RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité



Résilience de l'Internet français

2026

afnic
Internet
made in France

Table des matières

Synthèse 4

Présentation de l'observatoire 6

Introduction 7

1 Résilience sous l'angle du protocole BGP 8

1.1 Introduction 8

1.1.1 Fonctionnement du protocole BGP 8

1.1.2 Les objets route 9

1.1.3 La RPKI 9

1.2 Les ROA dans la RPKI 10

1.2.1 Préambule 10

1.2.2 Observations 12

1.2.3 Le test 12

1.2.4 Conséquence pratique directe 13

1.2.5 Recommandation 14

1.2.6 Autres considérations motivant l'application de cette recommandation 14

1.2.7 Conséquences possibles 15

1.3 Évolutions des AS français 15

1.3.1 Méthodologie 16

1.3.2 Évolution des AS français - données et analyse 17

1.3.2 Conclusion 23

1.4 Connectivité des AS français 23

1.4.1 Préambule 23

1.4.2 Méthodologie 24

1.4.3 Évolution des AS français avec AS pivots 26

1.4.4 Impact de la disparition d'un AS pivot 30

1.5 Concentration des AS 34

1.6 Conclusion 36

2 Résilience sous l'angle du protocole DNS 38

2.1 Introduction 38

2.1.1 Données et outils 41

2.2 Dispersion des serveurs de noms faisant autorité 42

2.2.1 Nombre de serveurs de noms faisant autorité 42

2.2.2 Dispersion topologique 43
2.2.3 Dispersion géographique 44
2.2.4 Dépendance à des noms tiers 45
2.3 Mise en œuvre de DNSSEC 46
2.3.1 Analyse des enregistrements DS 46
2.3.2 Analyse des algorithmes cryptographiques 46

3 Résilience sous l'angle du courrier électronique 48
3.1 Introduction 48
3.1.1 Transmission d'un message 48
3.1.2 Exemple d'échange en SMTP 48
3.1.3 Adresse d'enveloppe et adresse d'en-tête 49
3.1.4 Données et outils 50
3.2 Sécurité du courrier électronique 50
3.2.1 Adoption globale de SPF, DKIM et DMARC 51
3.2.2 Sender Policy Framework (SPF) 52
3.2.3 Domain-Based Message Authentication, Reporting, and Compliance (DMARC) 54

4 Résilience sous l'angle du protocole TLS 58
4.1 Introduction 58
4.1.1 Fonctionnement du protocole TLS 58
4.1.2 Les infrastructures de gestion de clés 59
4.1.3 Données et outils 60
4.2 Négociation de sessions 60
4.2.1 État général des serveurs TLS 60
4.2.2 Confidentialité persistante 61
4.3 Dispersion des certificats 62

Conclusion 64

Recommandations 65

Bibliographie 66

Acronymes 69

Synthèse

Depuis 2011, l'observatoire de la résilience de l'Internet français étudie les technologies critiques au bon fonctionnement de l'Internet. Afin d'appréhender les dépendances des activités économiques et sociales nationales vis-à-vis de l'étranger, l'observatoire se focalise sur l'Internet français. L'observatoire définit l'Internet français, comme un sous-ensemble de l'Internet contenant l'ensemble des acteurs français et les acteurs étrangers nécessaires à la communication entre opérateurs français.

La résilience est la capacité d'un système à continuer de fonctionner pendant un incident, puis à retrouver son état de fonctionnement nominal. Sur le plan technique, la résilience de l'Internet peut être caractérisée par un ensemble d'indicateurs mesurables, dont certains traduisent le respect de bonnes pratiques établies par la communauté technique et scientifique.

Rédigé par l'Afnic et l'ANSSI, ce rapport analyse la résilience de l'Internet français sous quatre angles complémentaires :

- Le protocole BGP permet d'établir les liens de communication pour échanger des données grâce aux annonces de routage.
- Le protocole DNS associe les noms de domaine aux adresses IP et sert aussi d'ancre de confiance à de nombreux services.
- Le protocole SMTP achemine le courrier électronique.
- Le protocole TLS est notamment utilisé pour chiffrer les communications entre un serveur web et ses clients.

Dans ce rapport, l'observatoire met en lumière quatre faits marquants.

Pour le premier, cela concerne la RPKI qui implique une signature cryptographique appliquée à un enregistrement appelé ROA[1] assurant de la légitimité d'un opérateur à annoncer un préfixe IP dont la taille est bornée dans cet enregistrement. Des expériences ont mis en évidence que certains opérateurs dévoluent l'entièreté du filtrage des annonces reçues à la RPKI au détriment des bonnes pratiques communément admises. Cela a conduit à voir des routes IPv4 et IPv6 acceptées et propagées alors qu'elles auraient dû être refusées, du fait de leur trop grande précision[2]. Ceci ouvrant la voie à des détournements de trafic pour les adresses IP comprises dans ces routes.

Le second est autour de BGP, et plus précisément sur l'évolution des AS[3] français. L'adoption d'IPv6 continue : de 2018 à 2025, le nombre d'AS français présents en IPv6 est passé de 411 à 764, et celui des AS exclusivement IPv6 de 13 à 101. À l'inverse, depuis 2023, plus d'AS exclusivement IPv4 disparaissent qu'il n'en apparaît, une tendance rejointe depuis 2024 par les AS exclusivement IPv6. Désormais, les nouveaux acteurs sont majoritairement présents simultanément en IPv4 et en IPv6.

1. Route Origin Authorization
2. Le préfixe IPv4 annoncé était plus spécifique que /24, et celui en IPv6 plus précis que /48 ne respectant pas les règles prévues.
3. Autonomous System, nom technique donné aux opérateurs en BGP 2. Autonomous System, nom technique donné aux opérateurs en BGP

Le troisième concerne les phénomènes de concentration. Près de 80 % des zones DNS déléguées sous `.fr` sont hébergées dans un seul AS. L'émission des certificats TLS est elle aussi très concentrée : près de 90 % des certificats sont émis par des autorités de certification américaines, dont 75 % par une unique organisation. Seuls 1,59 % des zones étudiées disposent d'un certificat émis par une autorité de certification française. Enfin, si SPF est publié par 73 % des domaines `.fr`, DKIM par 44 % et DMARC par 36 %, l'authentification du courrier électronique, étudiée pour la première fois dans ce rapport, introduit des dépendances fortes et concentrées vers des domaines tiers, qu'il s'agisse des sous-politiques SPF ou des services d'analyse des rapports DMARC.

Enfin, le quatrième concerne les progrès constatés. TLS 1.3 est désormais couramment pris en charge par les serveurs de la zone `.fr`, qui offrent presque tous la confidentialité persistante. Le déploiement de DNSSEC progresse, avec un peu plus de 22 % des zones étudiées correctement signées. Plus de 99 % des zones mettent en œuvre un algorithme de signature recommandé. Le déploiement d'IPv6 sur les serveurs DNS faisant autorité s'est nettement amélioré : environ 17 % des zones ne sont accessibles qu'en IPv4.

Le bilan de cette étude doit toutefois être nuancé. Les risques de déconnexion de certains AS est un fait. Le nombre d'AS pivots - c'est-à-dire un AS dont la disparition pourrait entraîner la déconnexion d'un ou plusieurs autres AS - a augmenté au fil des années. Néanmoins, le nombre d'AS qui viendraient à disparaitre sont répartis entre un plus grand nombre d'AS pivots, ce qui contribue à réduire l'impact d'une panne sur un de ces AS pivots. Mais le nombre d'AS concernés par ces dépendances sont toujours trop importants. La concentration du routage autour de certains acteurs est donc un fait, et l'étude de la centralité d'intermédiarité a permis de montrer la forte dépendance en IPv4 et IPv6 à des acteurs hors union européenne.

L'observatoire encourage l'ensemble des acteurs de l'Internet français à prendre connaissance de ce bilan général et à s'approprier, pour ce qui les concerne plus particulièrement, les bonnes pratiques d'ingénierie et de sécurité reconnues pour les protocoles BGP, DNS, SMTP et TLS. Il formule à cet effet les recommandations suivantes :

1. **diversifier les liens de transit**, notamment avec des opérateurs européens ;
2. **éviter de déclarer des ROA** pour des préfixes plus spécifiques que /24 en IPv4 et /48 en IPv6 ;
3. **déclarer systématiquement les objets route et les ROA** et les maintenir à jour, afin de faciliter la détection et le filtrage des annonces BGP illégitimes ;
4. **surveiller les annonces de préfixes** et se tenir prêt à réagir en cas d'usurpation ;
5. **multiplier et diversifier les serveurs DNS et SMTP** ainsi que leurs hébergeurs, afin de renforcer la robustesse de l'infrastructure et de limiter les dépendances à des noms de domaine tiers ;
6. **mettre en œuvre l'authentification du courrier électronique** (SPF, DKIM, DMARC) en maîtrisant les dépendances qu'elle introduit vis-à-vis de tiers ;
7. **poursuivre le déploiement d'IPv6 et de DNSSEC** et développer les compétences sur ces technologies, afin de mieux anticiper d'éventuels problèmes opérationnels.

Présentation de l'observatoire

L'Internet est une infrastructure essentielle pour les activités économiques et sociales aux échelles mondiale, nationale et locale. Une panne majeure affecterait considérablement la bonne marche de la France et de l'économie française. De plus, le fonctionnement de l'Internet dans son ensemble reste souvent méconnu. Ce système peut être perçu comme un système complexe, multi-acteurs dont les rôles s'avèrent parfois difficiles à identifier en termes de responsabilités.

Tous les jours, cette infrastructure est à la fois mise à l'épreuve de l'évolution des services qu'elle sous-tend. Afin de mieux comprendre et appréhender les risques de dysfonctionnement de l'Internet au niveau national, l'observatoire s'est attelé à publier ce document.

Mis en place sous l'égide de l'ANSSI en 2011, en coopération avec l'Afnic, l'observatoire de la résilience de l'Internet français vise ainsi à améliorer la connaissance de celui-ci en étudiant les pratiques susceptibles d'entraver son bon fonctionnement. Un de ses objectifs est d'augmenter la compréhension collective de l'Internet français afin d'en avoir une vision cohérente et aussi complète que possible.

Ce rapport, dans son édition 2026, propose de nouveaux indicateurs de résilience et de robustesse de l'Internet français, et en reprend certains depuis la dernière édition du rapport.

De par sa nature, l'Internet est international et ne possède pas de frontières. Il est cependant possible de définir l'Internet en France comme l'ensemble des acteurs français et internationaux exerçant une activité en lien avec les technologies de l'Internet sur le territoire. Dans le cadre de ses études, l'observatoire se concentre sur l'Internet français, un sous-ensemble de l'Internet en France, qui exclut les acteurs étrangers non nécessaires aux échanges entre acteurs français. L'étude de l'Internet français permet de mieux comprendre les interdépendances des activités économiques et sociales françaises vis-à-vis de sociétés ou d'organismes étrangers.

Qu'est-ce que la résilience dans le contexte de l'Internet et de ce rapport ?

La résilience est la capacité d'un système à continuer de fonctionner pendant un incident, puis à revenir à son état nominal. La robustesse complète cette notion de résilience, comme la capacité à limiter en amont, autant que possible, l'impact d'un incident sur l'état du système. Le niveau de dépendance d'un service internet à d'autres services ou infrastructures constitue un facteur de vulnérabilité qu'il est possible d'analyser au moyen d'indicateurs de résilience et de robustesse. Sur le plan technique, ces concepts peuvent être caractérisés par un ensemble d'indicateurs mesurables. La grande majorité relèvent de bonnes pratiques d'ingénierie, définies par la communauté technique et scientifique, notamment au sein d'organisations de normalisation, d'associations professionnelles, d'agences nationales ou de groupes de travail.

La mission de l'observatoire de la résilience de l'Internet français se donne ainsi pour objectif de définir et de mesurer des indicateurs représentatifs de la résilience, et de rendre leurs résultats publics. L'objectif est d'inciter le plus largement possible l'adoption des bonnes pratiques admises pour l'amélioration de la résilience de l'Internet français.

Quinze ans après sa création, l'observatoire fait évoluer son format et son périmètre. Nous avons souhaité le rendre plus accessible et plus lisible pour ses lecteurs, tout en restant fidèle à l'exigence technique de ses contributeurs. Cette édition comporte un nouveau chapitre consacré à la résilience de l'authentification du courrier électronique (SPF, DKIM, DMARC).

Introduction

Cette nouvelle édition est issue de deux contributions : l'évolution des indicateurs BGP de 2018 à 2025, réalisée par l'ANSSI, et les indicateurs relatifs au DNS, à TLS et à l'authentification du courrier électronique réalisés, en 2026, par l'Afnic.

Le premier chapitre consacré à BGP fait état d'une expérimentation autour de la RPKI et plus précisément des risques liés au filtrage des annonces BGP reposant exclusivement sur la RPKI. Ce chapitre porte ensuite sur l'évolution du graphe des AS français, leur connectivité via les AS pivots, c'est-à-dire des AS intermédiaires dont la disparition entraîne la déconnexion d'autres AS du graphe de l'Internet. Enfin, ce chapitre examine la concentration des AS, qui met en lumière des opérateurs qui sont des points de passage incontournables pour les communications entre AS français.

Le deuxième chapitre traite de DNS et plus particulièrement de la dispersion des serveurs de noms faisant autorité en IPv4 et IPv6, leur dispersion topologique et leurs dépendances à des serveurs de noms tiers, ainsi qu'un état des lieux sur la mise en œuvre de DNSSEC.

Le troisième chapitre décrit la situation de la sécurité du courrier électronique lié aux noms de domaine français, c'est-à-dire l'étude des mises en œuvre de SPF, DKIM et DMARC ainsi que des risques liés aux configurations constatées.

Enfin, le quatrième chapitre traite quant à lui de TLS. L'observatoire s'intéresse d'abord ici aux versions TLS et aux suites cryptographiques présentées lors de la négociation des sessions. Puis l'observatoire mène une analyse de la dispersion des certificats, c'est-à-dire leur répartition selon le pays d'émission de l'autorité de certification.

Cette nouvelle édition a été l'occasion de revoir en profondeur les développements et outils qui ont permis d'établir les indicateurs. En particulier, pour BGP, l'obsolescence des développements des éditions précédentes a rendu nécessaire la révision du processus de traitement des données dans son ensemble. Cela a aussi permis d'étudier un nouvel indicateur, la concentration des AS reposant sur la centralité d'intermédiarité.

Ce rapport rappelle l'importance du respect des bonnes pratiques, comme par exemple éviter de déclarer des ROA pour des préfixes plus spécifiques que /24 en IPv4 et /48 en IPv6, diversifier les opérateurs d'interconnexion et d'hébergement, ou encore mettre en œuvre l'authentification du courrier.

Chapitre 1
Résilience sous l'angle du protocole BGP

1.1 Introduction

1.1.1 Fonctionnement du protocole BGP

Chacun des opérateurs de l'Internet, que l'on appelle AS, gère des ensembles d'adresses de l'IP contiguës, appelés préfixes, qu'il peut diviser pour ses propres besoins ou ceux de ses clients. Afin de constituer l'infrastructure de l'Internet, les AS se connectent entre eux à l'aide du protocole BGP [25]. L'objectif de ce protocole est d'échanger des informations de joignabilité de préfixes entre deux AS directement connectés qui sont chacun identifiés par un numéro unique.

Chacun des AS informe son AS tiers, ou pair, qu'il a la possibilité d'acheminer le trafic à destination de ses préfixes. Les interconnexions BGP se divisent en deux catégories :

- **le *peering*** : accord où chaque pair annonce à l'autre les préfixes qu'il gère. Par exemple, si un fournisseur d'accès et un diffuseur de contenu passent un accord de *peering*, ils s'échangeront leur trafic directement ;
- **le transit** : accord commercial entre un client et son opérateur de transit. En pratique, le client annonce ses préfixes à son opérateur pour qu'il les propage. Ce dernier lui annonce en retour le reste des préfixes constituant l'Internet.

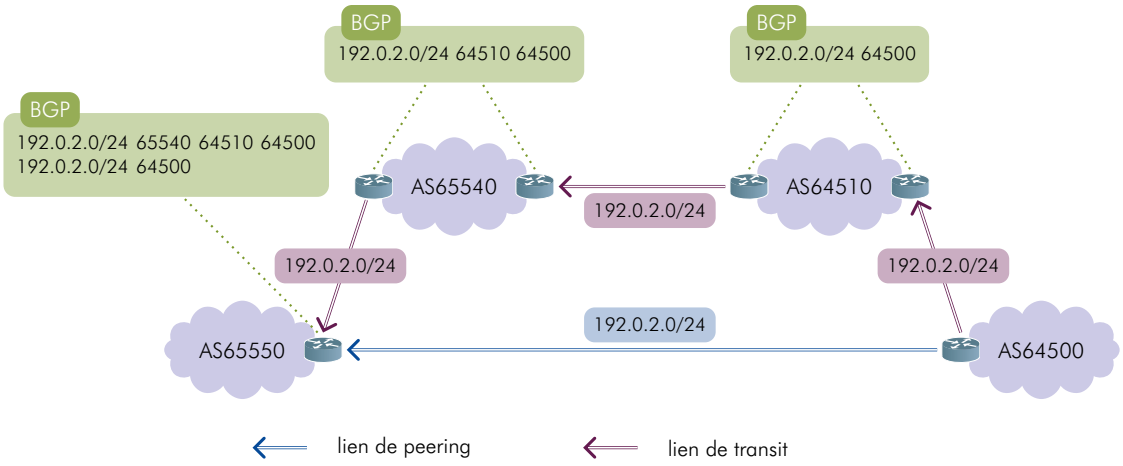


Figure 1.1 – Exemple de chemins d'AS sur des liens de transit et peering

Dans une interconnexion BGP, chaque pair associe un AS_PATH, ou chemin d'AS, aux préfixes qu'il annonce. Dans la figure 1.1, le routeur de l'AS65540 a appris l'AS_PATH 64510 64500 pour le préfixe 192.0.2.0/24. Pour joindre l'adresse IP 192.0.2.1, un paquet au départ de l'AS65540 traversera l'AS64510 avant d'arriver à l'AS64500. L'AS gérant le préfixe se situe à droite dans la liste constituant le chemin d'AS.

En pratique, un message BGP de type UPDATE est utilisé pour indiquer le chemin d'AS associé à un préfixe. Ce message BGP est responsable de l'annonce des routes. Dans la figure 1.1, le routeur de l'AS65550 possède deux routes pour joindre le préfixe 192.0.2.0/24. L'une a été apprise via une interconnexion de *peering* (en bleu), et l'autre via une interconnexion de transit (en violet). En l'absence d'autre information, le chemin d'AS le plus court détermine la route utilisée. Dans cet exemple, il s'agit du lien de *peering*.

Le protocole n'embarque pas de méthode d'authentification robuste des annonces de préfixes. Par conséquent, un AS malveillant peut effectuer une usurpation de préfixe en annonçant un préfixe appartenant à un autre AS. C'est ce que l'on appelle une usurpation de préfixe[1]. Le réseau victime peut ainsi devenir injoignable pour tout ou partie de l'Internet. Ce type d'incident peut également entraîner une redirection du trafic destiné au réseau victime vers le réseau ayant usurpé les préfixes. Les conséquences peuvent être plus ou moins graves selon l'annonce qui est faite.

1.1.2 Les objets `route`

Les bonnes pratiques [3] veulent qu'un organisme déclare, dans la base `whois`, les préfixes qu'il annonce en BGP. Ces déclarations doivent être effectuées par l'intermédiaire d'objets route et sont stockées dans les serveurs d'un IRR. Ce service `whois` est opéré par chaque RIR, dont le RIPE-NCC pour l'Europe. Un objet `route` permet d'identifier clairement les AS susceptibles d'annoncer les préfixes de l'organisation.

```
route:      192.0.2.0/24
descr:      Prefixe d'exemple
origin:     AS65500
mnt-by:     MNTNER-RO-EXEMPLE
```

Figure 1.2 – Exemple d'un objet `route`

L'objet `route` de la figure 1.2 indique que le préfixe 192.0.2.0/24 est annoncé par l'AS65500. L'organisation pourrait déléguer l'utilisation de ce préfixe à un client ou à un partenaire. Dans ce cas, l'attribut `origin` porterait sur un numéro d'AS différent de 65500. Afin d'autoriser certains types de déploiements, comme certaines formes de protection anti-DDoS, il est légitime pour le propriétaire du préfixe IP de déclarer différents objets `route` avec des attributs route identiques mais des attributs `origin` différents. L'attribut `mnt-by` indique, quant à lui, les personnes en charge de la déclaration et de la maintenance de cet objet `route`.

Les objets `route` permettent notamment à un fournisseur de transit de filtrer les annonces de ses clients. Ces filtres lui permettent, ainsi, de se prémunir contre des erreurs de configuration entraînant des annonces de préfixes ne leur appartenant pas.

1.1.3 La RPKI

Afin de renforcer la sécurité du routage d'Internet, plusieurs mécanismes complémentaires ont été développés. La spécification de la RPKI [34] définit une infrastructure cryptographique permettant aux détenteurs de ressources Internet[2] de publier des autorisations d'origine, appelées ROA [40]. Une ROA indique quel AS est autorisé à se déclarer comme origine d'un préfixe.

1. En anglais, *hijack*.
2. Entité (entreprise, opérateur, université, fournisseur de services, etc.) qui possède officiellement des ressources d'adressage IP et/ou des numéros d'AS (Autonomous System) attribués par un Registre Internet Régional (RIR : ARIN, RIPE NCC, APNIC, LACNIC, AfriNIC)

Les opérateurs peuvent ensuite mettre en œuvre la ROV [35] (basée sur les R0A) afin de vérifier, lors de la réception d'une annonce de préfixe via BGP, si l'AS qui en revendique l'origine est légitime. On notera ici que l'efficacité de la ROV dépend également d'un déploiement rigoureux des R0A : l'attaque visant Softaculous, éditeur de Virtualizor, plateforme d'installation et gestion de logiciels web, qui a eu lieu du 28 au 30 août 2026 [3][4][5][6] a rappelé qu'il est important de suivre les recommandations de la RFC 9319 [39] [7].

Par ailleurs, la validation de l'origine d'un préfixe ne permet pas à elle seule de déterminer si le chemin BGP annoncé est lui-même légitime. ASPA [10] apporte un niveau de validation supplémentaire. Fondée également sur la RPKI, ASPA permet à un AS de déclarer ses fournisseurs autorisés et de contribuer ainsi à la détection des fuites de routes et de certaines anomalies dans les chemins BGP.

Ainsi, RPKI, ROV et ASPA s'inscrivent dans une démarche incrémentale de sécurisation du routage Internet : la RPKI constitue l'infrastructure de confiance sur laquelle la ROV permet de valider l'origine des annonces de préfixes, tandis que ASPA étend cette logique à la validation des relations entre AS. L'étude de ces mécanismes permet donc de mieux comprendre les enjeux actuels de la sécurité du routage d'Internet et les moyens mis en œuvre pour rendre Internet plus résilient face aux erreurs de configuration et aux attaques de routage.

1.2 Les ROA dans la RPKI

À la suite d'investigations menées sur le routage d'Internet, certaines pratiques et leurs conséquences potentielles motivent la recommandation suivante : il est important de ne pas publier de R0A pour des préfixes plus spécifiques que /24 en IPv4 ou /48 en IPv6. Ne pas suivre cette recommandation peut mener au détournement des plages d'adresses correspondantes dans Internet.

Cette section rappelle les règles et les bonnes pratiques de routage dans Internet, puis décrit les observations faites et les tests réalisés ayant mené à cette recommandation. Elle rappelle également les conséquences possibles d'une usurpation d'adresses, soulignant ainsi l'importance d'appliquer cette recommandation.

1.2.1 Préambule

1.2.1.1 Rappel des règles et bonnes pratiques de routage dans Internet

1.2.1.1.1 Route plus spécifique

Une des règles du routage des paquets IP veut que, lorsque plusieurs routes correspondent à la destination d'un paquet, la route contenant le préfixe le plus long soit préférée pour router ce paquet (principe de routage via la route la plus spécifique).

3. https://www.softaculous.com/blog/security-incident-bgp-hijacking-update/
4. https://www.virtualizor.com/blog/security-incident-bgp-hijacking/
5. https://bgpkit.com/blog/virtualizor-bgp-hijack-anatomy/
6. https://www.kentik.com/blog/latest-bgp-hijack-targets-hosting-software-vendor/
7. La RFC 9319 émet des recommandations quant à l'utilisation de l'attribut de longueur maximale dans les R0A

Exemple :

Pour un paquet à destination de 192.0.2.12, le routeur de l'AS 64500 possède deux routes pouvant y correspondre :

- 192.0.2.0/24 indique d'envoyer le paquet à l'AS 64496 ;
- 192.0.2.0/25 indique d'envoyer le paquet à l'AS 64511.

En suivant la règle énoncée, le routeur de l'AS 64500 est censé envoyer le paquet à l'AS 64511, comme présenté dans la figure 1.3.

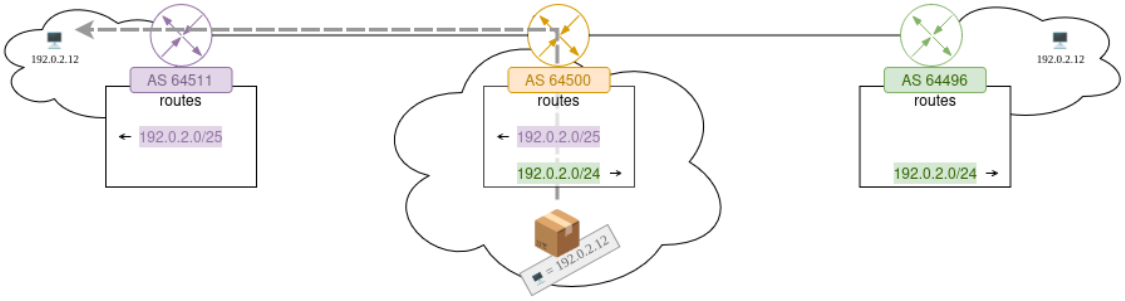


Figure 1.3 – Routage via la route la plus spécifique

1.2.1.1.2 Filtrage des annonces de routes par la longueur de préfixe

Une règle tacite usuelle est de ne pas accepter une route annoncée par un pair BGP si le préfixe est plus long que /24 en IPv4 ou /48 en IPv6. Cette règle, très communément appliquée, trouve son origine dans la volonté de préserver les ressources des routeurs en limitant ainsi la taille de la table de routage d'Internet.

En théorie, on s'attend donc à ce que le routeur de l'AS 64500 n'accepte pas la route annoncée par l'AS 64511, comme présenté dans la figure 1.4.

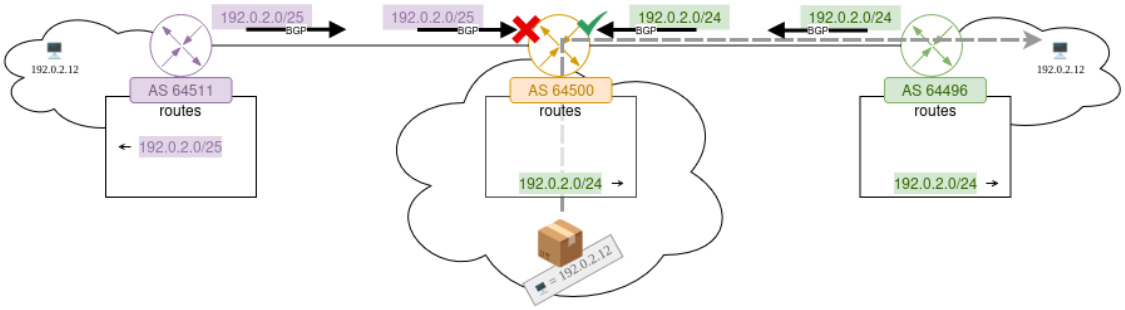


Figure 1.4 – Rejet typique d'une route IPv4 plus spécifique que /24

Dans cette section nous appellerons les préfixes plus longs que /24 en IPv4 et /48 en IPv6 des « préfixes de longueur non conventionnelle ».

1.2.2 Observations

Lors d'analyses de données BGP issues du RIS du RIPE-NCC, il a été constaté qu'un certain nombre de routes pour des préfixes de longueur non conventionnelle étaient apprises et redistribuées par des AS.

Afin d'en trouver les raisons, deux hypothèses ont été envisagées :

- ces AS ne faisaient pas de filtrage ;
- ils ont délibérément choisi de redistribuer ces routes.

La première hypothèse n'a pas semblé totalement pertinente car certains de ces AS appartiennent à des entités connues et reconnues, dont certains encouragent publiquement la mise en œuvre de la ROV. Il semblait donc peu probable qu'ils n'exercent aucun filtrage, ce qui aurait dû bloquer la propagation de ces routes.

La deuxième hypothèse n'a pas semblé totalement pertinente non plus, dans la mesure où la coordination avec ses voisins afin d'accepter et redistribuer des routes aussi spécifiques n'est pas une pratique commune sur Internet. Par ailleurs, les routes concernées étaient trop nombreuses et couvraient trop d'AS pour que cela paraisse plausible.

En observant les propriétés des routes concernées, il est apparu qu'elles avaient au moins un point en commun : elles étaient toutes valides du point de vue de la ROV. Une nouvelle hypothèse a donc été formulée : des AS pouvaient avoir choisi de considérer que la ROV était suffisante pour accepter une route.

Afin d'essayer de vérifier si des AS ont réellement fait ce choix de valider une route en considérant que la ROV est suffisante, le test suivant a été mené.

1.2.3 Le test

1.2.3.1 Phase 1

Afin de vérifier que les AS impliqués dans le test réalisent bien un certain niveau de filtrage hors ROV, une route pour un préfixe /32 sans déclaration de R0A a été annoncée. L'analyse des données du RIS pendant les jours qui suivirent l'annonce a montré qu'aucun de ces AS n'a appris la route annoncée : ces AS filtrent donc bien les annonces reçues.

1.2.3.2 Phase 2

À l'issue de la phase 1, une R0A correspondant au préfixe /32 de la route annoncée a été configurée.
L'analyse des données du RIS pendant les jours qui suivirent l'annonce a montré que plusieurs AS ont appris la route annoncée.

1.2.3.3 Conclusion

L'acceptation par ces AS de la route annoncée en /32 uniquement lorsqu'une R0A qui lui correspond existe, permet de confirmer que certains AS considèrent la procédure de ROV comme suffisante pour accepter une route (quelle que soit la longueur du préfixe contenu dans cette route).
Une hypothèse pour expliquer ce choix de filtrage est que ces AS n'ont peut-être pas envisagé que des R0A pouvaient (ou même allaient) être déclarés pour des préfixes de longueur non conventionnelle.

1.2.4 Conséquence pratique directe

Si un pair BGP d'un tel AS annonce une route pour un préfixe de longueur non conventionnelle pour laquelle une ROA existe (ce pair peut l'annoncer de façon à ce que son annonce soit valide[8]), cette route sera prioritaire car elle est plus spécifique, provoquant le routage d'un paquet à destination de ce préfixe vers ce pair BGP.

Afin d'illustrer cette conséquence, on imagine la situation simple suivante :

- l'AS 64496 déclare deux ROA, l'une couvrant le préfixe 192.0.2.0/24 et l'autre couvrant le préfixe 192.0.2.0/25, en se déclarant lui-même comme AS légitime de l'origine de l'annonce de ces préfixes ;
- l'AS 64496 n'annonce que la route concernant le préfixe 192.0.2.0/24 ;
- l'AS 64511 annonce la route concernant le préfixe 192.0.2.0/25 (avec comme origine forgée l'AS 64496).

Les AS PATH présentés par les 2 annonces sont les suivants :

```
192.0.2.0/24 [ 64496 ]
192.0.2.0/25 [ 64511 64496 ]
```

Si l'AS 64500 se contente de filtrer les annonces reçues en n'utilisant que la validation par la ROV, il va accepter ces deux routes (et potentiellement les redistribuer à d'autres pairs BGP), et les paquets à destination de 192.0.2.12 (par exemple) passeront par l'AS 64511, tel que décrit par la figure 1.5.

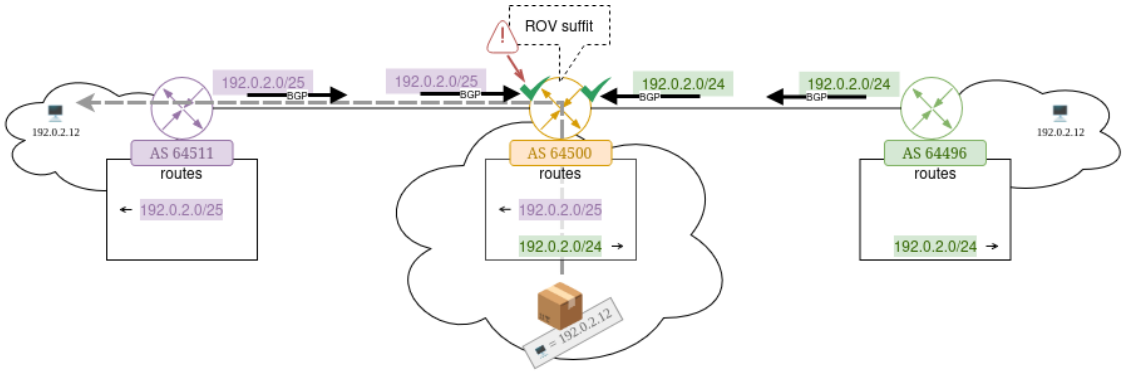


Figure 1.5 – Acceptation inattendue d'une route IPv4 plus spécifique que /24

8. En prenant soin d'indiquer l'AS légitime comme origine du préfixe.

1.2.5 Recommandation

Les observations et tests menés ont conduit à la recommandation formulée en introduction et reprise ici :

RECOMMANDATION

Dans le cadre des vérifications des annonces de routage effectuées via le protocole BGP à partir des informations de la RPKI via la ROV, autant que faire se peut, il est fortement recommandé d'éviter de déclarer des ROA pour des préfixes de longueur supérieure à /24 en IPv4 et à /48 en IPv6.

Le but de cette recommandation est d'éviter de faciliter le détournement de ses propres adresses.

1.2.6 Autres considérations motivant l'application de cette recommandation

En dehors de l'ensemble isolé d'AS observé lors des tests, on considère qu'il peut exister d'autres de ces ensembles isolés dont les AS acceptent des routes avec des préfixes de longueur non conventionnelle (qu'ils considèrent la ROV comme suffisante ou pour d'autres raisons) : il suffit qu'un AS malveillant d'un tel ensemble exploite une ROA couvrant des préfixes de longueur non conventionnelle pour détourner les paquets concernés des autres AS de l'ensemble.

Par ailleurs, étant donné qu'il reste malgré tout commun que des AS filtrent les annonces de routes pour des préfixes de longueur non conventionnelle, il est possible que ces annonces malveillantes passent totalement inaperçues à un autre endroit d'Internet. Ceci est également vrai pour les annonces que l'AS légitime ferait pour des préfixes de longueur non conventionnelle couverts par des ROA.

La figure 1.6 illustre en partie ces considérations.

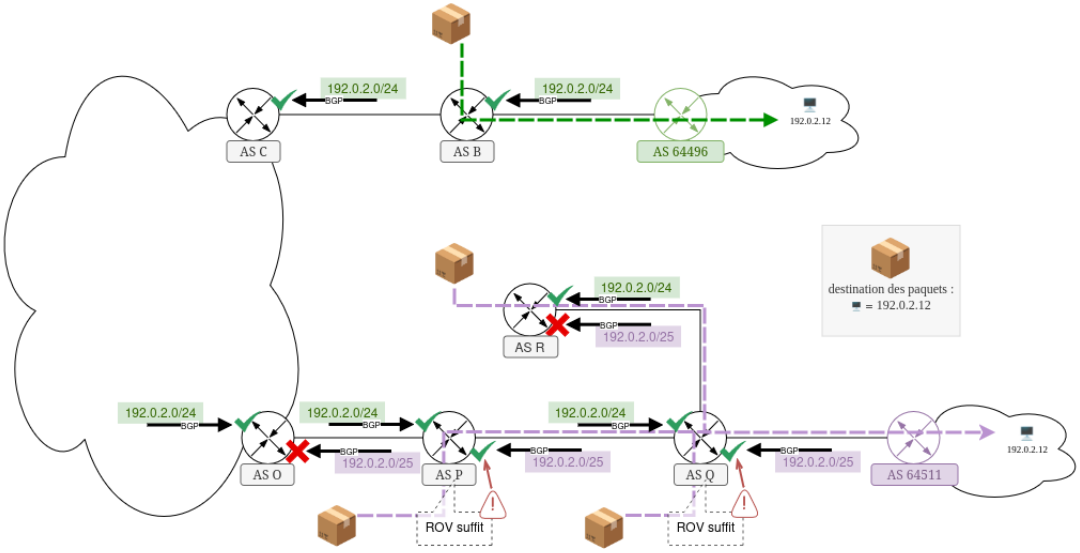


Figure 1.6 – Propagation inattendue d'une route IPv4 plus spécifique que /24

Sur cette figure 1.6, on peut également observer que même si l'AS R filtre l'annonce du préfixe en /25 cela n'empêche pas que ses paquets à destination de ce préfixe aillent vers l'AS 64511 (ici à cause de l'AS Q pour qui la ROV est suffisante pour accepter une annonce).

Enfin, la structure actuelle d'Internet est telle que des AS gérés par des entités éloignées géographiquement peuvent être aujourd'hui très proches et mêmes voisins d'un point de vue du réseau que constitue Internet. Par conséquent, les ensembles isolés d'AS mentionnés ci-dessus ne doivent pas être considérées comme uniquement « locaux » à une région du globe, mais peuvent au contraire le parcourir en totalité : il serait mal avisé de penser qu'un potentiel attaquant considéré comme lointain géographiquement aurait peu de chance de parvenir à détourner un trafic supposé comme hors de sa portée.

1.2.7 Conséquences possibles

Aujourd'hui, l'usage répandu de TLS (et de protocoles sécurisés en général) limite les possibilités d'usurpation de services. Cependant, il existe encore des services dont les utilisations non sécurisées sont encore très répandues, comme NTP ou DNS par exemple.

Mais l'utilisation par d'autres de ses blocs d'adresses peut également conduire à (liste non limitative) :

- l'accès à des ressources qui serait normalement filtré par des règles basées sur ces adresses
- le déni de service sur les adresses en question, les paquets ne pouvant plus atteindre leur destination légitime
- l'altération de la réputation de ces blocs d'adresses

On pensera également qu'en cas d'incident dû à ce genre de déclaration de R0A, une fois la R0A retirée de la base de référence du RIR, la mise à jour sur les routeurs ne pourrait survenir que beaucoup plus tard, prolongeant la durée du problème. Il est donc conseillé de ne pas attendre qu'un problème survienne pour retirer de telles R0A.

1.3 Évolutions des AS français

L'observatoire s'intéresse aux AS français, c'est-à-dire des AS opérés par une entreprise française ou dont l'activité principale est en France, et à leur évolution au sein de l'Internet depuis la seconde édition du rapport. L'internet n'ayant pas de frontière stricto sensu, l'observatoire définit les AS français comme les AS pour lesquels au moins deux des critères suivants sont remplis :

- une activité en France
- qui sont administrés en France
- dont les préfixes sont identifiés comme français par le RIPE-NCC ou des services de géolocalisation d'adresses IP
- dont le numéro de téléphone et/ou l'adresse de l'aut-num sont français.

L'intérêt de cette étude est de pouvoir :

- identifier les nouveaux acteurs qui apparaissent au fil du temps ;
- identifier les acteurs qui disparaissent ;
- constater les campagnes de suppression/réattribution d'AS par le RIPE ;

- confirmer ou infirmer l'augmentation de l'adoption d'IPv6 ;
- établir des tendances sur l'utilisation des AS par les opérateurs eux-mêmes.

Des détails sont fournis dans la partie suivante sur la méthodologie appliquée pour générer l'ensemble des AS français.

1.3.1 Méthodologie

Pour cette édition du rapport, la manière d'associer un pays aux AS a été quelque peu modifiée. Les outils utilisés lors des éditions précédentes n'étant plus disponibles, il a été nécessaire de s'adapter.

Dans un premier temps, les fichiers `asn.txt`[9] sont récupérés lorsqu'ils sont disponibles. Ce fichier contient les numéros d'AS, leur nom et un pays que le RIPE leur associe. Le fichier est mis à jour mensuellement par le RIPE en écrasant le fichier du mois précédent : non seulement les informations changent, mais celles spécifiques aux mois précédents disparaissent à chaque nouveau mois. La première récupération de ce fichier par l'observatoire n'a pris place qu'en 2023. Les fichiers précédents n'étant plus disponibles, il a été nécessaire de faire appel aux archives existantes lorsqu'elles étaient disponibles. Pour cela, nous faisons appel au site *Wayback Machine*[10]. Concrètement, les données de 2018, 2021, 2023, 2024 et 2025 ont pu être récupérées. Il s'avère après des analyses préliminaires que pour un certain nombre d'AS, l'association du pays est incorrecte. Aussi, il a été noté au cours de l'étude que plusieurs campagnes de réattribution de numéros d'AS, par le RIPE, avaient pris plac-e entre 2018 et 2025. Un AS catégorisé « FR » en 2019 a pu être réattribué à une autre `organisation`[11] et être affilié à un autre pays. Les AS concernés par ces campagnes de réattribution étaient alors inactifs d'un point de vue routage.

Puis les informations issues des fichiers `asn.txt` sont mises dans une base de données sous la forme du tuple suivant : numéro d'AS, année, pays. Dans le cas où le fichier n'a pas pu être récupéré pour l'année concernée le dernier fichier antérieur disponible a été utilisé, à la condition que l'AS ait été vu dans les annonces BGP au cours de l'année.

Ensuite, certaines données complémentaires accessibles via l'API REST[12] du RIPE sont utilisées. Dans une partie importante des cas, un numéro de téléphone et/ou une adresse figurent dans les données des organisations. Quand l'indicatif téléphonique est disponible, le code pays correspondant est ajouté à l'AS. Lorsque l'adresse est disponible, le service en ligne Nominatim[13] est utilisé pour identifier le pays, et le code pays ainsi obtenu est également attribué à l'AS. Le tuple après ces traitements a la forme suivante : numéro d'AS, année, pays, pays-téléphone, pays-adresse.

Pour terminer, dans le cas où un AS a les trois entrées pointant vers « FR », alors ce dernier est considéré comme étant français. Dans le cas contraire, si au moins un des paramètres est à « FR » alors un traitement manuel est effectué. Ces opérations ont été réalisées pour chaque ensemble d'AS par année permettant d'établir une liste d'AS français pour chacune des années. Ce procédé manuel a concerné à peu près 20% des AS identifiés comme étant français.

9. `https://ftp.ripe.net/ripe/asnames/asn.txt`
10. `https://web.archive.org/web/collections/*/https://ftp.ripe.net/ripe/asnames/`
11. `https://docs.db.ripe.net/RIPE-Database-Structure/How-to-Organise-Your-Data`
12. `https://rest.db.ripe.net/ripe/organisation/`
13. `https://nominatim.org/`

Une fois l'inventaire de chaque année réalisé, les AS annonçant des routes pour la période visée sont mis dans deux catégories qui ne sont pas exclusives (un AS peut être dans les deux), actif IPv4 ou actif IPv6.

Pour chaque année, une liste d'AS en IPv4 et IPv6 est établi. À partir de cette liste, nous comparons cette liste d'AS avec les AS_PATH de 2018 à 2025 extraits comme expliqué dans le chapitre 1.4.2

1.3.2 Évolution des AS français - données et analyse

De 2018 à 2025, les AS français recensés et visibles ont évolué dans le temps. Pour des raisons de lisibilité, les résultats du 1er janvier au 31 décembre de chaque année sont présentés dans le tableau 1.1.

Année	Nombre d'AS recensés	Nombre d'AS visibles IPv4	Nombre d'AS visibles IPv6	Nombre d'AS commun v4/v6
2018	1982	1144 (746)	411 (13)	398
2019	2010	1212 (772)	454 (14)	440
2020	1998	1262 (773)	526 (37)	489
2021	2098	1327 (799)	587 (59)	528
2022	2177	1349 (783)	658 (92)	566
2023	2295	1385 (783)	710 (108)	602
2024	2290	1388 (756)	737 (105)	632
2025	2239	1410 (747)	764 (101)	663

Tableau 1.1 – Évolution des AS entre 2018 et 2025

Ce tableau recense les évolutions en termes de nombre d'AS visibles en IPv4 et IPv6 au cours de chacune des années considérées dans l'étude. Un AS est considéré visible s'il a annoncé un ou plusieurs préfixes sur une durée totale minimale de cinq minutes sur la journée. Afin d'aller plus loin que les données présentées dans ce tableau, nous présentons ci-après le détail de ces évolutions. Entre parenthèses sont recensés les nombres d'AS qui sont exclusivement présents sur une seule version du protocole IP. Par exemple, en 2022, 92 AS ne sont présents sur Internet que sur IPv6.

Nous constatons que la tendance à l'augmentation globale en termes d'AS français présents sur Internet n'a pas changé en comparaison avec les éditions du rapport précédent et de nouveaux AS ne cessent de s'ajouter chaque année. Seul le nombre d'AS recensés diminue parfois. Ce point est dû à deux facteurs :

- Des entreprises cessent leur activité et leur AS est supprimé de la base de données de l'IRR du RIPE ;
- Le RIPE fait des campagnes de suppression dans la base de données de l'IRR sur des AS inutilisés depuis une longue période.

Mais en observant les valeurs exclusives à chaque protocole (IPv4 et IPv6), nous voyons que le nombre d'AS exclusivement en IPv4 a augmenté jusqu'en 2021 avec 799 AS puis a décru jusqu'à 747 en 2025. En opposition à cela, les AS exclusivement IPv6 ont dépassé la centaine en 2023.

À RETENIR

Les croissances du nombre d'AS déployant l'IPv6 et exclusivement IPv6 sont significatives, montrant une tendance forte vers l'adoption d'IPv6 dans un contexte d'épuisement des adresses IPv4. En l'espace de sept ans, le nombre d'AS présents en IPv6 est passé de 411 à 764, une croissance de 86 %. Aussi, pour les AS exclusivement IPv6, leur nombre est passé de 13 à 101 sur la période observée, soit une augmentation de 677 %.

1.3.2.1 Évolution des AS exclusivement IPv4

Le tableau 1.1 représente en valeur absolue le nombre d'AS qui sont vus sur une période mais ne permet pas d'appréhender le nombre de nouveaux acteurs qui sont apparus, ni ceux qui ont disparu du paysage. Pour mieux se rendre compte de l'évolution en termes de nouveaux acteurs et d'AS disparaissant nous affichons dans la figure 1.7 les courbes présentant ces changements.

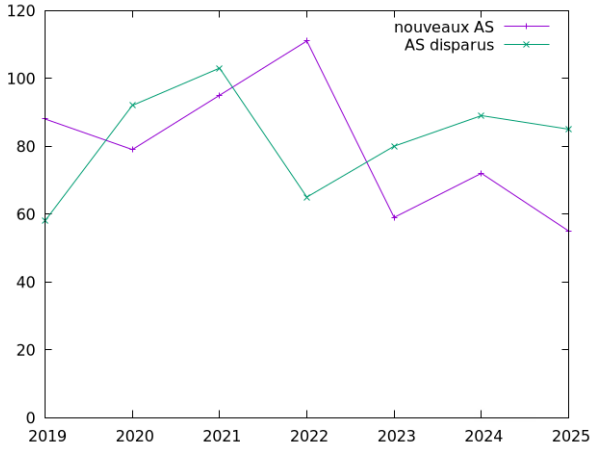


Figure 1.7 – Nouveaux AS français IPv4 de 2019 à 2025

Le nombre de nouveaux AS français exclusivement IPv4 a eu un pic de croissance en 2022 mais ce dernier s'est effondré par la suite. C'est en 2022 que nous observons un changement de tendance important sur les nouveaux acteurs et ceux qui disparaissent. En effet, à partir de cette année le nombre de nouveaux AS est en deçà du nombre d'AS qui disparaissent de l'Internet IPv4. L'hypothèse avancée ici serait liée à la pénurie d'adresses IPv4 et que les opérateurs afin d'avancer dans leur présence sur Internet se sont contentés dans un premier temps d'une présence sur IPv6 en attendant d'obtenir un préfixe IPv4. Cette hypothèse est renforcée par la baisse significative de nouveaux AS IPv4 sur cette période.

Si on compare les deux extrémités temporelles de cette étude, elles sont aux antipodes l'une de l'autre : en 2019, 88 nouveaux AS s'ajoutent quand 58 disparaissent, alors qu'en 2025 la situation est quasiment à l'inverse avec 85 AS qui se retirent pour en voir apparaître 55 nouveaux.

À RETENIR

Depuis 2023 dans les AS français exclusivement IPv4, nous constatons que plus d'AS disparaissent qu'il n'en apparait.

1.3.2.2 Évolution des AS exclusivement IPv6

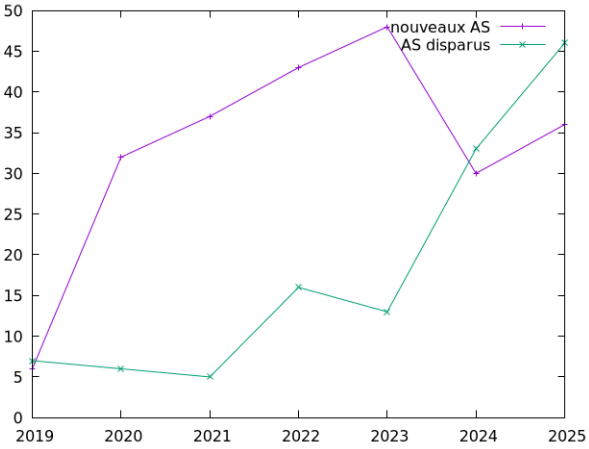


Figure 1.8 – Nouveaux AS français IPv6 de 2019 à 2025

La figure 1.8 représente les courbes pour les AS exclusivement IPv6. Durant un certain temps, les nouveaux AS ont été bien plus importants que les AS qui ont disparu. La pente de la courbe des nouveaux AS est importante et atteint son apogée en 2023 avec 48 AS. Pour la même année, seulement 13 AS quittaient l'Internet exclusivement IPv6. Toutefois, nous observons un changement drastique sur les tendances en 2024 où plus d'AS disparaissent qu'il n'en apparaît. Enfin, la période étudiée termine avec 46 AS en moins et 36 nouveaux acteurs.

À RETENIR

Depuis 2024 dans les AS français exclusivement IPv6, nous constatons que plus d'AS disparaissent qu'il n'en apparait, rejoignant la tendance des AS exclusivement IPv4.

1.3.2.3 Évolution des AS IPv4 et IPv6

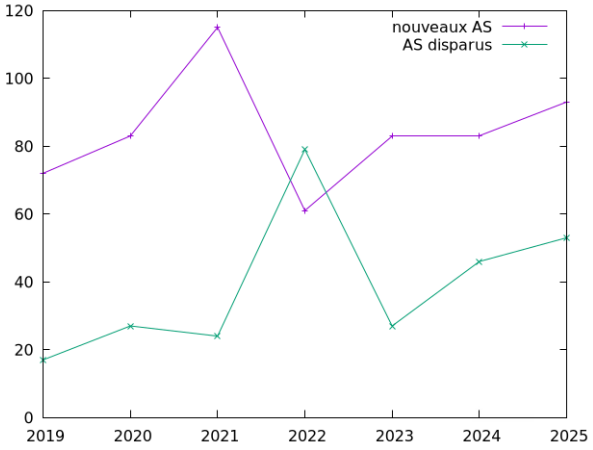


Figure 1.9 – Nouveaux AS français IPv4 et IPv6 de 2019 à 2025

Un des objectifs ici est tout d'abord d'analyser cet ensemble mais aussi de vérifier si des tendances observées dans les deux sections ne se sont pas reportées ici.

La figure 1.9 reporte les mêmes courbes que vues précédemment mais cette fois pour les AS qui sont simultanément présents en IPv4 et IPv6. Il apparaît que les pentes des courbes sont très similaires avec un décalage dans le temps d'une année. Les changements de pentes pour les nouveaux AS semblent s'appliquer l'année suivante pour ceux qui disparaissent. Néanmoins, nous n'avons pas pu constater clairement de reports significatifs d'AS quittant IPv4 exclusivement.

À RETENIR

Contrairement aux précédentes sections, nous constatons que plus d'AS simultanément IPv4 et IPv6 apparaissent qu'il n'en disparait.

1.3.2.3 AS apparus entre 2018 et 2025

Pour pouvoir comparer les valeurs des nouveaux arrivants selon les catégories précédentes, nous avons agrégé les mêmes données dans la figure 1.10.

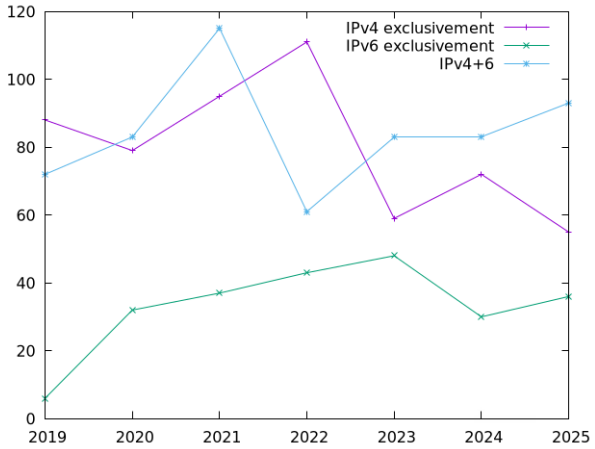


Figure 1.10 – Nouveaux AS français de 2019 à 2025

Cette figure illustre une tendance observée en 2025, qu'il conviendra de vérifier une fois l'année 2026 terminée, où le nombre de nouveaux AS exclusivement IPv4 est en déclin contrairement aux deux autres ensembles.

Ce diagramme permet aussi de mettre en exergue que jusqu'en 2023, la quantité de nouveaux AS devient majoritairement IPv4 et IPv6 contrairement à précédemment où la majorité étaient constituée d'AS exclusivement IPv4. Ce changement s'inscrit dans la durée et met en lumière un changement important de la distribution des nouveaux AS.

Le tableau 1.2 représente les AS qui étaient exclusifs sur un protocole et qui ont été ajoutés à l'ensemble d'AS présents en IPv4 et IPv6. L'objectif étant d'avoir des chiffres permettant de discriminer les AS qui existaient déjà et qui sont considérés comme nouveaux sur IPv4 et IPv6 de ceux qui arrivent directement dans cette catégorie. Nous observons un pic important en 2021 qui explique la courbe IPv4 et IPv6 de la figure 1.10 où 61 AS IPv4 se sont vus apparaître en IPv6.

Année	Nombre d'AS IPv6	Nombre d'AS IPv4
2019	6	27
2020	4	38
2021	3	61
2022	6	26
2023	12	22
2024	8	44
2025	17	38

Tableau 1.2 – Bascule de mono protocole vers IPv4+IPv6

À RETENIR

Le nombre de nouveaux AS exclusivement IPv4 décline fortement depuis 2022, tandis que le nombre de nouveaux AS exclusivement IPv6 et IPv4+IPv6 augmentent à partir de cette même année.

1.3.2.5 AS disparus entre 2019 et 2025

À l'instar des nouveaux AS qui s'ajoutent à l'Internet, des AS disparaissent. Il s'agit principalement d'entreprises qui cessent leur activité. Nous avons répliqué la même méthodologie que pour la section précédente mais cette fois en nous concentrant sur les AS qui ne sont plus présents au cours de l'année suivante. Les données sont présentées dans la figure 1.11.

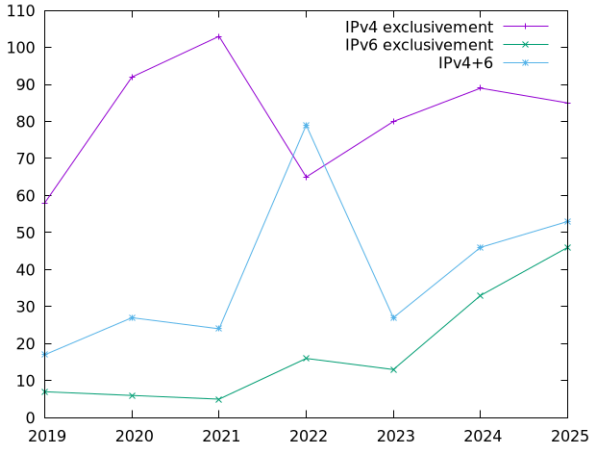


Figure 1.11 – AS français ayant disparu de l'Internet de 2019 à 2025

Globalement, hormis entre 2022 et 2023, la tendance entre les catégories est quasiment la même. Le nombre d'AS disparaissant croît avec en première ligne les AS en IPv4 puis les AS IPv4 et IPv6, et enfin les AS IPv6. En 2019, toutes catégories confondues cela concerne 82 AS pour terminer à 184 en 2025. Il n'y a pas de surprise ici étant donnée la taille des ensembles dont il est question. Il se pourrait que dans quelques années la courbe IPv4 et la courbe IPv6 se rejoignent, si les tendances observées en section 1.3 se confirment.

Nous notons un pic de disparition d'AS que l'on observe en 2022 qui concerne principalement IPv6. En 2021, un réseau universitaire français a mené des expérimentations pendant quelques semaines. Cette expérimentation a pu être observée grâce à l'utilisation de numéros d'AS jusque-là restés inutilisés. Ces numéros d'AS ont disparu en fin d'année 2021 pour ne plus apparaître sur la période mesurée. À cela s'ajoute peut-être l'impact du COVID sur les entreprises qui n'ont pas résisté aux conséquences de la crise sanitaire.

À RETENIR

En 2025 le nombre d'AS disparaissant diminue en IPv4 exclusivement quand en IPv6 exclusivement et IPv4+IPv6 leur quantité augmente.

1.3.3 Conclusion

L'ensemble des AS identifiés comme étant français a beaucoup changé au cours de la période étudiée. Les expérimentations universitaires, les réadressages de numéros d'AS inutilisés ou encore les conséquences de changements économiques tel que le COVID ont un impact direct sur cet ensemble. Néanmoins, l'analyse sur une longue période permet de voir que l'IPv6 continue de prendre de l'ampleur et s'intensifie. La pénurie d'adresses IPv4 disponibles et la disponibilité immédiate de préfixes IPv6 forcent les nouveaux acteurs à entrer sur ce secteur. En termes de résilience de service, le fait de constater qu'IPv6 continue de croître est très encourageant en cas de panne concernant exclusivement une seule version du protocole.

1.4 Connectivité des AS français

1.4.1 Préambule

L'observatoire étudie la connectivité des AS français en modélisant les relations inter-AS par l'intermédiaire de représentation sous forme de graphe. Une arête dans ce graphe indique que les deux AS de part et d'autre sont voisins. L'objectif principal de cet indicateur est de mesurer la résilience des opérateurs français, mais aussi identifier les points de concentration de trafic qui pourraient exister lors d'échanges d'AS français vers d'autres AS français.

Lors des éditions précédentes, l'inventaire des arêtes était cumulatif par l'extraction de tous les AS_PATH depuis les archives du projet RIS [14] au format MRT [15] de l'année analysée. Seulement, cette approche masquait un certain nombre de cas problématiques. Par exemple, un opérateur qui n'aurait qu'un seul fournisseur de transit pendant 6 mois, et en changerait pour les 6 mois suivants apparaîtrait comme ayant 2 fournisseurs de transit distincts sur le graphe cumulatif de l'année. Ou encore, un AS qui passerait de deux fournisseurs de transit en début d'année à un seul sur les onze derniers mois n'aurait pas pu être détecté comme potentiellement vulnérable. Pour ces raisons et pour avoir des résultats plus cohérents, il a été décidé de revoir la méthodologie pour limiter au maximum les faux positifs.

14. https://ris.ripe.net
15. https://datatracker.ietf.org/doc/html/rfc6396

1.4.2 Méthodologie

Le schéma fonctionnel de la figure 1.12 décrit le processus permettant d'aboutir aux données qui sont analysées pour cet indicateur.

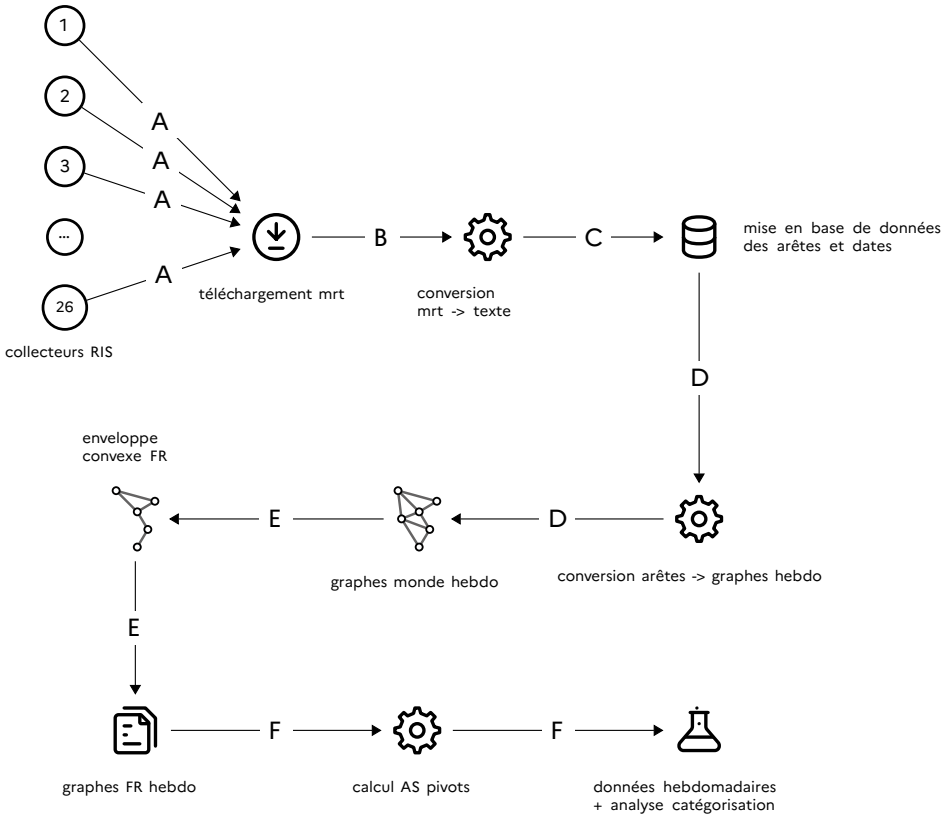


Figure 1.12 – Suite des process pour le traitement des données

Les étapes, de A à F, pour aboutir aux données qui servent à l'analyse et qui sont présentées dans la figure 1.12 sont les suivantes :

A) Les sources de données BGP au format MRT utilisées sont issues de l'ensemble des collecteurs RIS mis à disposition par le RIPE pour lesquels les archives BGP sont disponibles entre 2018 et 2025 inclus. Ces dernières sont téléchargées et stockées localement.

B) Les données au format MRT sont transposées au format texte à l'aide de l'outil bgpreader [16] et stockées sous la forme de fichiers textuels.

C) À partir des fichiers de chaque journée, la durée de vie de chaque arête est mesurée puis si elle dépasse 5 minutes, l'arête est stockée dans une base de données[17]. Ces opérations sont réalisées sur l'ensemble des données disponibles du projet RIS (du 1er janvier 2018 jusqu'au 31 décembre 2025). Pour chaque journée les arêtes du graphe de l'Internet sont stockées dans la base. Le calcul pour cette durée de vie d'une arête cumule le temps pendant lequel cette dernière est présente dans un AS_PATH, c'est-à-dire qu'un ou plusieurs préfixes sont associés à ce chemin pendant la journée. Pour

16. https://bgpstream.caida.org/docs/tools/bgpreader
17. https://www.postgresql.org/

réduire la présence de certains artefacts tels que des erreurs de configuration[18], le choix a été fait de ne pas enregistrer une arête si sa durée de vie est inférieure à cinq minutes sur l'ensemble de la journée analysée. Une fois ce traitement terminé, la base de données contient l'ensemble des informations nécessaires, c'est-à-dire les arêtes, pour reconstruire un graphe cumulatif de l'Internet pour n'importe quelles périodes et durées voulues.

D) Pour réduire le nombre de graphes à traiter de 2018 à 2025, le choix arbitraire de travailler sur des graphes cumulatifs d'une semaine a été fait. En utilisant les arêtes stockées dans la base de données, un peu plus de 800 graphes hebdomadaires, au format graphml[19] sont créés et stockés.

E) Toujours dans un objectif d'efficacité, le périmètre des graphes générés est restreint. Ces derniers sont tous réduits en dégageant l'enveloppe convexe (*convex hull*[20]) des AS français qui ont été préalablement identifiés, et ce pour chaque année liée à chaque graphe. L'enveloppe convexe du graphe des AS français représente le graphe minimal contenant les nœuds (AS) et arêtes permettant de rendre joignable l'ensemble des AS français entre eux. Cela permet d'obtenir le graphe minimal de communication inter AS français. La totalité de ces graphes est conservée sous la forme de fichiers.

F) Pour chacun des graphes de l'enveloppe convexe « FR », une recherche des AS pivots (*Articulation point ou cut vertex*[21] en anglais) est faite. Les résultats de ces recherches sont stockés sous la forme de fichiers au format json et dans la base de données PostgreSQL.

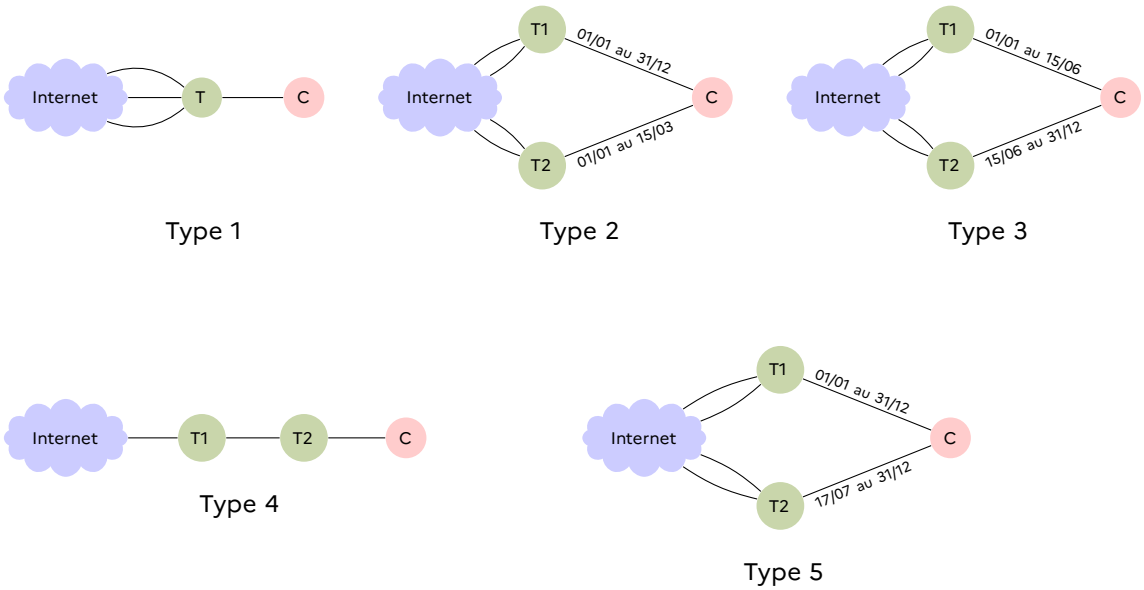


Figure 1.13 – Typologies de connectivité des AS avec pivot

18. https://datatracker.ietf.org/doc/html/rfc7908
19. https://en.wikipedia.org/wiki/GraphML
20. https://en.wikipedia.org/wiki/Convex_hull
21. https://en.wikipedia.org/wiki/Biconnected_component

Enfin toutes ces données sont analysées de manière automatique à l'aide d'un script. Pour attribuer une classification aux résultats, une typologie a été définie. La figure 1.13 les illustre. Les différentes typologies sont pour chaque AS étudié ceux qui sont :

1. avec un AS pivot toute l'année ou toute leur période d'activité ;
2. avec un AS pivot qui est apparu et reste présent ;
3. avec plusieurs AS pivots (étalés dans le temps) ;
4. avec plusieurs AS pivots (qui se cascadent) ;
5. qui avaient un pivot mais qui se sont améliorés.

Il est à noter que dans ces 5 catégories, les quatre premières constituent des situations défavorables car dans le cas où l'AS pivot disparait, l'AS en dépendant perd la connectivité avec la majorité des autres AS français. La dernière au contraire montre un changement de situation pour l'AS concerné qui passe d'une situation dangereuse à une situation plus sûre en cas de défaillance d'un de ses fournisseurs. Enfin, quelques résultats n'aboutissant pas automatiquement dans une de ces catégories, une analyse manuelle a été nécessaire pour les catégoriser.

1.4.3 Évolution des AS français avec AS pivots

1.4.3.1 IPv4

Les résultats sont issus des AS_PATH grâce auxquels des AS pivots ont pu être identifiés, ainsi que les AS français impactés par leur disparition. Les AS français ont été regroupés dans les catégories présentées dans la partie introductive. Les résultats de ces analyses en IPv4 sont présentés dans le graphique 1.14.

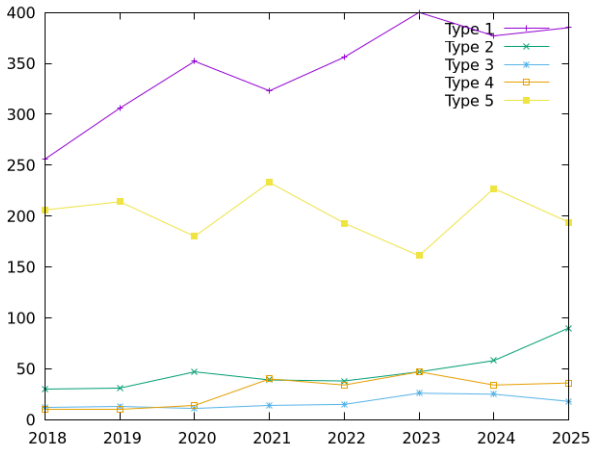


Figure 1.14 – Distribution des AS français impactés par des AS pivots en IPv4

Tout d'abord nous observons que le nombre d'AS français qui sont dans le type 1, avec un AS pivot tout au long de l'année étudiée, représente la plus grande proportion d'AS français identifiés ici. Leur nombre augmente globalement sur l'ensemble de la période de l'analyse avec une légère stabilisation au cours de deux dernières années. Toutefois, si l'on compare ces valeurs avec le nombre de nouveaux AS en IPv4, on constate que proportionnellement la tendance est constante. Si l'on compare ces chiffres avec ceux du nombre total d'AS visibles, la proportion d'AS de type 1 passe de 22 % en 2018 à 27 % en 2025.

Le nombre d'AS français en type 2, qui n'avaient antérieurement pas d'AS pivot et qui terminent l'année avec, augmente significativement dans le temps. Leur quantité était relativement stable jusqu'en 2023 en étant au maximum à 47 AS en 2020 et 2023. En 2024 et 2025 ils sont passés de 58 à 90 AS. Cette croissance n'est pas encourageante mais l'analyse des données a aussi montré qu'une partie des AS de type 2 étaient ventilés dans le type 1 mais aussi le type 5 l'année suivante. Aussi, la quantité d'AS de type 2 en 2025 ne représente que 6 % du nombre total d'AS visibles cette année-là. L'étude de 2026 permettra d'établir si ces AS viendront s'ajouter majoritairement à ceux du type 1 ou à ceux du type 5.

En ce qui concerne les AS qui entrent dans le type 3, dans cet ensemble nous retrouvons des AS qui changent d'opérateur de transit, mais aussi des AS qui ont plusieurs opérateurs de transit mais n'en utilisent qu'un seul de manière nominale. Le nombre d'AS dans cette typologie reste assez stable et représente 18 AS en 2025.

Le type le plus risqué, le type 4, représente heureusement un nombre restreint d'AS français. Ces AS ont un AS pivot, qui est lui-même soumis à un AS pivot. Ils souffrent donc de plusieurs *SPOF*[22]. Afin de mieux cerner le comportement de ces AS français, nous avons comptabilisé le nombre d'années durant lesquelles ils se retrouvent dans cette catégorie. Le tableau 1.3 recense ces AS.

Récurrence	Nombre d'AS	Proportion
1 fois	81	62,8 %
2 fois	24	18,6 %
3 fois	11	8,6 %
4 fois	7	5,4 %
5 fois	3	2,3 %
6 fois	2	1,5 %
7 fois	0	0 %
8 fois	1	0,8 %

Tableau 1.3 – Nombre d'années consécutives pour les AS de type 4 en IPv4

À l'étude de ce tableau, nous constatons que la majorité des AS de type 4, plus de 80 %, ne restent pas plus de deux ans dans cette catégorie. Le nombre d'AS concernés de manière durable par cette problématique reste très faible.

Enfin, les AS français entrant dans le type 5 sont assez nombreux et la courbe montre que, même si leur nombre varie d'une année à l'autre, ils sont entre 161, au plus bas, en 2023 et 233, au plus haut, en 2021 à faire partie de cette catégorie chaque année. La situation pour ces AS français s'améliore au fil du temps, ce qui est particulièrement encourageant. En effet, ces AS commencent l'année avec un AS pivot et se voient la terminer avec plus d'un opérateur de transit non soumis à un AS pivot.

22. SPOF : Single Point of Failure

À RETENIR

Les chiffres pour les AS de type 3, 4 et 5 sont plutôt stables alors que le type 1 augmente tant en nombre qu'en proportion ce qui n'est pas encourageant. Aussi, le type 2 augmente de manière très forte depuis 2 ans. L'analyse de 2026 permettra de voir si la situation empire ou s'améliore. Les opérateurs qui se retrouvent dans ces catégories sont sujets à des *SPOF*, le risque en cas de défaillance de leur fournisseur est une isolation totale du reste de l'Internet.

1.4.3.2 IPv6

Les AS français ont aussi été étudiés sous l'aspect IPv6. La méthode d'extraction de données et de classification en IPv6 est la même que pour IPv4. La figure 1.15 illustre les tendances comme dans la section précédente.

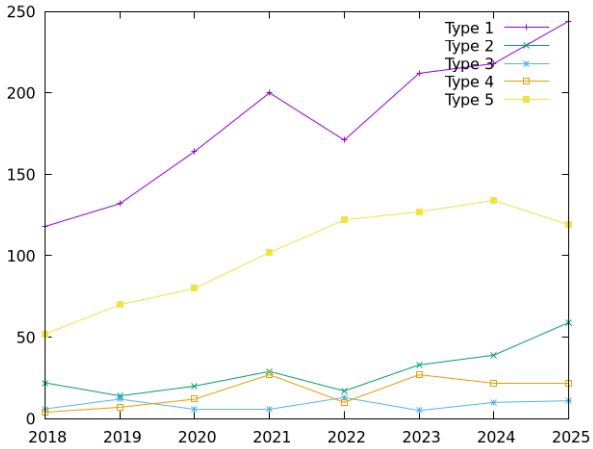


Figure 1.15 – Distribution des AS français impactés par des AS pivots en IPv6

Même si les profils des courbes semblent proches de celles étudiées en IPv4, des différences notables se dégagent. Les AS de type 1 en IPv6 ont suivi une progression similaire à IPv4 de 2018 à 2023. La tendance change en IPv6 à partir de 2024. En IPv4 nous avons pu constater une stabilisation du nombre d'AS dans cette catégorie. En IPv6 la tendance part, quant à elle, à la hausse. Toutefois, ne raisonner qu'en valeur absolue sans prendre en compte le nombre d'AS concernés pour la période biaise l'analyse. Pour amener un autre éclairage, le tableau 1.4 résume les évolutions du type 1 pour IPv4 et IPv6 en termes de proportions, c'est-à-dire en présentant le rapport du nombre d'AS dans le type 1 sur le nombre total d'AS visibles pour la période donnée.

Année	Nombre d'AS IPv6	Nombre d'AS IPv4
2018	22 %	28 %
2019	25 %	29 %
2020	28 %	31 %
2021	24 %	34 %
2022	26 %	26 %
2023	29 %	30 %
2024	27 %	29 %
2025	27 %	32 %

Tableau 1.4 – Proportion d'AS de type 1 en IPv4 et IPv6

Ce tableau met plusieurs éléments en lumière. Tout d'abord la proportion de type 1 en IPv6 est plus importante que celle d'IPv4, excepté pour l'année 2022. De plus, pour l'évolution des AS faisant partie du type 1, la tendance est moins forte que la courbe de la figure 1.15 semble indiquer. Certes une augmentation est visible, mais elle est bien moindre que celle observée en 2021. La situation s'avère moins critique que redouté.

Pour les AS de type 2, la courbe ressemble très fortement à celle d'IPv4. Néanmoins en termes de proportion, les valeurs sont plus importantes en IPv6 qu'en IPv4. La tendance à une augmentation importante en 2025 est constatée pour les deux protocoles. Mais en IPv6 nous parlons de 59 AS, quand en IPv4 cela concernait 90 AS. En termes de proportion, 6 % des AS visibles entrent dans le type 2 en IPv4. En IPv6 8 % des AS visibles sont dans cette catégorie. Comme pour IPv4, l'analyse de l'année 2026 permettra de mieux savoir où seront redistribués les AS de cette catégorie en IPv6.

Le type 3 représente une très faible proportion des AS en IPv6, qui changent d'opérateur de transit en cours d'année et présentent en permanence une situation de pivot. Entre 5 et 13 AS s'ajoutent à cette catégorie sur la période étudiée.

Le type 4 évolue peu mais représente une proportion plus importante qu'en IPv4. Quelque 22 AS terminent dans le type 4 au cours des deux dernières années analysées, ce qui représente une plus grande proportion que pour IPv4 mais pour lesquelles, comme le montre le tableau 1.5, les AS IPv6 restent moins longtemps concernés par cette problématique.

Récurrence	Nombre d'AS	Proportion
1 fois	76	77 %
2 fois	16	16 %
3 fois	5	5 %
4 fois	2	2 %

Tableau 1.5 – Nombre d'années consécutives pour les AS français de type 4 en IPv6

Enfin pour les AS de type 5, c'est-à-dire ceux pour lesquels la situation s'améliore dans le temps, le nombre d'AS concernés chaque année augmente quasiment linéairement, avec une exception pour 2025 où cela décroit légèrement. En 2018 cela concernait 52 AS, en atteignant au plus haut 134 AS en 2024 et pour finir à 119 AS en 2025. Ces chiffres sont assez encourageants et compensent en partie l'augmentation du nombre d'AS que l'on retrouve dans le type 1.

À RETENIR

Les tendances IPv6 sur les AS concernés par des pivots sont similaires en certains points à celles d'IPv4 tout en ayant des particularités qui poussent à mener des analyses dédiées à IPv4 et IPv6. Les proportions d'AS concernés par des pivots sont plus importantes en IPv6, c'est pour cette raison que l'observatoire encourage les opérateurs à prendre cet élément en compte.

1.4.4 Impact de la disparition d'un AS pivot

Pour des raisons de concision dans cette partie du document, nous adoptons une formulation spécifique pour les AS pivots. Lorsque nous parlons d' « AS pivot à 4 », cela signifie que la disparition de l'AS pivot entraine la perte de connectivité à Internet pour 4 AS.

Après avoir analysé les AS français directement, nous nous concentrons sur ces AS qui, par leur disparition, auront un impact significatif sur les AS français.

1.4.4.1 IPv4

Afin de pouvoir présenter les données de manière la plus lisible possible, le choix a été fait dans un premier temps de ne représenter dans la figure 1.16 que les chiffres pour les AS pivots à 1 jusqu'aux AS pivot à 10.

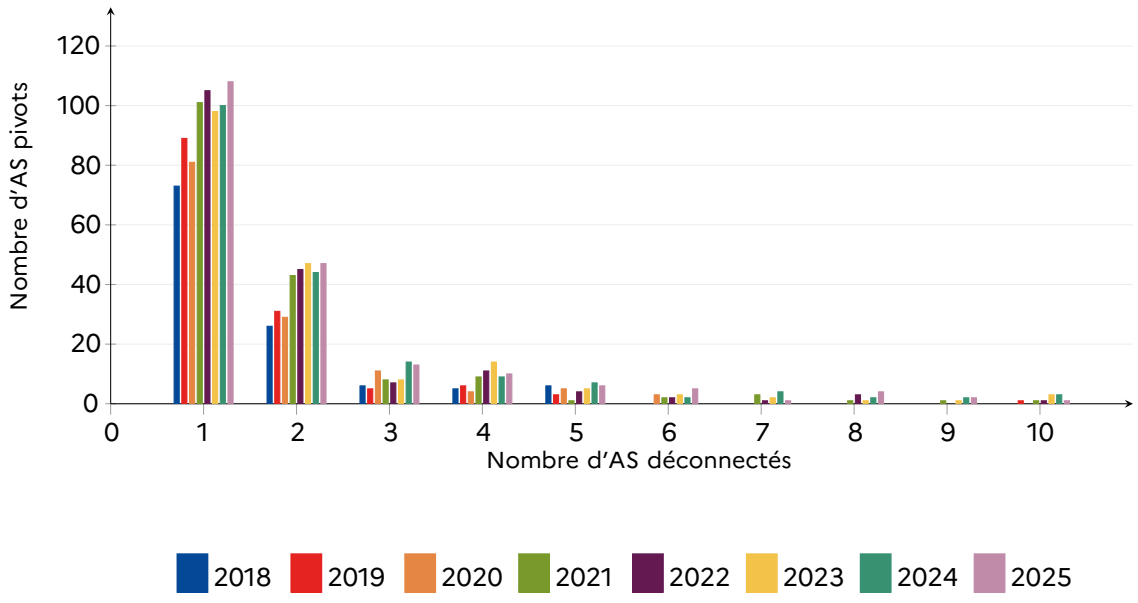


Figure 1.16 – AS pivots en fonction du nombre d'AS déconnectés (IPv4)

Il apparait que les valeurs croissent significativement pour les années 2018 à 2021 sur les AS pivots à 1 à 2 AS. Ces valeurs se stabilisent à partir de 2022 jusqu'à 2025. À partir de 2022, nous notons une faible croissance du nombre d'AS pivots de 3 à 10.

Pour les AS pivots à 10+, c'est-à-dire déconnectant plus de dix AS de l'Internet, les données sont présentées dans le tableau 1.6. Afin de pouvoir suivre l'évolution d'un AS pivot au fil des années, chaque AS pivot se voit attribuer une lettre. Cette attribution a pour but d'anonymiser ces résultats. Chaque AS pivot est suivi du nombre d'AS « FR » qu'il déconnecte s'il disparait. L'avant-dernière ligne additionne le nombre d'AS pivots total pour l'année en ajoutant les données de la figure 1.16. De plus, pour chaque entrée du tableau une couleur est associée. La couleur noire est pour les AS pivots « FR », le bleu pour les AS hors UE. Il est à noter que pour la période analysée, aucun AS pivot 10+ est un AS de l'UE, raison pour laquelle aucun n'est représenté dans le tableau 1.6.

	2018	2019	2020	2021	2022	2023	2024	2025
	A→11	**G→11**	B→12	J→12	I→11	M→11	J→13	O→11
	B→12	B→12	I→14	B→14	**G→13**	B→12	B→13	P→13
	C^{hce}→12	**C→15**	E→20	K→15	L→14	**N→13**	K→14	H→17B
	D→15	D→20	**C→22**	**G→17**	**C→19**	K→17	H→19	**C→19**
	E→19	E→20	D→23	D→17	K→20	**C→19**	**C→20**	E→23
	F→25	A→11	A→32	I→17	D→25	J→21	E→25	D→30
	G→27	F→35	H→39	E→21	E→25	E→23	D→28	A→31
	H→29	H→37	F→40	**C→22**	A→32	D→26	A→30	**G→43**
			G→45	A→23	H→32	A→27	F→46	F→47
				F→29	F→37	H→28		
				H→34		F→43		
						G→48		
∑ AS pivots	124	143	142	181	189	194	196	206
∑ AS pivots 10+	150	177	247	221	228	288	208	234

Tableau 1.6 – AS pivots à 10+ et nombre d'AS qu'ils déconnectent (IPv4)

Le tableau 1.6 permet de voir que l'AS H qui est l'AS pivot le plus important en 2018 avec 29 AS déconnectables reste dans les plus important jusqu'en 2023. En 2024, son importance se réduit pour terminer à 17 en 2025. Nous voyons aussi que l'AS G, hors UE, a une emprise qui change d'une année à l'autre. En 2020 et 2023 c'est l'AS pivot le plus important.

Globalement, sur la période analysée, le nombre d'AS pivot a quasiment tout le temps augmenté. Le nombre d'AS pivots à 10+ en revanche ne suit pas cette logique et le nombre maximum d'AS pivot à 10+ est atteint en 2023 avec 12 AS. C'est cette année où le maximum d'AS impactés par ces AS pivots 10+ a été atteint, où 288 AS se concentrent derrière ces 12 acteurs.

En 2024, alors que le nombre d'AS total visibles sur Internet n'a pas diminué mais crû, la quantité d'AS concernés par des AS pivots à 10+ est passée de 288 à 208. Diminuant la concentration des AS autour des mêmes acteurs.

2025 a en revanche vu la situation se dégrader légèrement par rapport à 2024 où 26 AS se sont ajoutés aux AS dépendants d'AS pivots à 10+.

À RETENIR

Le nombre d'AS potentiellement concernés par les grands AS pivots à 10+ a globalement diminué après avoir atteint son apogée en 2023.

1.4.4.2 IPv6

Pour faciliter la lecture nous avons produit, pour cette partie IPv6, les mêmes types de figures et tableaux que pour IPv4.

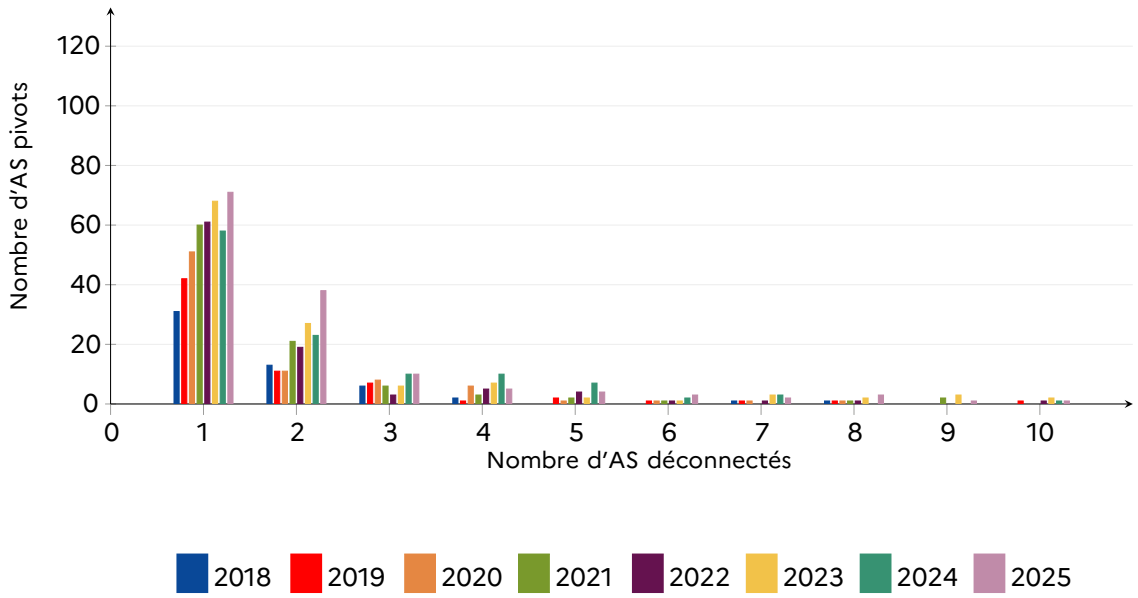


Figure 1.17 – AS pivots en fonction du nombre d'AS déconnectés (IPv6)

La figure 1.17 montre la distribution du nombre d'AS pivots à moins de 10. La tendance sur les AS pivots à 1 ne ressemble pas à celle observée en IPv4. La quantité d'AS pivots à 1 a continué d'augmenter significativement jusqu'en 2023, avec une légère baisse à 58 en 2024 puis à nouveau une hausse à 71 en 2025. A contrario les AS pivots à 2, après avoir été stables jusqu'en 2020, ont crû jusqu'à atteindre le nombre de 38 en 2025.

	2018	2019	2020	2021	2022	2023	2024	2025
	A→11	E→16	B→13	F→12	I→11	J→11	K→11	F→13
	B→13	C→22	E→19	E→13	C→12	C→12	F→13	M→13
	C→20	**D→24**	**D→25**	C→13	H→13	H→13	E→14	B→14
	D→26		C→25	B→14	E→13	B→16	H→15	E→17
				G→14	B→19	**D→23**	B→15	**D→19**
				D→27			L→15	J→30
				H→28			M→17	
				I→31			J→30	
∑ AS pivots	58	70	84	104	101	126	122	144
∑ AS pivots 10+	70	62	82	152	68	80	130	112

Tableau 1.7 – AS pivots à 10+ et nombre d'AS qu'ils déconnectent (IPv6)

Le tableau 1.7 nous donne les chiffres pour les AS pivots à 10+. L'année 2021 se dégage nettement avec l'apparition d'AS pivots qui ont un très fort impact sur leurs AS clients. Ceci fait écho au diagramme 1.10 de la section 1.3.2.4. En effet, dans ce diagramme nous avons observé un pic important de nouveaux AS français en 2021 avec une chute importante l'année suivante, visible dans le diagramme 1.11. Le nombre d'AS pivots total qui était de 84 l'année précédente passe à 104 en 2021 pour se stabiliser à 101 en 2022. Le pic de 2021 est dû à des activités d'interconnexions sur un réseau national universitaire qui ont pris place sur deux périodes. La première période est du 18 mai 2021 au 17 septembre 2021 et la seconde du 25 septembre 2021 au 2 octobre 2021. Ces AS qui ont été alors vus comme dépendants d'AS pivots sur cette période ont disparu et n'ont pas été actifs depuis. Cela permet de comprendre pourquoi en 2022, le nombre d'AS IPv6 qui se sont ajoutés, comme vu dans le tableau 1.1, n'ont été que de 9 alors que la tendance chaque année était de l'ordre de la centaine. En effet, de nombreux AS universitaires sont apparus en 2021 puis ont disparu par la suite, faussant la tendance et donnant l'impression d'une stagnation. Le nombre de nouveaux acteurs IPv6 qui sont arrivés sur le réseau a été masqué par la brusque disparition de ces plus de soixante AS universitaires.

L'AS D qui est un AS hors UE est un acteur majeur, et plus particulièrement dans la situation étudiée ici. Durant trois années il a été l'AS pivot à 10+ le plus important et a occupé une place majeure le reste du temps (il s'agit de l'AS G vu dans le tableau 1.6). Cet AS a une importance particulière que ce soit en IPv4 comme en IPv6.

L'AS J qui est apparu dans les AS pivots à 10+ en 2022 a pris une place de plus en plus prépondérante pour occuper la place d'AS pivot le plus important pour IPv6 en 2025. Dans le tableau 1.6, il s'agit de l'AS A qui a une place assez importante dans les AS pivots à 10+ dès 2019.

Le nombre d'AS pivots total s'est intensifié sur toute la période, exception faite pour 2022 et 2024. En revanche la concentration autour des mêmes acteurs (pivots à 10+) fluctue de manière importante et semble décorrélée. Ce point est rassurant d'un certain côté car même si le nombre d'AS pivots total augmente, la concentration autour de certains AS pivots à 10+ ne suit pas cette tendance.

À RETENIR

Les AS J et D du tableau 1.7 ont un impact important sur les AS concernés par des AS pivots. Ces AS revêtent une importance pour l'Internet français car leur impact ne se limite pas à IPv6 mais porte aussi sur IPv4.

1.5 Concentration des AS

Après nous être penchés sur les risques de déconnexion des AS français nous nous intéressons ici à la centralisation des chemins, c'est-à-dire des AS qui seraient de manière répétée sur le chemin des échanges entre AS français. En 2012 le BSI publiait un article [23] sur l'étude de la structure de l'Internet allemand. Nous avons décidé de reprendre un des éléments de ce document : la *betweenness centrality* ou la centralité d'intermédiarité [24] en français. L'objectif de cette analyse est de mettre en exergue des AS dans le graphe qui sont fréquemment utilisés dans les calculs de plus court chemin entre les nœuds. L'opportunité de faire une étude plus complète en intégrant l'hégémonie d'AS [25] pourrait être étudiée ultérieurement.

Comme pour la partie précédente sur les AS pivots, les graphes cumulatifs hebdomadaires ont été utilisés. À partir de ces derniers, le calcul des plus courts chemins a été fait pour chaque AS français à destination de chaque AS français. À partir de ces résultats le calcul de centralité d'intermédiarité a été fait et nous avons conservé pour chaque semaine les 300 premiers AS.

Ces analyses ont été menées de manières indépendantes pour IPv4 et IPv6.

1.5.0.1 IPv4

Les résultats pour les AS représentant des nœuds de concentration importants en IPv4 sont classés du plus au moins important dans le tableau 1.8. Comme pour la partie précédente, des lettres ont été attribuées aux AS afin de les anonymiser. En bleu sont représentés les AS étrangers qui sont hors de l'Union européenne. Ce tableau permet de se rendre compte de la dépendance à des AS de transits étrangers. L'AS A tient la tête du tableau tandis que le C passe de la 3ème place en 2018 à la 7ème en 2025. L'AS F en revanche est passé de la 6ème en 2018 pour terminer 2ème en 2025. Enfin l'AS J a disparu dès 2020 du top 10 et l'AS M lui fait sa première apparition en 2025 à la 8ème place. En ce qui concerne les AS français que l'on retrouve ici, nous notons que l'AS I a progressé au fil des années en passant de la 9ème place en 2018 à la 3ème en 2025.

23. https://link.springer.com/chapter/10.1007/978-3-642-28537-0_20
24. https://fr.wikipedia.org/wiki/Centralit\%C3\%A9
25. https://www.iijlab.net/en/members/romain/pdf/romain_pam2018.pdf

Position	2018	2019	2020	2021	2022	2023	2024	2025
1	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**
2	B	B	B	B	B	B	**F**	**F**
3	**C**	**C**	**F**	**F**	**F**	**F**	B	I
4	D	**F**	E	E	E	I	I	B
5	E	E	**C**	**C**	I	E	E	D
6	**F**	D	D	D	**C**	**C**	**C**	E
7	G	G	H	I	D	D	D	**C**
8	H	I	I	H	G	G	H	H
9	I	H	G	G	H	H	G	**M**
10	**J**	**J**	K	K	K	L	L	G

Tableau 1.8 – AS dans l'ordre d'importance en centralité d'intermédiarité en IPv4

À RETENIR

La dépendance aux AS en IPv4 met en évidence deux opérateurs de transit hors UE qui se retrouvent fréquemment dans la communication de certains AS français vers d'autres. Ces AS concentrateurs deviennent un point de vigilance car ils sont au cœur des échanges entre AS français et une panne sur leur infrastructure aurait un retentissement important sur l'Internet français.

1.5.0.2 IPv6

Les extractions pour la centralité d'intermédiarité ont aussi été réalisées en IPv6 et sont présentées dans le tableau 1.9. En plus du bleu qui correspond aux AS hors Union européenne, le violet a été ajouté et correspond à un AS issu de l'UE non français.

Comme pour IPv4, une dépendance à des opérateurs hors UE se dégage. Néanmoins, quand en 2018 les AS B et C occupaient respectivement la 2ème et 3ème place, ils se retrouvent en 1ère et 8ème place en 2025. Même si l'opérateur B occupe une place plus importante, en 2025 l'opérateur C a fortement reculé. L'AS P qui est apparu en 2022 à la 9ème place se retrouve à la 2ème place en 2025. Enfin, quand quatre opérateurs hors UE étaient dans le classement en 2018, ils ne sont plus que trois en 2025.

Position	2018	2019	2020	2021	2022	2023	2024	2025
1	A	A	A	**B**	**B**	**B**	**B**	**B**
2	**B**	**B**	**B**	A	A	D	D	P
3	**C**	**C**	**C**	D	D	A	A	D
4	D	D	G	**C**	**C**	G	E	A
5	E	G	D	G	G	**C**	Q	G
6	F	F	F	F	F	F	F	F
7	G	E	E	L	**M**	Q	O	**M**
8	**H**	**I**	**I**	E	O	**M**	P	**C**
9	**I**	**J**	L	**M**	P	E	**C**	O
10	J	K	K	N	Q	O	G	E

Tableau 1.9 – AS dans l'ordre d'importance en centralité d'intermédiarité en IPv6

À RETENIR

L'indépendance pour les communications entre AS français est dans une meilleure situation en IPv6 qu'en IPv4. Il est à noter que l'AS A de l'étude précédente et l'AS B de cette partie sont le même opérateur.

1.6 Conclusion

Cette nouvelle édition du rapport a été l'occasion de concentrer les travaux sur les indicateurs BGP autour de la RPKI, de l'évolution des AS français et du graphe de l'Internet français de 2018 à 2025.

Deux points importants sont rappelés à propos de la RPKI. Le premier est de s'assurer de la bonne déclaration des ROA en évitant de couvrir des préfixes plus spécifiques que /24 en IPv4 et /48 en IPv6, en accord avec les bonnes pratiques admises par la communauté. L'expérimentation a montré que cette bonne pratique mérite d'être rappelée. Le second est le risque associé à des ROA couvrant des préfixes trop spécifiques, comme le souligne la RFC 9319 [39]. En effet, cela permet à des attaquants de se faire passer pour l'AS visé et de détourner du trafic. L'attaque menée contre Softaculous [26] est un rappel important de ce risque.

Pour l'évolution des AS, un des premiers éléments marquants est le nombre d'AS IPv6 qui a quasiment doublé sur cette période en passant de 411 AS en 2018 à 764 AS en 2025, confirmant que l'adoption de ce protocole continue de prendre de l'ampleur. Quand en 2018, 398 des AS étaient simultanément IPv4 et IPv6 sur 1144 AS visibles, ils étaient 663 sur 1410 fin 2025. Aussi, les AS exclusivement IPv4 déclinent même s'ils représentent encore aujourd'hui une part importante des AS français. Ils représentaient respectivement 65 % des AS visibles en 2018 et 53 % en 2025.

26. https ://www.softaculous.com/blog/security-incident-bgp-hijacking-update/

Concernant la connectivité des AS, une nouvelle méthodologie a été appliquée. Dans les éditions précédentes un graphe annuel cumulatif des liens entre AS servait à établir la liste des AS soumis à des pivots et la liste des AS pivots. Les analyses ont été menées sur des graphes hebdomadaires cumulatifs, permettant de retirer des faux positifs et d'améliorer la confiance dans les résultats. Il faut être vigilant quant aux résultats sur la typologie des AS soumis à des pivots : les AS soumis à un pivot toute l'année (type 1) augmentent en nombre comme en proportion. Les AS qui acquièrent un pivot (type 2) connaissent une forte croissance depuis 2024, sans que l'amélioration des AS de type 5 ne contrebalance entièrement cette tendance. Ces augmentations ne sont pas contrebalancées par la croissance de l'Internet français. Les proportions d'AS concernés par des pivots continue d'augmenter d'année en année. Cette situation tend à se dégrader au fil des années, que ce soit en IPv4 comme en IPv6. Pour les AS pivots en eux-mêmes, leur nombre total a augmenté de manière quasiment continue, mais au fil des années la concentration des AS français autour des mêmes AS pivots diminue en IPv4, atténuant l'impact de la perte de l'un d'entre eux. Ce constat est encourageant.

Le dernier indicateur BGP est nouveau dans l'observatoire et s'attelle à identifier des nœuds dans le graphe de l'Internet français qui concentrent les communications d'opérateurs français entre eux, la centralité d'intermédiarité. Deux opérateurs de transit d'importance et hors union européenne se dégagent en IPv4. C'est l'un d'entre eux qui se retrouve en IPv6, où il est l'opérateur le plus important.

Il n'est toutefois pas un pivot important identifié dans l'indicateur précédent, ce qui diminue son impact en cas de panne, mais cela fait de lui un opérateur important dans le quotidien des échanges dans l'Internet français. L'observatoire rappelle aux opérateurs l'importance de diversifier leur transit avec des opérateurs européens et de surveiller les annonces de leurs propres préfixes afin de détecter au plus tôt d'éventuelles usurpations ou détournements de trafic.

Ce rapport s'est concentré sur la structure même de l'Internet au travers des interconnexions des opérateurs entre eux. Lors des travaux futurs, l'observatoire reprendra les études autour des préfixes et des données issues des IRR tout en prenant en compte les indicateurs relatifs à la connectivité des AS et de la RPKI.

Chapitre 2
Résilience sous l'angle du protocole DNS

2.1 Introduction

Le système de noms de domaine, géré par le protocole DNS [18, 19], est un système de nommage distribué et hiérarchique dont l'objectif principal est d'associer à une adresse IP un nom lisible par les utilisateurs. Ainsi, le nom `www.afnic.fr` permet de retrouver l'adresse IP 51.178.83.21. Dans le cas d'un changement d'hébergeur, seul le responsable du domaine doit modifier l'adresse IP pointée par le nom. Grâce au DNS, ce changement est donc transparent pour les utilisateurs.

La structure du DNS est illustrée dans la figure 2.1. Au sommet de la hiérarchie se trouve la racine représentée par un point « . ». Il s'agit du point final que l'on retrouve au niveau des noms de domaine comme « `www.afnic.fr.` » . Les noms juste en dessous de la racine, comme .fr, sont appelés des noms de premier niveau (TLD).

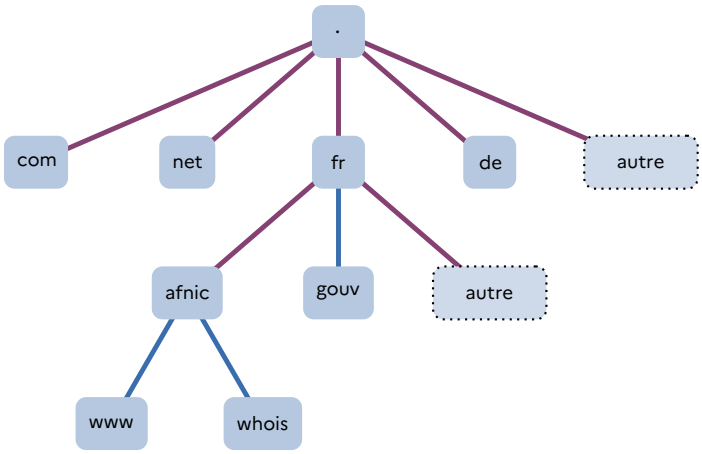


Figure 2.1 – Structure du DNS

À chaque niveau se trouvent un ou plusieurs nœuds de l'arbre DNS. L'arborescence issue d'un nœud donné est appelée domaine. Elle peut avoir à son tour des sous-domaines, et ainsi de suite.

La gestion d'un sous-domaine peut être « déléguée », c'est-à-dire confiée à un organisme différent de celui qui administre le domaine parent. À titre d'exemple, `.fr` a été délégué à l'Afnic, qui fixe les règles d'attribution des noms de domaine sous `.fr` indépendamment de la racine gérée par l'IANA, son domaine parent. Les délégations sont illustrées par des liens violets dans la figure 2.1.

Au sens strict, une zone désigne la partie d'un domaine gérée par une même entité, en dehors des sous-domaines délégués. Cette distinction n'ayant pas d'incidence sur les analyses présentées, ce rapport emploiera indifféremment les deux termes.

2.1.0.1 Informations stockées dans le DNS

Les ressources attachées à une zone sont décrites par des enregistrements DNS. Chaque enregistrement comporte un nom de domaine qui se décline à partir de celui de la zone (exemple : le nom `www.afnic.fr` sous la zone `afnic.fr`), un type et des données qui dépendent du type en question.

Les différents types d'enregistrement DNS sont publiés et maintenus par l'IANA [9] dans un registre dédié aux paramètres du DNS [9]. Les types d'enregistrement suivants sont étudiés dans ce rapport :

- A : une adresse IPv4 ;
- AAAA : une adresse IPv6 ;
- MX : le nom d'un relais de messagerie électronique entrant ;
- NS : le nom d'un serveur DNS ;
- Delegation Signer (DS) et DNSKEY : des informations cryptographiques utiles pour Domain Name System Security Extensions (DNSSEC).

2.1.0.2 Résolution DNS

La résolution DNS est le mécanisme qui permet de récupérer les enregistrements associés à un nom de domaine pour un type donné. Ce mécanisme de résolution fait intervenir deux types de serveurs DNS, comme l'illustre la figure 2.2, mettant en évidence des interactions ordonnées et numérotées :

- **un résolveur récursif** (ou plus communément appelé « résolveur »). La machine de l'utilisateur le connaît et lui soumet ses requêtes DNS (interaction 1). Ce serveur, habituellement géré par un Fournisseur d'Accès à l'Internet (FAI), interroge l'arborescence DNS en partant de la racine (interaction 2) et en suivant de proche en proche les points de délégation jusqu'au serveur faisant autorité pour le nom de domaine objet de la requête (interactions 3-4). Enfin, le résolveur récursif répond à la machine de l'utilisateur (interaction 5) et conserve en mémoire (fonction de cache) les informations reçues ;
- **des serveurs de noms faisant autorité** pour des zones données, qui répondent au résolveur récursif. Dans ce cas, s'ils font effectivement autorité pour le nom de domaine demandé par le résolveur récursif, ils lui retournent alors une réponse ; sinon, ils l'aiguillent vers d'autres serveurs de noms à interroger qui seraient plus susceptibles de faire autorité pour le nom de domaine recherché.

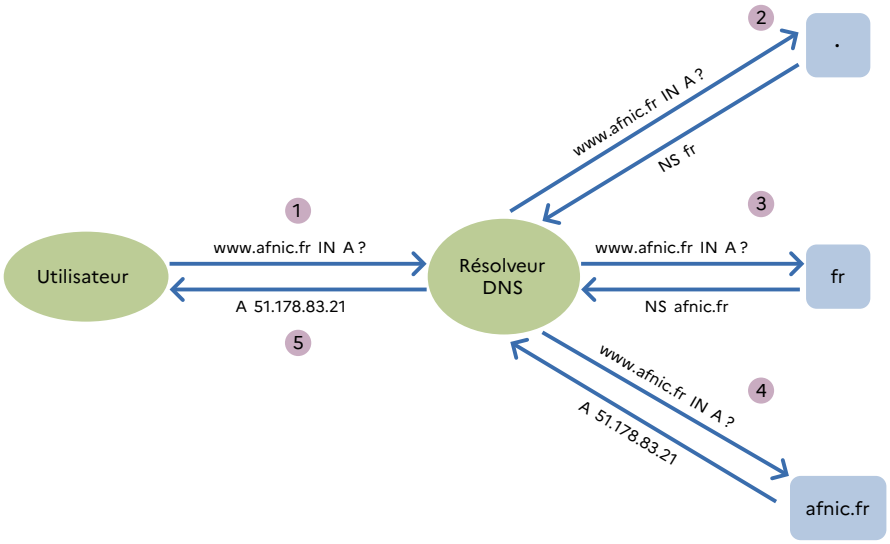


Figure 2.2 – Exemple de résolution DNS

2.1.0.3 Juridiction technique des noms de domaine

Les enregistrements DNS de type NS et MX contiennent des noms de serveur, comme illustré dans la figure 2.3. Le nom à gauche du type de l'enregistrement, ici `domaine-exemple.fr`, est l'emplacement dans l'arbre DNS de cet enregistrement. Le nom à droite du type, comme ici `ns1.domaine-exemple.fr`, est la donnée. Les noms à droite doivent généralement être résolus en adresses IP par un serveur récursif afin de répondre aux attentes d'un utilisateur du DNS.

```
domaine-exemple.fr    NS    ns1.domaine-exemple.fr
domaine-exemple.fr    NS    ns2.hebergeur-dns.fr
domaine-exemple.fr    NS    ns3.hebergeur-dns.example
```

Figure 2.3 – Exemples d'enregistrements NS et MX

Dans un enregistrement DNS, lorsque le nom à gauche du type est inclus dans le nom à droite, le nom de droite est dit être dans la « juridiction technique ». Par exemple, `ns1.domaine-exemple.fr` est dans la juridiction technique de `domaine-exemple.fr`. Le serveur renvoyant un tel enregistrement NS ou MX peut alors aussi répondre l'adresse IP correspondant au nom. Parfois, cela est même exigé par le protocole.

À l'inverse, les noms de serveur peuvent être situés dans un domaine tiers. Ils sont alors en-dehors de la juridiction technique. C'est le cas de l'enregistrement NS utilisant ns2.hebergeur-dns.example pour déléguer le nom de domaine `domaine-exemple.fr` dans la figure 2.3.

Les noms hors juridiction technique peuvent introduire une dépendance au bon fonctionnement d'un domaine tiers. En effet, chacun constitue un point de défaillance unique, ou Single Point of Failure (SPOF), si son dysfonctionnement peut causer l'impossibilité de résoudre un nom en adresse IP. La notion de degrés de dépendance quantifie le nombre de SPOF. Certains tiers sont indispensables et sont donc exclus de ce compte. Il s'agit notamment des zones parentes d'un nom, comme, par exemple, la racine ou `.fr` pour le nom `afnic.fr`.

Ainsi, à titre d'exemple, `domaine-exemple.fr` aurait un seul degré de dépendance si ce domaine était délégué à un serveur DNS dans le domaine `bonjour.example` et à un autre serveur dans le domaine `bonsoir.example`. En effet, la panne de `bonjour.example` pourrait être compensée par la disponibilité de `bonsoir.example` et inversement. Le seul SPOF serait alors `.example`. De même, `domaine-exemple.fr` aurait un degré de dépendance de deux s'il était uniquement délégué avec des noms de serveur faisant partie du domaine `bonjour.example`. En effet, le bon fonctionnement des serveurs de deux acteurs serait requis : ceux de `.example` et ceux de `bonjour.example`.

Le risque d'indisponibilité d'un TLD n'est pas juste théorique. Par exemple, en Mai 2026, le TLD `.de` a subi une panne pendant près de 3 heures [6], période pendant laquelle l'ensemble des noms de domaine sous ce TLD étaient inaccessibles pour la plupart des utilisateurs.

2.1.0.4 Noms de domaine publics

Dans ce rapport, le terme « noms de domaine publics » désigne les noms de domaine délégués depuis un des domaines définis dans une liste, appelée Public Suffix List (PSL) [15]. Celle-ci provient d'une initiative de Mozilla pour renforcer le cloisonnement logique des sites web dans les navigateurs. Cette liste, bien que n'ayant pas un rapport direct avec le DNS, permet de référencer les domaines gérés par des entités se comportant comme des registres. Cette information n'est pas systématiquement visible dans le DNS. En effet, certains registres n'opèrent pas toujours des noms de domaine constitués d'un seul composant. C'est le cas notamment du registre Nominet, responsable de `.co.uk`.

2.1.0.5 Sécurité des enregistrements

Conçu à une époque où les menaces d'usurpation ou de falsification des échanges numériques étaient moins prégnantes, le DNS ne bénéficiait pas de mécanismes de sécurité avancés lors de sa création, notamment pour garantir l'intégrité des réponses. Le protocole DNSSEC vise à remédier à ce manque. Il s'appuie sur la cryptographie asymétrique pour assurer l'authenticité et l'intégrité des données : les clés publiques sont stockées dans des enregistrements DNSKEY, tandis que les signatures numériques sont enregistrées dans des RRSIG. La chaîne de confiance est maintenue grâce aux enregistrements DS, publiés dans la zone parente. Grâce à ces mécanismes, un résolveur dit « validant » peut ainsi vérifier l'origine et l'intégrité des réponses DNS, rejetant ainsi les enregistrements frauduleux et protégeant efficacement contre les attaques dites d'« empoisonnement de cache ».

2.1.1 Données et outils

Les données proviennent d'un logiciel de type robot d'indexation, développé entièrement par l'Afnic, permettant de réaliser des mesures actives des zones DNS. La bibliothèque Python `dnspython` [4] est notamment utilisée à cette fin.

Les serveurs faisant autorité pour les zones déléguées de `.fr` sont interrogés au travers de résolveurs locaux Unbound [14], appliquant leur algorithme de résolution habituel. Lorsque plusieurs serveurs faisant autorité existent pour un même nom de domaine, le serveur interrogé est alors choisi aléatoirement, afin de limiter la charge imposée par la campagne de mesures.

2.1.1.1 Données utilisées

Les noms de domaine dont les réponses sont invalides ou n'ayant pas répondu à nos requêtes ne sont pas comptabilisés dans les statistiques. Ils constituent un biais de près de 5,8 % des noms de domaine délégués de la zone `.fr` en Juin 2026.

Les mesures actives ont été réalisées en utilisant la zone `.fr` qui varie au gré des créations, suppressions et modifications de zones déléguées. Lors de l'analyse, seules les zones pour lesquelles l'ensemble des mesures ont pu être conduites sans échec, sont comptabilisées. Elles sont appelées les « zones étudiées ». Ainsi, en 2026, le nombre de ces zones est de 4 219 051 au 10 Juin 2026.

Concernant les données de géolocalisation, la base de données Geolite de Maxmind [11] a été utilisée et téléchargée en Juillet 2026.

2.2 Dispersion des serveurs de noms faisant autorité

2.2.1 Nombre de serveurs de noms faisant autorité

Le nombre d'enregistrements NS par zone étudiée reste suffisant pour permettre une bonne résilience, du point de vue de cet indicateur. En effet, un nombre presque négligeable de zones 0,06 % n'utilisent qu'un seul enregistrement NS, qui pourrait donc constituer un SPOF.

Nombre d'enregistrements NS	Pourcentage de domaines
1	0,06
2	61,43
3	15,07
4	16,80
5+	6,64

La même étude peut être effectuée, une fois les noms de serveurs contenus dans les enregistrements NS résolus en adresse IP. Leur répartition protocolaire est la suivante :

Protocole	Pourcentage d'enregistrements NS
IPv4	54,10
IPv6	45,90

En IPv4, la répartition est sensiblement équivalente à celle observée lors de l'étude des enregistrements NS. Seule une infime part des zones étudiées ne dispose pas d'adresses IPv4 pour leurs serveurs de noms faisant autorité :

Nombre d'adresses IPv4	Pourcentage de domaines
0	<0,01
1	0,42
2	58,99
3	15,29
4	17,44
5+	7,86

En IPv6, la situation est différente. Environ 83 % des zones étudiées disposent d'au moins une adresse IPv6. Cependant, près de 17 % n'en ont pas, et dépendent alors de la disponibilité IPv4 pour leurs serveurs de noms :

Nombre d'adresses IPv6	Pourcentage de domaines
0	17,07
1	1,52
2	44,42
3	13,10
4	17,45
5+	6,44

À RETENIR

La résilience des serveurs de noms faisant autorité est satisfaisante, avec plus de 99,9 % des zones disposant d'au moins deux enregistrements NS. Leur répartition entre IPv4 et IPv6 est globalement équilibrée, reflétant une nette progression du déploiement d'IPv6 depuis le dernier rapport, avec environ 17 % des zones n'étant accessibles qu'en IPv4 uniquement.

2.2.2 Dispersion topologique

La dispersion topologique des serveurs de noms est une exigence issue de l'ingénierie de la résilience [21, 12]. La dispersion des serveurs de noms dans des AS distincts peut, dans certains cas, contribuer à éviter des indisponibilités en cas d'incident ayant un impact sur la totalité du réseau d'un opérateur. En 2026, près de 80 % des zones déléguées sont hébergées dans un seul AS :

Nombre d'AS	Pourcentage de domaines
1	79,73
2	16,24
3	3,26
4	0,72
5+	0,05

À RETENIR

La quasi-totalité des zones disposent d'au moins deux serveurs de noms, mais ceux-ci restent généralement hébergés dans un seul AS : c'est le cas de près de 80 % des zones, contre 83 % en 2016. La dispersion topologique ne progresse donc que très lentement, et une part importante des zones reste exposée à un risque d'indisponibilité en cas d'incident affectant l'opérateur qui les héberge.

2.2.3 Dispersion géographique

La dispersion géographique des serveurs de noms faisant autorité peut avoir un impact sur la disponibilité des services de l'Internet français. Par exemple, cela peut être le cas à la suite d'une rupture de câbles sous-marins isolant les utilisateurs d'un service des serveurs de noms renseignant l'adresse IP à contacter.

En utilisant la base GeoLite de Maxmind [11], il est possible d'estimer la géolocalisation des serveurs faisant autorité sur les zones étudiées. Cette pratique présente néanmoins un intérêt limité si la technique de routage *anycast* est employée. En effet, dans ce cas, l'adresse IP géolocalisée dans un pays sera annoncée avec BGP depuis plusieurs endroits dans le monde. Cet indicateur permet néanmoins d'obtenir une première approximation de l'emplacement de ces serveurs.

En 2026, le nombre de zones étudiées étant servies exclusivement par des serveurs faisant autorité situés dans un même pays a diminué par rapport à 2016. Ce phénomène est observé tant en IPv4 qu'en IPv6, où il est bien plus important pour ce dernier. Ainsi, en IPv4 ce taux est passé de 80 % à 73,4 %, et en IPv6 de 81 % à 60,1 %.

Si l'on regarde maintenant les zones étudiées étant servies exclusivement par des serveurs de noms faisant autorité situés en France, celles-ci s'élèvent à 45,9 % en IPv4 et 42,9 % en IPv6.

Enfin, les zones étudiées dont tous les serveurs de noms faisant autorité sont accessibles en IPv4 et se situent dans un même pays étranger sont de 38,8 %, contre 28 % en 2016. Et en IPv6, ce chiffre est de 30,4 %, contre 31 % en 2016.

Le tableau ci-dessous présente la répartition des zones étudiées selon le nombre de pays dans lesquels se situent les serveurs de noms faisant autorité. Il est à noter qu'un nombre de pays égal à 0 signifie que tous les serveurs de noms faisant autorité pour une zone étudiée n'ont pu être géolocalisés.

Nombre de pays	Pourcentage de domaines
0	10,99
1	64,08
2	23,47
3	0,78
4	0,65
5+	0,03

À RETENIR

La dispersion géographique des zones étudiées est globalement satisfaisante, tant en IPv4 qu'en IPv6. Presque la moitié des zones étudiées ont des serveurs de noms faisant autorité situés exclusivement en France.

2.2.4 Dépendance à des noms tiers

L'analyse des enregistrements NS révèle que près de 99 % des zones sont déléguées en utilisant exclusivement des serveurs de noms hors juridiction technique. Cette statistique n'a pas évolué depuis le dernier rapport.

En regardant maintenant les degrés de dépendance à des noms tiers, présentés dans le tableau ci-dessous, près de 80 % des zones déléguées étudiées en ont au moins un : tous les enregistrements NS utilisent un nom situé dans un même TLD distinct de `.fr`, par exemple `.net`. Cette statistique a diminué par rapport à 2016, où elle était de 87 %.

De plus la grande majorité, environ 72 %, ont deux degrés de dépendance, ce qui signifie que tous les enregistrements NS utilisent un nom situé dans un même TLD distinct de `.fr`, par exemple `.com`, et que tous ces noms sont eux-mêmes situés dans un même domaine de second niveau, par exemple `bonjour.com`.

Nombre de pays	Pourcentage de domaines
0	20,27
1	0,07
2	72,19
3	7,41
4+	0,06

À RETENIR

Pour environ 80 % des zones étudiées il existe un risque d'indisponibilité accru du fait des serveurs de noms choisis pour déléguer ces zones, où le degré de dépendance à des noms tiers est d'au moins deux.

2.3 Mise en œuvre de DNSSEC

2.3.1 Analyse des enregistrements DS

Le déploiement de DNSSEC se poursuit. Parmi les zones étudiées, environ 22 % sont correctement signées :

Zone signée	Pourcentage de domaines
Oui	22,15
Non	77,85

À RETENIR

Un peu plus de 22 % des zones étudiées mettent en œuvre DNSSEC en 2026. Le déploiement suit une progression lente mais continue depuis le dernier rapport.

2.3.2 Analyse des algorithmes cryptographiques

Près de 81 % des zones étudiées et disposant d'un enregistrement DS indiquent utiliser la suite cryptographique RSASHA256, et près de 18 % utilisent la suite ECDSAP256SHA256. Il s'agit de deux algorithmes robustes et recommandés. Enfin, les quelque 1 % restants incluent une part d'algorithmes dépréciés voir obsolètes (c'est à dire susceptible de ne plus être pris en charge par des résolveurs validants) :

Algorithme de signature	Pourcentage de domaines
ECDSAP256SHA256	17,76
ECDSAP384SHA384	0,14
ED25519	0,66
RSASHA256	81,21
RSASHA1-NSEC3-SHA1	0,20
Autres	0,03

Algorithme de hachage	Pourcentage de domaines
SHA1	1,78
SHA256	97,77
SHA384	0,45

La même étude peut être effectuée sur les enregistrements DNSKEY (ou plus simplement clés publiques) des zones étudiées. Des résultats similaires sont observés :

Algorithme de signature	Pourcentage de domaines
ECDSAP256SHA256	14,28
ECDSAP384SHA384	0,14
ED25519	0,01
RSASHA256	84,81
RSASHA1-NSEC3-SHA1	0,21
Autres	0,55

À RETENIR

Plus de 99% des zones étudiées mettent en œuvre un algorithme de signature recommandé. De même, environ 98% des zones étudiées utilisent un algorithme de hachage recommandé pour créer la chaîne de confiance DNSSEC.

Chapitre 3
Résilience sous l'angle du courrier électronique

3.1 Introduction

Le courrier électronique, ou « e-mail », est un système permettant à deux utilisateurs d'échanger des messages électroniques par Internet. Les messages sont relayés au moyen du protocole SMTP [29] et sont dans un format texte comportant un en-tête et un corps [30]. Enfin les boîtes de courrier électronique sont désignées par des adresses dont la forme habituelle est `partie-locale@domaine.tld`.

3.1.1 Transmission d'un message

La figure 3.1 présente le cheminement classique d'un courrier électronique. Dans cet exemple, Alice envoie un message à Bob. Après avoir rédigé son message dans un client de messagerie, aussi appelé Mail User Agent (MUA), Alice déclenche l'envoi du message : cette action transmet le message à l'agent de soumission de courrier ou Message Submission Agent (MSA) dans la messagerie d'Alice (étape ①). En fonction du client qu'Alice utilise, le message peut être soumis en Hypertext Transfer Protocol (HTTP), en SMTP ou par un autre moyen. Le MSA de la messagerie d'Alice relaie le message à un agent de transmission de courrier ou Message Transfer Agent (MTA). Ce dernier le relaie au MTA chez Bob (étape ②) ; cette étape se fait presque toujours en SMTP et c'est précisément à cette interaction que nous allons nous intéresser dans la suite du chapitre. Enfin, au sein de la messagerie de Bob, le MTA remet le message à un agent de remise de courrier ou Message Delivery Agent (MDA), qui stocke le message dans la boîte aux lettres de Bob (étape ③). Le destinataire peut alors prendre connaissance du message d'Alice en consultant une messagerie Web, en relevant le courrier via le protocole Post Office Protocol (POP) [20] ou Internet Message Access Protocol (IMAP) [24], ou par un autre moyen.

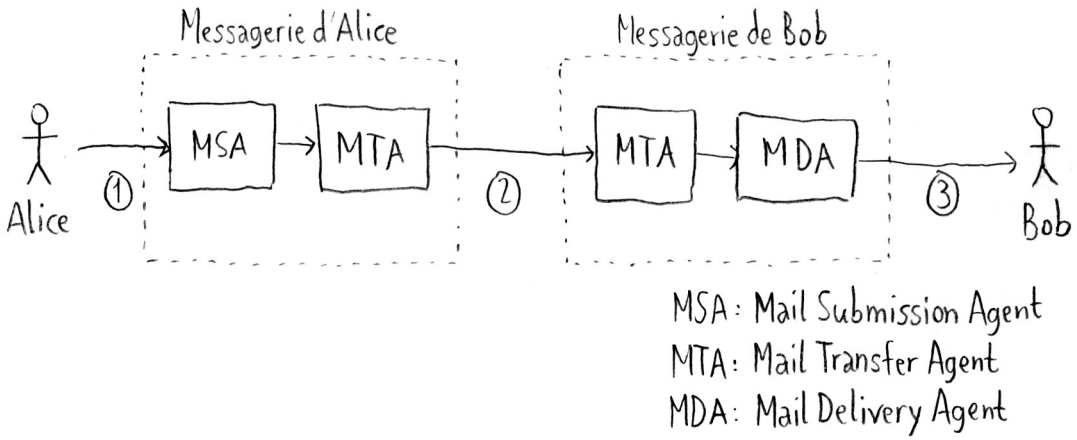


Figure 3.1 – Schéma de principe du courrier électronique

3.1.2 Exemple d'échange en SMTP

La figure 3.2 reproduit un exemple d'échange SMTP entre un MTA agissant en tant que client (ici `mta.domaine-a.example`) et un serveur (`mta.domaine-b.example`). Il s'agit de l'étape ② dans le schéma de la figure 3.1.

```
← 220 mta.domaine-b.example ESMTP Postfix
→ EHLO mta.domaine-a.example
← 250-mta.domaine-b.example
250-PIPELINING
250-SIZE 52428800
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 CHUNKING
MAIL FROM:<alice@domaine-a.example>
← 250 2.1.0 Ok
→ RCPT TO:<bob@domaine-b.example>
← 250 2.1.5 Ok
→ DATA
← 354 End data with <CR><LF>.<CR><LF>
→ From: Alice <alice@domaine-a.example>
To: Bob <bob@domaine-b.example>
Subject: Message
Date: Thu, 16 Sep 2026 09:54:13 +0200
Ceci est un message d'Alice, pour Bob
.
← 250 2.0.0 Ok: queued as 5194F107E5
→ QUIT
← 221 2.0.0 Bye
```

(Les lignes préfixées par ← sont des lignes envoyées par le serveur au client ; celles préfixées par → sont envoyées par le client au serveur.)

Figure 3.2 – Exemple d'échange SMTP

3.1.3 Adresse d'enveloppe et adresse d'en-tête

De manière analogue au courrier postal, un courrier électronique contient une enveloppe et un message. Dans l'enveloppe figurent l'adresse de l'expéditeur, transmise par la commande SMTP `MAIL FROM` et celle du destinataire, transmise par la commande `RCPT TO`. Dans l'en-tête du message figurent également les adresses de l'expéditeur et du destinataire, dans les champs d'en-tête `From` et `To` respectivement.

Les adresses de l'enveloppe et de l'en-tête jouent des rôles différents. L'adresse de l'en-tête (`From`) est l'auteur du contenu du message, à qui le destinataire pourrait souhaiter répondre, tandis que l'adresse de l'enveloppe (SMTP `MAIL FROM`) est utilisée pour transmettre un avis de non-remise si le message n'a pas pu être remis à son destinataire. Dans le cas de messages interpersonnels, les adresses de l'enveloppe et de l'en-tête sont généralement identiques ; mais dans le cas d'envois en masse, de courrier réexpédié ou de listes de diffusion, ces adresses peuvent être différentes. Dans ces cas-là, l'adresse de l'enveloppe identifie plutôt une entité à même de gérer les problèmes de délivrabilité. Par exemple, si un internaute est abonné à une infolettre, les messages ont pour adresse d'en-tête une adresse comportant le nom de domaine de l'enseigne à l'origine de cet envoi et pour adresse d'enveloppe une adresse chez le prestataire chargé de l'envoi de messages en masse. Ainsi, le prestataire peut désinscrire automatiquement les abonnés dont l'adresse cesse de fonctionner.

De l'expéditeur jusqu'au destinataire, un message est amené à transiter par un ou plusieurs serveurs appelés MTA. Le ou les MTA responsables du courrier pour un domaine sont désignés par la publication dans le DNS d'enregistrements MX. Dans l'exemple ci-dessous, on désigne deux machines comme responsables de la réception du courrier pour toutes les adresses finissant par `@domaine.tld` :

```
domaine.tld.    IN MX 10 mx-principal.domaine.tld.
                IN MX 20 mx-secondaire.domaine.tld.
```

Le bon fonctionnement de la messagerie d'un domaine dépend donc du bon fonctionnement des serveurs de messagerie référencés par les enregistrements MX, mais aussi de la capacité à résoudre ces noms. Si les noms sont dans un domaine tiers (par exemple, celui d'une plateforme d'hébergement), alors le nom de domaine de ce tiers devient une dépendance supplémentaire. La panne du nom de domaine de ce tiers peut alors entraîner la non-remise de courrier destiné au domaine.

3.1.4 Données et outils

Pour la mesure de la résilience sous l'angle de la messagerie, l'observatoire a utilisé les mêmes outils de mesure active que pour les mesures DNS (*cf.* section 2.1).

Les enregistrements DNS de politiques SPF et DMARC ont été récupérés directement. Concernant DomainKeys Identified Mail (DKIM), il n'est pas possible de déduire directement la présence ou non de clés publiques dans le domaine car celles-ci sont publiées au nom de domaine `sélecteur._domainkey. domaine.tld`, où `sélecteur` est une chaîne nommant la clé et `domaine.tld` est le domaine utilisé pour la signature DKIM.

Nous supposons donc qu'un domaine a déployé DKIM si les deux conditions ci-après sont vraies :

- une requête de type `TXT` pour le sous-domaine `_domainkey.domaine.tld` donne une réponse NODATA, *i.e.* une réponse dont le code d'erreur est NOERROR, la section réponse est vide et le drapeau AA est positionné. Si le code d'erreur est NXDOMAIN, nous considérons que le domaine n'a pas déployé DKIM.
- une requête de type `TXT` pour le sous-domaine `*.domaine.tld` donne une réponse dont le code d'erreur est NXDOMAIN. Ceci afin de s'assurer que la réponse à la première requête ne provienne pas de la synthèse d'un joker (*wildcard, cf.* [18]). Dans le cas contraire, le résultat est indéterminé.

Cette méthodologie souffre de quelques limitations. Un domaine ayant publié une SPF sur un sous-domaine (par exemple `sous-domaine.domaine.tld`) mais pas au sommet de la zone (c'est-à-dire `domaine.tld`) n'est pas comptabilisé comme ayant déployé SPF. Il en va de même pour DMARC.

Quant à DKIM, la méthode présentée ci-dessus suppose que les serveurs de noms faisant autorité interrogés respectent la RFC 8020 ([38]) et suppose que si la première requête a donné NODATA, alors le sous-arbre `_domainkey.domaine.tld` contient au moins un enregistrement TXT pour une clé publique DKIM correctement formée.

Ainsi, un domaine publiant une entrée A sur `exemple._domainkey.domaine.tld` et aucun autre enregistrement dans le sous-arbre dédié à DKIM serait alors compté à tort comme ayant adopté DKIM. À l'inverse, un domaine peut être considéré à tort comme n'ayant pas déployé DKIM si le serveur de noms faisant autorité a répondu NXDOMAIN à la requête pour `_domainkey.domaine.tld`, même si un sous-domaine comme `sélecteur._domainkey.domaine.tld` existe. Des serveurs de noms comportant cette erreur précise dans la mise en œuvre du DNS sont rares, mais ont été constatés au cours de la mesure.

3.2 Sécurité du courrier électronique

Du fait de sa conception ancienne dans un contexte où l'état de la menace en cybersécurité était très différent de celui d'aujourd'hui, le courrier électronique ne bénéficiait pas de mécanismes de sécurité. Les messages sont échangés en clair et il n'est pas possible de contrôler la véracité des informations figurant dans l'enveloppe et dans l'en-tête. Il est en particulier possible de forger les adresses SMTP `MAIL FROM` et `From` et donc d'usurper l'identité d'un tiers. Ce qui rend à son tour les hameçonnages plus convaincants.

Afin d'authentifier le domaine d'origine d'un courrier et ainsi rendre plus difficile ces usurpations d'identité, plusieurs mécanismes de sécurité ont été ajoutés au courrier électronique : SPF [36], DKIM [33] et DMARC [41, 42, 43]. Un message réussissant les tests supplémentaires introduits par SPF, DKIM et par DMARC a ainsi de grandes chances de provenir du domaine apparaissant dans l'adresse de l'en-tête.

Nous discuterons plus en détail de SPF et de DMARC car certaines spécificités de ces protocoles peuvent introduire des dépendances supplémentaires à des noms de domaine tiers.

3.2.1 Adoption globale de SPF, DKIM et DMARC

Parmi les domaines étudiés, l'état actuel de l'adoption globale de SPF, DKIM et DMARC est présenté dans le tableau 3.1.

Récurrence	Domaines	Pourcentage
Total .fr	4 229 451	100
Avec SPF	3 096 570	73,2
Avec DKIM	1 846 324	43,7
Avec DMARC	1 513 264	35,8

Tableau 3.1 – Nombre de domaines en .fr adoptant SPF, DKIM et DMARC

À RETENIR

Parmi tous les noms de domaine du .fr, 73,2 % adoptent SPF, 43,7 % adoptent DKIM et 35,8 % adoptent DMARC.

3.2.2 Sender Policy Framework (SPF)

Avec SPF, l'administrateur d'un domaine publie dans le DNS l'ensemble des adresses IP des machines autorisées à envoyer du courrier où le nom de domaine figure dans l'adresse de l'enveloppe SMTP. Cette déclaration se fait en publiant un enregistrement TXT au domaine concerné, contenant une chaîne de caractères suivant une syntaxe spécifique [36]. On autorise un client au moyen d'un ou plusieurs mécanismes, comme :

- `ip4` et `ip6`, pour lister une adresse IP ou une plage d'adresses IP directement ;
- `a`, pour autoriser les adresses IPv4 et IPv6 associées à un nom de domaine ;
- `mx`, pour autoriser les relais de messagerie associés au nom de domaine par un ou plusieurs enregistrements MX ;
- `include`, pour évaluer récursivement une sous-politique publiée à un autre domaine et autoriser les machines listées dans cette sous-politique.

Le terme `include` est particulièrement utile quand le courrier est envoyé via un prestataire spécialisé dans l'envoi de courrier en masse ou lorsque la messagerie est hébergée dans une infrastructure tierce dans le cloud. Mais il introduit un double risque : l'évaluation de la politique SPF de départ dépend ainsi de l'intégrité et de la disponibilité d'un enregistrement TXT à un nom tiers. Un échec de la résolution DNS de ce domaine tiers provoque en cascade un échec de l'authentification SPF pour le domaine qui en a importé la sous-politique et une modification frauduleuse de la sous-politique par un tiers non autorisé peut avoir pour conséquence qu'un message frauduleux soit authentifié à tort.

3.2.2.1 Dépendances à des sous-politiques SPF externes

Le tableau 3.2 liste, pour les 20 noms de sous-politiques les plus souvent relevées dans des politiques SPF de noms de domaine en .fr, le nombre de domaines qui en sont dépendants et la nationalité de l'entité qui contrôle le nom de la sous-politique.

Nom inclus	Nationalité	Domaines	Pourcentage
`mx.ovh.com`	FR	1 045 179	33,753
`_spf-eu.ionos.com`	DE	456 711	14,749
`spf.protection.outlook.com`	US	225 881	7,295
`_mailcust.gandi.net`	FR	179 558	5,799
`spf.jabatus.fr`	FR	144 531	4,667
`_spf.google.com`	US	104 228	3,366
`_spf.mail.hostinger.com`	LT	89 723	2,897
`spf.infomaniak.ch`	CH	69 851	2,256
`spf.mailjet.com`	FR	48 583	1,569
`_spf.webador.com`	NL	31 489	1,017
`spf.webapps.net`	FR	30 814	0,995
`wanadoo.fr`	FR	19 079	0,616

_spf.hostedemail.com	US	16 451	0,531
sendgrid.net	US	13 978	0,451
spf.sendinblue.com	FR	12 905	0,417
_spf.mx.cloudflare.net	US	12 375	0,400
emailsrvr.com	US	10 533	0,340
_spf.alwaysdata.com	FR	9759	0,315
_spf.protonmail.ch	CH	9687	0,313
mailgun.org	US	9075	0,293
Uniquement hors top 20		399 796	12,911
Sans include ni redirect		473 194	15,281

Remarque : puisqu'il est possible d'inclure plus d'une sous-politique SPF, le total de la colonne « Domaines » dépasse le nombre total de domaines avec une politique SPF. La ligne « Uniquement hors top 20 » compte les domaines dont aucune sous-politique ne figure parmi les 20 noms listés.

Tableau 3.2 – Noms de domaine des sous-politiques les plus souvent relevées dans les politiques SPF des noms de domaine en `.fr`

Ainsi, on voit par exemple que la sous-politique SPF située au nom de domaine `mx.ovh.com` est utilisée par 1 045 179 domaines, ce qui représente 33,8 % des domaines publiant une politique SPF. Un attaquant parvenant à modifier frauduleusement la donnée publiée à ce nom de domaine influence alors la configuration SPF de plus d'un million de domaines.

À RETENIR

Parmi les noms de domaine en .fr ayant une politique SPF, 71,8 % incluent une sous-politique SPF parmi les 20 sous-politiques les plus couramment observées.

Si nous regardons uniquement les 10 domaines de premier niveau les plus fréquents, on obtient les données présentées dans le tableau 3.3.

TLD	Domaines	Pourcentage
com	2 056 793	66,422
net	304 900	9,846
fr	225 801	7,292
ch	80 401	2,596
de	17 169	0,554
org	12 501	0,404
nl	8794	0,284
eu	7857	0,254
email	5683	0,183
tools	4267	0,138
Autres	24 452	0,790

Tableau 3.3 – Noms de domaine de premier niveau des sous-politiques les plus souvent relevées dans les politiques SPF des noms de domaine en .fr

À RETENIR

Parmi les noms de domaine en .fr ayant une politique SPF, 66,4 % incluent une sous-politique SPF sur un nom en .com. Trois quarts dépendent d'un .com ou d'un .net.

3.2.3 Domain-Based Message Authentication, Reporting, and Compliance (DMARC)

DMARC s'appuie sur SPF et DKIM et comble quelques lacunes de ces deux mécanismes. Il contrôle l'alignement entre le domaine de l'auteur du message (champ d'en-tête From) d'une part et ceux de l'adresse d'enveloppe et ceux du domaine utilisé pour la signature DKIM d'autre part ; il permet à l'administrateur du domaine de recommander une action quand un message échoue simultanément aux contrôles réalisés par SPF et par DKIM ; enfin, il permet à ce même administrateur de solliciter des rapports automatisés pour vérifier le bon fonctionnement de SPF et de DKIM.

Pour publier une politique DMARC s'appliquant au domaine domaine.tld, l'administrateur d'un domaine publie un enregistrement DNS de type TXT au sous-domaine _dmarc.domaine.tld.

L'action en cas d'échec est spécifiée par le terme p. Il peut prendre les valeurs suivantes :

- none : ne réaliser aucune action particulière ;
- quarantine : placer le message en quarantaine ou dans un répertoire dédié au courrier indésirable ;
- reject : rejeter le message au moment de la transaction SMTP.

Il est possible de solliciter deux sortes de rapports automatisés : les rapports agrégés [42] avec le terme `rua` et les rapports individuels [43] avec le terme `ruf`. Ces rapports sont utiles pour vérifier le bon fonctionnement de SPF et de DKIM, tant pour vérifier que le courrier légitime est correctement authentifié que pour vérifier que le courrier frauduleux soit identifié comme des usurpations d'identité. Pour ce faire, la politique DMARC associée au nom de domaine doit publier une ou plusieurs adresses de courrier destinées à recevoir ces rapports.

Seuls les domaines spécifiant le terme `p=quarantine` ou `p=reject` sont considérés comme étant durcis contre le risque d'usurpation d'identité dans le courrier électronique. Néanmoins, publier une politique p=none associée à un `rua`, ce qui est communément appelé le « mode supervision » de DMARC, permet d'obtenir des rapports sans pour autant risquer le rejet accidentel de courrier légitime.

Par exemple, cette politique DMARC recommande une action de rejet et indique que le gestionnaire de la messagerie du domaine souhaite recevoir des rapports à l'adresse `dmarc-rua@domaine.tld` :

```
v=DMARC1; p=reject; rua=mailto:dmarc-rua@domaine.tld
```

Sur les politiques DMARC en .fr, la répartition des configurations des termes p et `rua` est donnée dans le tableau 3.4.

Terme p	Sans rua	Avec rua	Total
p=none	871 428	157 563	1 028 991
p=quarantine	149 612	59 125	208 737
p=reject	182 147	88 671	270 818
Tous	1 203 187	305 359	1 508 546

Tableau 3.4 – Paramétrage des rapports DMARC dans les politiques relevées sur les domaines en `.fr`

3.2.3.1 Dépendances à des tiers pour l'analyse des rapports DMARC

Un domaine à l'origine d'un grand nombre de messages peut être amené à recevoir de nombreux rapports venant d'un grand nombre de messageries qui en sont les destinataires, ce qui rend leur analyse manuelle rapidement fastidieuse.

C'est pourquoi il existe des services tiers d'analyse de rapports DMARC. L'enrôlement d'un tel service consiste à ajouter l'adresse de courrier désignée à cet effet dans la politique DMARC du domaine concerné. Adresse qui est donc nécessairement celle d'un domaine tiers. Le recours à de tels services introduit donc nécessairement des enjeux de respect de la vie privée, une dépendance à un nom de domaine tiers et plus généralement une dépendance à une infrastructure tierce.

Si nous nous restreignons aux domaines qui sollicitent l'envoi de rapports, nous constatons que les domaines les plus fréquemment observés dans les adresses de courrier où envoyer les rapports sont ceux listés dans le tableau 3.5.

Domaine en ruf/rua	Nationalité	Domaines	Pourcentage
Même domaine ou sous-domaine		81 084	25,801
dmarc.brevo.com	FR	62 676	19,984
emaildefense.proofpoint.com	US	21 290	6,792
onsecureserver.net	US	14 808	4,724
vali.email	US	8093	2,581
dmarc-reports.cloudflare.net	US	7019	2,239
mailinblue.com		6911	2,205
gmail.com	US	6169	1,964
emailsecurity.merox.io		4931	1,573
ag.eu.dmarcadvisor.com	NL	4534	1,437
csdg.org		4062	1,296
dmarc.ca-gip.fr	FR	2594	0,828
rep.dmarcanalyzer.com	UK	2412	0,770
inbox.ondmarc.com	UK	2330	0,743
for.dmarcanalyzer.com	UK	2256	0,720
inbox.eu.redsift.cloud	UK	2193	0,700
prowebce.com	FR	2169	0,691
ag.eu.dmarcian.com	US	2114	0,674
reportdmarc.nl		2028	0,646
webcd.fr	FR	2020	0,644
dr.dmarc.fr	HU	1844	0,588
Autre domaine tiers		85 877	27,397

Remarques:

- *la somme de la colonne « pourcentage » peut dépasser 100 % car il est possible, pour un domaine, de lister plusieurs adresses de courrier dans un tag* `ruf` *ou* `rua`.
- *pour les noms de domaine* `mailinblue.com`, `csdg.org` *et* `reportdmarc.nl`, *il n'a pas été possible de déterminer avec certitude la nationalité de l'entité qui en est responsable.*

Tableau 3.5 – Domaines recensés dans les termes `rua` *et* `ruf` *parmi les politiques DMARC recensées sur le* `.fr`

Ainsi, parmi tous les domaines dont la politique DMARC sollicite des rapports, près de 20 % les font envoyer vers une adresse chez `dmarc.brevo.com`. Mais la pratique la plus courante est de déclarer une adresse avec le même domaine que la politique DMARC à laquelle elle s'applique : celle-ci a été observée sur plus d'un quart des domaines sollicitant des rapports. Il s'agit la plupart du temps d'une adresse dédiée, pouvant ensuite faire l'objet d'une réexpédition, le cas échéant vers un service tiers.

À RETENIR

Près de trois quarts des politiques DMARC sollicitant des rapports les font expédier à une adresse chez un domaine tiers. La plupart sont des services gérés par des entreprises tierces dont une proportion non négligeable sont des entités hors UE. Le quart restant déclare une adresse dans le même domaine ou dans un sous-domaine.

Le tableau 3.6 compte le nombre de domaines qui dépendent d'un autre nom de domaine de premier niveau pour l'envoi des rapports DMARC.

TLD	Domaines	Pourcentage
Même domaine ou sous-domaine	81 084	25,868
.com	147 369	47,015
.fr (tiers)	34 122	10,886
.net	25 925	8,271
.email	8286	2,643
.io	5638	1,799
.org	5396	1,721
.cloud	2483	0,792
.nl	2417	0,771
.eu	1855	0,592
.dev	1120	0,357
Autres TLD	6976	2,226

Remarque : la somme de la colonne « pourcentage » peut dépasser 100 % car il est possible, pour un domaine, de lister plusieurs adresses de courrier dans un tag `ruf` *ou* `rua`.

Tableau 3.6 – Noms de domaine de premier niveau recensés dans les termes `rua` *et* `ruf` *parmi les politiques DMARC recensées sur le* `.fr`

À RETENIR

Parmi les politiques DMARC sollicitant des rapports, près de la moitié dépendent d'un nom de domaine en `.com` pour la bonne réception des rapports ; un peu plus du quart les font envoyer au même domaine ou un sous-domaine ; le dernier quart dépend d'autres domaines dans une variété de domaines de premier niveau.

Chapitre 4
Résilience sous l'angle du protocole TLS

4.1 Introduction

4.1.1 Fonctionnement du protocole TLS

Le protocole TLS offre à un client et à un serveur la possibilité d'établir un canal de communication chiffré, donc protégé en confidentialité et en intégrité, indépendamment de la nature de l'application utilisée. Parmi les utilisations les plus courantes de TLS figure HTTPS, qui consiste à échanger des requêtes et des réponses HTTP au sein d'un canal préalablement établi avec TLS. D'autres exemples sont SMTPS (SMTP sur TLS), IMAPS (IMAP sur TLS), LDAPS (LDAP sur TLS), etc.

TLS est un successeur du protocole SSL, désormais obsolète [37]. Il a connu plusieurs itérations, désignées respectivement par les numéros de version 1.0 [22], 1.1 [26], 1.2 [27] et 1.3 [17]. Par souci d'interopérabilité, les spécifications permettent aux deux parties impliquées de négocier la version du protocole à adopter communément.

De même, TLS autorise l'utilisation de différentes combinaisons d'algorithmes cryptographiques pour assurer la confidentialité et l'intégrité des échanges ; les deux parties impliquées ont la possibilité de négocier la suite cryptographique[1] à utiliser pour la session.

Cette négociation intervient pendant une phase d'initialisation appelée *TLS handshake*, qui précède le chiffrement effectif des échanges.

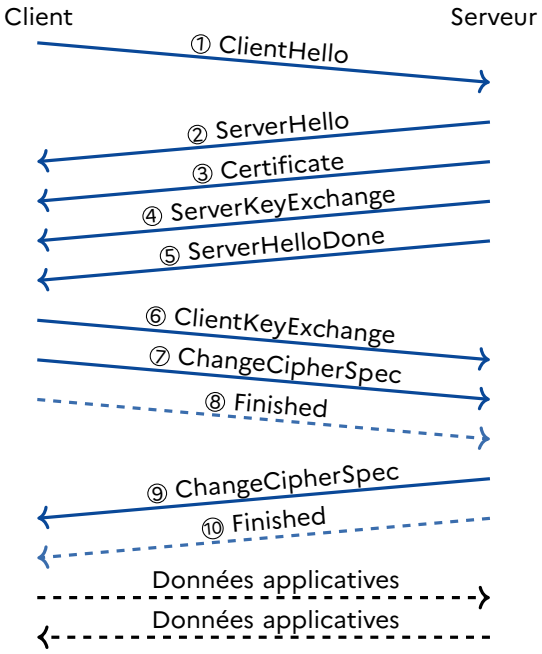


Figure 4.1 – Initiation générique d'une session TLS

Sans se substituer aux références plus précises [1, 44], la figure 4.1 illustre la négociation de ces paramètres dans un cas générique à l'aide d'interactions numérotées :

1. le client initie une requête en envoyant un message de type `ClientHello`, contenant notamment les suites cryptographiques qu'il prend en charge ;

1. En anglais, *ciphersuite*.

2. le serveur répond par un `ServerHello` qui contient la suite retenue ;
3. le serveur envoie un message `Certificate`, qui contient en particulier sa clé publique au sein d'un certificat numérique ;
4. le serveur transmet dans un `ServerKeyExchange` une valeur éphémère qu'il signe à l'aide de la clé privée associée à la clé publique précédente ;
5. le serveur manifeste sa mise en attente avec un `ServerHelloDone` ;
6. après vérification du certificat et authentification de la valeur précédente, le client choisit à son tour une valeur éphémère qu'il chiffre à l'aide de la clé publique du certificat puis transmet dans un `ClientKeyExchange` ;
7. le client signale l'adoption de la suite négociée avec un `ChangeCipherSpec` ;
8. le client envoie un `Finished`, premier message protégé selon la suite cryptographique avec les secrets issus de l'échange de clés éphémères précédent ;
9. le serveur signale l'adoption de la même suite avec un `ChangeCipherSpec` ;
10. le serveur envoie à son tour un `Finished`, son premier message sécurisé.

Le cas générique décrit ici sous-entend l'adoption d'une des suites cryptographiques qui assurent la propriété de confidentialité persistante, ou PFS. Celle-ci consiste à prévenir le déchiffrement de messages de sessions passées même si la clé privée du serveur était compromise, en négociant un secret éphémère à l'aide d'un échange Diffie–Hellman [23].

Les spécifications du protocole définissent par ailleurs plusieurs messages supplémentaires et extensions qui permettent d'encadrer et d'enrichir la protection des communications [31]. Un `ClientHello` peut par exemple contenir une extension précisant les capacités de cryptographie sur courbes elliptiques du client.

4.1.2 Les infrastructures de gestion de clés

La validité du certificat envoyé par le serveur au cours de l'initiation de la session TLS est au cœur de la sécurité du protocole. L'ensemble des mécanismes et des entités qui formulent cette validité et la maintiennent représente une Infrastructure de IGC.

Pour un certificat conforme à la norme X.509 [28] suivie dans le cadre de TLS, l'assurance que la clé publique qu'il contient appartienne effectivement au serveur qu'il annonce en tant que sujet (généralement sous la forme d'un nom de domaine) repose sur la transmission de confiance depuis une autorité déjà reconnue jusqu'au serveur en question. Les liens de confiance successifs établis par des AC sont matérialisés par des signatures cryptographiques apposées aux différents certificats.

Ainsi, le message `Certificate` dont est extraite la clé à l'origine des secrets de session contient en réalité une chaîne de certificats, dont le client attend qu'elle forme un lien depuis une racine de confiance jusqu'au serveur interrogé. Dans le cas de navigateurs web, ces racines correspondent généralement à un registre public, tel que le magasin de certificats NSS maintenu par Mozilla pour son navigateur Firefox [13]. Certaines applications interagissent directement avec le registre public concerné pour mettre à jour leur magasin de certificats de confiance, tandis que d'autres s'appuient sur la maintenance opérée par le système d'exploitation hôte.

Les certificats contiennent plusieurs attributs, tels qu'une clé publique et une période de validité, qui sont habituellement complétés par des extensions X.509v3. Celles-ci permettent notamment de préciser le cadre d'utilisation du certificat en question et de renforcer les assurances de l'IGC. L'ANSSI recommande à cet effet le suivi de l'annexe A4 du RGS [2].

4.1.3 Données et outils

Les mesures de l'observatoire se sont concentrées sur les ressources Web accessibles à travers l'Internet français. Elles concernent plus spécifiquement les ressources exposées via le port 443, traditionnellement alloué par les serveurs aux échanges HTTPS. Les enjeux liés aux ressources de messagerie en ligne diffèrent en plusieurs points [7] et ne sont pas abordés dans le présent rapport.

Les données proviennent d'un logiciel de type robot d'indexation, développé entièrement par l'Afnic, permettant de réaliser des mesures actives des ressources Web des noms de domaines concernés. Les bibliothèques Python `HTTPX` [8], `pyOpenSSL` [16], `Cryptography` [5] sont notamment utilisées à cette fin.

Les noms de domaine issus du registre maintenu par l'Afnic ont été préfixés de `www.` avant d'être résolus, si nécessaire. Par exemple, les mesures effectuées sur le domaine `afnic.fr` correspondent à l'adresse IPv4 résolue pour `www.afnic.fr`. Lorsque le port 443 du serveur interrogé était ouvert, l'observatoire a envoyé différents stimulus `ClientHello`, dont les variations visaient à évaluer plusieurs capacités du serveur, telles que sa prise en charge de la confidentialité persistante ou encore sa tolérance envers des versions obsolètes du protocole.

4.1.3.1 Données utilisées

Le nombre de zones étudiées dont les échanges HTTPS ont pu être collectés avec succès s'élève à 2 963 264 au 10 juin 2026. Parmi celles-ci, la part disposant d'un certificat valide est de 95 %, et celles disposant d'un certificat invalide est de 5 %.

4.2 Négociation de sessions

Parmi les paramètres de session initialement définis par les spécifications, certains sont reconnus d'usage sûr en 2026, tandis que d'autres ont été déclarés obsolètes car sujets à des attaques [32, 37]. Les attributs établis via la phase de négociation ont donc une influence directe sur la sécurité des échanges subséquents. Pour cette raison, l'observatoire a cherché à établir un profil des serveurs de la zone .fr exposant des ressources HTTPS.

Dans la mesure où, soumis aux `ClientHello` appropriés, un même serveur peut par exemple accepter la version recommandée TLS 1.3 mais aussi les versions proscrites comme TLS 1.0 ou SSLv3, l'examen d'un seul paramètre ne permet pas de juger la sécurité d'un ensemble de serveurs de façon absolue. La mise en commun de ces paramètres permet cependant un constat qualitatif du respect des bonnes pratiques.

4.2.1 État général des serveurs TLS

En 2026, considérant l'ensemble des stimuli tentant de négocier une session TLS 1.3, 1.2 ou 1.0, avec des variations notamment au niveau des suites cryptographiques proposées, 96 % des serveurs présentant un port 443 ouvert permettaient d'initier une session TLS.

Concernant les versions de TLS acceptées par les serveurs, presque 100 % d'entre eux sont aptes à négocier une session TLS 1.3 ou TLS 1.2 :

Version de TLS	Pourcentage de domaines
TLS 1.3	94,00
TLS 1.2	5,99
TLS 1.0	0,01

À RETENIR

TLS 1.3 est couramment pris en charge par les serveurs de la zone `.fr` en 2026. TLS 1.2 est encore présent, mais clients comme serveurs devraient privilégier la version la plus récente du protocole.

4.2.2 Confidentialité persistante

La réalisation des échanges TLS est conditionnée par le choix d'une suite cryptographique appropriée. Le respect de la confidentialité persistante peut donc être mesuré en dénombrant les serveurs qui acceptent l'utilisation de telles suites.

Algorithme de chiffrement TLS	Pourcentage de domaines
ECDHE-RSA-AES128-GCM-SHA256	1,49
ECDHE-RSA-AES256-GCM-SHA384	3,76
TLS_AES_128_GCM_SHA256	15,73
TLS_AES_256_GCM_SHA384	78,02
TLS_CHACHA20_POLY1305_SHA256	0,24
Autres	0,76

À RETENIR

En 2026, l'offre de confidentialité persistante s'est généralisée sur la zone `.fr`. Les serveurs doivent privilégier cette méthode auprès des clients qui la prennent en charge.

4.3 Dispersion des certificats

Tout comme pour les serveurs DNS faisant autorité, la dispersion géographique des certificats TLS est un indicateur de résilience. À ce titre, l'observatoire a étudié la répartition des signatures de certificats TLS par pays d'émission. Seulement 1,59 % des zones étudiées disposent d'un certificat émis par une autorité de certification française, alors que près de 90 % des certificats TLS sont émis par des autorités de certification américaines :

Code pays de l'émetteur	Pourcentage de domaines
US	90,31
GB	6,59
FR	1,59
BE	0,63
AT	0,61
NL	0,11
GR	0,07
PL	0,03
LV	0,02
IE	0,01
Autres	0,03

La même étude peut être effectuée sur les organisations émettrices de ces certificats. Une seule organisation est responsable de près de 75 % des certificats. De même, plus de 91 % des certificats sont émis par seulement trois organisations.

Organisation	Code pays de l'émetteur	Pourcentage de domaines
Let's Encrypt	US	75,13
Google Trust Services	US	10,89
Sectigo Limited	GB	6,56
DigiCert Inc	US	1,65
Gandi	FR	1,58
GoDaddy	US	1,53
Amazon	US	0,96
GlobalSign	BE	0,63
ZeroSSL	AT	0,60
Trust Provider B.V.	NL	0,08
Autres	Divers	0,39

À RETENIR

Environ 1,59% des zones étudiées disposent d'un certificat émis par une autorité de certification française, dont près de 99% par la même organisation. La très grande majorité restante dispose d'un certificat émis par une organisation américaine, largement partagée entre seulement deux organisations.

Conclusion

Cette édition du rapport de l'observatoire de la résilience de l'Internet français dresse un bilan sur l'état du routage (BGP), de la résolution de noms (DNS), de l'authentification du courrier électronique et du chiffrement des communications web (TLS). Les données de l'étude BGP s'étendent de 2018 à 2025, tandis que les mesures DNS, courrier électronique et TLS portent sur l'année 2026.

En ce qui concerne BGP, l'incident de Softaculous en 2026 et l'expérimentation menée à la suite de la mise en garde de la RFC 9319 montrent que les opérateurs ne doivent pas reposer exclusivement sur la ROV pour filtrer les annonces BGP reçues. Il convient donc de limiter au strict nécessaire la longueur maximale (*maxLength*) déclarée dans les ROA, et de continuer à appliquer les bonnes pratiques de filtrage des interconnexions BGP.

IPv6, conçu pour pallier l'épuisement des adresses IPv4 et accompagner la croissance de l'Internet, continue de progresser : le nombre d'AS français présents en IPv6 est passé de 411 en 2018 à 764 fin 2025, et celui des AS exclusivement IPv6 de 13 à 101. Le nombre d'AS de type 1, c'est-à-dire dépendant toute l'année d'un même AS pivot, continue de croître. Enfin, l'étude de la centralité d'intermédiarité met en lumière, en IPv4 comme en IPv6, la dépendance à des opérateurs situés hors de l'union européenne.

Du côté du DNS, l'un des constats marquants est que près de 80 % des zones sont hébergées dans un seul AS. Par ailleurs, près de 99 % des zones sont déléguées exclusivement à des serveurs de noms situés hors de leur juridiction technique. Des progrès sont en revanche à noter : près de 22 % des zones sont désormais signées avec DNSSEC, et seules 17 % ne sont accessibles qu'en IPv4, contre 37 % en 2016.

Nouveauté de cet observatoire, l'étude de l'authentification du courrier électronique montre une adoption croissante de ces mécanismes : 73 % des domaines étudiés publient une politique SPF, 44 % mettent en œuvre DKIM et 36 % publient une politique DMARC. Ces chiffres doivent toutefois être nuancés, car une large part de ces mécanismes repose sur un petit nombre de tiers, notamment des hébergeurs de messagerie, auprès desquels la gestion du courrier électronique est déléguée.

Enfin, la sécurisation des communications web montre une adoption massive de TLS 1.3, proposé par 94 % des sites. Ce constat est toutefois tempéré par la très forte concentration des certificats auprès d'autorités de certification américaines.

Plus globalement, l'actualité et l'évolution du contexte international encouragent à mesurer l'indépendance des communications électroniques vis-à-vis d'acteurs extra-européens. Les données recueillies sur les AS pivots, les autorités de certification ou encore les politiques SPF reposant sur des tiers nous poussent à encourager les acteurs à identifier ces dépendances géographiques, et à chercher à les réduire.

D'autres publications sous l'égide de l'observatoire permettront d'approfondir les perspectives évoquées dans ce document, comme l'analyse des préfixes, le déploiement d'ASPA ou l'hégémonie des AS pour BGP.

1. Route Origin Authorization
2. Autonomous System, nom technique donné aux opérateurs en BGP

Recommandations

Les constats de cette édition conduisent l'observatoire à formuler les recommandations suivantes, regroupées par protocole et destinées aux opérateurs de réseaux, aux gestionnaires de zones DNS et aux responsables de services de messagerie et de sites web.

Pour BGP, l'observatoire recommande aux opérateurs :

- de diversifier leurs liens de transit, notamment avec des opérateurs européens ;
- d'éviter de déclarer des ROA pour des préfixes plus spécifiques que /24 en IPv4 et /48 en IPv6 ;
- de déclarer systématiquement les objets route et les ROA, et de les maintenir à jour, afin de faciliter la détection et le filtrage des annonces BGP illégitimes ;
- de surveiller les annonces de leurs préfixes et de se tenir prêts à réagir en cas d'usurpation.

Pour le DNS, l'observatoire recommande aux gestionnaires de zones :

- de répartir leurs serveurs de noms faisant autorité dans plusieurs AS et, si possible, auprès de plusieurs opérateurs ;
- de limiter les dépendances à des noms tiers, en hébergeant si possible au moins un serveur de noms dans la juridiction technique du domaine ;
- de rendre leurs serveurs de noms accessibles en IPv6 ;
- de mettre en œuvre DNSSEC avec des algorithmes recommandés, tels que RSASHA256 ou ECDSAP256SHA256.

Pour le courrier électronique, l'observatoire recommande :

- de publier SPF, DKIM et DMARC, en commençant par une politique DMARC de supervision (`p=none` avec `rua`) avant de la durcir progressivement (`p=quarantine`, puis `p=reject`) ;
- de maîtriser les dépendances introduites par ces mécanismes : les inclusions SPF et les services d'analyse des rapports DMARC placent une partie de la messagerie entre les mains de tiers, un même nom pouvant être utilisé par plus d'un million de domaines ;
- de diversifier les relais de messagerie (MX) et leurs hébergeurs.

Pour TLS, l'observatoire recommande :

- de privilégier TLS 1.3, avec TLS 1.2 au minimum, et de désactiver les versions obsolètes du protocole ;
- de conserver des suites cryptographiques assurant la confidentialité persistante ;
- de ne pas dépendre d'une seule autorité de certification, près de 90 % des certificats étant émis par des organisations américaines, dont 75 % par une seule, et de prévoir des procédures de remplacement rapide des certificats.

Bibliographie

[1] Agence nationale de la sécurité des systèmes d'information (ANSSI) . *Recommandations de sécurité relatives à TLS*. <https://messervices.cyber.gouv.fr/guides/recommandationsde-securite-relatives-tls>. Mars 2020.

[2] Agence nationale de la sécurité des systèmes d'information (ANSSI) . *Référentiel Général de Sécurité - Annexe A4*. <https://cyber.gouv.fr/documents/336/RGS_v- 2- 0_A4.pdf>.Version 2.

[3] ANSSI . *Bonnes pratiques de configuration de BGP*. Rapp. tech. 2013.

[4] Bob Halley . *DNSPython Library*. <http://www.dnspython.org/>.

[5] *Cryptography Python library*. <https://cryptography.io/>.

[6] DENIC. *.de DNS Outage*. <https://blog.denic.de/en/final-report-dns-outage-of-5-may-2026/>. Mai 2026.

[7] Zakir Durumeric et al. « Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security ». In : *Internet Measurement Conference (IMC)*. Oct. 2015.

[8] HTTPX *Python library*. <https://www.python-httpx.org/>.

[9] IANA. *Domain Name System (DNS) Parameters*. <http://www.iana.org/assignments/dnsparameters/dns-parameters.xhtml>.

[10] Job Snijders, Alexander Azimov, Eugene Uskov, Randy Bush, Russ Housley, Ben Maddison. *A Profile for Autonomous System Provider Authorization*. <https://www.ietf.org/archive/id/draft-ietf-sidrops-aspa-profile-26.html>. 2026.

[11] MaxMind. *GeoIP | IP geolocation services*. <https://www.maxmind.com/en/solutions/ipgeolocation-databases-api-services>.

[12] G. Moura et al. *Considerations for Large Authoritative DNS Server Operators*. RFC 9199. Mars 2022. DOI : 10.17487/RFC9199. URL : https://www.rfc-editor.org/info/rfc9199/.

[13] Mozilla. *Network Security Services*. <https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS>.

[14] NLNetLabs. *Unbound*. <https://www.nlnetlabs.nl/projects/unbound/about/>.

[15] *Public Suffix List*. <https://publicsuffix.org/>.

[16] *pyOpenSSL Python library*. <https://www.pyopenssl.org/>.

[17] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 9846. Juill. 2026. DOI : 10.17487/RFC9846. URL : https://www.rfc-editor.org/info/rfc9846/.

[18] P. Mockapetris. *Domain names - concepts and facilities*. RFC 1034 (Internet Standard). RFC. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4592, 5936, 8020, 8482, 8767, 9471. Fremont, CA, USA : RFC Editor, nov. 1987. DOI : 10.17487/RFC1034. URL : https://www.rfc-editor.org/rfc/rfc1034.txt.

[19] P. Mockapetris. *Domain names - implementation and specification*. RFC 1035 (Internet Standard). RFC. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2137, 2181, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8490, 8767, 9619. Fremont, CA, USA : RFC Editor, nov. 1987. DOI : 10.17487/RFC1035. URL : https://www.rfc-editor.org/rfc/rfc1035.txt.

[20] J. Myers et M. Rose . *Post Office Protocol - Version 3*. RFC 1939 (Internet Standard). RFC. Updated by RFCs 1957, 2449, 6186, 8314. Fremont, CA, USA : RFC Editor, mai 1996. DOI : 10.17487/RFC1939. URL : https://www.rfc-editor.org/rfc/rfc1939.txt.

[21] R. Elz et al. *Selection and Operation of Secondary DNS Servers*. RFC 2182 (Best Current Practice). RFC. Fremont, CA, USA : RFC Editor, juill. 1997. DOI : 10.17487/RFC2182. URL : https://www.rfc-editor.org/rfc/rfc2182.txt.

[22] T. Dierks et C. Allen. *The TLS Protocol Version 1.0*. RFC 2246 (Historic). RFC. Obsoleted by RFC 4346, updated by RFCs 3546, 5746, 6176, 7465, 7507, 7919. Fremont, CA, USA : RFC Editor, jan. 1999. DOI : 10 . 17487 / RFC2246. URL : https://www.rfc-editor.org/rfc/rfc2246.txt.

[23] E. Rescorla. *Diffie-Hellman Key Agreement Method*. RFC 2631 (Proposed Standard). RFC. Fremont, CA, USA : RFC Editor, juin 1999. DOI : 10.17487/RFC2631. URL : https://www.rfceditor. org/rfc/rfc2631.txt.

[24] M. Crispin. *INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1*. RFC 3501 (Proposed Standard). RFC. Obsoleted by RFC 9051, updated by RFCs 4466, 4469, 4551, 5032, 5182, 5738, 6186, 6858, 7817, 8314, 8437, 8474, 8996. Fremont, CA, USA : RFC Editor, mars 2003. DOI : 10.17487/RFC3501. URL : https://www.rfc-editor.org/rfc/rfc3501.txt.

[25] Y. Rekhter (Ed.) , T. Li (Ed.) et S. Hares (Ed.). *A Border Gateway Protocol 4 (BGP-4)*. RFC 4271 (Draft Standard). RFC. Updated by RFCs 4724, 6286, 6608, 6793, 7606, 7607, 7705, 8212, 8654, 9072, 9687, 9774. Fremont, CA, USA : RFC Editor, jan. 2006. DOI : 10.17487/RFC4271. URL : https://www.rfc-editor.org/rfc/rfc4271.txt.

[26] T. Dierks et E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.1*. RFC 4346 (Historic). RFC. Obsoleted by RFC 5246, updated by RFCs 4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919. Fremont, CA, USA : RFC Editor, avr. 2006. DOI : 10.17487/RFC4346. URL : https://www.rfc-editor.org/rfc/rfc4346.txt.

[27] T. Dierks et E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246 (Proposed Standard). RFC. Obsoleted by RFC 8446, updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685, 7905, 7919, 8447, 9155. Fremont, CA, USA : RFC Editor, août 2008. DOI : 10.17487/RFC5246. URL : https://www.rfc-editor.org/rfc/rfc5246.txt.

[28] D. Cooper et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280 (Proposed Standard). RFC. Updated by RFCs 6818, 8398, 8399, 9549, 9598, 9608, 9618, 9925. Fremont, CA, USA : RFC Editor, mai 2008. DOI : 10.17487/ RFC5280. URL : https://www.rfc-editor.org/rfc/rfc5280.txt.

[29] J. Klensin. *Simple Mail Transfer Protocol*. RFC 5321 (Draft Standard). RFC. Updated by RFC 7504. Fremont, CA, USA : RFC Editor, oct. 2008. DOI : 10.17487/RFC5321. URL : https://www.rfc-editor.org/rfc/rfc5321.txt.

[30] P. Resnick (Ed.). *Internet Message Format*. RFC 5322 (Draft Standard). RFC. Updated by RFC 6854. Fremont, CA, USA : RFC Editor, oct. 2008. DOI : 10.17487/RFC5322. URL : https://www.rfc-editor.org/rfc/rfc5322.txt.

[31] D. Eastlake 3RD. *Transport Layer Security (TLS) Extensions : Extension Definitions*. RFC 6066 (Proposed Standard). RFC. Updated by RFCs 8446, 8449, 9325. Fremont, CA, USA : RFC Editor, jan. 2011. DOI : 10 . 17487 / RFC6066. URL : https://www.rfc-editor.org/rfc/rfc6066.txt.

[32] S. Turner et T. Polk. *Prohibiting Secure Sockets Layer (SSL) Version 2.0*. RFC 6176 (Proposed Standard). RFC. Updated by RFC 8996. Fremont, CA, USA : RFC Editor, mars 2011. DOI : 10.17487/RFC6176. URL : https://www.rfc-editor.org/rfc/rfc6176.txt.

[33] D. Crocker (Ed.) , T. Hansen (Ed.) et M. Kucherawy (Ed.). *DomainKeys Identified Mail (DKIM) Signatures*. RFC 6376 (Internet Standard). RFC. Updated by RFCs 8301, 8463, 8553, 8616. Fremont, CA, USA : RFC Editor, sept. 2011. DOI : 10.17487/RFC6376. URL : https://www.rfc-editor.org/rfc/rfc6376.txt.

[34] M. Lepinski et S. Kent. *An Infrastructure to Support Secure Internet Routing*. RFC 6480 (Informational). RFC. Fremont, CA, USA : RFC Editor, fév. 2012. DOI : 10.17487/RFC6480. URL : https://www.rfc-editor.org/rfc/rfc6480.txt.

[35] G. Huston et G. Michaelson. *Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)*. RFC 6483 (Informational). RFC. Fremont, CA, USA : RFC Editor, fév. 2012. DOI : 10.17487/RFC6483. URL : https://www.rfc-editor.org/rfc/rfc6483.txt.

[36] S. Kitterman. *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1*. RFC 7208 (Proposed Standard). RFC. Updated by RFCs 7372, 8553, 8616. Fremont, CA, USA : RFC Editor, avr. 2014. DOI : 10 . 17487 / RFC7208. URL : https://www.rfc-editor.org/rfc/rfc7208.txt.

[37] R. Barnes et al. *Deprecating Secure Sockets Layer Version 3.0*. RFC 7568 (Proposed Standard). RFC. Updated by RFC 8996. Fremont, CA, USA : RFC Editor, juin 2015. DOI : 10.17487/ RFC7568. URL : https://www.rfc-editor.org/rfc/rfc7568.txt.

[38] S. Bortzmeyer et S. Huque. *NXDOMAIN : There Really Is Nothing Underneath*. RFC 8020 (Proposed Standard). RFC. Fremont, CA, USA : RFC Editor, nov. 2016. DOI : 10 . 17487 / RFC8020. URL : https://www.rfc-editor.org/rfc/rfc8020.txt.

[39] Y. Gilad et al. *The Use of maxLength in the Resource Public Key Infrastructure (RPKI)*. RFC 9319 (Best Current Practice). RFC. Fremont, CA, USA : RFC Editor, oct. 2022. DOI : 10.17487/RFC9319. URL : https://www.rfc-editor.org/rfc/rfc9319.txt.

[40] J. Snijders et al. *A Profile for Route Origin Authorizations (ROAs)*. RFC 9582 (Proposed Standard). RFC. Fremont, CA, USA : RFC Editor, mai 2024. DOI : 10.17487/RFC9582. URL : https://www.rfc-editor.org/rfc/rfc9582.txt.

[41] T. Herr (Ed.) et J. Levine (Ed.) . Domain-Based Message Authentication, Reporting, and Conformance (DMARC). RFC 9989 (Proposed Standard). RFC. Fremont, CA, USA : RFC Editor, mai 2026. DOI : 10 . 17487 / RFC9989. URL : https://www.rfc-editor.org/rfc/rfc9989.txt.

[42] A. Brotman (Ed.). *Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Aggregate Reporting*. RFC 9990 (Proposed Standard). RFC. Fremont, CA, USA : RFC Editor, mai 2026. DOI : 10.17487/RFC9990. URL : https://www.rfc-editor.org/rfc/rfc9990.txt.

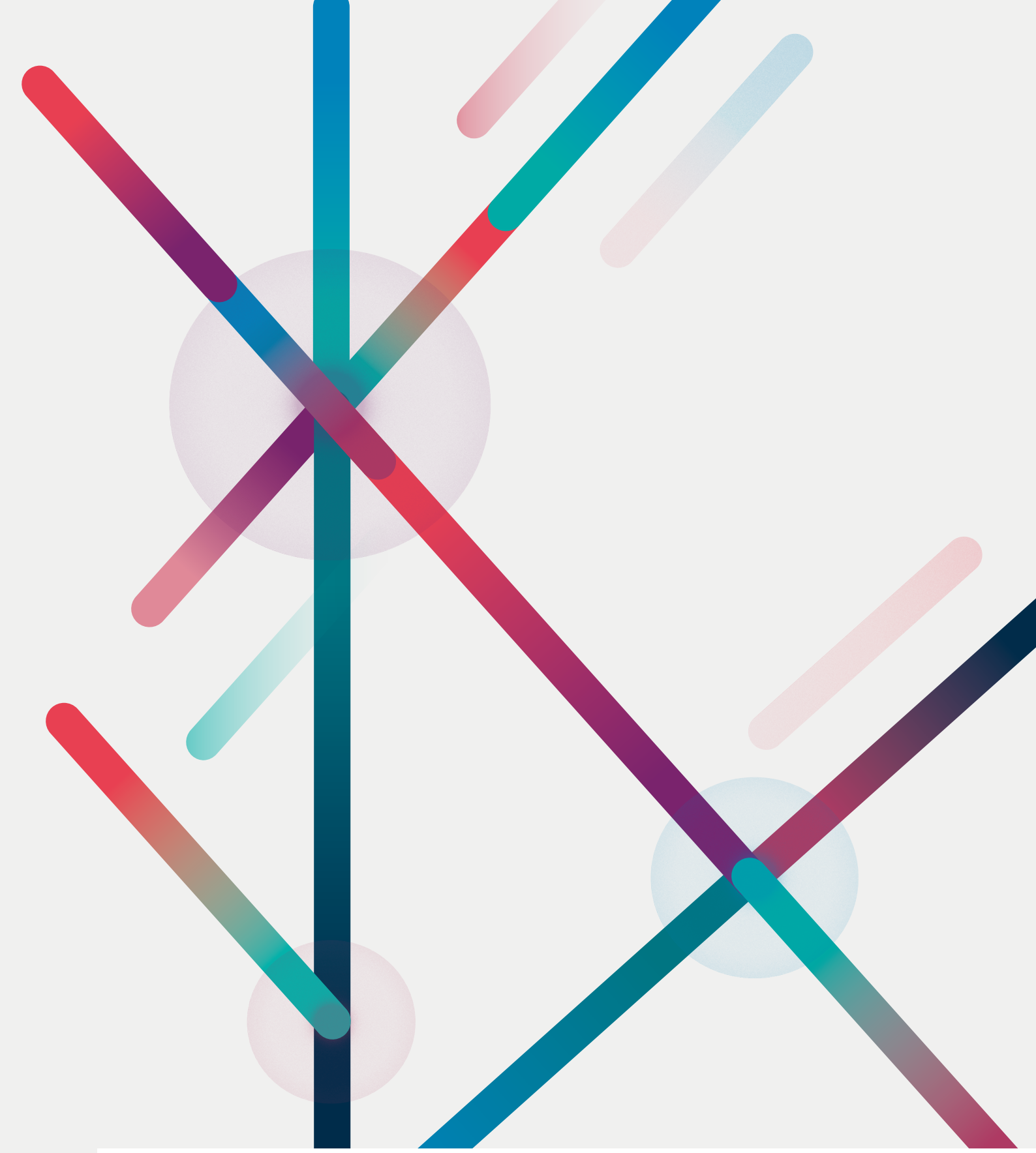
[43] S. Jones (Ed.) et A. Vesely (Ed.). *Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Failure Reporting*. RFC 9991 (Proposed Standard). RFC. Fremont, CA, USA : RFC Editor, mai 2026. DOI : 10 . 17487 / RFC9991. URL : https://www.rfc-editor.org/rfc/rfc9991.txt.

[44] Ivan Ristić . In : *Bulletproof SSL and TLS*. Feisty Duck, jan. 2022.

Acronymes

AC	Autorité de Certification
Afnic	Association Française pour le Nommage Internet en Coopération
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARIN	American Registry for Internet Numbers
AS	Autonomous System
ASPA	Autonomous System Provider Authorization
BGP	Border Gateway Protocol
BGPsec	Border Gateway Protocol Security
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHE	Diffie–Hellman Ephemeral
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Compliance
DNSSEC	Domain Name System Security Extensions
DNS	Domain Name System
DS	Delegation Signer
ECDH	Elliptic Curve Diffie–Hellman
ECDHE	Elliptic Curve Diffie–Hellman Ephemeral
FAI	Fournisseur d'Accès à l'Internet
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IRR	Internet Routing Registry
LIR	Local Internet Registry
MDA	Message Delivery Agent
MSA	Message Submission Agent
MTA	Message Transfer Agent
MUA	Mail User Agent
NSS	Network Security Services
PFS	Perfect Forward Secrecy
POP	Post Office Protocol

PSL	Public Suffix List
RGS	Référentiel Général de Sécurité
RIPE-NCC	RIPE Network Coordination Centre
RIR	Regional Internet Registry
RIS	Routing Information Service
ROA	Route Origin Authorization
ROV	Route Origin Validation
RPKI	Resource Public Key Infrastructure
SMTP	Simple Message Transfer Protocol
SNI	Server Name Indication
SPF	Sender Policy Framework
SPOF	Single Point of Failure
SSL	Secure Sockets Layer
TLD	Top Level Domain
TLS	Transport Layer Security



Novembre 2026

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr