ROYAUME DU MAROC
ADMINISTRATION DE LA DÉFENSE NATIONALE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ
DES SYSTÈMES D'INFORMATION

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن
نظم المعلومات

RECOMMANDATIONS ET BONNES PRATIQUES DE CONFIGURATION DES PROTOCOLES BGP ET DNS

DGSSI

Administration de la Défense Nationale, Méchouar Saïd,
10 090 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@dgssi.gov.ma
Web : www.dgssi.gov.ma

إدارة الدفاع الوطني، المشور السعيد،
10 090 الرباط – هاتف: 0537572147 – فاكس: 0537572053
البريد الإلكتروني: contact@dgssi.gov.ma
الموقع الإلكتروني: www.dgssi.gov.ma

TABLE DES MATIÈRES

1 Introduction

Le protocole BGP permet d'échanger des informations de routage et d'accessibilité de réseaux (appelés préfixes) entre les systèmes autonomes (AS) qui composent l'infrastructure Internet. Tout acteur disposant d'un ou plusieurs AS (Fournisseur de service de transit Internet, fournisseur d'accès Internet, point d'échange, etc.) apporte, ainsi, sa contribution au bon fonctionnement de l'Internet mais aussi son lot de vulnérabilités spécifiques, notamment celles qui permettent aux "hackers" d'usurper des préfixes.

Par ailleurs, pour faciliter l'exploitation du web, le service DNS permet de surmonter la difficulté d'utiliser les longues séries de chiffres que représentent les adresses IP en leur associant des noms de domaines. Toutefois, plusieurs cyberattaques (DNS ID Spoofing, DNS Cache Poisoning, etc.) permettent aux pirates de faire correspondre des adresses IP de machines qu'ils contrôlent à des noms réels et valides de machines publiques.

Pour contrer ces défaillances, le présent document détaille les bonnes pratiques se rapportant aux protocoles BGP et DNS. Les acteurs de l'Internet au niveau national devraient s'approprier ces recommandations afin d'être en mesure d'anticiper, d'une part, les attaques par déni de service distribué (Distributed Denial of Service ou DDoS) et d'autre part, d'assurer l'intégrité et l'authenticité des réponses DNS.

2 Protocole BGP

2.1 Recommandations au niveau architecture

2.1.1 Supervision du lien de “peering”

La supervision consiste à surveiller les liens de "peering" et à récupérer les informations permettant d'en déduire l'état et le comportement de ces liens. Ces informations peuvent provenir de requêtes envoyées périodiquement ou récupérés directement des équipements réseaux.
Seule une surveillance permanente de ces liens permettrait de réagir le plus rapidement possible et d'éviter un arrêt prolongé du lien de "peering".

Recommandation

Implémenter un mécanisme de détection rapide de l'échec du lien.
Exemple : utiliser le BFD[a] qui permet d'avoir un temps de détection très minime par rapport aux minuteurs du protocole.

[a]Bidirectional Forwarding Detection (BFD) est un protocole réseau utilisé pour détecter les défauts entre deux équipements reliés par un lien tout en ayant un faible encombrement.

2.1.2 Réseaux “Multihomed non-transit”

Un AS qui autorise l'acheminement d'un trafic provenant de réseaux externes à un AS est appelé un "AS de transit". De ce fait, un AS de "non-transit" ne doit autoriser aucun trafic en transit (Un trafic en transit est celui qui a une destination et une source n'appartenant pas à l'AS qu'il veut emprunter).

Recommandation

Un AS de "non-transit" ne doit annoncer que ses propres préfixes et ne doit, en aucun cas, propager les préfixes utilisés par d'autres AS. Cela garantit que le trafic, ayant une destination qui n'appartient pas à cet AS, ne lui serait jamais dirigé.

2.1.3 Réseaux “Multihomed transit”

Un AS est appelé "multihomed" s'il possède plus d'un point de sortie vers l'extérieur. Il peut être "multihomed" à un seul ou plusieurs fournisseurs de services.

Recommandation

Pour les AS de transit, un filtrage doit s'appliquer aux préfixes annoncés depuis l'AS source. Une vérification des autres préfixes peut être faite grâce à la RPKI[a].

[a]La RPKI, Resource Public Key Infrastructure, a été conçue spécialement pour assurer l'intégrité de l'infrastructure de routage d'internet.

2.2 Sécurisation des routeurs et des équipements d'administration

2.2.1 Endurcissement des équipements d'administration

Afin de limiter la surface d'attaque se rapportant aux systèmes pouvant donner accès à l'environnement de routage central, il est recommandé aux propriétaires des AS d'endurcir la sécurité de ces systèmes.

Check-list

- Configurer les systèmes de manière à désactiver tous les services qui ne sont pas nécessaires ;
- Appliquer les règles de sécurité basiques ;
- Supprimer toutes les configurations et les comptes par défaut.

Les standards d'endurcissement du Centre pour la Sécurité d'Internet (CIS, Center for Internet Security) sont disponibles sur le lien : http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks

Check-list

- Tous les postes de travail et serveurs ayant accès à l'environnent de routage central doivent avoir une configuration standard et endurcie.
- Toutes les composantes du réseau supportant l'environnement de routage central ou supportant l'accès à l'environnement de routage central devraient avoir une configuration standard et endurcie.

Recommandation

Il faut veillez à ce que les accès d'administration ne s'effectuent que depuis des réseaux dédiés à l'administration.

2.2.2 Endurcissement des routeurs

Recommandation

Il faut s'assurer que les sessions BGP ne soient établies qu'avec les routeurs autorisés en utilisant des listes de contrôle d'accès.

Recommandation

En cas d'utilisation du SNMP[a], il faut vérifier que les requêtes SNMP ne proviennent que du serveur d'administration autorisé. En outre, il faut utiliser un nom de communauté[b] non-trivial.

[a]Simple Network Management Protocol est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

[b]Dans SNMP, Un nom de communauté peut être assimilé à un mot de passe connu par l'agent et utilisé par le manageur pour se faire reconnaître. Les noms de communautés sont configurés sur l'agent et définissent les types d'accès sur les variables gérée par l'agent.

2.2.3 Journalisation des évènements

Il faut activer la journalisation des évènements relatifs à la sécurité sur toute l'infrastructure supportant l'environnement de routage central. Ceci inclut le stockage des évènements de sécurité à travers la centralisation des journaux de tous les systèmes concernés, notamment, ceux qui se connectent ou supportent l'environnement de routage central.

Recommandation

Désactiver l'envoi des logs vers la sortie standard du routeur (console) et utiliser un stockage local des logs en veillant à limiter la taille maximale à occuper au niveau du routeur. Le mieux est d'utiliser un serveur de logs dédié, car une activation des logs de débogage vers la sortie standard peut devenir très gourmande en ressources et bloquer ainsi l'accès au routeur lui-même.

Check-list

- Journaliser les authentifications, les accès et les évènements de modification de l'environnement de routage central et de l'infrastructure technique qui le supporte.
- Journaliser et surveiller tous les évènements de sécurité pertinents ayant trait à l'environnement de routage central ou à l'infrastructure qui le supporte.
- Implémenter un processus d'analyse, de validation et d'escalade des évènements de sécurité pertinents.

Check-list

- Configurer les routeurs pour le stockage des événements BGP.
- Externaliser l'enregistrement des logs au lieu de les envoyer à la console pour éviter tout blocage de cette dernière.
- Vérifier que la fonctionnalité de journalisation n'épuise pas toutes les ressources du routeur.
- Si les ressources disponibles sont suffisantes, journaliser les événements ayant une sévérité du niveau "Error (3)" ou niveau "Warning (4)".
- Activer de préférence la journalisation de tout changement d'état des "Peers".

2.3 Sécurisation de la session

2.3.1 Sécurisation par Time to live (TTL)

Recommandation

Définir un TTL[a] pour les session BGP entrantes. Cette action représente la première ligne de défense contre les attaques de "Hijacking"[b].

[a]Time to live, indique le temps pendant lequel une information doit être conservée, ou le temps pendant lequel une information doit être gardée en cache.

[b]attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

2.3.2 Authentification des Peers

L'authentification réciproque des routeurs BGP est primordiale. Le MD5[1], qui n'est pas une méthode de cryptographie robuste, permet au moins d'assurer une authentification acceptable à travers un mot de passe commun robuste et crypté.

Recommandation

Activer l'authentification MD5 avec les autres routeurs BGP. Il est primordiale d'une part, d'établir un standard robuste pour les mots de passe d'authentification MD5 et d'autre part, de mettre en place un processus de création, d'attribution d'accès, et de modification des mots de passe d'authentification MD5.

[1]L'algorithme MD5, pour Message Digest 5, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de message).

Check-list

- Activer l'authentification MD5 avec d'autres routeurs BGP.
- Établir un standard robuste pour les mots de passe d'authentification MD5.
- Établir un processus de création, d'attribution d'accès, et de modification des mots de passe d'authentification MD5.

2.4 Filtrage des annonces

2.4.1 Filtrage des numéros d'AS et des préfixes privés

Pour pouvoir utiliser le BGP, il n'est pas nécessaire d'avoir un numéro d'AS unique attribué par un registre internet. On a recours à cet effet à des numéros dits privés. Ces numéros d'AS privés s'étendent de 64512 à 65534 et de 4200000000 à 4294967294 pour les numéros sur 32 bits (RFC6996)[2]. Cette règle s'applique aussi aux préfixes et de ce fait il est possible d'annoncer des préfixes privés.

Les numéros d'AS ainsi que les préfixes privés ne doivent pas être présents dans les annonces sur Internet puisqu'ils peuvent être utilisés simultanément par plusieurs AS. Il est nécessaire de mettre en place un filtrage en sortie qui permet de supprimer ces numéros.

Recommandation

Les préfixes privés ainsi que les numéros d'AS (ASN) privés ne doivent pas figurer dans les tables BGP communiquées aux "peers". Les annonces de ce type doivent être filtrées.

2.4.2 Filtrage des Préfixes

Recommandation

Faire en sorte d'agréger au maximum les préfixes annoncés afin d'éviter la surcharge des ressources du routeur. Il est recommandé que la longueur des masques des préfixes annoncés n'excède pas 24 bits en IPv4 et 48 bits en IPv6.

2.4.3 Filtrage sur les préfixes du "peer"

Recommandation

Afin de se prémunir contre une mauvaise configuration au niveau des clients, les fournisseurs de services doivent mettre en place des filtres pour n'accepter que les préfixes propres aux clients.

[2]http://www.iana.org/assignments/as-numbers/as-numbers.txt

2.4.4 Filtrage sur le nombre maximal des préfixes reçus

Recommandation

Mettre en place un seuil maximal de préfixes à recevoir à partir de chaque "peer" afin d'éviter l'utilisation excessive des ressources du routeur. En recevant un grand nombre de préfixes suite à une probable erreur de configuration, le routeur peut se voir ses ressources diminuées d'une manière inacceptable.

2.4.5 Bogons routes (Bogons route servers)

Les préfixes "bogons" incluent des préfixes IPv4/IPv6 qui ne doivent pas être utilisés. Ils englobent les préfixes qui ne sont pas alloués aux RIRs[3] ainsi que les préfixes qui ne sont pas assignés par les RIRs à leurs clients. Cette liste doit être mise à jour régulièrement.
Afin d'avoir une mise à jour automatique et de profiter de la liste entière ("Fullbogons"), on peut réaliser un "peering" avec les "route-servers" de l'équipe "Team-Cymru"[4].

Check-list

- Configurer des règles de filtrage pour les préfixes réservés.
- Configurer des règles de filtrage pour les préfixes trop spécifiques.
- Établir un processus pour examiner, régulièrement, la liste publique des préfixes réservés afin d'affiner les règles de filtrage.
- Filtrer les préfixes "bogons" en utilisant la liste publiée par "Team-Cymru" à travers un "peering". A cet effet, il faut s'appuyer sur les modèles de configuration cités sur le lien : http://www.team-cymru.org/bogon-reference-bgp.html pour mettre en place un lien de "peering" avec "Team-Cymru".

2.5 Certification des ressources

La Certification des ressources est un moyen qui permet de vérifier l'association entre les ressources Internet (adresses IP et les numéros d'AS) et leurs propriétaires légitimes. Elle vise à ajouter une information qui permet de vérifier le droit d'utiliser ces ressources sur Internet.

Une composante importante du mécanisme de certification des ressources Internet est la RPKI (Resource Public Key Infrastructure). Elle permet de lier les numéros des systèmes autonomes et les préfixes à une "ancre de confiance" en associant à ces ressources des certificats de type "X.509"[5] traditionnels. Ainsi, une extension est

[3]Registre Internet régional.

[4]http://www.team-cymru.org/bogon-reference-bgp.html

[5]X.509 est une norme de cryptographie pour les infrastructures à clés publiques (PKI). X.509 établit entre autres un format standard de certificat électronique

ajoutée aux adresses IP et aux identifiants des systèmes autonomes. Cette extension permet de vérifier l'autorité qui a annoncé le préfixe en question ainsi que la longueur du chemin qui y amène.

2.5.1 Participation à la RPKI

Recommandation

Il est recommandé que chaque entité participe à la RPKI en signant ses propres préfixes et numéros d'AS. Ceci peut se faire sur le portail du RIR (Afrinic)[a].

[a] http://www.afrinic.net/initiatives/resource-certification

2.5.2 Mise en place d'un validateur

Le validateur est un outil qui permet de télécharger toutes les données de la RPKI et d'intégrer une validation de l'origine de l'annonce dans le processus de décision du routage BGP.

Recommandation

Il faut installer le validateur pour synchroniser la liste des préfixes avec leurs états respectifs.
Il faut vérifier que le protocole "rsync" est autorisé en sortie depuis la machine contenant le validateur.

Plusieurs validateurs sont disponibles. Exemple : RIPE NCC RPKI Validator (www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources).

2.5.3 Configuration des routeurs

Une fois le validateur en place, il faut configurer les routeurs pour valider les préfixes auprès de ce dernier.

Il faut noter que la RPKI n'est toujours pas implémentée par l'ensemble des propriétaires des ressources Internet au Maroc. Pour cette raison, il faut donner une préférence inférieure aux préfixes non-valides par rapport aux préfixes valides mais sansles rejeter.

Check-list

- Obtenir les certificats des ressources de l'Afrinic pour les systèmes autonomes et les préfixes IP.
- Activer la validation "RPKI" à travers l'infrastructure de routage centrale.
- Si possible, implémenter les politiques de routage pour gérer les mises à jour basées sur la validation RPKI.

2.6 Utilisation de l'objet "route"

Il est recommandé qu'un organisme déclare, dans la base de données "whois" du registre internet compétent (AFRINIC dans le cas du Maroc), les informations relatives aux préfixes qu'il annonce en BGP. Ceci peut être fait à travers la création d'objets "route".

Un objet "route" permet d'identifier, de manière précise, les AS susceptibles d'annoncer les préfixes de l'organisation.

```
route:          196.13.108.0/24
descr:          DGSSI IPv4 network
origin:         AS327917
notify:         admin@macert.gov.ma
mnt-by:         DGSSI-MNT
changed:        admin@macert.gov.ma 20161111
source:         AFRINIC
```

Figure 1: l'objet route de la DGSSI (AFRINIC).

L'objet "route" de la figure 1 ci-dessus indique que le préfixe 196.13.108.0/24 est annoncé par l'AS327917. Une organisation peut déléguer l'utilisation de ce préfixe à un client ou à un partenaire. Dans ce cas, l'attribut "origin" pointe sur un numéro d'AS différent de 327917. Afin d'autoriser certains types de déploiements, il est légitime de déclarer différents objets route avec des attributs route identiques et des attributs "origin" différents. Les attributs "route" et "origin" jouent le rôle de clés primaires et ne peuvent ainsi être dupliqués en même temps. Quant à l'attribut "mnt-by", il indique 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, par exemple, de se prémunir des erreurs de configuration entraînant des annonces de préfixes qui ne leur appartiennent pas.

Dans le cas des préfixes IPv6, le même traitement est fait à travers l'objet "route6". Le reste des attributs reste identique.

```
route6:         2001:43f8:b30::/48
descr:          Direction Generale de la Securite des Systemes d'Information- DGSSI
origin:         AS327917
org:            ORG-DGDL1-AFRINIC
notify:         admin@macert.gov.ma
mnt-by:         DGSSI-MNT
changed:        admin@macert.gov.ma 20161111
source:         AFRINIC
```

FIGURE 2: l'objet route6 de la DGSSI (AFRINIC).

Recommandation

Il est fortement recommandé de créer des objets "route" pour tous les titulaires de numéros d'AS au Maroc.

3 Protocole DNS

3.1 Sensibilité du service par rapport aux dépendances hiérarchiques

L'architecture DNS repose sur une arborescence hiérarchique stricte. Toute défaillance d'un nœud père remet en cause la résolution d'une zone fille.

Dans le cas d'un serveur de premier niveau, par exemple ".com", ".org" et ".ma", pour assurer une bonne résilience, il faut penser à mettre en place des architectures fortement redondantes au niveau international.

Recommandation

Pour les niveaux sous-jacents, il faudra s'assurer que la zone "parent" à laquelle on se rattache propose un niveau de résilience élevé.

3.2 Isolement des serveurs par rôle

Lors de la construction d'une infrastructure DNS, les rôles les plus importants à considérer sont les serveurs primaires et les serveurs secondaires.

D'autres rôles pourraient faire partie d'une infrastructure DNS tels que les serveurs DNS "cache uniquement" et les serveurs DNS Redirecteurs. Il est fortement recommandé de bien comprendre ces rôles et de les séparer, si nécessaire, des autres rôles.

Serveur primaire : Un serveur primaire contient la seule copie inscriptible de la zone DNS. Il est chargé de communiquer aux serveurs secondaires les mises à jour relatives aux informations de zone.

Serveur secondaire : Les serveurs secondaires sont installés pour assurer la tolérance aux pannes, l'équilibrage de la charge et la réduction des besoins en bande passante. Ils hébergent une copie, en lecture seule, du fichier de zone et sont en mesure de répondre aux demandes des clients.

Serveur DNS "cache uniquement" : Chaque serveur DNS peut fournir des services de mise en cache. Les serveurs DNS "cache uniquement" ne contiennent ni des informations sur les zones, ni la base de données des zones. Ils peuvent être essentiels dans une conception d'un DNS résilient.

Serveur DNS Redirecteur : Dans un réseau, un redirecteur est un serveur DNS utilisé pour transférer des requêtes DNS pour des noms DNS externes vers des serveurs DNS situés à l'extérieur de ce réseau. L'utilisation d'un redirecteur permet de gérer la résolution des noms externes ce qui peut améliorer l'efficacité de la résolution de noms.

Tout serveur DNS peut résoudre les requêtes des clients DNS. Il est recommandé de ne pas utiliser le serveur principal comme résolveur de requêtes des clients DNS, mais plutôt compter sur une combinaison résiliente de serveurs secondaires, de redirecteurs DNS et de serveurs "cache uniquement".

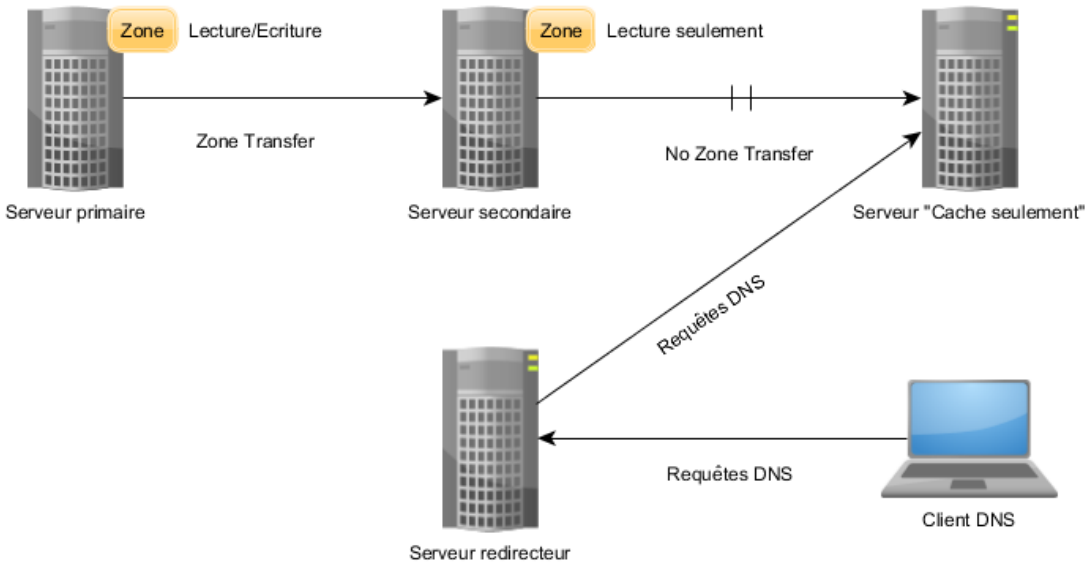

FIGURE 3: Rôles des serveurs DNS

Recommandation

Il est fortement conseillé de séparer, sur des plateformes distinctes, les serveurs ayant des rôles différents.

Recommandation

Il est recommandé de ne pas utiliser le serveur principal comme résolveur pour les requêtes des clients DNS.

3.3 Séparation des zones publiques et privées

Les zones publiques sont destinées à être visibles sur tout le réseau Internet afin que les services qui en dépendent (serveur web, messagerie, etc.) soient accessibles. Quant aux zones privées, elles contiennent des adresses internes qui intéressent uniquement les clients internes. On en déduit que les besoins de sécurité sont différents selon les zones : publiques ou privées.

Recommandation

Il est recommandé de séparer les données des zones publiques et celle des zones privées sur des serveurs dédiés. L'isolation de l'accès à ces zones privées garantit la non-divulgation d'informations vers l'extérieur : architecture du réseau interne, plans d'adressage, noms des serveurs, etc.

Bien qu'il soit recommandé d'utiliser des serveurs dédiés pour les zones internes et externes, ceci n'est pas toujours techniquement faisable. A cet effet, il est possible

de mettre en œuvre des listes de contrôle d'accès au niveau du serveur DNS. Cela garantit que seules les adresses IP ou les plages de la liste blanche peuvent interroger une zone spécifique.

3.4 "Name Servers" (NS) esclaves

Afin d'assurer la continuité de service en cas de défaillance du NS maître, il est indispensable de prévoir des NS esclaves afin de répartir le service sur plusieurs NS.

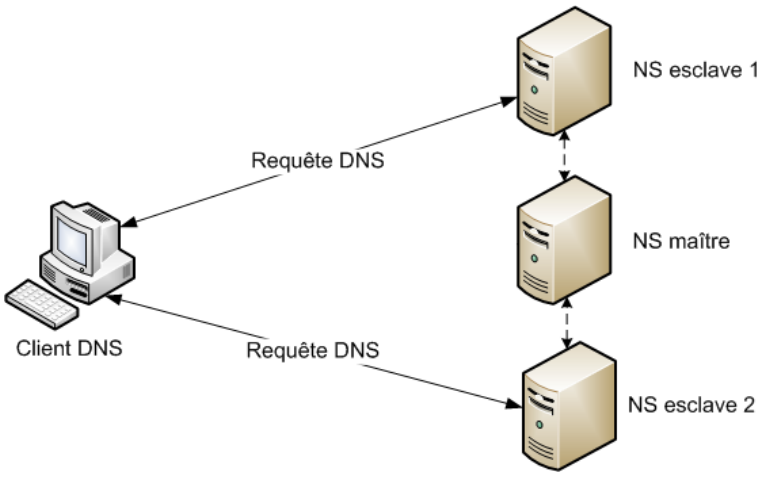

FIGURE 4: NS maître et deux NS esclaves.

Recommandation

Il est préconisé d'avoir au moins 3 NS :

- un NS maître : serveur de nom primaire ;
- et deux NS esclaves : serveurs de noms secondaires.

Recommandation

Il est recommandé de ne pas utiliser le serveur primaire pour la résolution de noms. Il faut annoncer seulement des serveurs secondaires (serveurs esclaves) pour résoudre des noms.

3.5 Hébergement des “Name Servers” (NS) esclaves

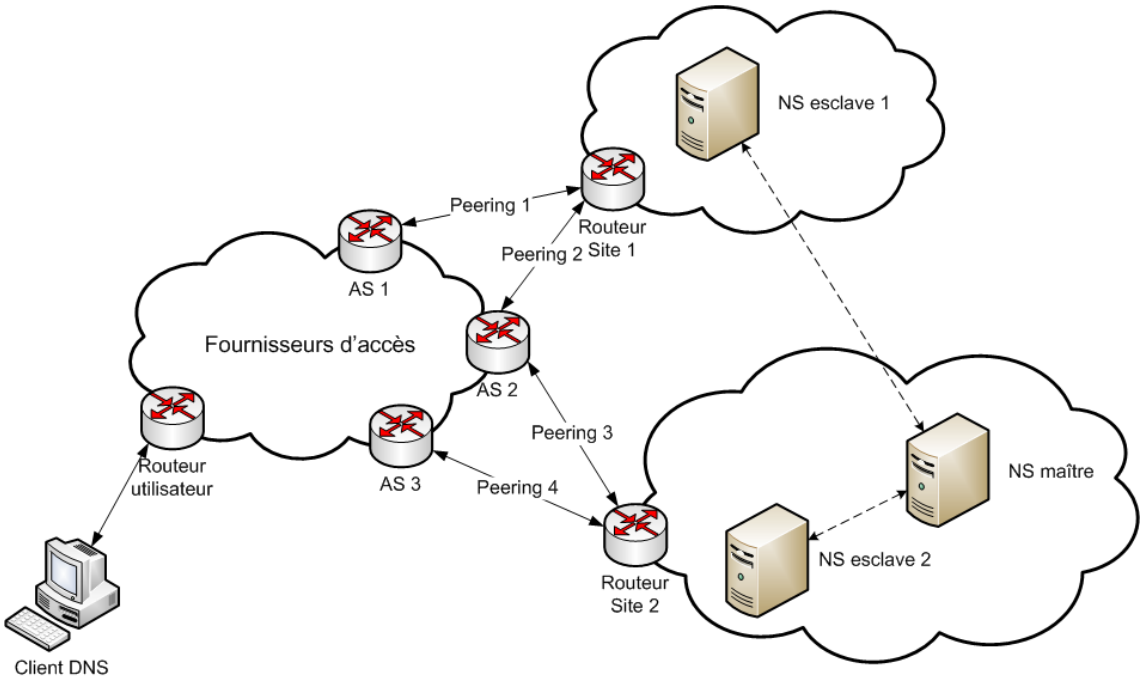

FIGURE 5: Séparation réseaux/sites.

Recommandation

Pour augmenter la résilience, il est conseillé de mettre en place des serveurs NS esclaves sur des réseaux IP distincts et sur des sites distincts.

Recommandation

Dans le cadre de l'échange de bons procédés, il est recommandé de demander l'hébergement d'un serveur NS esclave à un partenaire et vice versa. Des communautés peuvent aussi formaliser un agrément d'hébergement de serveurs esclaves.

Recommandation

Il est très judicieux de prévoir des canaux de communications entre les gestionnaires du serveur NS maître et ceux des serveurs NS esclaves.

3.6 “Name Servers” (NS) esclaves sans autorité

Il faut être très attentif aux risques que présentent les serveurs esclaves qui ne font plus autorité. Il peut arriver que le gestionnaire du serveur maître supprime l'esclave dans sa liste des esclaves à notifier en cas de modification ou dans la liste des serveurs

autorisés à transférer les zones. Dans ce cas, le serveur esclave risque de continuer à desservir pendant quelque temps des données obsolètes.

Recommandation

Les gestionnaires du serveur "NS maître" doivent absolument notifier les serveurs esclaves de tout changement.

Recommandation

Il est recommandé que la liste des serveurs secondaires à notifier soit cohérente avec les enregistrements de type "NS".

3.7 Activation de la notification

Recommandation

Afin que les mises à jour de zones, entre le maître et les esclaves, soient les plus rapides possible, il est recommandé d'activer la notification (Exemple pour Bind : notify yes ;).

3.8 Contrôle des transferts de zones

Le protocole de réseau TSIG (Transaction Signature ou signature de transaction) est principalement utilisé par le système des noms de domaine(DNS) pour fournir une forme d'authentification pour les mises à jour dynamiques des bases de données DNS. Il peut aussi être utilisé entre les serveurs pour les requêtes.
TSIG utilise un secret partagé et une fonction de hachage unidirectionnelle, ceci est nécessaire pour identifier chaque extrémité de la connexion comme ayant le droit d'effectuer ou de répondre à une demande de mise à jour DNS.

Recommandation

Il est conseillé de mettre en place une signature symétrique TSIG (Transaction SIGnature) lors des transferts de zones.

3.9 Synchronisation des horloges systèmes

Pour réaliser une synchronisation de temps précise pour les serveurs DNS, il est recommandé d'utiliser le protocole NTP.

Dans NTP, les serveurs sont référencés avec des niveaux "stratum". Un serveur de stratum 0 est une horloge de référence supposée être précise. Les serveurs de Stratum 0 ne sont jamais connectés au réseau mais directement connectés à un serveur

de stratum 1. Les niveaux inférieurs synchronisent leur temps avec un serveur de stratum supérieur et rajoutent généralement "1/2 - 100 microsecondes" d'imprécision du temps en raison des retards du réseau lors de la synchronisation.

Recommandation

Il est recommandé, lors de l'utilisation de NTP, que la synchronisation soit configurée avec un serveur de stratum 2 si les serveurs de stratum 1 ne sont pas disponibles. La mise en œuvre d'un serveur dédié de stratum 0 devrait être prise en considération pour les infrastructures critiques.

3.10 Mises à jour dynamiques

Recommandation

Il est fortement déconseillé d'autoriser une adresse IP à effectuer des mises à jour dynamiques.

Recommandation

Si cette fonctionnalité est vraiment nécessaire, il faut utiliser TSIG pour authentifier les mises à jour dynamiques.

3.11 Durée de validité des enregistrements d'une zone "TTL"

Les résolveurs ont la faculté de garder en cache les enregistrements trouvés et les réponses indiquant qu'un enregistrement n'existe pas. Ces informations peuvent rester en cache pour une durée allant de plusieurs minutes à plusieurs heures selon le TTL (Time To Live) défini. Par exemple, si lors de la modification d'un enregistrement, entre le moment de la suppression et le moment de la re-création, il y a un grand risque qu'un résolveur mette en cache la réponse négative.

Recommandation

Il est conseillé que Le TTL (Time To Live) soit supérieur à la durée d'une interruption du service DNS.

Recommandation

Il est recommandé que le TTL dépende directement de la charge du DNS : Lorsque le TTL est important, la fréquence d'interrogation du DNS diminue.

Recommandation

Il est recommandé que la durée de validité des enregistrements d'une zone (TTL) soit faible afin de réduire les risques d'empoisonnement du cache. Les valeurs les plus communes sont situées entre 3600 et 86400 secondes.

Recommandation

Afin d'éviter les délais de mise à jour des zones liées au TTL, il est recommandé de déclarer ces zones en esclaves sur les résolveurs internes.

3.12 Diversification des systèmes d'exploitation et des types de serveurs

Recommandation

Il faut employer différents logiciels de serveurs DNS et de systèmes d'exploitation sur les différents serveurs faisant autorité.

3.13 Attribution des adresses IP au NS

Recommandation

Chaque NS doit avoir une adresse IP destinée à la gestion (accès SSH, supervision, etc.) et une adresse IP dédiée au service DNS.

Ceci permet de séparer l'administration du serveur et l'accès au service. Elle autorise également les différentes techniques de redondance (VRRP, Anycast, etc.).

3.14 Politique de sécurité et de filtrage des serveurs

Recommandation

Pour tout serveur public, le seul et unique port accessible de l'Internet doit être "53" en TCP et en UDP.

Recommandation

Aucun autre service ne devrait tourner sur les serveurs en dehors du DNS.

Recommandation

Il faut veiller à maintenir à jour le logiciel du serveur de noms, à appliquer les correctifs de sécurité et à limiter l'accès à ce serveur.

Recommandation

Afin de limiter la portée d'une exploitation de faille de sécurité, il est recommandé de mettre le service DNS dans une arborescence dédiée.

Recommandation

Le serveur DNS doit fonctionner sous l'identité d'un utilisateur avec un minimum de privilèges. Cette identité doit être créée spécifiquement pour ce rôle. Par exemple, "named".

Recommandation

Il ne faut jamais mettre des données sensibles ou qui pourraient faciliter des attaques au niveau des serveurs DNS.

Recommandation

Il est recommandé de définir et d'appliquer une politique de nommage sur l'ensemble des serveurs et des fichiers de zone.

3.15 Protocole de transport du DNS

Le protocole UDP est le protocole de transport du DNS. Mais, lui seul, ne peut pas faire face à un ensemble de problèmes, tels que les attaques par pollution de cache qui exploitent la fragmentation IP et qui ne peuvent être contrées qu'à travers le protocole TCP.

Recommandation

En complément du protocole UDP, il faut impérativement configurer le protocole TCP comme protocole de transport pour le DNS.

3.16 EDNS0

Selon la RFC 6891[6], l'EDNS0 est un mécanisme d'extension du DNS et une première extension, pour indiquer une taille supérieure aux 512 octets. L'extension se fait en "squattant" (exploitant) des champs inutilisés du paquet et en créant un pseudo-type d'enregistrement nommé OPT.

L'EDNS0 est devenu indispensable à toute mise en œuvre du DNS. Il permet la préparation de toute l'infrastructure au déploiement du DNSSEC.

Recommandation

Il faut configurer les infrastructures de manière à prendre en charge EDNS0.

3.17 Création et suivi d'un domaine

Recommandation

Lors de la création, il faut vérifier que les enregistrements de la zone sont corrects. "Zonemaster" peut être utilisé à cet effet.

Recommandation

Pour augmenter la résilience, il est conseillé d'enregistrer :

- Des déclinaisons du nom (exemple : mydomain.ma, my-domain.ma, etc.)
- Et sous différents TLDs (exemple : mydomain.ma, mydomain.org etc.)

Recommandation

Il faut vérifier régulièrement les informations concernant le domaine grâce à Whois.

[6] https://tools.ietf.org/html/rfc6891

ACRONYMES

DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
AFRINIC	African Network Information Center
BGP	Border Gateway Protocol
AS	Autonomous System
RPKI	Resource Public Key Infrastructure
DNS	Domain Name System
DNSSEC	DNS SECurity extensions
SPF	Sender Policy Framework
NS	Name Server
MX	Mail Exchanger
TTL	Time to live
RFC	Request for Comments
PKI	Public Key Infrastructure

Administration de la Défense Nationale
Direction Générale de la Sécurité des Systèmes d'Information
Méchouar Saïd, 10 090 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@dgssi.gov.ma - Web : www.dgssi.gov.ma