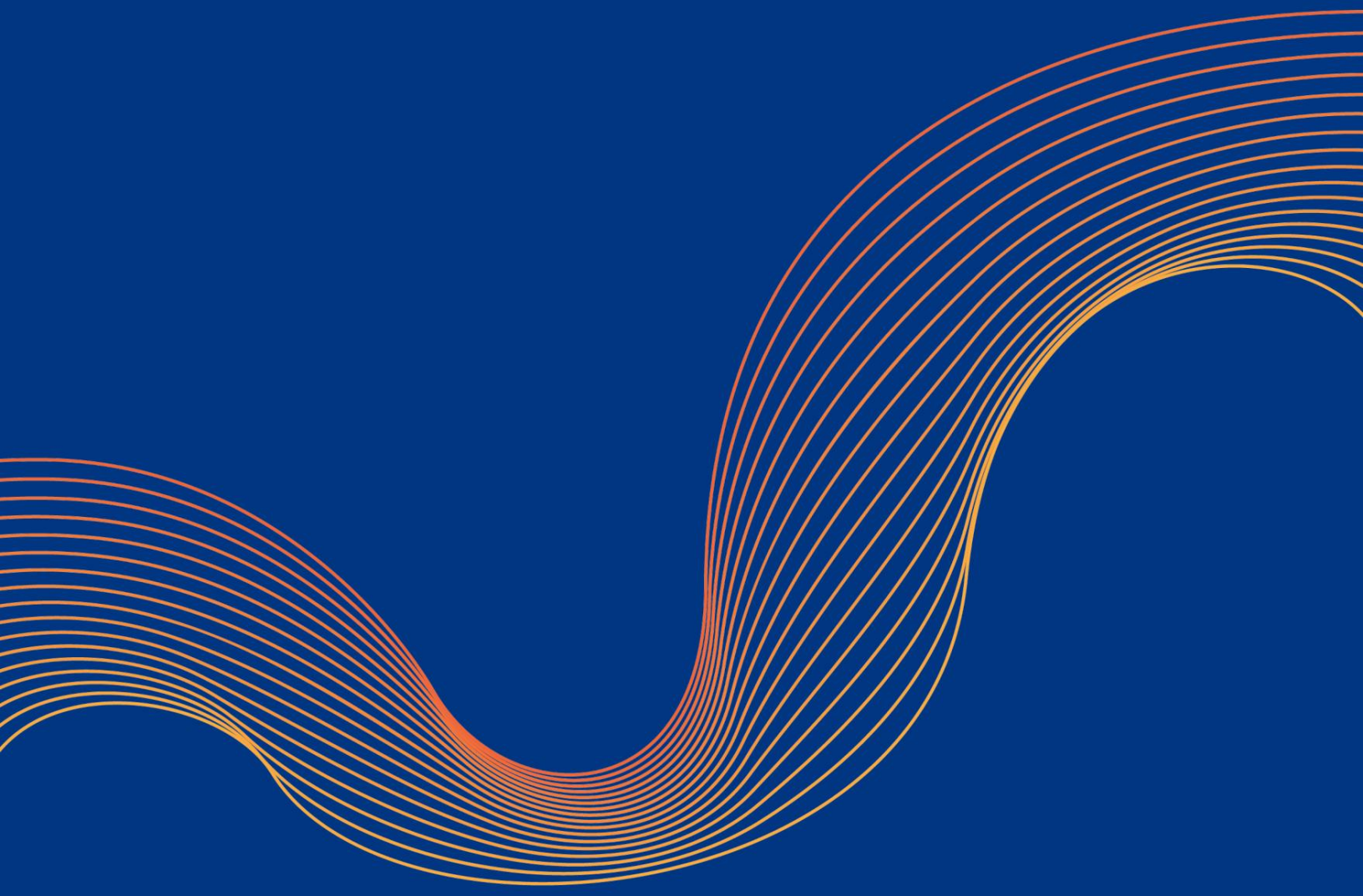
LIVRE BLANC

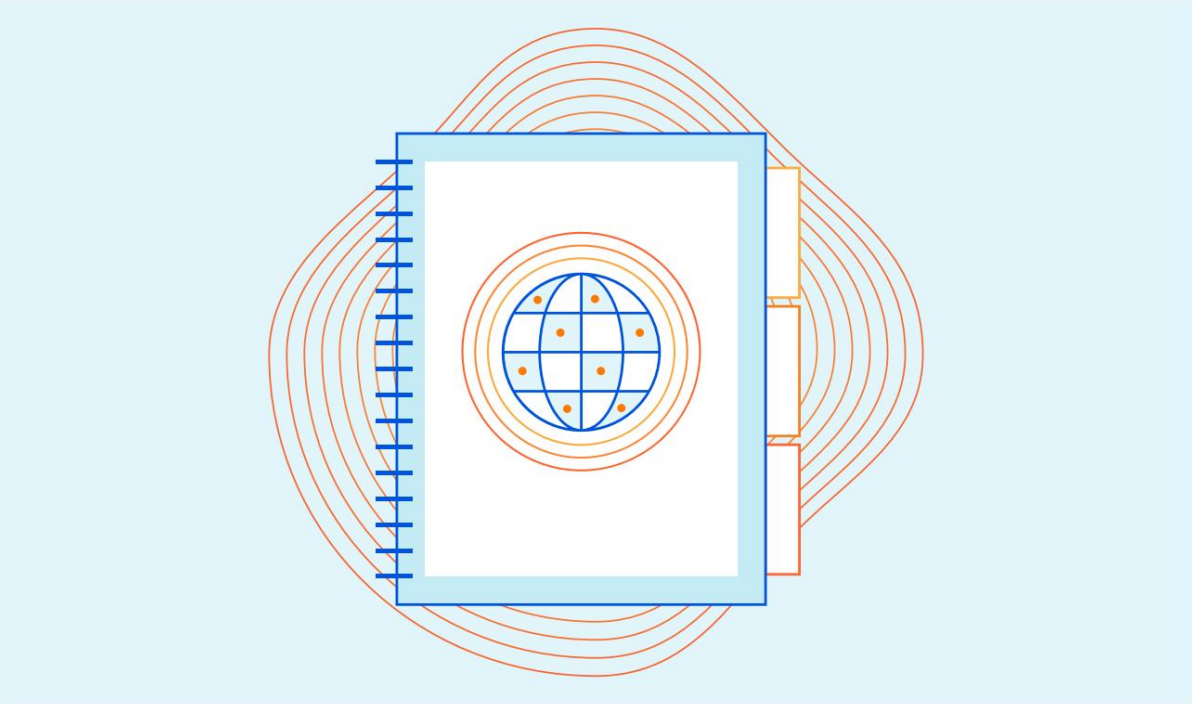
CLOUDFLARE

Améliorer la sécurité, les performances et la fiabilité du DNS



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

I. Résumé



La vitesse d'un site Web ou d'une application mobile dépend de celle de son composant le plus lent. Comment pouvez-vous vous assurer que le DNS ne devienne pas ce point d'étranglement ?

Lorsqu'il est utilisé et mis en œuvre correctement, le DNS peut améliorer considérablement la sécurité, les performances et la fiabilité d'une propriété Internet. Cependant, l'infrastructure DNS est extrêmement vulnérable à un large éventail de cyberattaques de plus en plus courantes qui peuvent dégrader les performances ou faire tomber complètement les serveurs DNS. Ces attaques, ainsi que les attentes croissantes des utilisateurs en matière de performances et de disponibilité des sites Web, font qu'il est risqué pour le DNS d'être un point de défaillance unique.

Pour garantir la sécurité, les performances et la fiabilité d'un site, il faut une sécurité DNS intégrée et une infrastructure DNS redondante optimisée pour les performances. Ce document explique comment bénéficier de ces avantages.

II. La sécurité DNS : un maillon faible de la cybersécurité des entreprises

L'infrastructure DNS utilisée aujourd'hui a été conçue dans les années 1980, lorsque l'accès à Internet était limité aux agences gouvernementales, aux scientifiques et à l'armée. Les architectes du système se préoccupaient de la fiabilité et de la fonctionnalité, et non de la sécurité.1 Par conséquent, les serveurs DNS du monde moderne sont

vulnérables à un large éventail de types d'attaques, notamment l'usurpation d'identité, les logiciels malveillants, le tunneling DNS et les attaques DoS/DDoS. Ces attaques se produisent de plus en plus fréquemment et deviennent plus coûteuses. Selon le rapport mondial sur les menaces DNS 2019 d'IDC : • 82 % des organisations ont subi une attaque DNS au cours des deux dernières années

- Des augmentations significatives d'une année sur l'autre ont été signalées pour tous les types d'attaques, du volumétrique au signal faible
- Le coût moyen par attaque a dépassé 1 million de dollars en 2019, soit une augmentation de 49 % par rapport à l'année précédente2

Une autre raison de se montrer vigilant est que les attaques DNS sont souvent déployées en conjonction avec d'autres cyberattaques pour détourner l'attention du personnel de sécurité de la véritable cible. Verizon estime que les attaques DNS sont impliquées dans environ un tiers des violations de données3.

Types d'attaques DNS

Il existe de nombreuses attaques DNS. La plupart sont des variantes d'attaques par déni de service distribué (DDoS), dans lesquelles un volume de trafic tellement important est envoyé à une machine ciblée que le trafic légitime ne peut pas passer.

Les méthodes d'attaque courantes incluent :

- Amplification DNS. Ces attaques utilisent un point de terminaison compromis pour envoyer des paquets UDP avec des adresses IP usurpées à un récurseur DNS. Chacun des paquets UDP envoie une requête à un résolveur DNS, en passant souvent un argument tel que « ANY » afin de recevoir la plus grande réponse possible. Après avoir reçu les requêtes, le résolveur DNS, qui essaie d'être utile en répondant, envoie une réponse volumineuse à l'adresse IP usurpée. L'adresse IP de la cible reçoit la réponse et l'infrastructure réseau environnante est submergée par le déluge de trafic, ce qui entraîne un déni de service.

- Torture DNS. Ces attaques génèrent des chaînes aléatoires (c'est-à-dire de faux noms de sous-domaines aléatoires) pour obliger les serveurs DNS à tenter de résoudre l'adresse IP de sous-domaines qui n'existent pas, comme xxyyzz.foo.com. En conséquence, foo.com doit répondre à la requête même si xxyyzz.foo.com n'existe pas.

- Usurpation DNS/empoisonnement du cache : dans ces attaques, des données DNS falsifiées sont introduites dans le cache d'un résolveur DNS, ce qui amène le résolveur à renvoyer une adresse IP incorrecte pour un domaine.
  Au lieu d'aller vers le bon site Web, le trafic peut être détourné vers une machine malveillante ou vers n'importe quel autre endroit souhaité par l'attaquant ; il s'agira souvent d'une réplique du site d'origine utilisée à des fins malveillantes telles que la distribution de logiciels malveillants ou la collecte d'informations de connexion.

Optimisation du DNS pour la sécurité

Étant donné la grande diversité des menaces DNS, l'atténuation efficace des attaques DNS nécessite une stratégie de sécurité intégrée qui inclut tous les éléments suivants :

Activez DNSSEC, un ensemble de protocoles de sécurité qui vérifie les enregistrements DNS à l'aide de signatures cryptographiques. En s'assurant que la signature d'un site correspond à son enregistrement, les résolveurs DNS peuvent authentifier l'origine des données envoyées depuis le serveur DNS, empêchant ainsi toute usurpation d'identité.

Mettez en œuvre une atténuation des attaques DDoS multicouches, notamment des mesures de filtrage du trafic telles que la limitation du débit, la mise sur liste blanche/bloquée des adresses IP et le suivi des connexions pour bloquer les requêtes malveillantes tout en autorisant le trafic légitime. En plus d'améliorer la sécurité, l'atténuation des attaques DDoS améliorera également la fiabilité et les performances en empêchant le trafic malveillant de submerger les serveurs DNS.

Déployez des pare-feu DNS (également appelés filtrage DNS et blocage DNS) pour bloquer l'accès à partir de domaines malveillants connus.

Activer la journalisation DNS. En plus de vous avertir si un pirate tente de falsifier vos serveurs DNS, la journalisation DNS offre une visibilité sur les problèmes liés aux requêtes ou aux mises à jour DNS.

Forcer HTTPS. En exigeant que les navigateurs chargent toujours les sites Web via HTTPS, on empêche l'usurpation de domaine en authentifiant chaque site avec un certificat SSL/TLS.

Utilisez la résolution multi-nœuds. Cela signifie que le processus de recherche DNS doit être confié à différents serveurs (souvent avec des fournisseurs ou des réseaux différents) pour créer une redondance en cas d'attaque.

III. Performances DNS : un maillon faible potentiel dans les performances d'un site Web

Lorsque les utilisateurs accèdent à un élément Web, leurs appareils interrogent un résolveur DNS qui associe le nom de domaine de l'élément à son adresse IP, puis renvoie l'adresse IP correcte à l'appareil. Chaque fois qu'un utilisateur accède à une nouvelle page dans son navigateur, il doit effectuer au moins une recherche DNS. De nombreuses pages chargent des éléments de plusieurs domaines, ce qui nécessite plusieurs recherches. Ce processus est appelé résolution DNS, et le temps nécessaire pour résoudre chaque domaine demandé s'accumule rapidement. C'est pourquoi l'optimisation de la vitesse de résolution DNS est essentielle pour obtenir une faible latence.

Tous les fournisseurs DNS ne sont pas optimisés pour la vitesse de résolution. Un fournisseur DNS lent peut prendre plus de 120 millisecondes pour résoudre chaque requête DNS.4 Les fournisseurs DNS les plus rapides résoudront les requêtes en moins de 20 millisecondes ; Cloudflare DNS, par exemple, résout les requêtes en moins de 12 millisecondes en moyenne.5

- Les utilisateurs du Web d'aujourd'hui exigent que les ressources numériques se chargent instantanément. Même les petits problèmes peuvent avoir un impact notable sur les taux d'engagement et de conversion.
- Une latence accrue du site, aussi faible que 100 à 400 millisecondes, a un impact mesurable sur le comportement des consommateurs6
- Une seule seconde supplémentaire de temps de chargement peut entraîner une baisse des conversions de 7 %7
- Environ la moitié des utilisateurs mobiles s'attendent à ce que les applications répondent en deux secondes ou moins8
- Google utilise la vitesse de la page comme facteur de classement pour la recherche sur ordinateur et sur mobile9

Optimisation du DNS pour les performances

Voici quelques mesures que vous pouvez prendre pour garantir des performances élevées sur un marché où chaque milliseconde compte.

Utilisez un routage basé sur la géolocalisation globale. Tous les 100 miles de distance géographique entre les utilisateurs finaux et les ressources numériques ajoutent environ 0,82 milliseconde de latence10. Il est donc important de géo-orienter les visiteurs vers l'infrastructure DNS située dans leur région du monde.

Déterminez une durée de vie optimale (TTL). Les TTL contrôlent indirectement la mise en cache du résolveur DNS. Les TTL faibles peuvent dégrader les performances, mais peuvent aider à l'équilibrage de charge basé sur DNS. Les TTL élevés améliorent les performances, mais peuvent amener les utilisateurs à être redirigés vers un serveur mis en cache qui est depuis tombé en panne. Étant donné que de nombreux facteurs sont impliqués, il n'existe pas de valeur TTL optimale universelle.

Utilisez Anycast. Recherchez un fournisseur DNS qui utilise Anycast, ce qui permet à plusieurs serveurs DNS répartis dans le monde entier de publier la même adresse IP. Cela améliore la vitesse de résolution DNS et offre également une protection DNS de secours transparente.

Déplacez votre DNS vers la périphérie du réseau

11 millisecondes
vitesse moyenne
de recherche DNS

<5 secondes
pour le monde entier
Propagation DNS

IV. Fiabilité DNS : la redondance évite les temps d'arrêt

Si rien n'est fait, les problèmes de latence peuvent entraîner, dans le pire des cas, une panne totale de votre site Web. Les coûts des temps d'arrêt sont élevés : une étude a révélé que le coût moyen par minute d'une panne de centre de données est de 8 851,11 USD.

L'objectif de toute entreprise doit être de garantir une disponibilité de ses systèmes à 100 %. Même si cela peut paraître ambitieux, il est réalisable si les entreprises adoptent une approche à plusieurs volets centrée sur la redondance.

Optimisation du DNS pour la fiabilité

Les performances et la fiabilité sont comme la tête et le cou : elles sont étroitement liées. L'une ne peut exister sans l'autre. Toutes les mesures que vous prenez pour améliorer la fiabilité amélioreront également les performances. Par exemple, l'utilisation de deux fournisseurs DNS améliore les temps de chargement des pages, car la résolution des serveurs de noms se fera par défaut sur le fournisseur DNS le plus rapide.

- Utilisez une approche multi-DNS. Dans une configuration DNS à fournisseur unique, tous les utilisateurs reçoivent une réponse de ce fournisseur. Les serveurs de noms du fournisseur sont définis, ce qui rend les sites vulnérables aux pannes du fournisseur. Les alternatives incluent :
  - Deux fournisseurs DNS (primaire/secondaire). L'ajout d'un deuxième fournisseur DNS double le nombre d'ensembles de serveurs de noms disponibles pour ces domaines. Si le fournisseur faisant autorité n'est pas disponible, le trafic de requêtes est automatiquement acheminé vers l'ensemble de serveurs de noms de secours. • Principal masqué. Dans ce modèle, le serveur faisant autorité n'est pas visible sur l'Internet public et est souvent caché derrière un pare-feu. Ses enregistrements DNS sont répliqués sur le serveur DNS secondaire, qui répond aux requêtes.
  - Primaire-Primaire. Dans ce modèle, les deux serveurs sont visibles sur l'Internet public.
- DNS basé sur le cloud. Peu d'organisations disposent des ressources et de l'expertise internes pour gérer leurs propres serveurs DNS.
- Segmentation des serveurs de noms. Certains fournisseurs DNS regroupent un grand nombre, voire la totalité, de leurs clients dans le même enregistrement de serveur de noms. Si un client subit une attaque DDoS, tous ses « voisins » sont gravement touchés. Assurez-vous que votre fournisseur DNS segmente son réseau de manière à ce que seul un petit nombre de clients partagent les enregistrements de serveur de noms.
- Un réseau mondial très étendu de nœuds DNS. Le réseau DNS de votre fournisseur doit inclure un grand nombre de nœuds DNS répartis dans le monde entier, de sorte que si l'un d'eux tombe en panne, le trafic peut être acheminé vers l'un des nœuds restants. Un réseau mondial permet également le géo-pilotage, ce qui améliore les performances.
- Équilibrage de charge global et local. En plus de garantir qu'aucun serveur ne soit surchargé, si un Si le serveur tombe en panne, un équilibreur de charge redirige le trafic vers les serveurs restants.

V. Conclusion

Quelques millisecondes de temps de chargement peuvent faire ou défaire votre expérience utilisateur et votre taux de conversion. Les performances et la fiabilité d'un site Web dépendent de la vitesse de résolution DNS, mais les serveurs DNS sont extrêmement vulnérables à une grande variété de cyberattaques. Pour garantir une infrastructure DNS sécurisée et performante avec une disponibilité de 100 %, il faut adopter une approche intégrée de la sécurité, de la fiabilité et des performances.

VI. Comment Cloudflare peut vous aider

Cloudflare propose un service DNS de qualité professionnelle qui reflète bon nombre de ces bonnes pratiques, offrant le temps de réponse le plus rapide, une redondance inégalée et une sécurité avancée avec une atténuation DDoS et DNSSEC intégrées. Pour en savoir plus et parler à un membre de notre équipe, visitez www.cloudflare.com/dns/.

Notes de fin

1. ICANN, « DNSSEC : qu'est-ce que c'est et pourquoi est-ce important ? » https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en. Consulté le 27 janvier 2020.
2. IDC, « Rapport mondial sur les menaces DNS 2019 », https://www.efficientip.com/resources/idc-dns-threat-report-2019/. Consulté le 26 janvier 2020.
3. Global Cyber Alliance, « La valeur économique de la sécurité DNS », https://www.globalcyberalliance.org/wp-content/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf. Consulté le 27 janvier 2020.
4. Mann, Bill. « Les meilleurs serveurs DNS en termes de vitesse et de confidentialité en 2019. » Blokt, https://blokt.com/guides/best-dns-servers. Consulté le 27 janvier 2020.
5. « Analyse et comparaison des performances DNS. » DNSPerf, https://www.dnsperf.com/. Consulté le 23 juillet 2019.
6. Brutlag, Jake. « Speed Matters », blog Google AI, https://ai.googleblog.com/2009/06/speed-matters.html. Consulté le 27 janvier 2020.
7. Rodman, Tedd. « Marketing et performances Web : comment la vitesse du site affecte les indicateurs », Yotta, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. Consulté le 27 janvier 2020.
8. Dimensional Research. « Ne pas répondre aux attentes des utilisateurs d'applications mobiles : une enquête auprès des utilisateurs d'applications mobiles », https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf. Consulté le 27 janvier 2020.
9. « Utilisation de la vitesse de la page dans le classement des recherches mobiles », blog Google Webmaster Central, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. Consulté le 27 janvier 2020.
10. Sherman, Fraser. « Latence du réseau en millisecondes par mile », Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile/ Consulté le 27 janvier 2020.
11. Priceonomics Data Studio. « Quantifier le coût exorbitant des pannes informatiques », https://priceonomics.com/quantifying-the-staggering-cost-of-it-outages/. Consulté le 27 janvier 2020.