RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS RELATIVES AUX ARCHITECTURES DES SERVICES DNS

GUIDE ANSSI

ANSSI-PA-105
17/07/2024

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Recommandations relatives aux architectures des services DNS ».** Il est téléchargeable sur le site `cyber.gouv.fr`.

Sauf disposition réglementaire contraire, les recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	17/07/2024	Version initiale

Table des matières

1 Préambule **3**
- 1.1 Objectifs de ce guide . . . 3
- 1.2 Le protocole et les services DNS . . . 3
- 1.3 Périmètre du guide . . . 4
- 1.4 Convention de lecture . . . 4

2 Fonctions, services et attaques du DNS **6**
- 2.1 Types de serveurs DNS . . . 6
- 2.2 Services DNS . . . 7
- 2.3 Attaques sur les services DNS . . . 8

3 Principes généraux d'architecture et de sécurisation des services DNS **10**
- 3.1 Cloisonnement des services . . . 10
- 3.2 Cloisonnement des fonctions . . . 12
- 3.3 Sécurisation des services DNS . . . 13
- 3.4 Administration et supervision de sécurité . . . 18

4 Service de résolution des noms de domaine internes **20**
- 4.1 Composition du service . . . 20
- 4.2 Accès au service . . . 20
- 4.3 Architecture physique et logique du service . . . 21

5 Service de résolution des noms de domaine Internet **23**
- 5.1 Composition du service . . . 23
- 5.2 Accès au service . . . 23
- 5.3 Architecture physique et logique du service . . . 25

6 Service d'hébergement des noms de domaine Internet **27**
- 6.1 Composition du service . . . 27
- 6.2 Accès au service . . . 27
- 6.3 Architecture physique et logique du service . . . 27

Liste des recommandations **31**

Bibliographie **32**

1
Préambule

1.1 Objectifs de ce guide

Ce guide traite des architectures et de la sécurisation des services DNS. Il s'adresse aux architectes, RSSI et administrateurs des services DNS d'entités publiques ou privées.

Information

Même si certaines définitions sont rappelées plus loin dans le document, le lecteur est supposé disposer des connaissances minimales sur le protocole DNS, son principe d'architecture hiérarchique ainsi que le caractère récursif ou itératif des requêtes DNS.
Préalablement à la lecture de ce guide, il est recommandé d'avoir lu le guide de l'ANSSI sur les bonnes pratiques pour l'acquisition et l'exploitation des noms de domaine [2].

1.2 Le protocole et les services DNS

Le protocole DNS (*Domain Name System*) a été introduit en 1983 afin de résoudre des noms de domaine Internet en adresses IP. Il est rapidement devenu un protocole clé aussi bien dans le développement des réseaux internes que celui d'Internet. Il a également évolué avec la capacité de résoudre les adresses des serveurs de courriels ou stocker des informations supplémentaires (ex. : enregistrements spécifiques pour la protection contre les courriels indésirables ou pour les signatures DNSSEC).

Les services implémentant le protocole DNS sont désormais incontournables pour le bon fonctionnement des systèmes d'information. Cependant, il est important de souligner que ce protocole n'a été créé qu'avec un minimum de sécurité alors que l'atteinte en disponibilité ou intégrité des services DNS a généralement des conséquences majeures sur l'accès aux services des SI.

Les services DNS étant distribués et reposant sur une architecture hiérarchique, plusieurs acteurs, notamment externes au SI de l'entité considérée dans le cas des DNS publics, participent à son bon fonctionnement. Il est donc indispensable de prendre en compte ces fortes dépendances.

Par ailleurs, l'absence de protection en intégrité et les limites ou l'absence d'authentification peuvent mener à des intrusions ou à des exfiltrations de données.

Enfin, la potentielle mutualisation des moyens informatiques pour les besoins de DNS internes, d'une part, et ceux pour l'interconnexion à Internet de l'autre, peut augmenter la surface d'attaque du SI de l'entité.

1.3 Périmètre du guide

Ce guide présente des recommandations pour la sécurisation des architectures de trois services DNS :

- le service DNS de résolution des noms de domaine internes ;
- le service DNS de résolution des noms de domaine Internet ;
- le service DNS d'hébergement des noms de domaine Internet.

Les deux premiers services sont mis en œuvre et configurés par une entité pour ses utilisateurs internes, alors que le dernier est destiné à ses partenaires et clients externes. Ces services sont présentés en détail dans le chapitre 2.

1.4 Convention de lecture

Pour certaines recommandations de ce guide, il est proposé, compte tenu de l'état de la menace constaté lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Par ailleurs, dans ce guide, l'utilisation du verbe « *devoir* » ou encore les formulations « *il faut* » ou « *il est important* » ou « *il est nécessaire* » sont volontairement plus prescriptives que les formulations « *il est recommandé* » ou « *il est conseillé* ».

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R --

Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

R +

Recommandation renforcée complémentaire

Cette recommandation complémentaire permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information.

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information [1], la pertinence de la mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

Quelles que soient les recommandations finalement retenues, l'application de ces mesures ne peut en aucun cas remplacer une évaluation du niveau de sécurité du SI par un audit, ni dispenser d'évaluer le niveau de risque résiduel sur les actifs métier.

La liste récapitulative des recommandations est disponible en page 31.

1. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [7].

2
Fonctions, services et attaques du DNS

Selon ses besoins, une entité propose plusieurs fonctions liées au DNS. Ces fonctions sont listées et rappelées dans la section 2.1. Ces fonctions sont portées par un ou plusieurs services DNS au sein du SI de l'entité, décrits dans la section 2.2. La section 2.3 décrit les menaces auxquelles ces services peuvent être confrontés.

Les chapitres suivants (3 à 6) présentent différents exemples d'architectures associées à ces services, selon la finalité du service et le niveau de sécurité recherché.

2.1 Types de serveurs DNS

Le présent guide fait référence à différentes fonctions DNS portées par les serveurs suivants :

Serveur faisant autorité

Un serveur faisant autorité est un serveur DNS (parfois abusivement appelé *serveur SOA* [2]) répondant aux requêtes DNS pour les zones placées sous son autorité (par exemple, le serveur DNS faisant autorité sur la zone *cyber.gouv.fr*) sans devoir faire appel à d'autres serveurs DNS. Il dispose de la base de données des enregistrements relatifs à chacune de ces zones.

Serveur primaire

Un serveur primaire est un serveur DNS faisant autorité sur lequel les modifications des enregistrements d'une zone sont réalisées. Un serveur primaire est dit « caché » lorsque ses interactions sont limitées aux serveurs secondaires.

Ce serveur est particulièrement critique dans la mesure où sa compromission entraîne la compromission de toutes les zones qui lui sont attachées.

Serveur secondaire

Un serveur secondaire est un serveur DNS faisant autorité disposant d'une copie de la base de données du serveur primaire. Cette base est mise à jour régulièrement à l'aide d'un mécanisme nommé *transfert de zone*.

La compromission d'un serveur secondaire, bien que dommageable, peut être résolue par un retrait du serveur compromis.

2. *Start Of Authority.*

Serveur récursif

Un serveur récursif est un serveur DNS capable de parcourir la hiérarchie DNS lorsqu'il ne connaît ni la réponse à la requête ni le serveur faisant autorité associé au domaine recherché.

Serveur cache

Un serveur cache est un serveur DNS portant une fonction lui permettant de stocker les réponses aux requêtes DNS qui lui sont adressées. À la réception d'une requête DNS, ce serveur consulte d'abord son cache. S'il détient la réponse, celle-ci est fournie directement au client améliorant ainsi les performances du service.

Serveur relais

Un serveur relais (ou *forwarder*) est un serveur DNS servant d'intermédiaire à un groupe de machines pour la résolution de noms de domaines. Ce serveur ne résout pas les noms de domaine lui-même, mais relaye les requêtes vers un serveur DNS cache/récursif. Cette fonction peut être utile pour des raisons opérationnelles de résilience ou de partage de charge.

Attention

Afin de faciliter la lecture du guide, et parce que les deux fonctions sont usuellement portées par un même serveur, la notion de « serveur cache » sera ici utilisée afin de désigner un serveur à la fois cache et récursif.

Attention

Outre l'amélioration des performances du service DNS, la mise en œuvre d'une fonction de cache permet, pour certains cas d'usage, de réduire l'exposition des serveurs faisant autorité, et les risques de compromission de ces derniers. Néanmoins, il est important de noter que la mise en œuvre de cette fonction peut aussi prolonger dans le temps les compromissions, notamment lors d'un empoisonnement du cache.

Information

Sauf mention contraire, l'ensemble des figures de ce document ne préjugent pas du niveau de mutualisation de ces serveurs et services sur l'infrastructure sous-jacente.

2.2 Services DNS

Ce guide s'intéresse à trois services DNS qu'une entité peut être amenée à déployer.

Service DNS de résolution des noms de domaine internes

Pour les besoins strictement internes du SI (hors interconnexion à Internet), une entité met en œuvre un service DNS de résolution des noms de domaine internes.

Ce service a vocation à être exposé exclusivement sur le SI interne de l'entité.

Service DNS de résolution des noms de domaine Internet

Afin de fournir la résolution des noms de domaine Internet aux systèmes internes de l'entité qui ont un besoin opérationnel (ex. : serveurs mandataires pour la navigation Web ou applications métier qui ont des échanges avec Internet), une entité met en œuvre un service DNS de résolution des noms de domaine Internet.

Service DNS d'hébergement des noms de domaine Internet

Héberger un ou plusieurs noms de domaine Internet implique l'exposition sur Internet de serveurs DNS faisant autorité sur ces domaines. Ce service permet à un serveur cache ou, plus rarement, un poste client, de résoudre les noms portés par ces domaines.

Attention

Un service d'hébergement exposé sur Internet implique des flux entrants sur une partie du SI de l'entité. Cela nécessite donc une maturité forte de l'entité sur les problématiques de sécurité afférentes. Dans le cas contraire, le recours à un prestataire de confiance est préférable.

2.3 Attaques sur les services DNS

De nombreuses attaques informatiques s'appuient sur le détournement du protocole DNS ou la compromission des serveurs participant aux résolutions de noms de domaines. Les principaux types d'attaques sont détaillés ci-dessous.

Attaque par redirection DNS (DNS hijacking)

Ce type d'attaque consiste à rediriger les requêtes d'une victime vers un service contrôlé par un attaquant. À titre d'exemple, rediriger des victimes vers des sites Web usurpant l'identité visuelle de certains services en vue de récupérer des données d'utilisateurs. Pour procéder à cette redirection, l'attaquant peut compromettre un serveur DNS afin d'y modifier ses enregistrements. Ces compromissions peuvent viser les serveurs de type « cache » ou « faisant autorité » dont les détails sont décrits en section 2.1.

Empoisonnement de cache DNS (DNS poisonning)

Dans le cas d'une compromission des réponses fournies à la suite d'une requête d'un serveur DNS cache (voir section 2.1), il est possible de modifier les entrées dans le cache du DNS afin de faire correspondre aux noms de domaine qui y sont répertoriés des adresses IP sous contrôle d'un attaquant. L'empoisonnement de cache DNS peut se propager à d'autres caches DNS.

Usurpation DNS (DNS spoofing)

Lors d'une requête DNS envoyée par un client, une attaque de type usurpation DNS consiste pour l'attaquant à envoyer une réponse malveillante à la place du serveur DNS interrogé, ou à modifier la réponse légitime de ce dernier. Ces attaques de type « homme du milieu » ne nécessitent aucune

interaction préalable avec la victime ni la compromission d'un serveur DNS. Il est intéressant de noter qu'une usurpation DNS peut occasionner l'empoisonnement des caches de serveurs DNS.

Détournement de noms de domaine

Il est possible pour un attaquant de prendre le contrôle d'un nom de domaine à travers la compromission directe du système d'information du registraire [3] ou celui de l'hébergeur du domaine opérant les serveurs de noms faisant autorité, ou encore en récupérant les accès d'administration légitimes du détenteur du nom de domaine. Il peut ainsi associer des domaines légitimes à des adresses IP sous son contrôle ou créer de nouveaux sous-domaines illégitimes auxquels seront également associées des adresses IP qu'il contrôle.

Communications malveillantes au travers d'un tunnel DNS

Il est aussi possible pour un attaquant d'utiliser le protocole DNS afin de faire communiquer discrètement deux systèmes. Par exemple, un code malveillant sur un système compromis communiquant avec une infrastructure de commande et de contrôle extérieure à ce système. Il est également possible de procéder à de l'exfiltration de données de cette manière.

Attaques par réflexion et amplification DNS

La taille des paquets d'une réponse à une requête DNS peut être plus importante que la taille des requêtes. Le ratio de tailles entre les requêtes et les réponses est appelé « facteur d'amplification ». Le facteur d'amplification potentiellement élevé du protocole DNS fait de ce dernier un moyen de choix pour des attaques de type déni de service distribué (DDoS [4]).

Les communications DNS s'appuyant traditionnellement sur UDP, protocole non connecté, un attaquant peut générer un très grand volume de données à destination d'une victime. Pour cela, il peut forger un grand nombre de requêtes DNS depuis un réseau de machines compromises en remplaçant l'adresse IP source de ces requêtes par l'adresse IP de leur victime (procédé de « réflexion »).

Attaques en déni de service contre un serveur DNS

Enfin, les services DNS sont par nature très exposés. Ce niveau d'exposition en fait une cible privilégiée pour les attaques en disponibilité de type DoS [5] le rendant incapable de répondre à des requêtes DNS. Ces attaques usuelles ne consistent pas en une manipulation du protocole DNS même, mais il est intéressant de les évoquer, au vu des conséquences qu'elles peuvent avoir sur la disponibilité des systèmes d'information en général.

3. Également appelé « bureau d'enregistrement » ou *registrar* en anglais, il désigne l'entité gérant la réservation des noms de domaines Internet.
4. L'acronyme anglais DDoS pour *Distributed Denial of Service* est le plus couramment utilisé.
5. *Denial of Service*.

3
Principes généraux d'architecture et de sécurisation des services DNS

Quels que soient les services DNS proposés par une entité, des principes généraux s'appliquent pour en optimiser la sécurité :

- cloisonner les services selon leur exposition (section 3.1);
- cloisonner les fonctions qu'ils portent (section 3.2);
- sécuriser les fonctions, protocoles et infrastructures portant les services DNS (section 3.3);
- sécuriser des moyens pour administrer les services DNS (section 3.4).

3.1 Cloisonnement des services

Les services DNS peuvent être distingués en deux types selon leur exposition :

- les services DNS *internes*, exposés sur le SI interne : le service DNS de résolution des noms de domaine internes exposé aux seules ressources internes de l'entité (postes de travail, serveurs);
- les services DNS *externes*, interconnectés avec Internet : d'une part le service DNS de résolution des noms de domaine Internet exposé à ses clients internes spécifiques et nécessitant un accès vers Internet; et d'autre part le service DNS d'hébergement des noms de domaine Internet nécessitant une exposition sur Internet à des clients externes.

La distinction entre ces deux types de services DNS permet l'application d'un premier grand principe d'architecture de SI sécurisé : proscrire la mutualisation des infrastructures dès lors que les services ou fonctions qu'elles soutiennent ont des sensibilités ou des niveaux d'exposition différents. Ainsi l'exposition des services DNS *externes* implique un cloisonnement strict de ceux-ci.

Attention

La notion de services DNS *externes* utilisée dans ce guide signifie bien « en interaction avec l'extérieur » ou « en interaction avec Internet » et ne préjuge pas si le service est hébergé par un tiers externe à l'entité ou non.

R1

Cloisonner physiquement les infrastructures entre services DNS internes et externes

Le niveau de menace induit par une exposition à Internet impose un cloisonnement physique des infrastructures entre services internes et externes. Comme tous les services exposés ou accédant à Internet, les services DNS externes doivent être placés dans une passerelle d'interconnexion sécurisée avec des ressources dédiées (serveurs, pare-feux, commutateurs). À l'inverse, le service DNS interne doit rester à l'intérieur du SI de l'entité.

Afin de réduire fortement les risques portant sur l'intégrité et la disponibilité des services DNS, l'ensemble des flux entre ces deux types de services doivent être bloqués afin de ne laisser aucune adhérence entre eux.

R2

Interdire les flux entre services DNS internes et externes

Les flux entre les services DNS *internes* et les services DNS *externes* doivent être interdits.

La définition dans ce guide des bonnes pratiques en matière d'architecture de ces services DNS *externes* se fait en adéquation avec le guide de l'ANSSI relatif à l'interconnexion d'un SI à Internet [9]. Plusieurs recommandations faites ici sont donc le résultat de l'application des grands principes de sécurité des interconnexions avec Internet adaptés au contexte spécifique des services DNS.

Dans le contexte des services DNS *externes*, le service DNS d'hébergement des noms de domaine Internet et le service DNS de résolution des noms de domaine Internet sont de niveaux d'exposition différents. Ils trouvent donc naturellement leur place dans deux zones de sécurité distinctes. Au-delà du cloisonnement physique des services DNS *externes*, le guide sur l'interconnexion d'un SI à Internet recommande aussi en particulier la mise en œuvre d'un cloisonnement, si possible physique, entre ces différentes zones de sécurité.

R3

Suivre les recommandations du guide sur les passerelles Internet sécurisées pour les services DNS externes

Il est nécessaire d'appliquer aux services DNS *externes* les recommandations du guide de l'ANSSI sur l'interconnexion d'un système d'information à Internet [9]. Respecter en particulier les bonnes pratiques de cloisonnement entre les différents services. La figure 1 illustre un exemple de cloisonnement minimum des services DNS dans un SI.

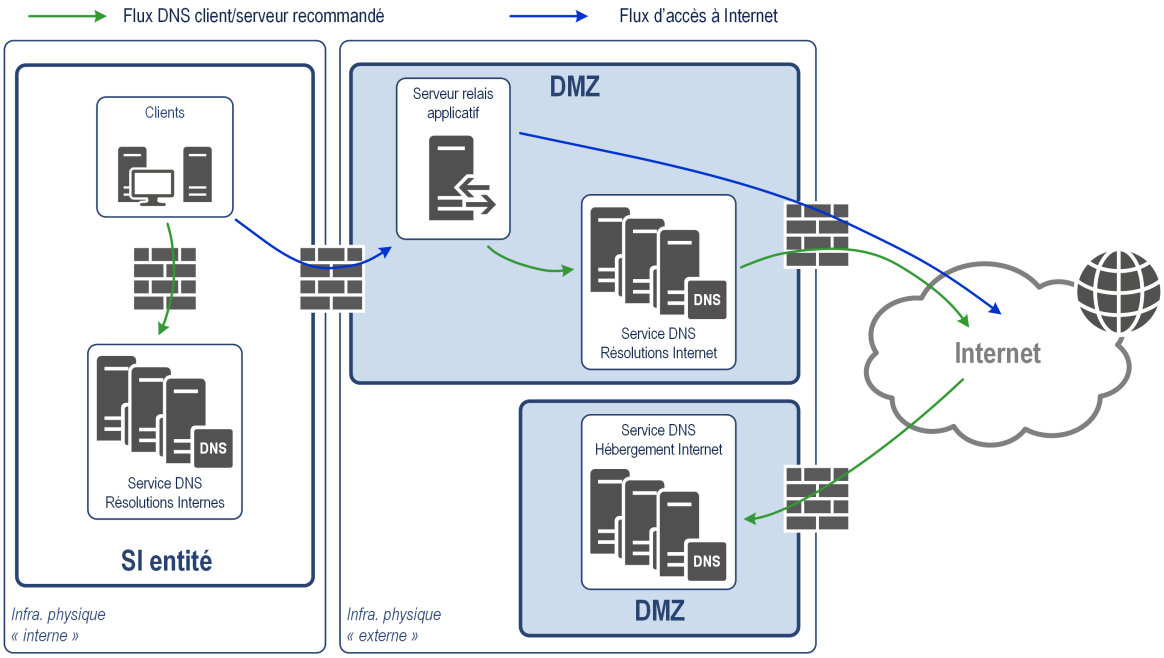

FIGURE 1 – Exemple de cloisonnement minimum des services DNS dans le SI de l'entité

3.2 Cloisonnement des fonctions

Les solutions logicielles DNS du marché permettent de disposer de plusieurs fonctions distinctes avec l'exécution d'une seule instance logicielle. Chaque fonction ayant un besoin de sécurité et un niveau d'exposition qui lui est propre, une bonne pratique consiste à ne pas mutualiser des fonctions distinctes avec une même instance logicielle. Pour la même raison, l'exécution d'instances logicielles supportant des fonctions distinctes sur un même serveur doit être évitée.

R4

Cloisonner les fonctions DNS sur des serveurs distincts

Les différentes fonctions DNS doivent être déployées dans des environnements système distincts (serveur physique ou machine virtuelle).
Il est néanmoins acceptable de mutualiser les fonctions de cache et de serveur récursif sur une même instance.

Information

À la date d'écriture de ce guide, le cloisonnement de processus et d'applications à travers l'utilisation de machines virtuelles a fait preuve d'une plus grande robustesse que le cloisonnement par conteneurs. Ainsi, l'emploi de conteneurs ne peut être considéré pour le moment comme adapté pour le cloisonnement de fonctions DNS différentes, en particulier lorsqu'elles n'ont pas la même exposition.

3.3 Sécurisation des services DNS

Filtrage réseau

Si le cas du filtrage des flux réseau entre les fonctions d'un même service DNS est traité dans les chapitres propres à chaque service, il est globalement recommandé de filtrer tous les types de flux au seul besoin opérationnel légitime.

R5

Filtrer les flux réseau

Il est nécessaire de filtrer les flux réseau au seul besoin opérationnel légitime. Ce filtrage est particulièrement important lors des interactions entre le SI interne et Internet, ainsi que lors des transferts de zone entre serveurs DNS.

Serveur primaire caché (Hidden master)

Un serveur primaire caché a la particularité de n'interagir qu'avec les serveurs secondaires et, plus particulièrement, de n'autoriser les transferts de zone qu'à destination de ces derniers. En particulier, les clients finaux et les serveurs récursifs ne sont pas autorisés à lui soumettre de requêtes. Dans le contexte d'un service d'hébergement des noms de domaine Internet, ce serveur caché n'apparaît pas dans les enregistrements de la zone DNS.

Ce type de déploiement permet de protéger l'intégrité des données hébergées sur le serveur primaire en limitant leur exposition.

R6

Déployer un serveur primaire caché

Il est nécessaire de mettre en œuvre le serveur primaire comme serveur *caché* afin de maîtriser son exposition et les données qu'il héberge.

Dans la suite du document, l'expression *serveur primaire caché*, lorsque employée seule, désigne donc un serveur primaire ne traitant pas de requêtes directes de la part des clients, celles-ci étant traitées par les serveurs secondaires.

Protection des transferts de zone

Les transferts de zone entre le serveur primaire et les serveurs secondaires doivent être protégés afin de garantir l'intégrité des données des zones. Il est possible d'utiliser le protocole TSIG (*Transaction signature*). Ce protocole permet une authentification entre les parties ainsi qu'une protection en intégrité des données à travers l'utilisation d'un secret partagé et d'une fonction de hachage.

R7

Protéger en intégrité les transferts de zones avec TSIG

La protection des transferts de zones entre le serveur primaire et les serveurs secondaires doit être assurée au minimum avec le protocole TSIG. Respecter les recommandations du guide des mécanismes cryptographiques [10] pour le choix de la

fonction de hachage.

Si des besoins supplémentaires de protection en confidentialité des données se révèlent nécessaires, les transferts de zone peuvent être protégés en utilisant TLS (« XoT »[6], Zone transfer over TLS).

R7 +

Protéger en intégrité les transferts de zones avec XoT

La protection des transferts de zones entre le serveur primaire et les serveurs secondaires peut être assurée avec TLS. La configuration de TLS doit être conforme aux recommandations du guide TLS de l'ANSSI [8].

Diversification logicielle

Afin de réduire les risques de perte de disponibilité des services DNS liés à une faille ou plus simplement à un dysfonctionnement logiciel, il est recommandé de diversifier les logiciels assurant une même fonction d'un service DNS. En cas de perte des instances d'exécution d'une fonction assurée par un logiciel, la disponibilité globale de la fonction est assurée par les instances d'exécution d'autres logiciels.

L'objectif est de pouvoir disposer simultanément d'au moins deux solutions logicielles différentes en service pour répondre aux requêtes clientes. En cas d'anomalie sur l'une des deux solutions, celle-ci pourra être neutralisée temporairement, mais le service restera disponible uniquement avec la seconde solution. Le nombre d'instances en service de la seconde solution est augmenté afin de compenser la neutralisation de la solution en dysfonctionnement et ainsi éviter une dégradation du service.

R8 +

Diversifier les logiciels DNS

Il est recommandé de diversifier les logiciels pour réaliser une même fonction d'un service DNS ou entre les différentes fonctions d'un même service DNS.

Attention

Si la mise en œuvre de plusieurs solutions logicielles est recommandée, cette mise en œuvre ne peut se faire que dans le cas où les équipes en charge du service possèdent un niveau de compétences suffisant et où la charge supplémentaire de maintien en conditions opérationnelles et de sécurité peuvent être absorbées. Certains logiciels comme BIND peuvent remplir toutes les fonctions mais peuvent se révéler assez complexes. Certains comme NSD (pour les serveurs faisant autorité), Unbound (pour les serveurs récursifs/caches) ou encore Dnsmasq (pour les serveurs Relais), sont plus simples. La mise en œuvre de solutions maîtrisées reste prioritaire par rapport à la diversification logicielle.

6. https://datatracker.ietf.org/doc/rfc9103/

Durcissement des systèmes et applications

Considérant le niveau de sensibilité des services DNS et leur niveau d'exposition, notamment ceux en interaction avec Internet, il est nécessaire de porter une attention toute particulière sur le durcissement des configurations de l'ensemble des éléments composant les services.

R9

Durcir les composants des services DNS

Il est nécessaire de procéder au durcissement de l'ensemble des équipements participant à la fourniture des services DNS. Cette recommandation s'applique entre autres aux pare-feux, serveurs, commutateurs et logiciels sur la chaîne de traitement des services.

Information

À ce titre, le lecteur est invité à lire l'ensemble des guides ANSSI suivants :

- Recommandations pour la sécurisation d'un commutateur de desserte [1];
- Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu [4];
- Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet [6];
- Recommandations de sécurité relatives à un système GNU/Linux [3].

Afin de limiter les risques de propagation latérale d'une intrusion entre serveurs, il est recommandé d'activer leur pare-feu local.

Plus généralement, cette mesure s'inscrit dans une démarche de défense en profondeur permettant d'élever significativement le niveau de sécurité global des infrastructures des services DNS.

R10

Activer le pare-feu local des serveurs DNS

Le pare-feu local de chaque serveur DNS doit être activé avec une politique de filtrage adaptée au juste besoin opérationnel.

DNSSEC

DNSSEC est un protocole de sécurité adossé au protocole DNS permettant d'améliorer significativement l'intégrité et l'authenticité des informations transmises lors de requêtes de noms entre un serveur récursif et un serveur faisant autorité. Cette intégrité est maintenue à travers la mise en œuvre d'une chaîne de confiance, elle-même s'appuyant sur des mécanismes de signatures et de validation par les différents acteurs sur cette chaîne.

DNSSEC offre deux avantages majeurs :

- Le premier est qu'il représente une mesure efficace contre les empoisonnements de cache (cf. section 2.3). Un serveur DNS procédant à des requêtes DNSSEC est en mesure de valider les

signatures de la chaîne récursive et de rejeter les réponses issues d'un empoisonnement, ces dernières n'étant pas signées par les serveurs faisant autorité sur ces domaines.

- Le deuxième est qu'il apporte une plus-value dès lors qu'il est mis en œuvre en complément de protocoles tels que SPF, DKIM, DMARC[7], DANE, etc. Ceux-ci visent à protéger les communications de certaines applications et s'appuient à cette fin sur les enregistrements DNS. DNSSEC est alors un complément indispensable pour la protection en intégrité et en authenticité des informations du DNS.

À ces avantages, spécifiques à certains cas d'usages ou risques bien identifiés, s'ajoutent plusieurs inconvénients et limites.

Le déploiement de DNSSEC soulève plusieurs questions importantes qu'il convient de traiter en amont, par exemple :

- Quelles menaces cherche-t-on à contrer et quels risques cherche-t-on à couvrir ?
- Quelles solutions de sécurité sont éventuellement déjà en place pour couvrir ces risques (exemple : certificats TLS sur le service final) ?
- Quelles sont les zones DNS concernées, où sont-elles hébergées et quelles sont les zones dont elles dépendent sur la chaîne ?
- Quel est le niveau de compétence des administrateurs – internes ou externes – et quels moyens leur sont-ils alloués ?
- Comment les administrateurs gèrent-ils les rotations de clés, les enregistrements, les relations avec les responsables des zones parentes ?
- Si la gestion du DNS est externe, quels sont les coûts et quelles sont les garanties apportées par le prestataire ?
- Comment prendre en compte la réversibilité dans le cas d'un changement de prestataire ?

Attention

Ce guide ne recommande pas formellement l'implémentation de DNSSEC. Ce sont les questions ci-dessus et le niveau de maturité atteignable qui doivent guider les DSI et les responsables SSI afin de prendre une décision éclairée sur la mise en œuvre ou non de DNSSEC sur les zones portées par leurs propres DNS. Cette décision doit se prendre à travers une analyse de risque.

R11

Procéder à une analyse de risque spécifique à DNSSEC

La décision de mise en œuvre de DNSSEC dans une entité doit s'appuyer sur une analyse de risque prenant en compte les coûts et bénéfices spécifiques à ce protocole.

Il est important de considérer la complexité du protocole DNSSEC car sa maîtrise nécessite des compétences fortes et un nombre conséquent de ressources, tant humaines que techniques.

7. https://www.afnic.fr/observatoire-ressources/papier-expert/protegez-vos-e-mails-grace-au-dns-spf-dkim-dmarc/

D'une part le déploiement de DNSSEC implique un processus de génération, de séquestre et de gestion de secrets qui n'est pas trivial. D'autre part, il entraîne également la mise en œuvre d'un processus complexe de gestion de signature des enregistrements, de leur période de validité, de la publication de ces enregistrements ainsi que des clés correspondantes dans les zones parentes.

R12

Définir un processus de gestion spécifique à DNSSEC

Définir et mettre en œuvre un processus spécifique à la gestion des secrets et aux signatures pour DNSSEC. Ce processus doit s'accompagner de la mise en œuvre de moyens techniques et organisationnels à l'état de l'art.

Attention

Une erreur sur la configuration de DNSSEC sur la chaîne de confiance ou encore sur la gestion des signatures peut entraîner un impact conséquent sur l'ensemble des résolutions de noms. Cet impact peut aller jusqu'à l'indisponibilité totale du domaine signé par DNSSEC pendant plusieurs heures ou plusieurs jours.

À ces processus s'ajoute la nécessité de mettre en œuvre une surveillance spécifique du bon fonctionnement des entrées DNSSEC sur les zones concernées ainsi que la bonne publication des clés sur la totalité de la chaîne.

R13

Mettre en œuvre une supervision spécifique à DNSSEC

Une supervision spécifique à DNSSEC doit être mise en œuvre afin de détecter les événements propres à DNSSEC tels qu'une erreur de configuration, l'expiration d'une signature ou d'une clé, un changement non planifié, ou une incohérence dans la chaîne de confiance.

Enfin, DNSSEC n'apporte pas non plus de garantie sur la véracité de l'information. En effet, le risque d'une modification frauduleuse par des moyens légitimes – tel que la compromission d'un portail de gestion des enregistrements mis à disposition d'un prestataire pour un client – ne peut être couvert par DNSSEC puisque le prestataire de service DNS signe avec DNSSEC ces modifications frauduleuses.

Néanmoins la mise en œuvre de la validation DNSSEC sur les serveurs cache reste une mise en œuvre relativement simple et permet d'améliorer la confiance dans les réponses DNS publiques.

R14

Activer DNSSEC sur le service DNS de résolution des noms de domaine Internet

Il est recommandé d'activer la validation DNSSEC sur les serveurs cache/récursifs publics. Une analyse particulière doit être menée en amont de la mise en œuvre de cette mesure afin de déterminer si l'échec de la validation DNSSEC doit être suivie ou non d'une résolution DNS classique.

Information

Sur les questions liées à la mise en œuvre de DNSSEC, la lecture du document de l'AFNIC « Déployer DNSSEC, comment, quoi, où ? » [8] est recommandée.

3.4 Administration et supervision de sécurité

Les moyens d'administration de tout système d'information, en particulier ceux des services critiques tels que le DNS, sont une cible de choix pour un attaquant. En effet, leur compromission peut avoir des conséquences importantes sur la disponibilité voire l'intégrité du SI.

Afin de limiter la surface d'attaque de ces moyens, l'ANSSI recommande fortement l'application des mesures présentes dans le guide sur l'administration sécurisée des systèmes d'information [11].

R15

Appliquer les bonnes pratiques d'administration sécurisée

L'administration des services DNS doit être conforme aux bonnes pratiques d'administration sécurisée des SI présentées dans le guide afférent de l'ANSSI [11].

Attention

S'il y a bien lieu de distinguer l'administration des infrastructures techniques hébergeant les services DNS (ex. : administration des serveurs) et l'administration fonctionnelle du service DNS (ex. : modification des fichiers de zone), les recommandations d'accès sécurisés aux différentes interfaces d'administration sont valables quelle que soit la population d'administrateurs et quel que soit le contexte (ex. : hébergement du service sur une plateforme de type *cloud*).

Si le niveau de sécurité des plateformes et applications DNS courantes s'est significativement amélioré, leur niveau de criticité reste élevé. Il convient de formaliser et appliquer avec attention un processus de maintien en condition de sécurité (MCS) de ces services.

R16

Formaliser et appliquer un processus de MCS des services DNS

Le processus de MCS doit inclure non seulement l'application des mises à jour de sécurité des logiciels mais aussi une veille sur les événements de sécurité liés aux services DNS.

Enfin, les services DNS doivent être en capacité de transférer leurs journaux d'événements afin d'alimenter les systèmes de supervision de la sécurité du SI pour la détection des attaques portant atteinte aux services DNS ou utilisant les flux DNS. Ces journaux permettent aussi la corrélation avec d'autres événements de sécurité.

8. https://www.afnic.fr/wp-media/uploads/2021/01/Afnic-dnssec-howto-fr-v3.pdf

R17

Centraliser la journalisation des services DNS

Les journaux d'événements des services DNS doivent être centralisés et intégrés aux systèmes de supervision de sécurité du SI.

4
Service de résolution des noms de domaine internes

Ce chapitre décrit les bonnes pratiques applicables à un service DNS proposant de résoudre des noms de domaines internes, à destination d'équipements eux aussi internes. Après un rappel des fonctions associées à ce service (section 4.1), les contraintes d'accès sont décrites (section 4.2) avant d'en présenter l'architecture (section 4.3).

4.1 Composition du service

Le service DNS de résolution des noms de domaine internes est usuellement constitué de trois fonctions :

- une fonction de DNS *primaire caché* ;
- une fonction de DNS *secondaire* ;
- une fonction de cache.

4.2 Accès au service

Considérant le cloisonnement physique recommandé en section 3.1, le service DNS de résolution des noms de domaine internes est isolé d'Internet et ne doit pas permettre la résolution des noms de domaine Internet (ce service doit être assuré par le service DNS de résolution des noms de domaine Internet, possiblement à travers l'utilisation d'un serveur Relais, cf. chapitre 5).

R18

DNS-PRIV - Interdire la résolution de noms de domaine Internet

La résolution des noms de domaine Internet par le service DNS de résolution des noms de domaine internes doit être interdite.

Le service DNS de résolution des noms de domaine internes a pour objet de fournir exclusivement la résolution de noms de domaine internes à des équipements internes. L'exposition du service DNS de résolution des noms de domaine internes doit donc être limitée au réseau et aux ressources interne du SI.

R19

DNS-PRIV - Interdire les accès au service depuis Internet

L'accès au service DNS de résolution des noms de domaine internes doit être limité aux équipements internes. Son accès doit être interdit depuis Internet.

Information

Dans un contexte de nomadisme, il est recommandé de consulter le guide de l'ANSSI sur les « recommandations sur le nomadisme numérique » [12], en particulier son paragraphe 3.4.3.3 sur la maîtrise des flux DNS des terminaux.

Enfin, les serveurs faisant autorité (primaire et secondaires) pour les zones internes ne doivent pas être exposés directement aux équipements internes et ne doivent pas recevoir de requêtes directes de ces derniers. Un serveur portant la fonction de cache doit être mis en œuvre afin de traiter les requêtes clientes.

R20

DNS-PRIV - Limiter l'accès des clients au seul serveur cache

Les requêtes DNS des clients doivent être adressées exclusivement au serveur cache. Ce serveur cache interroge un serveur faisant autorité dans les cas où il n'est pas en mesure d'apporter seul une réponse à la requête cliente.

4.3 Architecture physique et logique du service

La figure 2 présente une proposition d'architecture d'un service de résolution de noms de domaines internes.

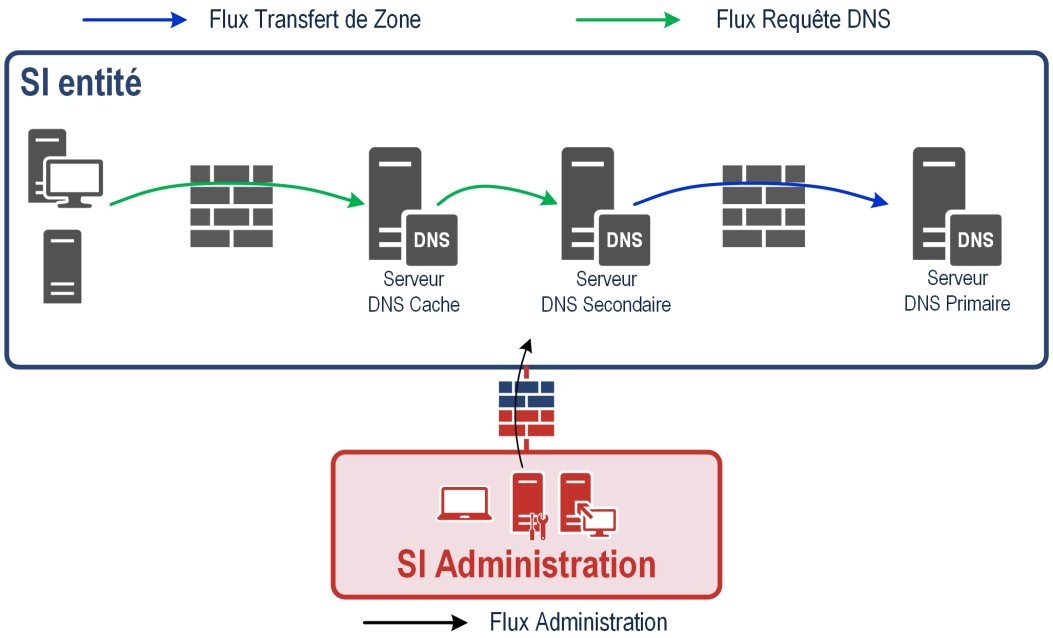

FIGURE 2 – Exemple d'architecture d'un service DNS interne

Les fonctions mises en œuvre étant de nature et d'exposition différentes, celles-ci doivent être cloisonnées, au moins logiquement, entre elles. Les serveurs faisant autorité (primaire et secondaires) sont les garants de l'intégrité des données qu'ils hébergent. Leur niveau de sensibilité impose la mise en œuvre d'un cloisonnement physique de ces derniers.

R21

DNS-PRIV - Cloisonner les fonctions DNS

Les différentes fonctions du service DNS de résolution des noms de domaine internes doivent être cloisonnées entre elles au moins logiquement tant au niveau système (ex. : machine physique ou virtuelle) qu'au niveau réseau (ex. : commutateur physique ou VLAN dédié). Les serveurs faisant autorité doivent être cloisonnés physiquement des serveurs portant des fonctions différentes.

Afin de limiter l'exposition des services au strict nécessaire, une fonction de filtrage doit être mise en œuvre afin de limiter les échanges.

R22

DNS-PRIV - Filtrer les flux et échanges internes

Les flux entre les différentes fonctions DNS du service DNS de résolution des noms de domaine internes doivent être filtrés selon le strict besoin opérationnel. Pour cela, il est recommandé d'utiliser un équipement de type pare-feu.

Information

Dans un contexte de DNS *interne*, et suivant les résultats de l'analyse de risques, les fonctions de filtrage représentées sur la figure 2 peuvent être mutualisées sur un même pare-feu.

5
Service de résolution des noms de domaine Internet

Ce chapitre décrit les bonnes pratiques applicables à un service DNS proposant de résoudre des noms de domaines sur Internet, à destination d'équipements internes. Après un rappel de la fonction associée à ce service (section 5.1), les contraintes d'accès sont décrites (section 5.2) avant d'en présenter l'architecture (section 5.3).

5.1 Composition du service

Le service DNS de résolution des noms de domaine Internet est constitué d'une seule fonction DNS : une fonction de cache portée par un ou plusieurs serveurs.

5.2 Accès au service

Afin de limiter son exposition, un filtrage conforme au strict besoin opérationnel doit être mis en œuvre au niveau du service DNS de résolution des noms de domaine Internet pour réduire les risques d'utilisation du service dans le cas d'une attaque. Ce besoin s'inscrit là encore dans les recommandations du guide ANSSI sur l'interconnexion des SI à Internet [9] et l'éclairage qu'il apporte dans sa section dédiée au DNS.

Dans le cas d'usage considéré ici, le service DNS de résolution des noms de domaine Internet ne doit pas recevoir de requête directe depuis des réseaux autres que les réseaux internes autorisés de l'entité.

R23

DNS-PUB - Interdire les accès au service depuis Internet

L'accès au service DNS de résolution des noms de domaine Internet doit être limité aux équipements internes. Son accès doit être interdit depuis Internet ou un réseau tiers.

Concernant les requêtes internes, la résolution des noms de domaine Internet doit être interdite par défaut aux équipements terminaux (postes utilisateurs ou serveurs). Le service doit être réservé aux besoins spécifiques et justifiés de systèmes ou ressources identifiés. En particulier, l'accès au service par des serveurs cache internes utilisés par des postes utilisateurs ou des postes administrateurs est à éviter. Dans le cas des postes utilisateurs devant accéder à Internet, un serveur relais (par exemple, un serveur mandataire – *proxy Web* – pour l'accès au Web, ou encore un relais

de messagerie pour les courriels) doit être mis en œuvre. Seul ce serveur relais doit avoir accès au service DNS de résolution des noms de domaine Internet.

R24

DNS-PUB - Limiter les accès internes au service

Des règles de filtrage répondant au strict besoin opérationnel doivent être mises en place sur les pare-feux en coupure interne du service DNS de résolution des noms de domaine Internet, limitant l'accès au service uniquement depuis les adresses IP source des équipements et ressources spécifiquement autorisés à consulter le service.

Néanmoins, il existe des cas d'usage particuliers où certaines ressources nécessitent à la fois une résolution de noms de domaine internes et de noms de domaine Internet. Pour répondre à ce besoin, un serveur de type « Relais » doit être mis en œuvre. Déployé dans le SI interne, ce serveur Relais est utilisé par les ressources pour leur besoin de résolution en permettant l'aiguillage des résolutions des noms de domaine internes et Internet vers les services *ad hoc*. Ce serveur Relais doit être dédié et cloisonné des autres serveurs DNS et un filtrage doit limiter son accès aux seules ressources spécifiques ayant ces besoins de résolution.

R25

DNS-PUB - Mettre en œuvre un serveur Relais

Il est recommandé de mettre en œuvre sur le SI interne des serveurs DNS Relais cloisonnés et filtrés du reste du SI pour les ressources spécifiques du SI interne ayant besoin de résoudre à la fois des noms de domaine internes et des noms de domaine Internet.

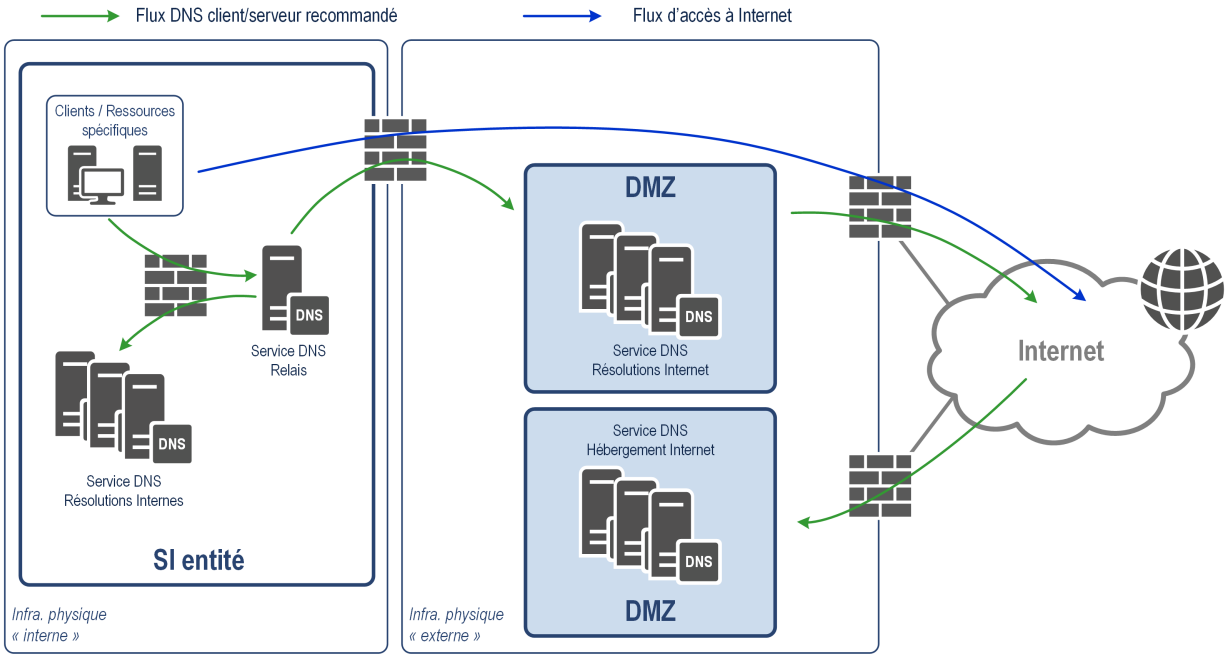

FIGURE 3 – Exemple de cloisonnement d'un serveur Relais

5.3 Architecture physique et logique du service

La figure 4 présente une proposition d'architecture d'un service DNS de résolution des noms de domaine Internet.

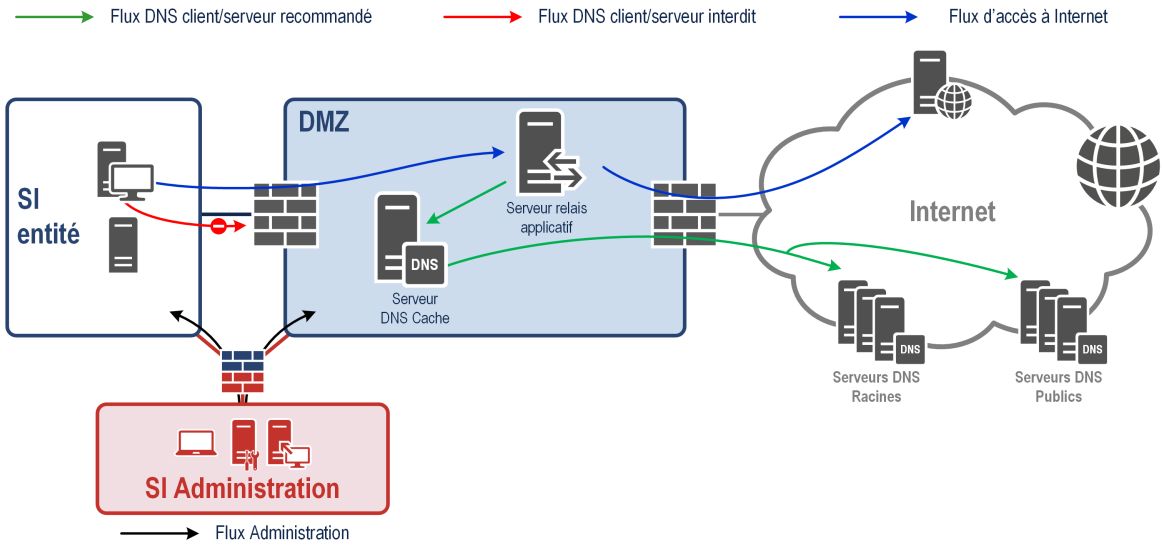

FIGURE 4 – Exemple d'architecture d'un service DNS de résolution des noms de domaine Internet

R26

DNS-PUB - Cloisonner physiquement la fonction de cache

Il est recommandé que le service DNS de résolution des noms de domaine Internet bénéficie de serveurs physiques dédiés pour la fonction de cache.

Le serveur cache public doit bénéficier de deux interfaces afin d'être positionné en coupure d'Internet ainsi que d'une fonction de filtrage afin de limiter son exposition. Idéalement, le cache doit être positionné entre deux pare-feux, l'un filtrant l'interconnexion avec Internet, l'autre l'interconnexion avec le SI interne ou les autres équipements de la DMZ elle-même.

R27

DNS-PUB - Positionner les serveurs cache en coupure avec Internet

Les serveurs cache accédant à Internet doivent être positionnés en coupure, au minimum « logique » d'un point de vue réseau, entre le SI interne et Internet.

Attention

Les pare-feux en coupure avec Internet peuvent être mutualisés pour assurer la protection de plusieurs services du SI. Néanmoins, l'exposition de services sur Internet (tel que le service DNS d'hébergement des noms de domaine Internet) implique un plus grand risque de compromission de la fonction de filtrage des flux entrants par rapport à la fonction de filtrage des flux sortants.

Même si ce point n'est pas détaillé dans le présent document, le guide sur l'interconnexion d'un système d'information à Internet [9], recommande de cloisonner les fonctions de filtrage entrantes et sortantes sur deux instances distinctes, ceci afin

de conserver la disponibilité de certains accès en cas de compromission ou de défaillance.

Dans une démarche de défense en profondeur, il peut être utile de limiter l'espace des zones qui sont résolues par le service, voire même le limiter à quelques FQDN [9] précis. Cette restriction peut être appliquée au niveau du client, à l'aide de mécanismes particuliers, ou directement au niveau du service DNS de résolution des noms de domaine Internet au profit de tous les clients.

Pour chaque besoin spécifique, une politique de filtrage doit être appliquée, autorisant la résolution de noms de domaine pour un ou plusieurs enregistrements DNS, une zone spécifique ou tout Internet. Il est également possible d'interdire les requêtes en fonction du type d'enregistrement DNS.

Il est donc recommandé de configurer des listes d'autorisation ou d'interdiction pour un filtrage plus fin par noms de domaine ainsi que les outils nécessaires à leur gestion.

R28

DNS-PUB - Mettre en place des listes d'interdiction

La mise en place et la gestion de listes d'autorisation pouvant être complexes, il peut être envisagé de commencer par la mise en place de listes d'interdiction pour permettre de bloquer certains noms de domaine en cas d'incident de sécurité.

R28 +

DNS-PUB - Mettre en place des listes d'autorisation

Pour contribuer à la réduction de la surface d'attaque des systèmes clients, il est recommandé de mettre en place un filtrage par liste d'autorisation des requêtes DNS.

En complément, il est recommandé de mettre en place par système client des seuils adaptés au besoin, en nombre de requêtes par seconde :

- un premier seuil bas qui provoque une journalisation d'événements à superviser ;
- un second seuil haut qui provoque un rejet des requêtes.

R29

DNS-PUB - Limiter le nombre de requêtes par système client

Il est recommandé de limiter le nombre de requêtes autorisées par système client en configurant des seuils d'alerte puis de rejet des requêtes.

9. *Fully Qualified Domain Name*.

6
Service d'hébergement des noms de domaine Internet

Ce chapitre décrit les bonnes pratiques applicables à un service DNS proposant d'héberger des noms de domaines sur Internet. Après un rappel des fonctions associées à ce service (section 6.1), les contraintes d'accès sont décrites (section 6.2) avant d'en présenter l'architecture (section 6.3).

6.1 Composition du service

Le service DNS d'hébergement des noms de domaine Internet est constitué de trois fonctions :

- une fonction de DNS *primaire caché* ;
- une fonction de DNS *secondaire* ;
- une fonction de DNS dite *tampon*.

6.2 Accès au service

Ce service d'hébergement de noms de domaine est exposé sur Internet. Afin de veiller à sa disponibilité, une protection contre les attaques en déni de service distribué (anti-DDoS) est fortement recommandée. Les mesures de détection doivent être adaptées spécifiquement au service DNS d'hébergement des noms de domaine Internet.

R30

DNS-HEB - Mettre en place des mesures de protection anti-DDoS

Il est recommandé de mettre en place un service anti-DDoS avec des mesures de détection adaptées spécifiquement au service DNS d'hébergement des noms de domaine Internet.

Information

Pour plus d'informations concernant ce type d'attaque, la lecture du guide « Comprendre et anticiper les attaques DDoS » [5] est recommandée.

6.3 Architecture physique et logique du service

La figure 5 présente une proposition d'architecture d'un service d'hébergement de noms de domaines Internet.

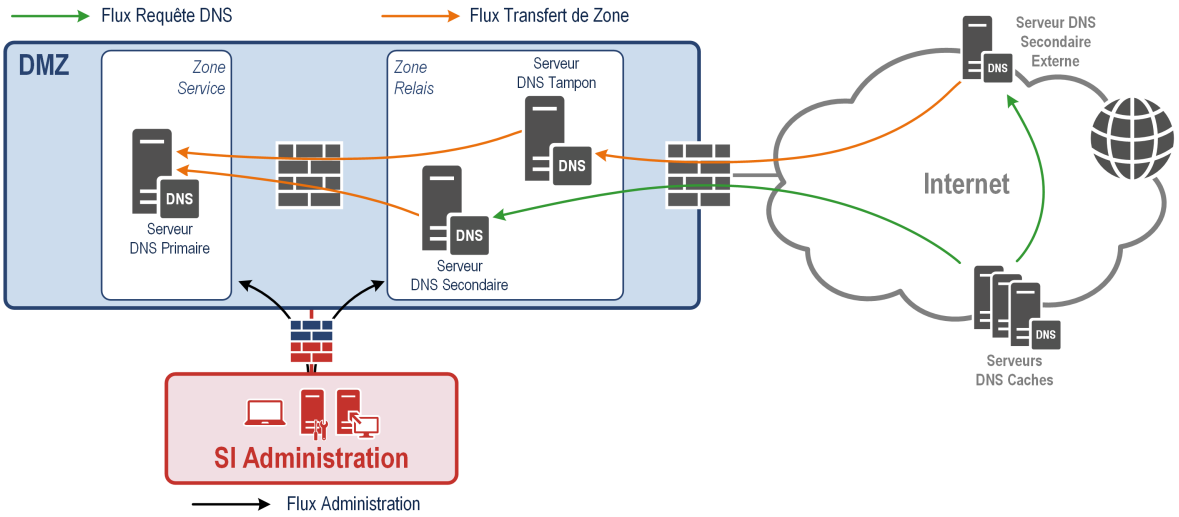

FIGURE 5 – Exemple d'architecture d'un service DNS d'hébergement de noms de domaine Internet

Comme pour tout service exposé sur Internet, les contraintes spécifiques du service DNS d'hébergement des noms de domaine Internet impliquent de lui dédier une zone de sécurité. En suivant les recommandations du guide relatif à l'interconnexion d'un système d'information à Internet [9], il est fortement recommandé de mettre en œuvre une infrastructure physiquement dédiée à ce type d'exposition et indépendante de tout autre élément du SI.

R31

DNS-HEB - Cloisonner physiquement les serveurs hébergeant le service

L'ensemble des fonctions du service DNS d'hébergement des noms de domaine Internet doit s'appuyer sur une infrastructure dédiée aux services exposés à Internet. Son infrastructure ne doit pas être mutualisée avec d'autres services internes de l'entité.

Étant donnés les risques inhérents à l'exposition de ce type de service sur Internet, une attention particulière doit être portée à leur disponibilité. En particulier, il existe deux problématiques spécifiques à ces architectures.

D'une part, afin de pallier la panne ou la compromission d'un des serveurs, il est recommandé de déployer plusieurs services DNS d'hébergement des noms de domaines Internet, idéalement sur des sites géographiques distincts. Le protocole DNS permet de répliquer les données d'un site vers l'autre afin d'assurer la synchronisation des données hébergées, y compris à travers Internet dans le cas d'une externalisation du service.

D'autre part, la disponibilité de ce service est aussi dépendante de la disponibilité des services DNS de tiers. Plusieurs ressources sont disponibles en ligne afin de vérifier et valider ces dépendances.

Ces problématiques sont présentées dans le guide des bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine [2].

R32

DNS-HEB - Suivre les recommandations du guide sur les noms de domaines

Pour assurer le maintien en disponibilité du service DNS d'hébergement des noms de domaine Internet, appliquer les recommandations du guide de l'ANSSI sur l'exploitation de noms de domaine [2], en particulier son chapitre sur la résilience des services.

Information

Sur les problématiques de dépendances à des noms tiers, et pour obtenir un diagnostic complet sur l'état d'un domaine sur Internet, l'AFNIC et son homologue suédois The Swedish Internet Foundation mettent à disposition le service *Zonemaster*[a]. Ce service permet entre autre de valider l'exposition, la syntaxe, et la cohérence d'un nom de domaine Internet.

La mise à jour des enregistrements DNS sur le service DNS d'hébergement des noms de domaine Internet se fait sur le serveur primaire *caché*. Les serveurs secondaires sont alors mis à jour automatiquement par transferts de zones.

Si, pour des raisons de disponibilité, des serveurs DNS secondaires sont hébergés à l'extérieur du SI de l'entité, alors la mise à jour de ces serveurs DNS secondaires doit se faire à travers un serveur intermédiaire, en conformité avec la recommandation R3, afin de limiter l'exposition du serveur primaire caché.

Ce serveur intermédiaire, dit « tampon », assure à la fois une fonction de serveur primaire pour les secondaires externes, et une fonction de serveur secondaire vis-à-vis du serveur primaire *caché*.

Tous les transferts de zone doivent être protégés en intégrité par le protocole TSIG, conformément à la recommandation R7.

R33

DNS-HEB - Utiliser un serveur « tampon » pour les serveurs secondaires externes à l'entité

Mettre en œuvre un serveur « tampon » pour les transferts de zone entre un serveur primaire interne et des serveurs secondaires externes à l'entité.

Les flux vers le serveur primaire *caché* depuis les serveurs secondaires et tampon doivent être filtrés entre la zone des services relais et la zone des services internes.

R34

DNS-HEB - Cloisonner le serveur primaire caché d'Internet

Le serveur *caché* du service DNS d'hébergement des noms de domaine Internet ne doit pas être exposé sur Internet.

Le serveur primaire doit être physiquement distinct des serveurs secondaires et tampon. À l'instar des serveurs cache du service DNS de résolution des noms de domaine Internet, les serveurs secondaires ainsi que le serveur tampon doivent être positionnés en coupure logique avec Internet.

a. https://zonemaster.net/fr/run-test

Ils doivent aussi bénéficier de deux interfaces afin d'être positionnés en coupure d'Internet, ainsi que d'une fonction de filtrage afin de limiter leur exposition.

R35

DNS-HEB - Positionner les serveurs secondaires en coupure d'Internet

Les serveurs exposés sur Internet doivent être positionnés en coupure, au minimum « logique », d'un point de vue réseau entre le serveur primaire et Internet.

Liste des recommandations

R1	Cloisonner physiquement les infrastructures entre services DNS *internes* et *externes*	11
R2	Interdire les flux entre services DNS *internes* et *externes*	11
R3	Suivre les recommandations du guide sur les passerelles Internet sécurisées pour les services DNS *externes*	11
R4	Cloisonner les fonctions DNS sur des serveurs distincts	12
R5	Filtrer les flux réseau	13
R6	Déployer un serveur primaire caché	13
R7	Protéger en intégrité les transferts de zones avec TSIG	14
R7+	Protéger en intégrité les transferts de zones avec XoT	14
R8+	Diversifier les logiciels DNS	14
R9	Durcir les composants des services DNS	15
R10	Activer le pare-feu local des serveurs DNS	15
R11	Procéder à une analyse de risque spécifique à DNSSEC	16
R12	Définir un processus de gestion spécifique à DNSSEC	17
R13	Mettre en œuvre une supervision spécifique à DNSSEC	17
R14	Activer DNSSEC sur le service DNS de résolution des noms de domaine Internet	17
R15	Appliquer les bonnes pratiques d'administration sécurisée	18
R16	Formaliser et appliquer un processus de MCS des services DNS	18
R17	Centraliser la journalisation des services DNS	19
R18	DNS-PRIV - Interdire la résolution de noms de domaine Internet	20
R19	DNS-PRIV - Interdire les accès au service depuis Internet	21
R20	DNS-PRIV - Limiter l'accès des clients au seul serveur cache	21
R21	DNS-PRIV - Cloisonner les fonctions DNS	22
R22	DNS-PRIV - Filtrer les flux et échanges internes	22
R23	DNS-PUB - Interdire les accès au service depuis Internet	23
R24	DNS-PUB - Limiter les accès internes au service	24
R25	DNS-PUB - Mettre en œuvre un serveur Relais	24
R26	DNS-PUB - Cloisonner physiquement la fonction de cache	25
R27	DNS-PUB - Positionner les serveurs cache en coupure avec Internet	25
R28	DNS-PUB - Mettre en place des listes d'interdiction	26
R28+	DNS-PUB - Mettre en place des listes d'autorisation	26
R29	DNS-PUB - Limiter le nombre de requêtes par système client	26
R30	DNS-HEB - Mettre en place des mesures de protection anti-DDoS	27
R31	DNS-HEB - Cloisonner physiquement les serveurs hébergeant le service	28
R32	DNS-HEB - Suivre les recommandations du guide sur les noms de domaines	29
R33	DNS-HEB - Utiliser un serveur « tampon » pour les serveurs secondaires externes à l'entité	29
R34	DNS-HEB - Cloisonner le serveur primaire *caché* d'Internet	29
R35	DNS-HEB - Positionner les serveurs secondaires en coupure d'Internet	30

Bibliographie

[1] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://cyber.gouv.fr/guide-commutateurs.

[2] *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*.
Guide ANSSI-BP-038 v1.3, ANSSI, novembre 2017.
https://cyber.gouv.fr/guide-dns.

[3] *Recommandations de sécurité relatives à un système GNU/Linux*.
Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022.
https://cyber.gouv.fr/guide-linux.

[4] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://cyber.gouv.fr/guide-politique-filtrage-pare-feu.

[5] *Comprendre et anticiper les attaques DDoS*.
Guide Version 1.0, ANSSI, mars 2015.
https://cyber.gouv.fr/guide-ddos.

[6] *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet*.
Guide ANSSI-PA-044 v1.0, ANSSI, janvier 2018.
https://cyber.gouv.fr/guide-pare-feux-internet.

[7] *Maîtrise du risque numérique - l'atout confiance*.
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance.

[8] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://cyber.gouv.fr/guide-tls.

[9] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.
https://cyber.gouv.fr/guide-interconnexion-si-internet.

[10] *Guide de sélection d'algorithmes cryptographiques*.
Guide ANSSI-PA-079 v1.0, ANSSI, mars 2021.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[11] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[12] *Recommandations sur le nomadisme numérique*.
Guide ANSSI-PA-054 v2.0, ANSSI, novembre 2023.
https://cyber.gouv.fr/guide-nomadisme-numerique.

Version 1.0 - 17/07/2024- ANSSI-PA-105
Licence ouverte / Open Licence (Étalab - v2.0)
ISBN : 978-2-11-167172-0 (papier)
ISBN : 978-2-11-167171-3 (numérique)
Dépôt légal : juillet 2024

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité