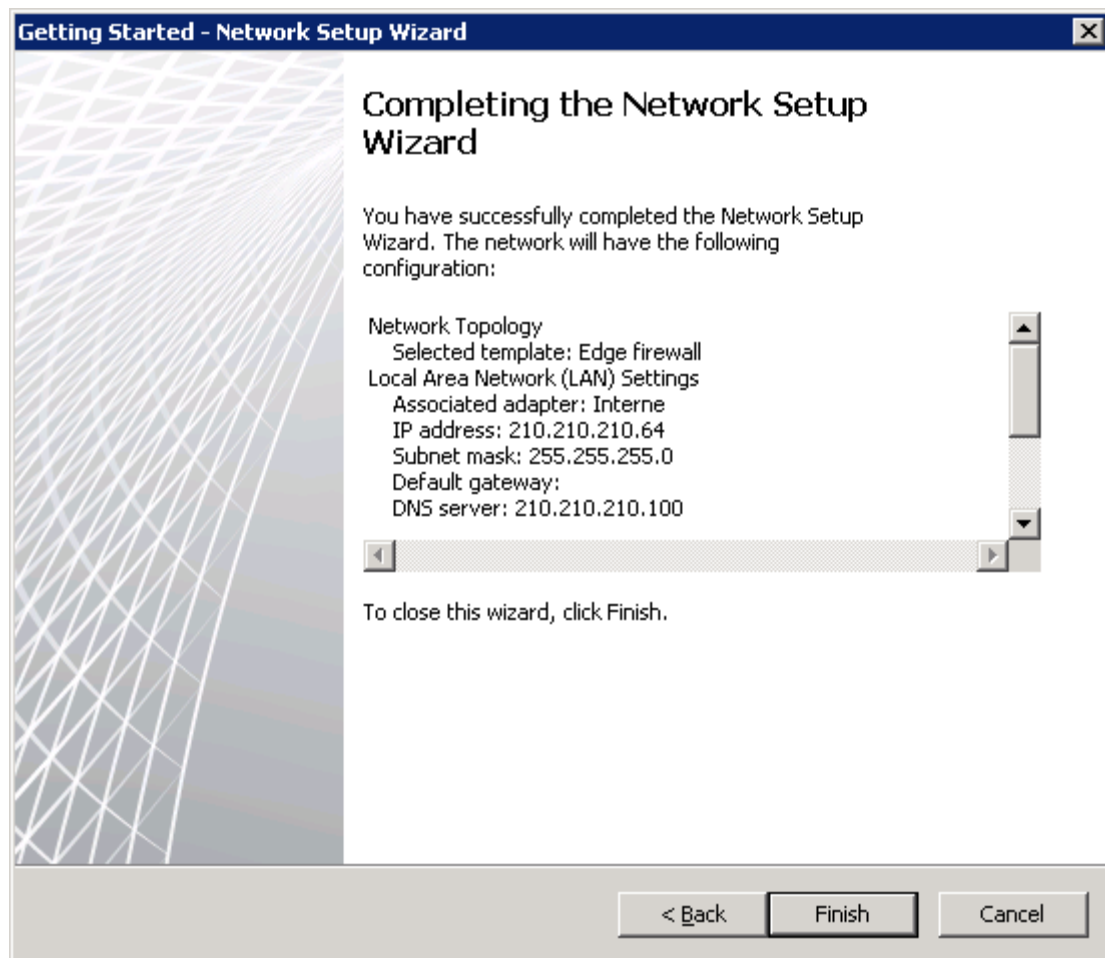


Figure 72: fin de l'assistant de configuration des paramètres réseaux

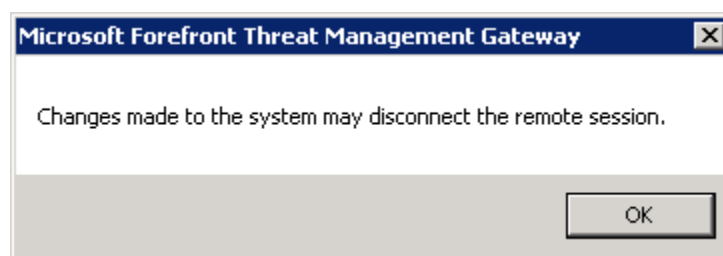


Figure 73: avertissement : les changements des paramètres réseau peuvent déconnecter la session distante

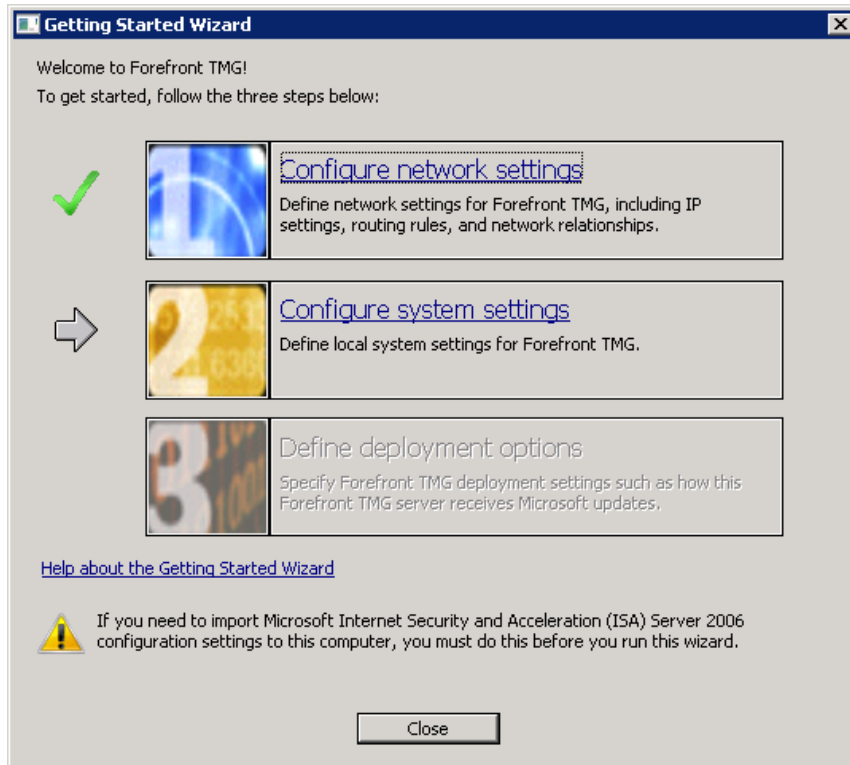


Figure 74: assistant de démarrage de TMG, configuration des paramètres du système

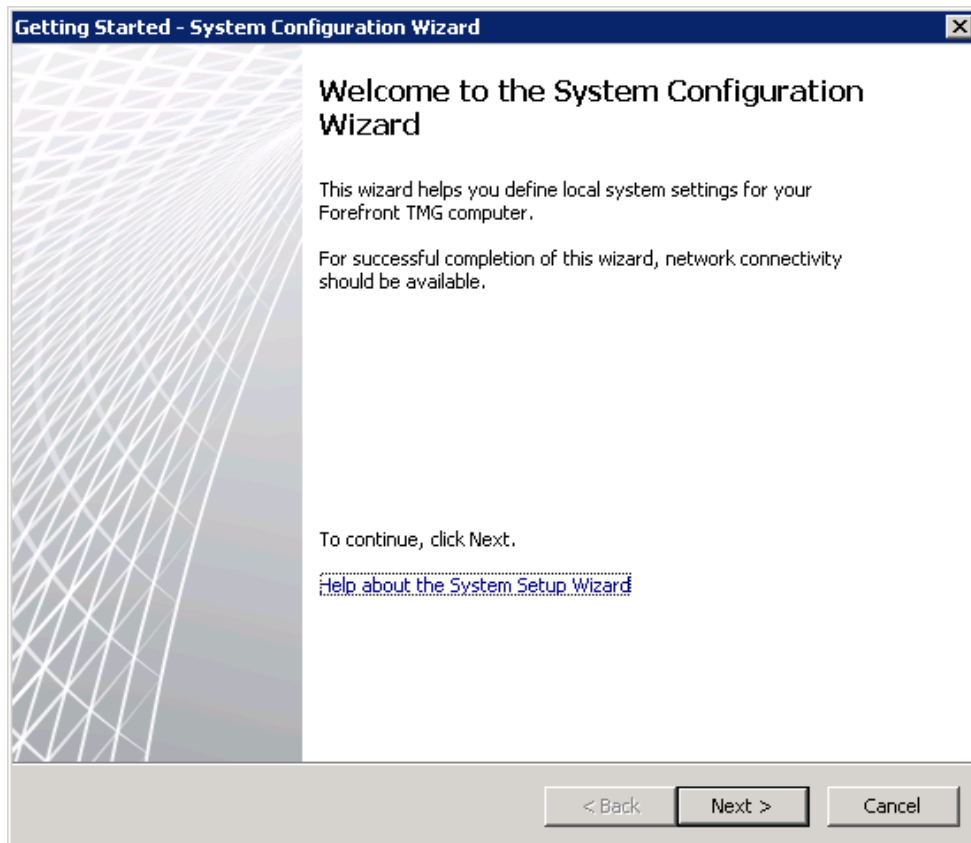


Figure 75: assistant de configuration du système

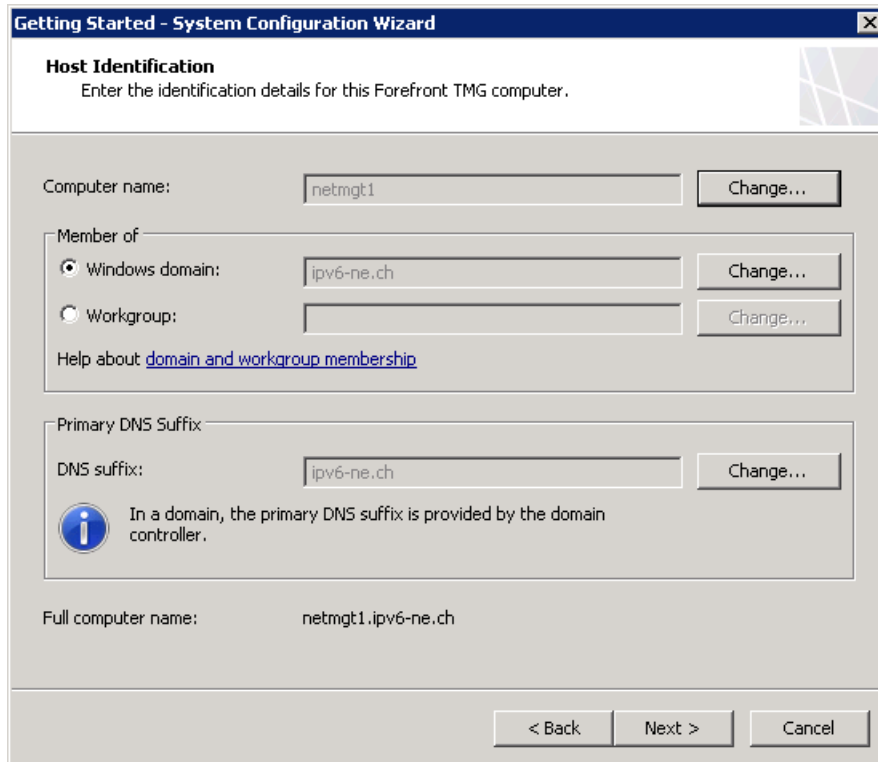


Figure 76: entrer les détails d'identification de l'hôte

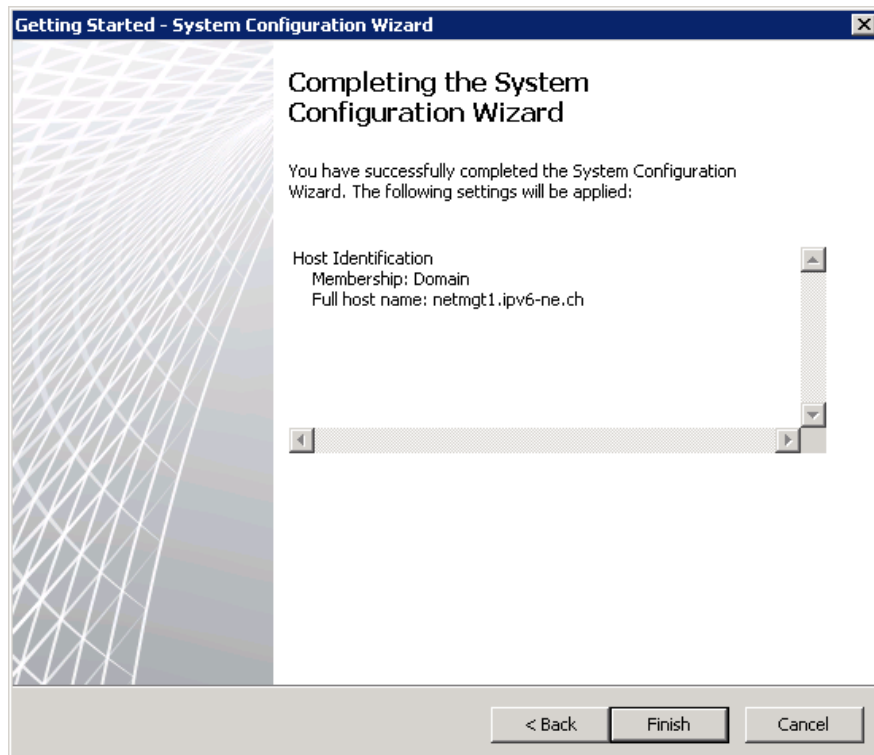


Figure 77: fin de l'assistant de configuration du système



Figure 78: assistant de démarrage de TMG, configuration des options de déploiement

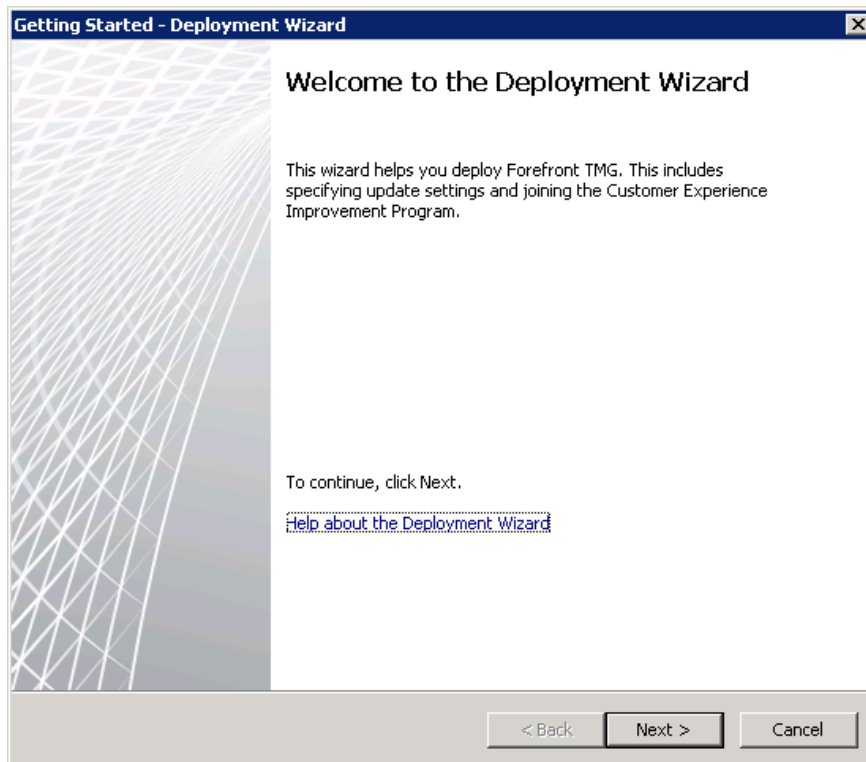


Figure 79: assistant de déploiement

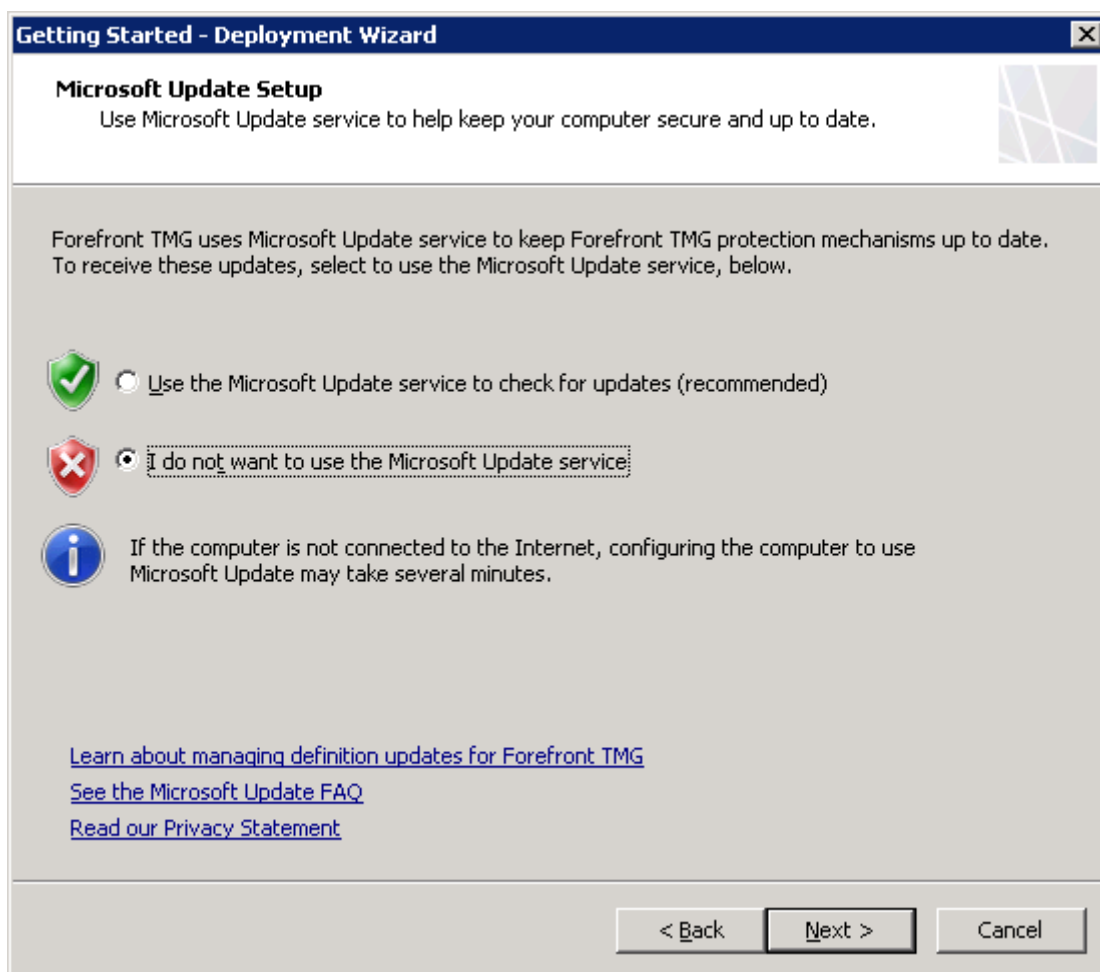


Figure 80: paramètre de mise à jour Microsoft

Il n'est pas nécessaire d'utiliser le service de mise à jour Microsoft Update, car le SIEN dispose de son propre serveur Windows Server Update Services.

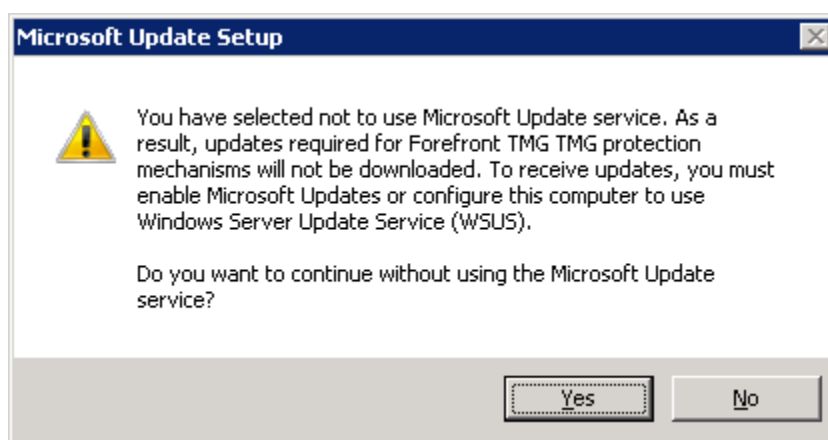


Figure 81: avertissement, car les mise-à-jour automatique ne sont pas activées

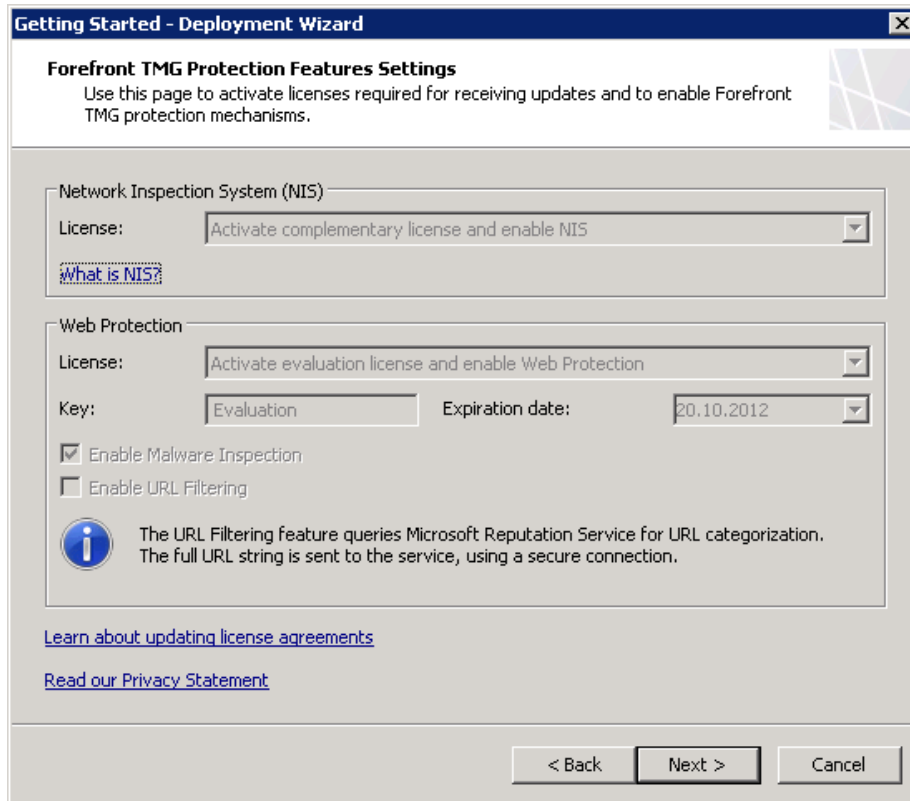


Figure 82: paramètres des fonctions de protection du TMG

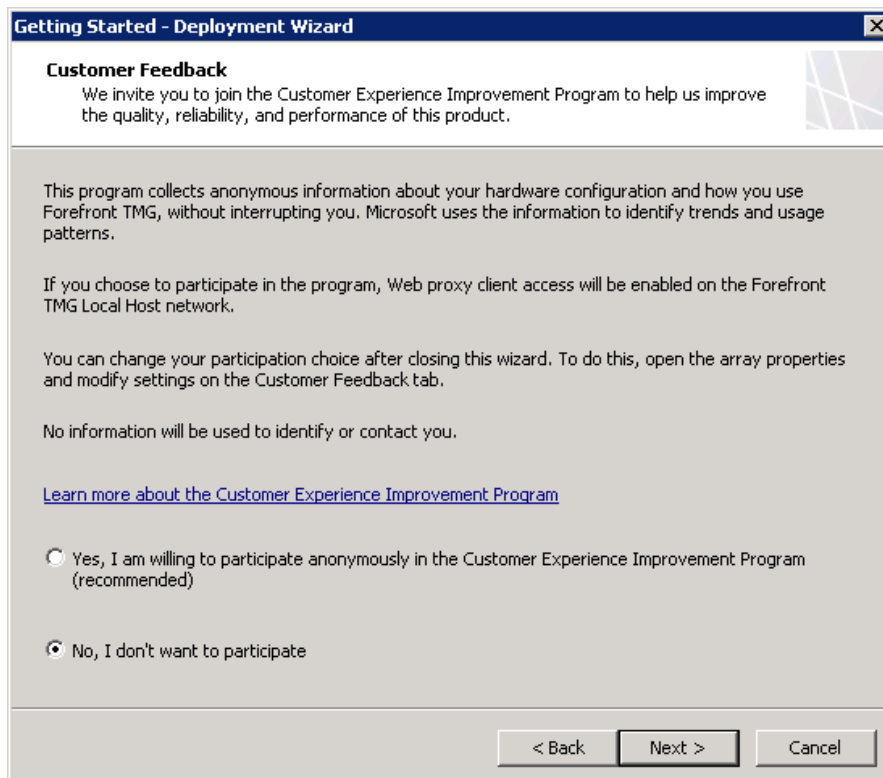


Figure 83: participation à l'amélioration du produit

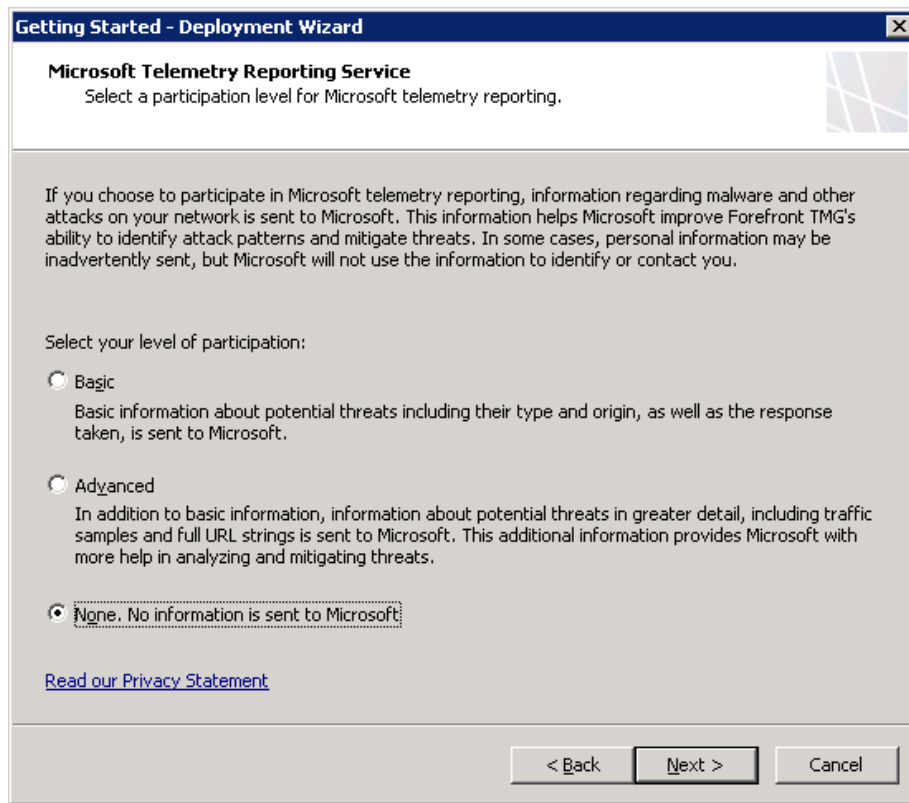


Figure 84: participation au rapport d'attaque et de virus

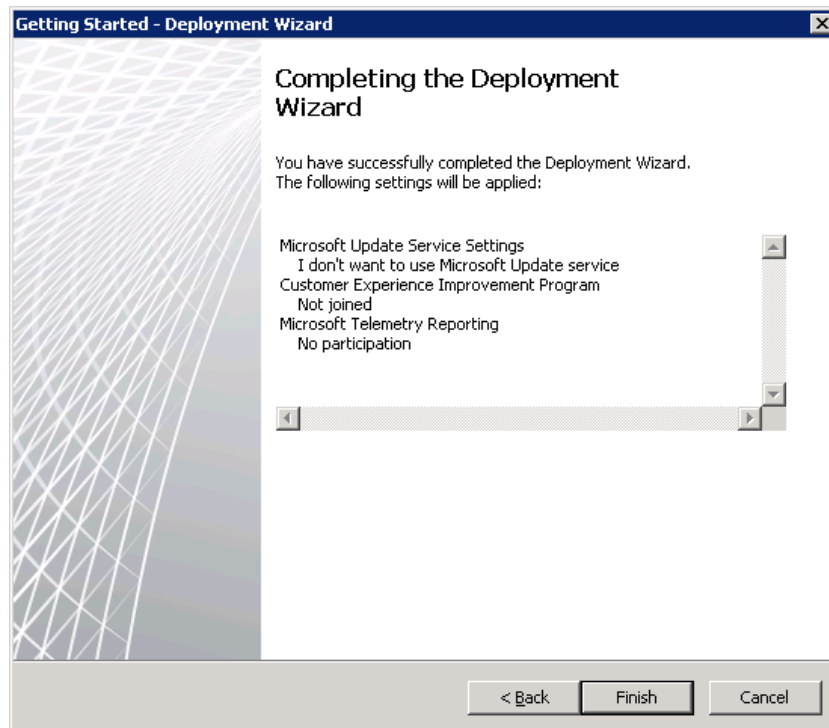


Figure 85: fin de l'assistant de déploiement



Figure 86: fin de l'assistant de démarrage de TMG

Cette étape termine donc l'assistant de démarrage, comme on peut le voir à la Figure 86.

15.2.5 Configuration TMG

Ce chapitre est consacré à la configuration du TMG.

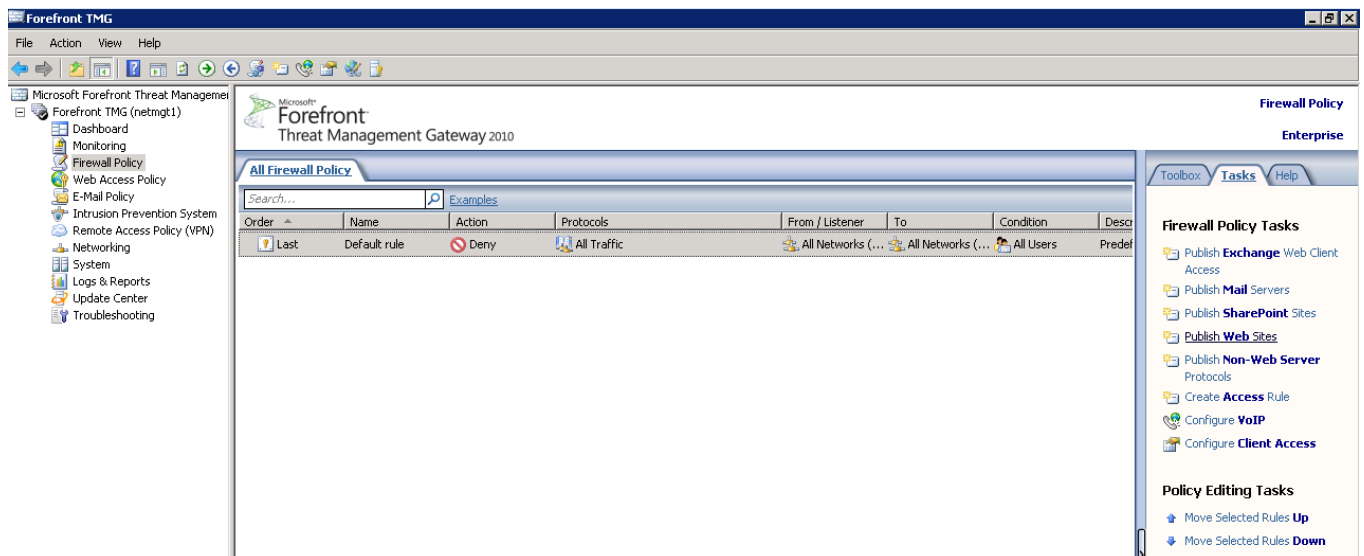


Figure 87: console d'administration du TMG, rubrique *Firewall Policy*

Afin de créer une nouvelle de publication règle de publication il faut sélection « Firewall Policy » dans le volet de gauche de l'interface du TMG, comme on peut le voir à la Figure 87. Ensuite, il faut sélectionner l'onglet « Tasks » dans le volet de droite, puis cliquer sur « Publish Web Sites ».

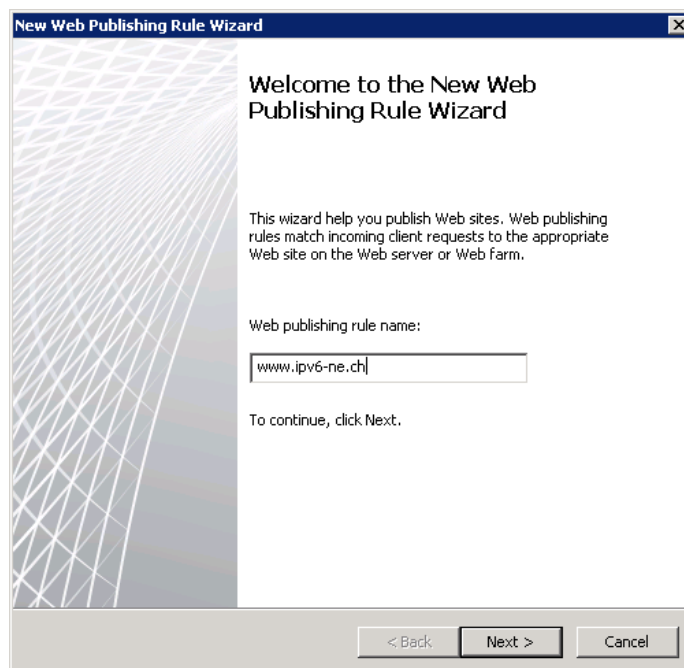


Figure 88: assistant de création d'une nouvelle règle de publication web

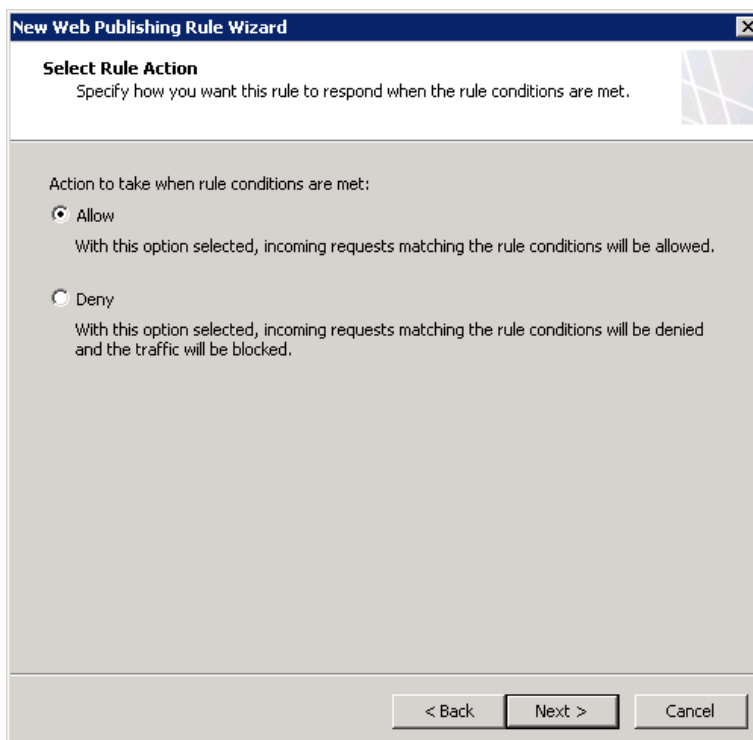


Figure 89: sélection de l'action de la règle de publication web

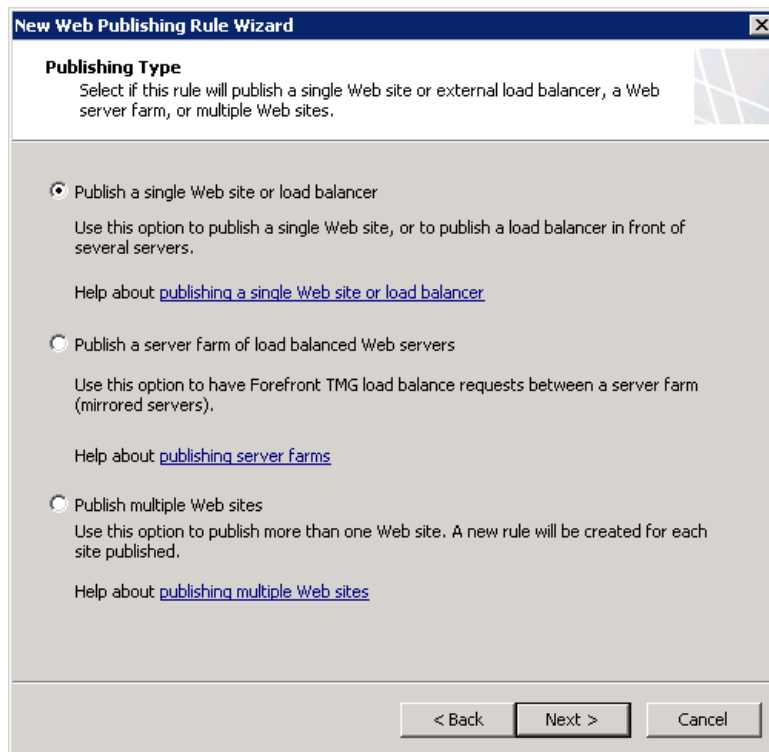


Figure 90: sélection du type de publication

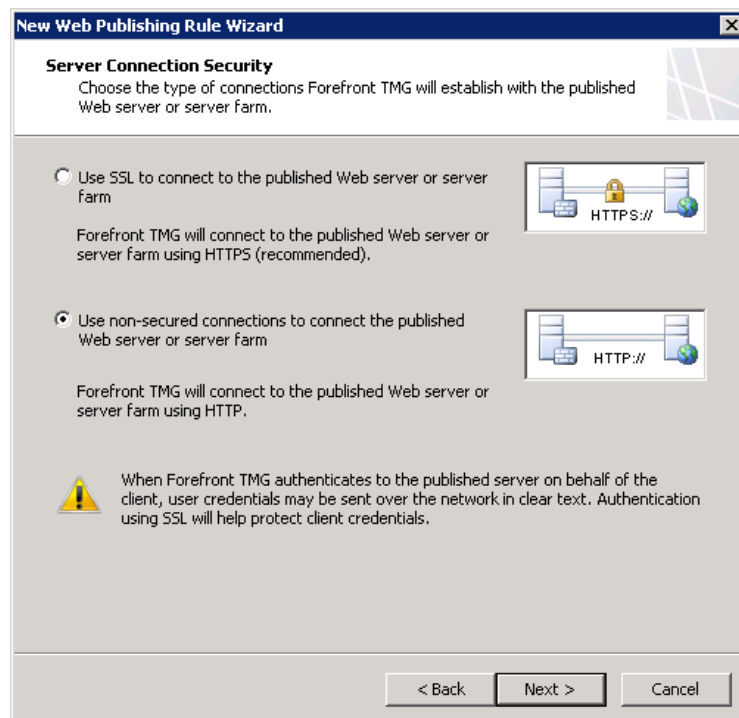


Figure 91: sélection de la sécurisation de la connexion au serveur

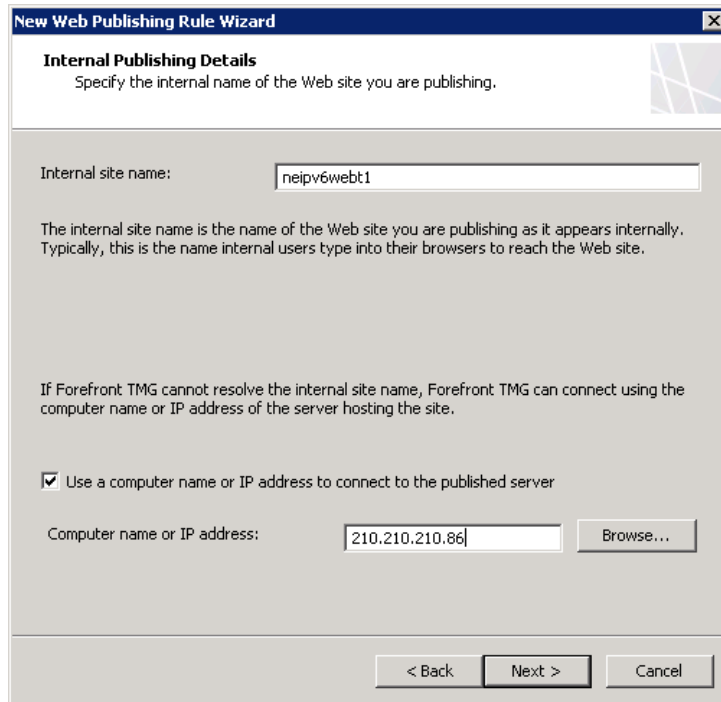


Figure 92: sélection des détails de publication interne, nom et adresse IP

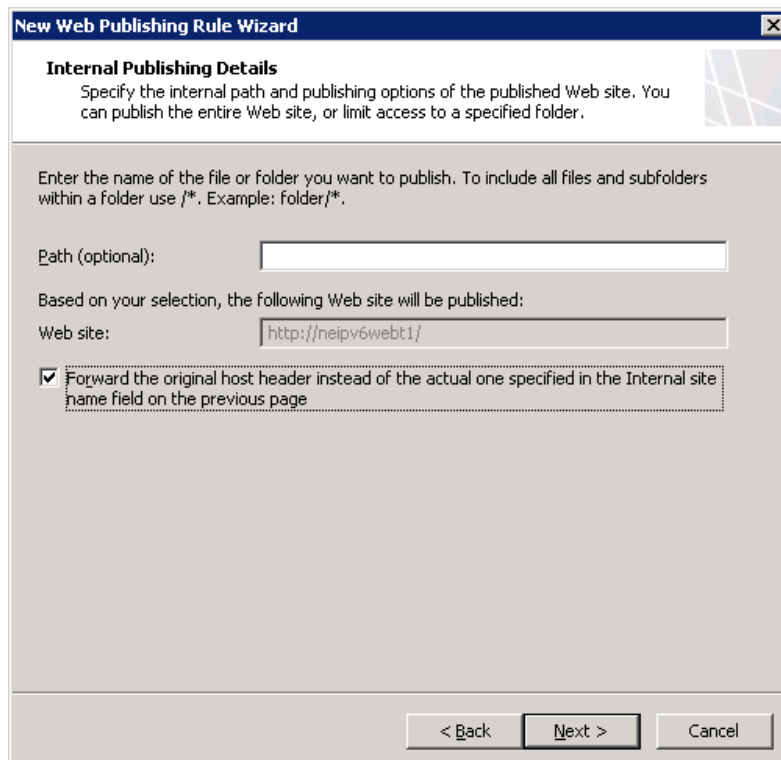


Figure 93: sélection des détails de publication interne, chemin et options

New Web Publishing Rule Wizard

Public Name Details
Specify the public domain name (FQDN) or IP address users will type to reach the published site.

Accept requests for: ▼
Only requests for this public name or IP address will be forwarded to the published site.

Public name:
Example: www.contoso.com

Path (optional):

Based on your selections, requests sent to this site (host header value) will be accepted:

Site:

< Back Next > Cancel

Figure 94: choix du nom public du site web

New Web Listener Definition Wizard

Welcome to the New Web Listener Wizard

This wizard helps you create a new Web listener. Web listeners specify how Forefront TMG listens for and authenticates incoming Web requests from clients.

Web listener name:

To continue, click Next.

< Back Next > Cancel

Figure 95: assistant de définition d'un nouveau *web listener*

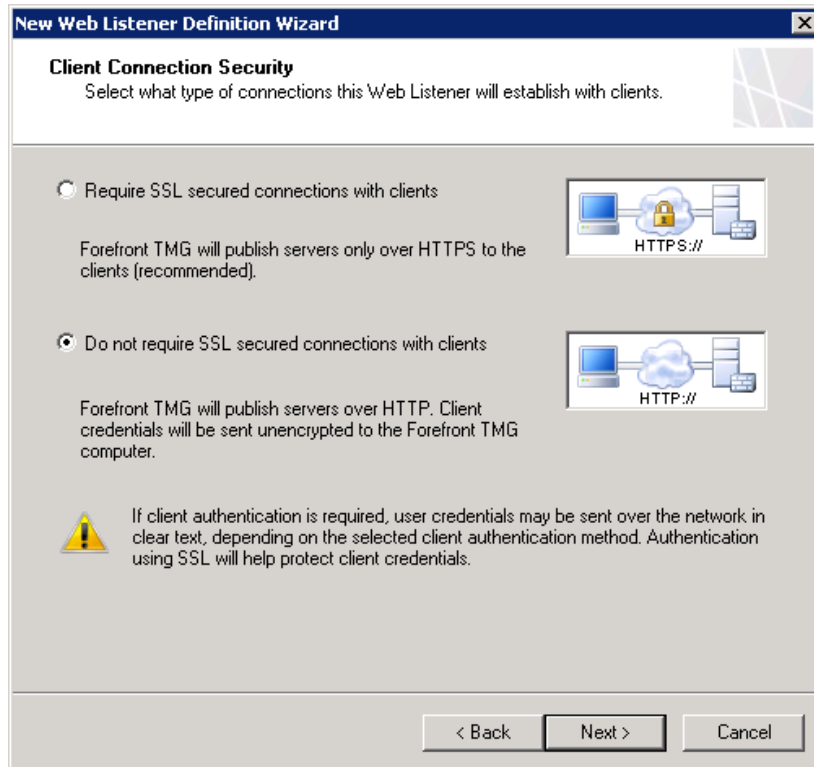


Figure 96: sélection de la sécurisation de la connexion du client

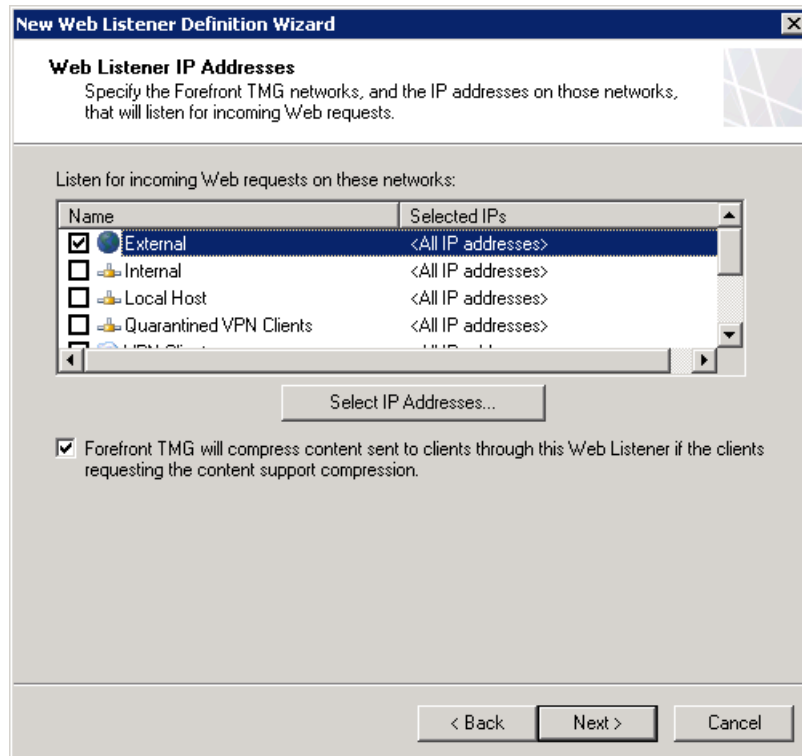


Figure 97: sélection des IP d'écoute du web listener

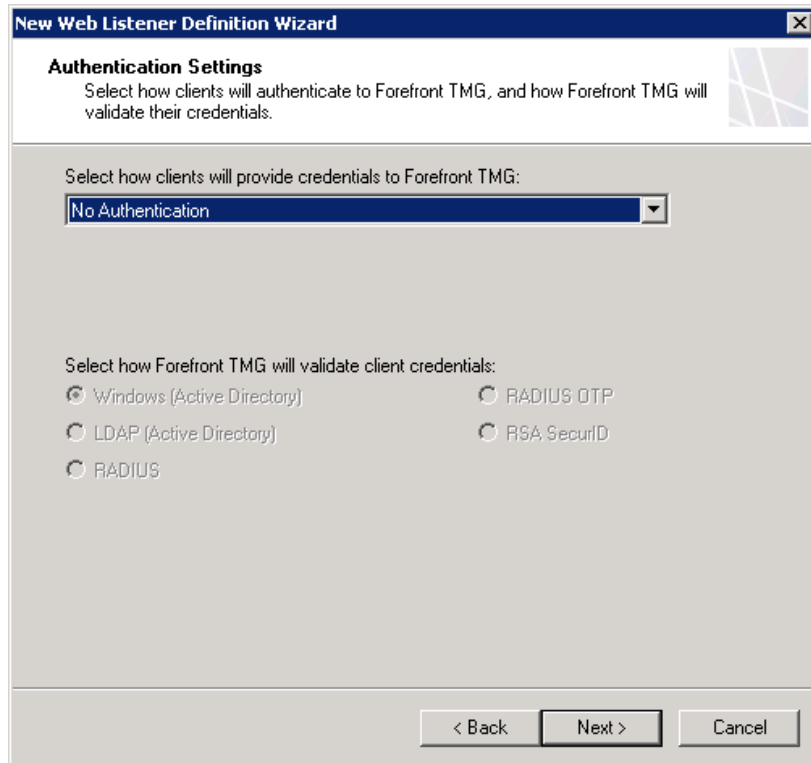


Figure 98: sélections des paramètres d'authentification des clients

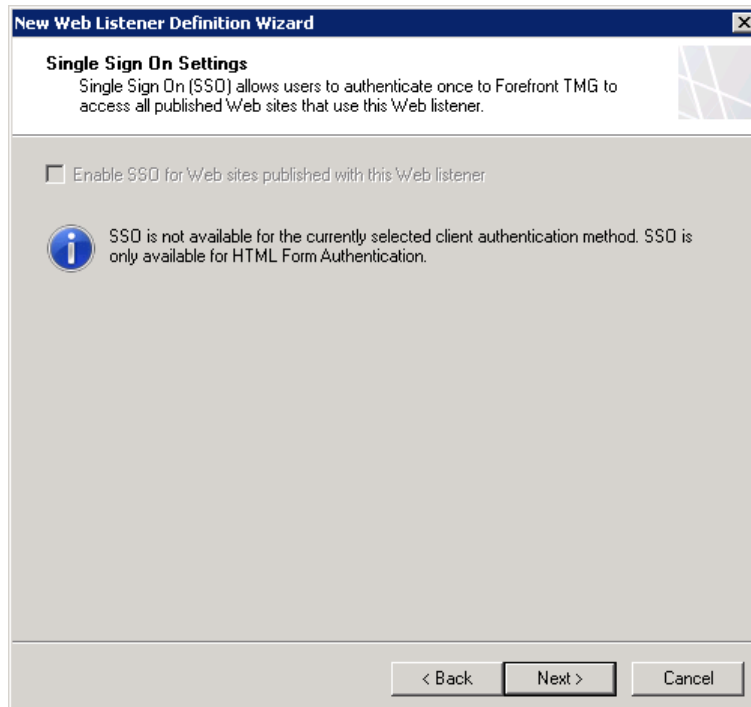


Figure 99: sélection du *single sign on*

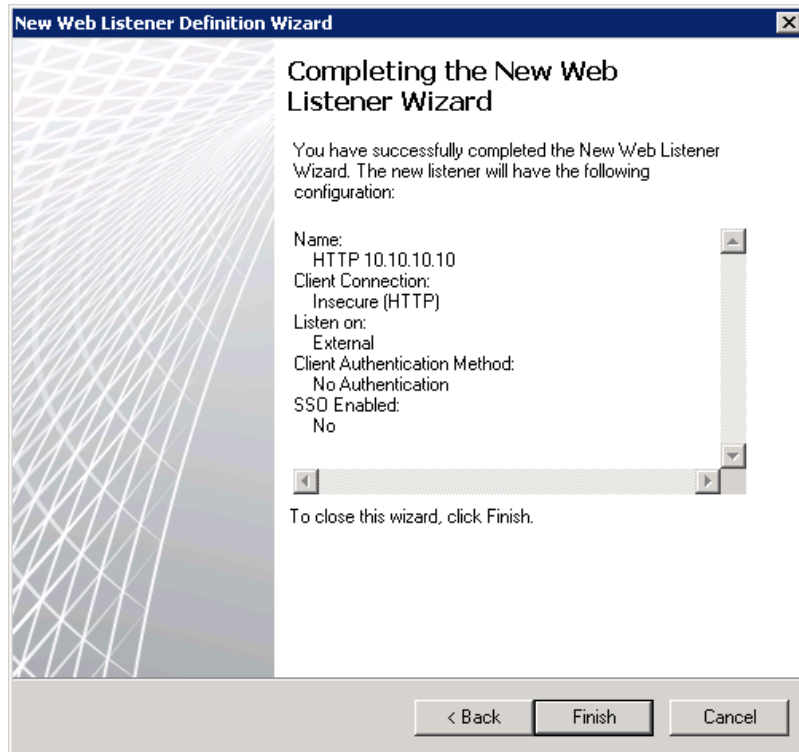


Figure 100: fin de l'assistant de définition d'un nouveau *web listener*

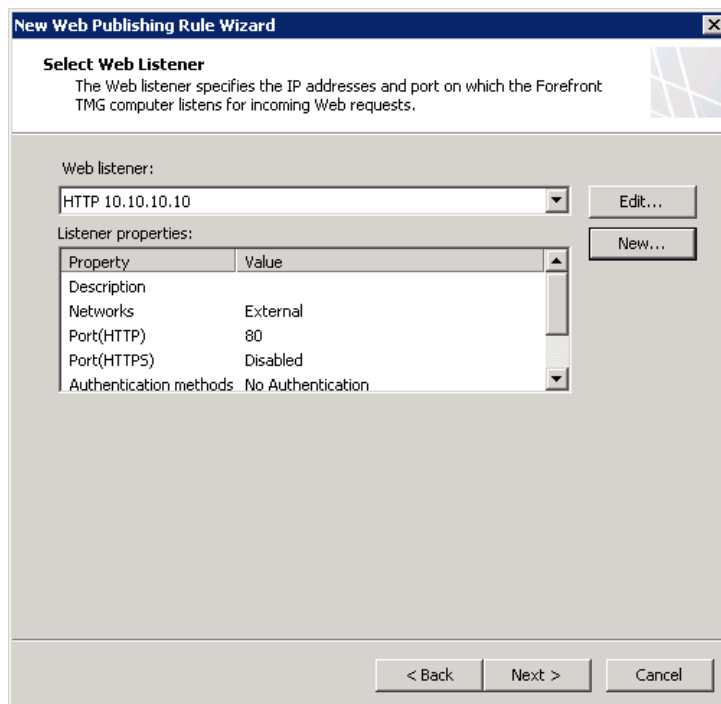


Figure 101: Sélection du *web listener* pour la nouvelle règle de publication web

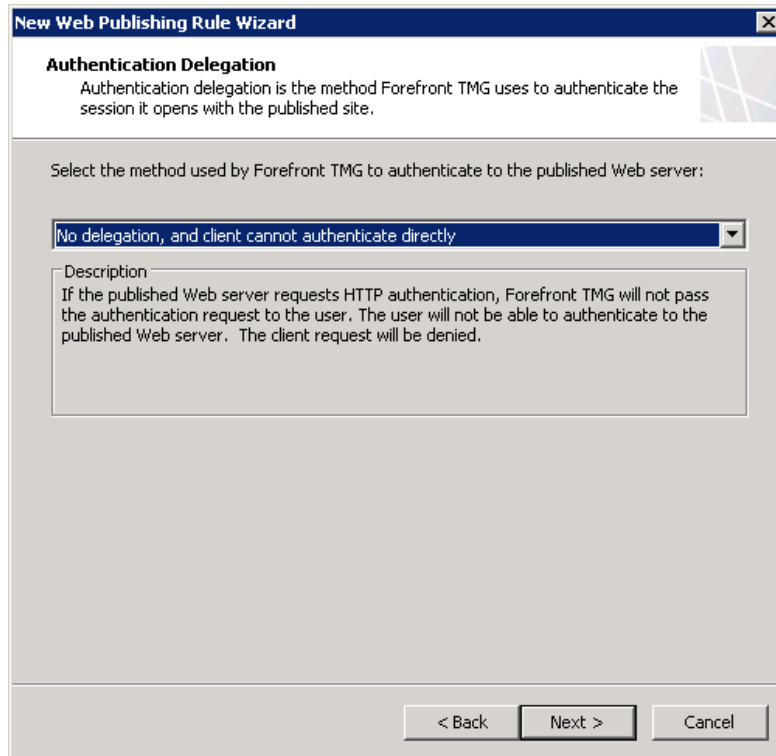


Figure 102: sélection de la délégation de l'authentification

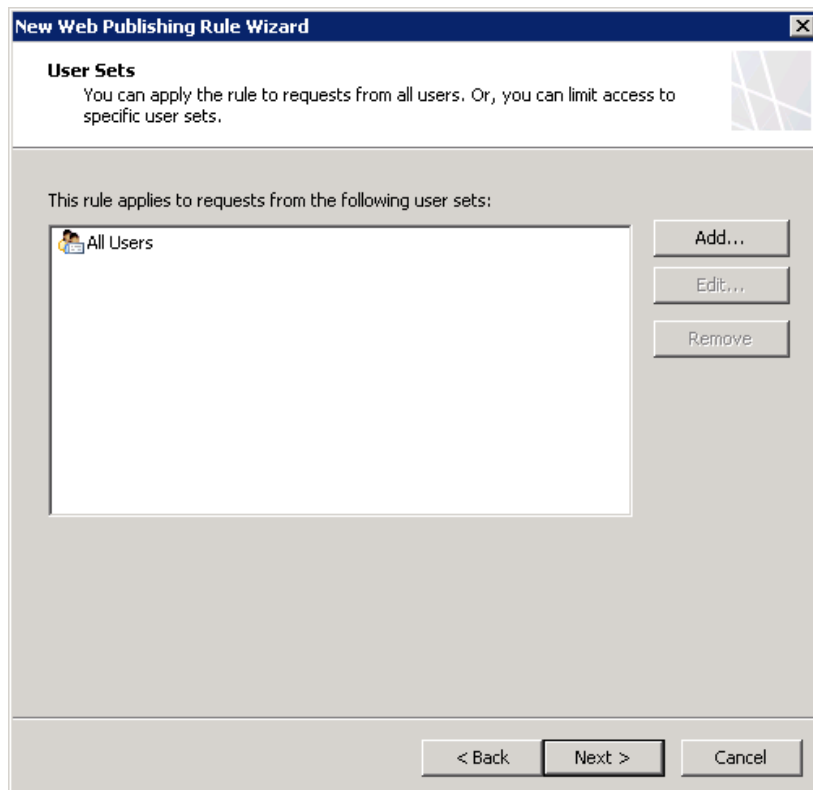


Figure 103: sélection du groupe d'utilisateur

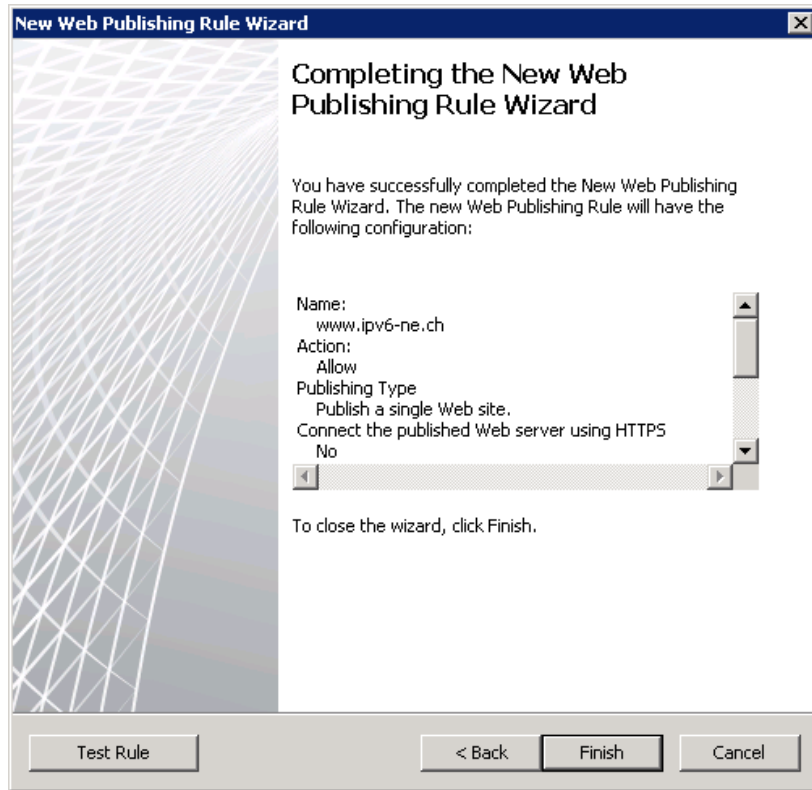


Figure 104: fin de l'assistant de création d'une nouvelle règle de publication web

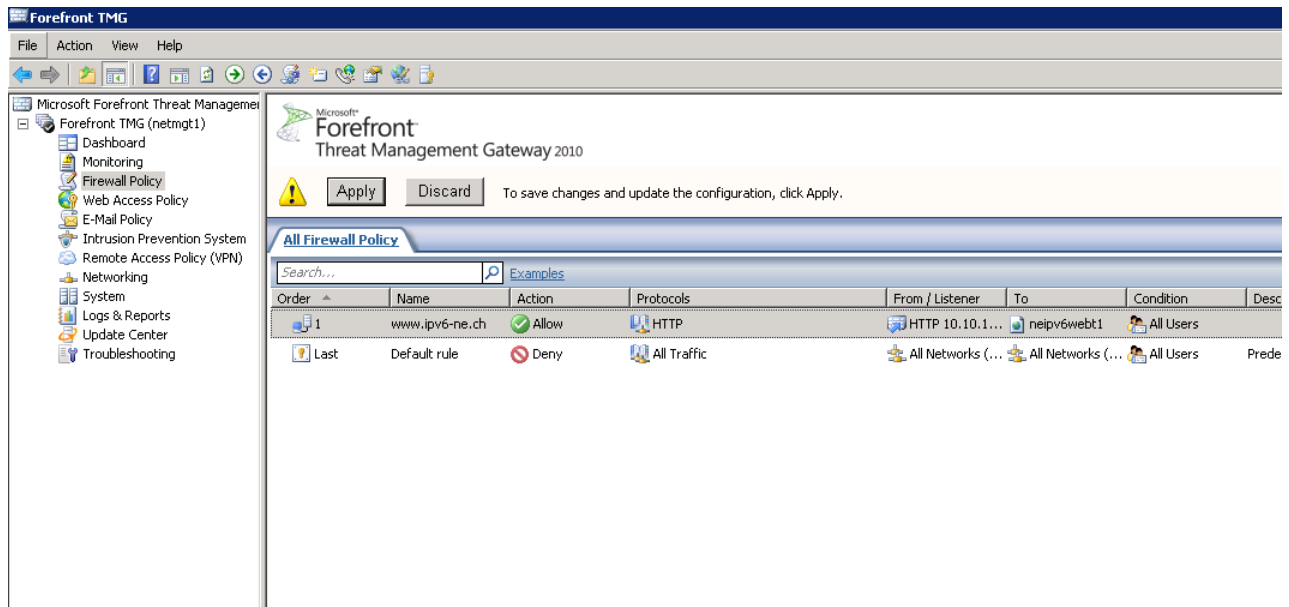


Figure 105: cliquer sur *Apply* pour valider les changements

Après avoir cliqué sur « Apply », l'utilisateur est invité à décrire les changements de configuration effectués, comme on peut le voir à la Figure 106.

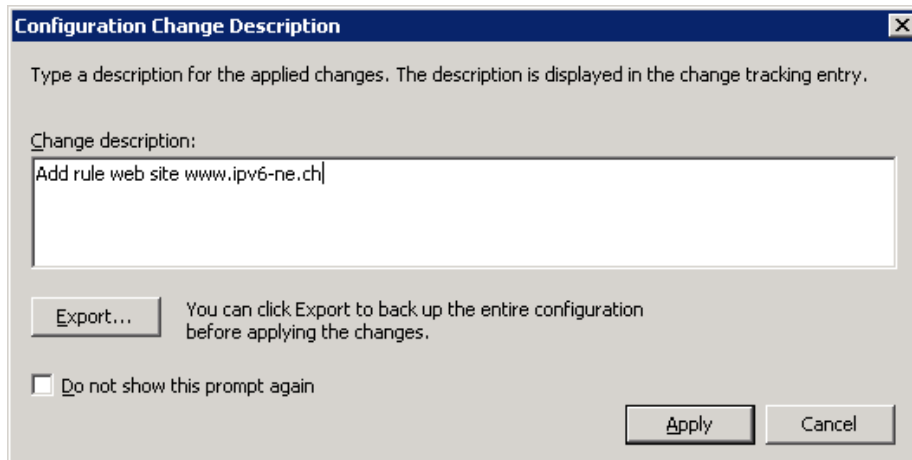


Figure 106: ajout d'une description du changement de configuration du TMG

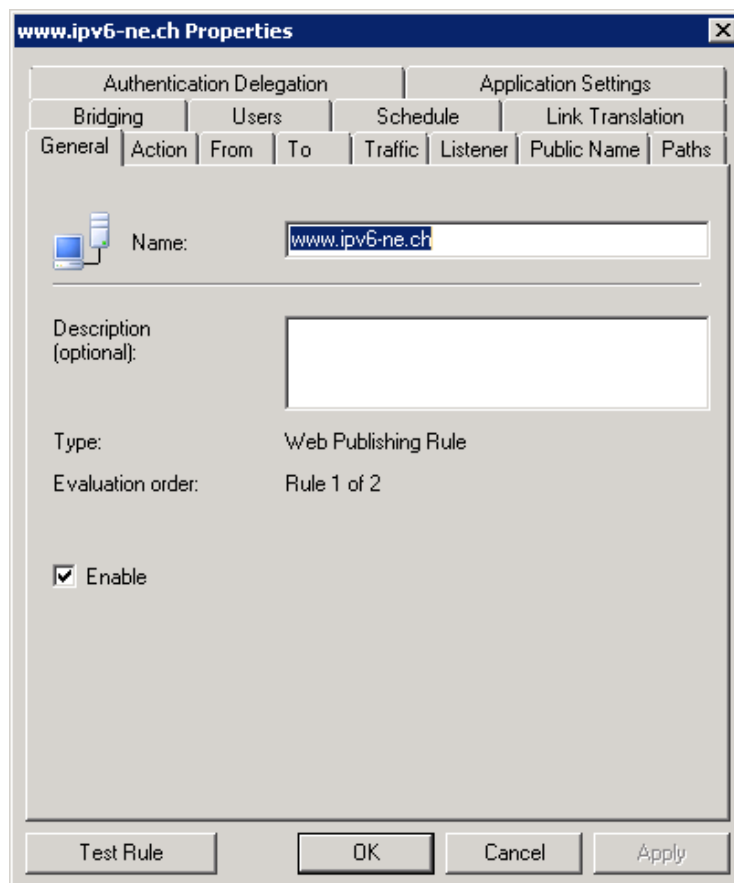


Figure 107: fenêtre de propriété de la règle de publication

On clique maintenant sur « Test Rule », afin de tester notre règle d'impression.

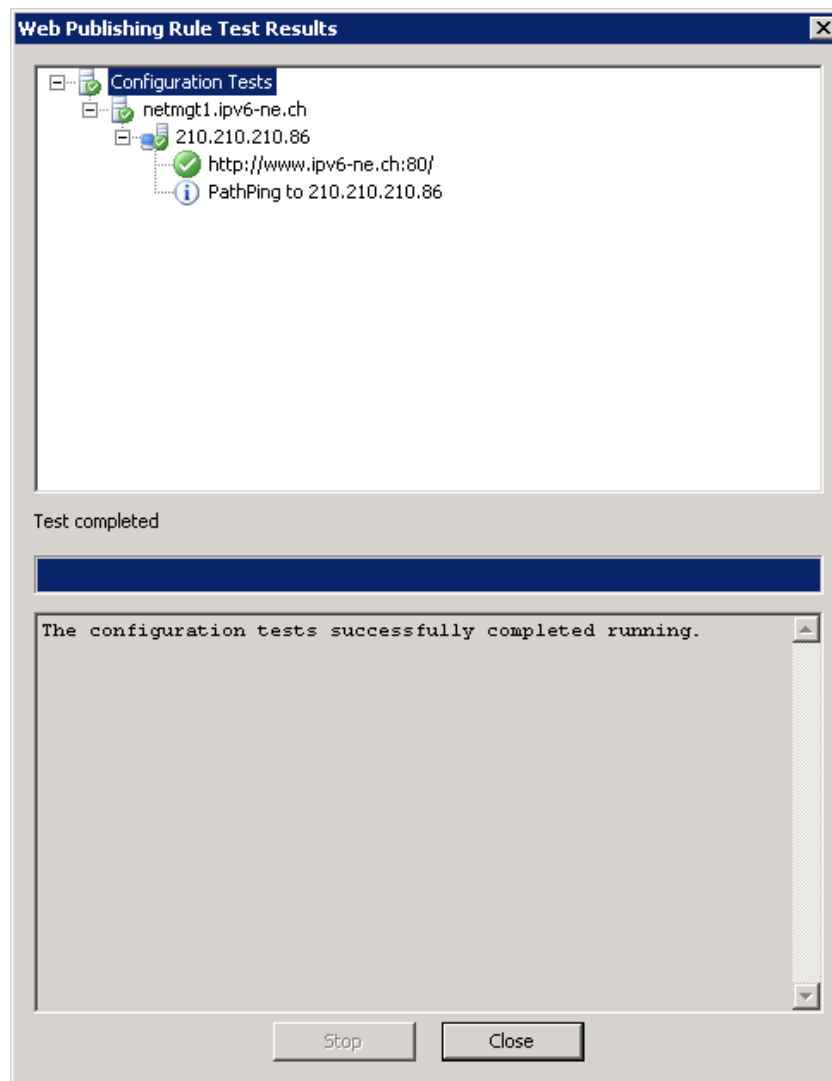


Figure 108: résultat du test de la règle

Le test est réussi, comme on peut le voir à la Figure 108. La configuration du TMG est donc terminée.

15.3 Configuration du prototype dual stack

15.3.1 Routeur accessa-ipv6

```
show run
Building configuration...

Current configuration : 2639 bytes
!
! Last configuration change at 09:41:15 UTC Fri Jul 13 2012
! NVRAM config last updated at 14:44:59 UTC Fri Jul 13 2012
! NVRAM config last updated at 14:44:59 UTC Fri Jul 13 2012
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname accessa-ipv6
!
boot-start-marker
boot system flash c1900-universalk9-mz.SPA.152-2.T1.bin
boot-end-marker
!
!
enable secret 5 $1$N1gI$YkOW2t1.YbLYcFA9f7V1S.
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
!
!
!
!
ip cef
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO1921/K9 sn FCZ154391RC
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.135.151.3 255.255.255.255
 ipv6 address 2001:4DA0:C7F:FC00::50/128
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description connection to accessa-ncn
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.151
 encapsulation dot1Q 151
 ip address 192.135.151.201 255.255.255.192
```

```
ip access-group 10 in
ipv6 address 2001:4DA0:C7F:FC31::10/64
ipv6 enable
ipv6 ospf 151 area 151
ipv6 traffic-filter GlobalUnicastOnly in
!
interface GigabitEthernet0/1
description connection to Firewall
no ip address
duplex auto
speed auto
ipv6 enable
!
interface GigabitEthernet0/1.251
encapsulation dot1Q 251
ip address 148.196.21.253 255.255.255.252
ipv6 address 2001:4DA0:C7F:FC32::1/64
ipv6 enable
!
router ospf 40
redistribute static subnets
network 148.196.21.252 0.0.0.3 area 1
network 192.135.151.192 0.0.0.63 area 1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 148.196.255.192 255.255.255.192 148.196.21.254
!
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 deny 172.16.0.0 0.15.255.255
access-list 10 deny 192.168.0.0 0.0.255.255
access-list 10 permit any
ipv6 route 2001:4DA0:C00::/40 2001:4DA0:C7F:FC32::2
ipv6 router ospf 151
router-id 1.1.31.2
redistribute static
!
!
!
!
!
ipv6 access-list ACL-Console
permit ipv6 2001:4DA0:C00::/40 any
!
ipv6 access-list GlobalUnicastOnly
permit ipv6 2000::/3 any
permit ipv6 FE80::/10 any
!
control-plane
!
!
banner login ^CBachelor Work S.DUNAND, contact SIEN Jerome VERNEZ ^C
!
line con 0
password 7 05080F1C2243
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
```

```
password 7 13061E010803
ipv6 access-class ACL-Console in
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

15.3.2 Firewall

```
fw-ipv6# sh run
: Saved
:
ASA Version 8.4(3)
!
hostname fw-ipv6
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
no nameif
security-level 0
no ip address
ipv6 enable
!
interface Ethernet0/0.251
vlan 251
nameif Outside
security-level 0
ip address 148.196.21.254 255.255.255.252
ipv6 address 2001:4da0:c7f:fc32::2/64
ipv6 enable
!
interface Ethernet0/1
no nameif
security-level 0
no ip address
ipv6 enable
!
interface Ethernet0/1.50
vlan 50
nameif Inside
security-level 100
ip address 148.196.255.193 255.255.255.192
ipv6 address 2001:4da0:c01:30::1/64
ipv6 enable
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
management-only
!
banner login Coucou
```

```
banner login #SIEN, authorised people only#
boot system disk0:/asa843-k8.bin
boot system disk0:/asa821-k8.bin
ftp mode passive
clock timezone CEST 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
object network dmz-web-ipv6
  subnet 2001:4da0:c01:30::/64
object network DNS
  host 2001:4da0:c01:30::aaaa
object network UAG
  host 2001:4da0:c01:30::64
object-group service DM_INLINE_TCP_2 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_3
  service-object tcp destination eq domain
  service-object udp destination eq domain
object-group service DM_INLINE_TCP_1 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_4
  service-object tcp destination eq domain
  service-object udp destination eq domain
object-group service DM_INLINE_SERVICE_1
  service-object icmp6 echo
  service-object icmp6 echo-reply
object-group service DM_INLINE_SERVICE_2
  service-object icmp6 echo
  service-object icmp6 echo-reply
object-group service DM_INLINE_SERVICE_5
  service-object tcp destination eq domain
  service-object udp destination eq domain
object-group service DM_INLINE_TCP_7 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_TCP_8 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_6
  service-object icmp6 packet-too-big
  service-object icmp6 parameter-problem
  service-object icmp6 time-exceeded
  service-object icmp6 unreachable
  service-object icmp6 neighbor-advertisement
  service-object icmp6 neighbor-solicitation
object-group service DM_INLINE_SERVICE_7
  service-object icmp6 packet-too-big
  service-object icmp6 parameter-problem
  service-object icmp6 time-exceeded
  service-object icmp6 unreachable
  service-object icmp6 neighbor-advertisement
  service-object icmp6 neighbor-solicitation
object-group service DM_INLINE_SERVICE_8
  service-object tcp destination eq domain
  service-object udp destination eq domain
access-list Outside_access_in extended permit tcp any host 148.196.255.196 object-
group DM_INLINE_TCP_7
access-list Outside_access_in extended permit object-group DM_INLINE_SERVICE_8 any
host 148.196.255.194
access-list Outside_access_in extended permit icmp any host 148.196.255.196 echo
inactive
access-list Inside_access_in extended permit tcp host 148.196.255.196 any object-
group DM_INLINE_TCP_8 inactive
access-list Inside_access_in extended permit object-group DM_INLINE_SERVICE_5 host
148.196.255.194 any
access-list Inside_access_in extended permit icmp host 148.196.255.196 any echo-
reply inactive
```

```
pager lines 24
logging enable
logging asdm-buffer-size 512
logging asdm debugging
mtu Outside 1500
mtu management 1500
mtu Inside 1500
ipv6 icmp permit any Outside
ipv6 route Outside ::/0 2001:4da0:c7f:fc32::1
ipv6 access-list Outside_access_ipv6_in permit tcp any host 2001:4da0:c01:30::100
object-group DM_INLINE_TCP_2 log critical
ipv6 access-list Outside_access_ipv6_in permit object-group DM_INLINE_SERVICE_3 any
object DNS
ipv6 access-list Outside_access_ipv6_in permit object-group DM_INLINE_SERVICE_2 any
host 2001:4da0:c01:30::100 inactive
ipv6 access-list Outside_access_ipv6_in permit object-group DM_INLINE_SERVICE_7 any
host 2001:4da0:c01:30::100
ipv6 access-list Outside_access_ipv6_in deny ip any any log emergencies
ipv6 access-list Inside_access_ipv6_in permit tcp host 2001:4da0:c01:30::100 any
object-group DM_INLINE_TCP_1 log critical inactive
ipv6 access-list Inside_access_ipv6_in permit object-group DM_INLINE_SERVICE_4
object DNS any
ipv6 access-list Inside_access_ipv6_in permit object-group DM_INLINE_SERVICE_1 host
2001:4da0:c01:30::100 any inactive
ipv6 access-list Inside_access_ipv6_in permit object-group DM_INLINE_SERVICE_6
object dmz-web-ipv6 any
ipv6 access-list Inside_access_ipv6_in deny ip any any log emergencies
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-647.bin
no asdm history enable
arp timeout 14400
access-group Outside_access_in in interface Outside
access-group Outside_access_ipv6_in in interface Outside
access-group Inside_access_in in interface Inside
access-group Inside_access_ipv6_in in interface Inside
route Outside 0.0.0.0 0.0.0.0 148.196.21.253 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 management
http 2001:4da0:c01:30::/64 Inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 2001:4da0:c01:30::/64 Inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics host
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
!
```

```
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:a265382c730c94bf127053ff5b9b81ce
: end
```

15.3.3 Proxy TCP générique

```
netsh interface portproxy add v6tov4 listenaddress=2001:4da0:c01:30::100
listenport=80 connectaddress=148.196.255.196 connectport=80
```

15.3.4 TMG

La configuration du TMG est identique au prototype précédent.