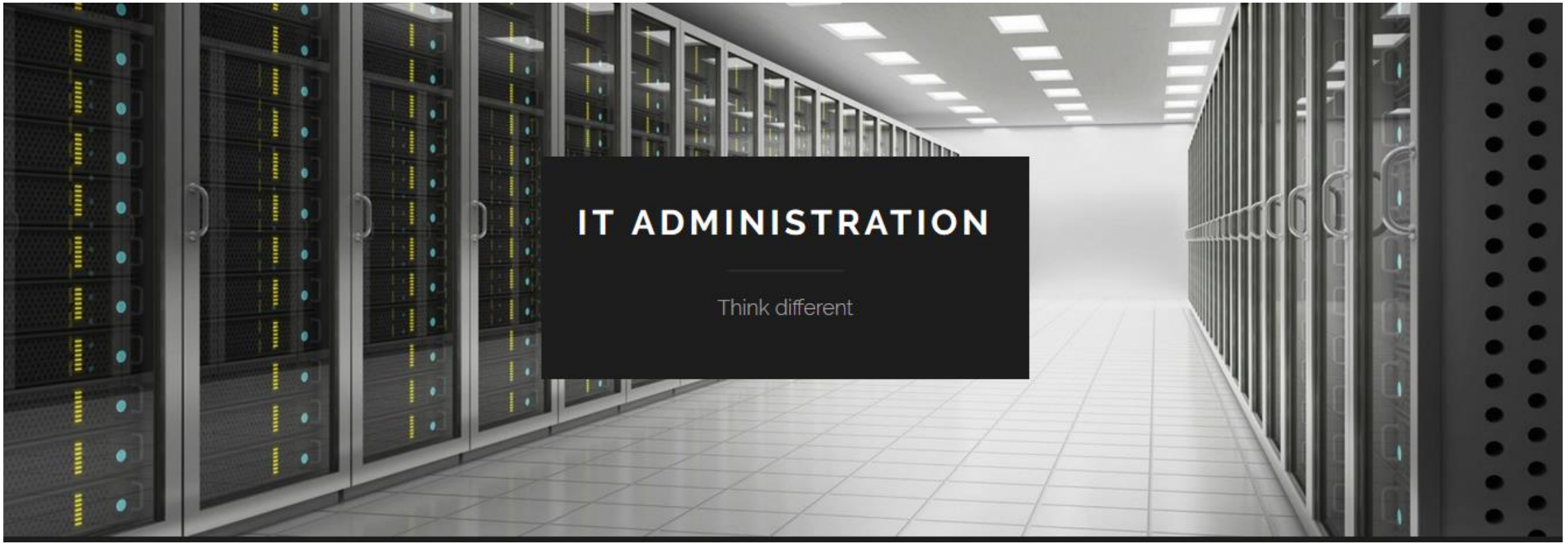

IT ADMINISTRATION
Think different

Importance du DNS dans le déploiement d'un serveur de messagerie

Noé GLELE

13 Octobre 2018

Démarche

- Cette présentation est une démarche méthodologique d'implémentation des composants d'un serveur de messagerie.
- Cette présentation attire l'attention sur le rôle d'un serveur DNS dans l'implémentation de serveur de messagerie publique.
- Cette présentation partage un ensemble de respect de bonnes pratiques et informe sur quelques types d'attaques du DNS.

1

Comprendre le fonctionnement d’un serveur de messagerie

Si vous choisissez de mettre en place votre serveur de messagerie :

- **Vous aurez le contrôle sur la messagerie de votre domaine, mais vous devrez également gérer les tracas associés à la configuration d’un environnement logiciel complexe.**

- **L'utilisation d'un service de messagerie tiers est plus simple, mais vous sacrifierez le contrôle et la flexibilité.**

Dans cette section, nous examinons les avantages et les inconvénients liés à l’exploitation de votre propre serveur de messagerie, ainsi que la manière de choisir un service de messagerie externe, si vous décidez de suivre cette voie.

Avantages ----------

- Contrôle total sur le serveur et votre email
- Choisissez les applications que vous souhaitez utiliser et ajustez-les à vos besoins
- Afficher les journaux des messages entrants et sortants
- Afficher les journaux des tentatives de connexion et d'autorisation des clients de messagerie locaux pour IMAP, POP3 et SMTP

Inconvénients ----------

- La configuration est compliquée
- Les temps d'arrêt peuvent entraîner une perte de courrier électronique
- Le filtrage anti-spam et anti-virus doit être optimisé pour bloquer les emails non désirés et autoriser les emails légitimes
- Si un polluposteur découvre un exploit, il peut utiliser votre serveur pour envoyer du spam et votre adresse IP peut figurer sur une liste noire.
- Aucune assistance tierce pour résoudre les problèmes de messagerie.

Services de messagerie externes

Plusieurs services de messagerie tiers sont disponibles :

- Fastmail
- Google Apps
- Office 365

Principe et Composants

- **Trois composants logiciels distincts :**

1. MTA : l'agent de transfert du courrier relaie le courrier entre votre serveur et l'Internet en général, qu'il s'agisse de transmettre un courrier électronique externe à l'un de vos utilisateurs ou d'envoyer un courrier électronique de l'un de vos utilisateurs. Le courrier entrant accepté est ajouté à la file d'attente du MTA sur le serveur.

2. MDA : l'agent de remise de courrier prend le courrier dans la file d'attente du MTA et l'enregistre dans des boîtes aux lettres individuelles sur votre serveur.

3. Serveur IMAP / POP3 : Gère les utilisateurs et leurs boîtes aux lettres lorsqu'ils vérifient leurs courriels via des connexions IMAP / POP3.

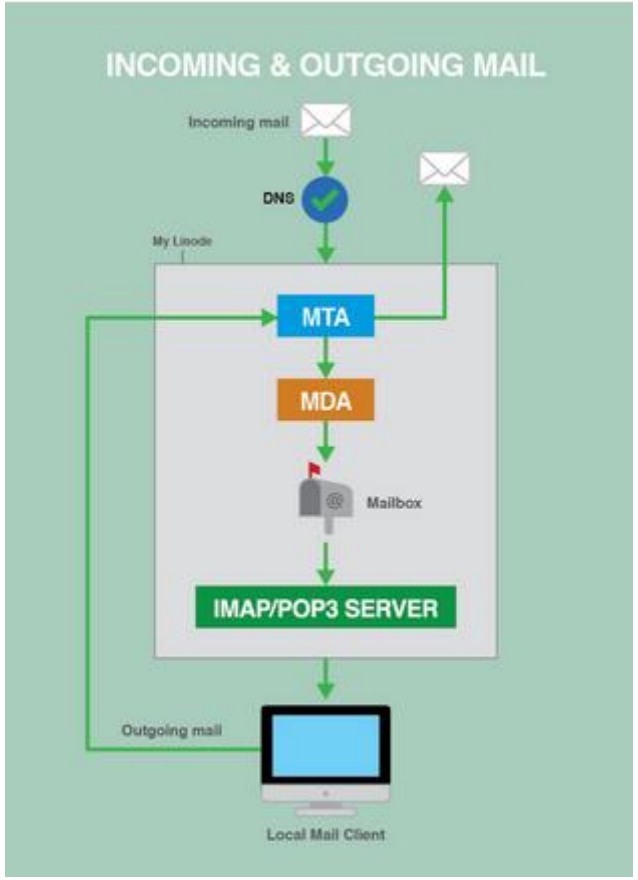
Le processus du serveur de messagerie

1. Un message entrant est dirigé vers votre serveur via **DNS.**

2. Une fois qu'il a traversé le MTA et le MDA, il est stocké dans la boîte aux lettres de l'utilisateur sur le serveur.

3. Lorsque le message est demandé, le serveur IMAP / POP3 établit la connexion entre votre serveur et le client de messagerie local de l'utilisateur.

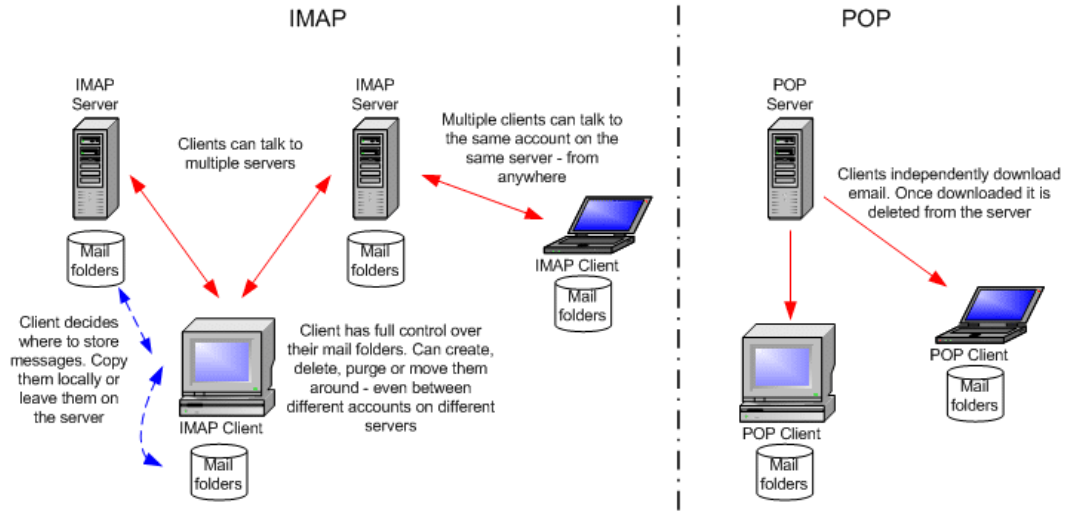
4. Le courrier sortant est envoyé à partir du client de messagerie local de l'utilisateur, traité par le MTA de votre serveur, puis envoyé à sa destination sur Internet.



- **Choisir les composants du serveur de messagerie**

Plusieurs packages logiciels peuvent être utilisés en tant que MTA, MDA et serveurs IMAP / POP3.
Voici quelques options les plus courantes.

Les exemples dans cet atelier, utilisent Postfix en tant que MTA et Dovecot en tant que serveurs MDA et IMAP / POP3.



MTA

Voici les services MTA les plus populaires disponibles :

- **Courier Mail Server** est livré avec Courier-IMAP, qui est la partie populaire de la suite de serveurs de messagerie Courier, mais Courier-MTA inclut également des fonctionnalités de relais de messagerie. C’est un MTA plus simple mais quelque peu limité.
- **Exim** est moderne et orienté vers la flexibilité. C’est sécurisé, mais pas aussi sécurisé que Postfix. C’est très personnalisable, mais c’est l’un des MTA les plus complexes à configurer.
- **Postfix** fait partie de la construction recommandée du serveur de messagerie. C’est moderne, orienté sécurité et très flexible. C'est un peu plus simple à configurer qu'Exim.
- **Qmail** est un MTA moderne et prend en charge les répertoires de style Maildir. Qmail n'a pas reçu de mise à jour depuis 2007, mais reste très populaire.
- **Sendmail** est un ancien MTA qui a un public nombreux et un bon support.
- **Zimbra** est un service de messagerie tout-en-un. Zimbra offre une installation simple, mais peu d'options configurables.

MDA

Voici quelques-uns des MDA les plus populaires disponibles :

- **Cyrus's MDA** fait partie du serveur Cyrus IMAP / POP3. Cyrus est un serveur IMAP / POP3 moderne et axé sur la sécurité, conçu pour fonctionner sur des serveurs où les utilisateurs ne se connectent pas directement.
- **Deliver** est un utilitaire de distribution de courrier Linux simple configuré par défaut dans les fichiers de configuration d'Imapd.
- **Le LDA de Dovecot et le serveur LMTP de Dovecot** font partie du serveur IMAP / POP3 de Dovecot. Dovecot est un serveur de messagerie léger, moderne et configurable.
- **Maildrop** est le MDA de Courier. Courier est un serveur de messagerie tout-en-un.
- **Le MDA de Postfix** fait partie du logiciel Postfix MTA. Postfix est un MTA flexible, moderne et axé sur la sécurité.
- **Le MDA de Sendmail** fait partie du logiciel Sendmail MTA. Sendmail est un ancien MTA qui reste populaire.

IMAP et POP3

Voici les serveurs IMAP et POP3 les plus populaires disponibles :

- **Citadel** est un service de messagerie tout-en-un qui comprend la messagerie, les calendriers, la messagerie instantanée, les listes de diffusion et d'autres outils de collaboration. Il est open source et destiné aux petites et moyennes entreprises.
- **Courier** possède un serveur IMAP très populaire appelé Courier IMAP. Il s'agit d'une suite logicielle tout-en-un pour serveur de messagerie, mais Courier IMAP peut être installé seul si c'est le seul élément dont vous avez besoin.
- **Cyrus** est un serveur IMAP / POP3 moderne et axé sur la sécurité, conçu pour fonctionner sur des serveurs scellés où les utilisateurs ne se connectent pas directement.
- **DBMail** est un projet open source qui stocke le courrier dans des bases de données au lieu de fichiers plats.
- **Dovecot** est un serveur de messagerie léger, moderne et configurable, qui fait partie de la construction de notre serveur de messagerie recommandée.
- **Xmail** est un serveur POP3 complet, mais ne prend pas en charge IMAP.
- **Zimbra** est un service de messagerie tout-en-un qui est beaucoup plus simple à installer que d'autres options, mais moins personnalisable.

2

Construisez votre serveur de messagerie

Certificat SSL

Un certificat SSL chiffre les connexions sur votre serveur de messagerie. Il est possible d'exécuter un serveur de messagerie sans certificat SSL, mais cela n'est pas recommandé.

Tout type de certificat SSL fonctionnera, mais certains certificats ont un degré de confiance différent pour vos utilisateurs. Si vous souhaitez obtenir le plus haut niveau de confiance, vous devez acheter un certificat SSL signé auprès d'une entreprise réputée.

Vous pouvez également utiliser un certificat auto-signé gratuit si vous êtes à l'aise avec les avertissements qu'il génère. Vous pouvez créer votre propre certificat SSL auto-signé ou, si vous suivez notre version recommandée, vous pouvez utiliser celui fourni avec Dovecot par défaut.

Installation du logiciel

Installez et configurez le serveur MTA, MDA et IMAP / POP3. Pour vous aider à gérer les domaines, les adresses électroniques, les informations d'identification de l'utilisateur, les alias, etc., installez un serveur de base de données tel que **MySQL ou PostgreSQL**.

Pour obtenir des instructions de configuration détaillées (Postfix, Dovecot, Mysql), je vous conseille fortement le lien suivant :

https://www.linode.com/docs/email/postfix/email-with-postfix-dovecot-and-mysql/

Enregistrements DNS

Les enregistrements DNS aident le courrier électronique à atteindre votre serveur. Les bons enregistrements DNS aident également à désigner votre serveur en tant que **serveur de messagerie légitime**.

Synoptique ----------

Apprenons ensemble à définir les enregistrements MX, SPF et PTR appropriés pour votre domaine et serveur.

Temps de vie (TTL)
Réduire le temps de vie (TTL) de vos enregistrements DNS existants à la valeur minimale autorisée au moins 24 à 48 heures avant toute autre modification DNS. Propagation rapide.

MX Records
Les enregistrements MX indiquent à Internet où envoyer les emails de votre domaine.

BDF MX record en exemple :

Domain	TTL	Type	Priority	Target
dnsforum.bj	86400	MX	10	192.64.117.169

Un enregistrement MX typique ressemble à ceci :

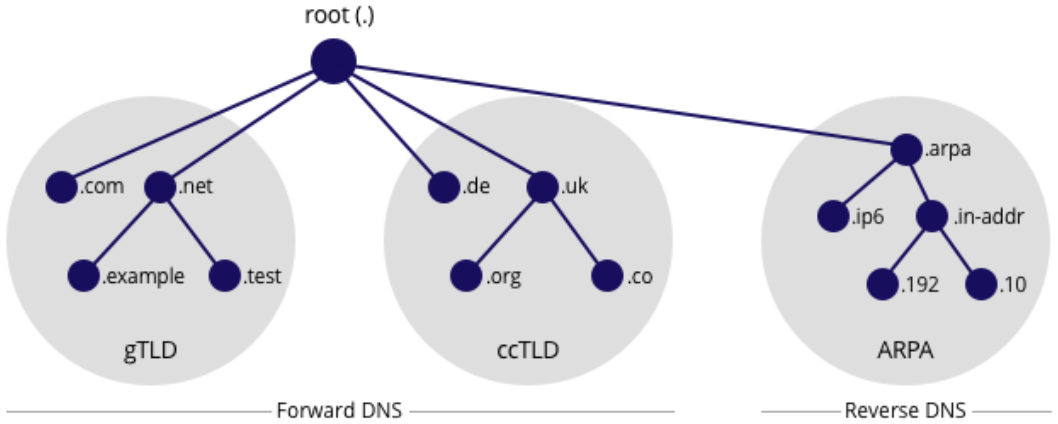
dnsforum.bj	*86400*	*MX*	*10*	*dnsforum.bj*
dnsforum.bj	*86400*	*MX*	*10*	*192.64.117.169*
mail. dnsforum.bj	*86400*	*MX*	*10*	*192.64.117.169*

Enregistrements SPF

Les enregistrements SPF aident à établir la légitimité de votre serveur de messagerie et à réduire les risques d'usurpation d'identité, ce qui se produit lorsque quelqu'un simule les en-têtes d'un e-mail pour lui donner l'impression qu'il provient de votre domaine, même s'il ne l'a pas été. Les spammeurs peuvent essayer de le faire pour contourner les filtres anti-spam.

DNS inversé

Définissez un DNS inversé pour le domaine ou le sous-domaine de votre serveur de messagerie.



Protection anti-spam et anti-virus, clients de messagerie, etc.

À ce stade, vous devez avoir un serveur de messagerie de base opérationnel. Il reste cependant un peu plus à faire si vous souhaitez offrir à vos utilisateurs la meilleure expérience de messagerie possible. Cela inclut l'ajout **de filtres anti-spam et antivirus pour protéger vos utilisateurs**, la configuration de clients de messagerie, la fourniture d'une solution de messagerie Web et l'ajout des extras de votre choix, tels que des listes de diffusion.

- ## Protection anti-spam et anti-virus

Voici quelques-uns des services de filtre anti-spam et antivirus les plus populaires :

- **Amavis** est un filtre de contenu open source pour la messagerie électronique qui s'intègre directement à votre MTA. Il effectue lui-même certaines vérifications et peut également être utilisé avec des filtres anti-spam et antivirus plus robustes.
- **Clam AntiVirus** est un scanner de virus populaire, gratuit et à code source ouvert.
- **SpamAssassin** est un filtre anti-spam gratuit très populaire.

Que faire si votre serveur a été mis sur liste noire

Si votre serveur est ajouté à une liste de blocage, prenez des mesures pour atténuer la source du spam. Une fois ces problèmes atténués, contactez le fournisseur de messagerie qui vous a bloqué et suivez ses étapes pour être autorisé à envoyer de nouveau du courrier.

Clients de messagerie

Les clients de messagerie font partie intégrante de l'expérience de messagerie pour vos utilisateurs. Microsoft Outlook, Apple Mail et Mozilla Thunderbird sont tous des exemples de clients de messagerie.

- Protocoles: Choisissez IMAP ou POP3 pour la réception et SMTP pour l'envoi.
- Cryptage: Choisissez le cryptage SSL et / ou TLS, en fonction des paramètres de votre serveur.

Voici quelques exemples de ports de messagerie:
110: POP3 995: SSL-POP (crypté) 143: IMAP 993: IMAPS (crypté) 25: SMTP (parfois bloqué par les FAI)

587: SMTP (le port préféré non chiffré pour les connexions sortantes à partir de clients de messagerie)
465: SSMTP (crypté)

Pare-feu

Si vous utilisez un pare-feu, veillez à éditer les règles des ports de votre serveur de messagerie.

Webmail

Webmail est un type de client de messagerie pouvant être installé sur votre serveur et accessible à partir d'un navigateur Web.
Voici quelques-uns des clients de messagerie Web les plus populaires:

- **Mail-in-a-box** est une option de messagerie tout-en-un qui offre une approche simple pour configurer un serveur de messagerie et un composant de messagerie Web.
- **Citadel** est un service de messagerie tout-en-un qui comprend la messagerie, les calendriers, la messagerie instantanée, les listes de diffusion et d'autres outils de collaboration. Il est open source et destiné aux petites et moyennes entreprises.

- **Horde Webmail** est un client IMAP open source associé à des fonctions supplémentaires telles que la gestion de compte et les calendriers.
- **RoundCube** est un client IMAP avec des fonctionnalités modernes et une mise en page propre.
- **SquirrelMail** est une option solide, mais possède une interface utilisateur plus ancienne.
- **Zimbra** est un service de messagerie tout-en-un qui est beaucoup plus simple à installer que d'autres options, mais moins personnalisable.

3

DNS : types d’attaques et techniques de sécurisation

Attaques visant directement le DNS

Par Noé GLELE

Les atteintes aux infrastructures DNS sont essentiellement d'ordre technique, faisant appel à des stratégies d'attaques massives ou de corruption des informations échangées entre les résolveurs et les serveurs DNS :

l'empoisonnement vise à intoxiquer le résolveur pour qu'il considère que le serveur « pirate » est légitime, en lieu et place du serveur originel. Cette opération permet notamment de capter et de détourner les requêtes vers un autre site web sans que les utilisateurs puissent s'en rendre compte, avec à la clé, le risque de les voir confier des données personnelles en se croyant sur le site légitime de la victime de l'attaque.

le déni de service (Denial of Service ou DoS) a pour objectif de rendre l'accès à un service impossible ou très pénible. Cette attaque peut se faire de manière brutale (saturation des serveurs par envoi massif de requêtes simultanées) ou plus subtile si l'attaquant essaie d'épuiser une ressource rare sur le serveur.

le déni de service distribué (distributed Denial of Service ou dDoS), forme élaborée du DoS impliquant plusieurs milliers d'ordinateurs, en général dans le contexte d'un BOTNET ou roBOT NETwork

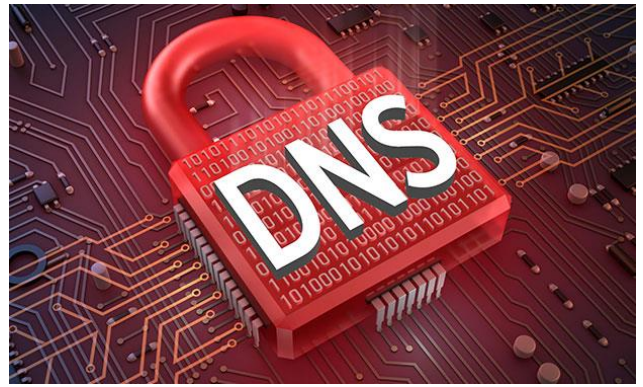
la réflexion : des milliers de requêtes sont envoyées par l'attaquant au nom de la victime. Lorsque les destinataires répondent, toutes les réponses convergent vers l'émetteur officiel, dont les infrastructures se trouvent affectées

la réflexion combinée à l'amplification : si la taille de la réponse est plus grosse que celle de la question, on dit qu'il y a amplification. La technique est la même que pour la réflexion, mais la différence de poids entre question et réponses crée un effet amplificateur. Une variante peut exploiter les mécanismes de protection mis en place, qui ont besoin de temps pour décoder les réponses longues avec pour effet éventuel un ralentissement dans la résolution des requêtes

le Fast flux : afin de ne pas être identifié, l'attaquant peut, en plus de la falsification de son adresse IP, utiliser cette technique reposant sur la rapidité de la diffusion des informations de localisation pour masquer l'origine de l'attaque. Diverses variantes existent, comme le Simple flux, ou le Double Flux (changer en permanence l'adresse du serveur web mais aussi les noms des serveurs DNS).

Les principales techniques de sécurisation

1. assurer la meilleure redondance possible
2. veiller à utiliser des versions à jour des logiciels DNS
3. assurer une surveillance régulière de ses serveurs et de leur configuration (ZoneCheck)
4. envisager de déployer
5. définir un « Plan de continuité d'activité »



La sécurité de l'infrastructure de l'Internet repose sur une répartition adéquate des rôles entre les différents acteurs (opérateurs de service, FAI, registres, bureaux d'enregistrement, hébergeurs, points d'échange, autorités publiques, CERT…). La diversité des structures, des technologies et des approches est l'un des principaux gages de la résilience de l'Internet.

Chacun des acteurs de cet écosystème doit ensuite appliquer les principes de base d'une sécurité efficace : **coordination, communication et coopération**, qui constituent les « 3 C ». Dans le cas de l'Internet, la variété et le nombre des acteurs impliqués soulèvent un défi important, tant au plan national qu'international.

Quelques conseils

- Implémentation – Accompagnement – Stratégie

Ipv6 taskforce
bdsec

- Infrastructure

- Perspectives 2019

BENIN DNS FORUM

4ème Edition

Et si on rêvait un peu …

Par Noé GLELE