Se lancer avec Cloudflare

Cloudflare est un service populaire qui offre une gamme d'outils pour améliorer les performances, la sécurité et la fiabilité de votre site web. Que vous gériez un petit blog ou un grand site de commerce électronique, les fonctionnalités de Cloudflare, comme la gestion DNS, le réseau de distribution de contenu (CDN) et les protections de sécurité, peuvent faire une différence significative. Dans cet article de blog, nous allons passer en revue trois tâches clés : la configuration DNS, la gestion des enregistrements A et l'interdiction des régions IP. Ce sont essentiels pour tirer le meilleur parti de Cloudflare, et ils sont plus faciles à configurer que vous pourriez le penser !

Pourquoi utiliser Cloudflare ?

Avant de plonger dans le comment faire, jetons un coup d'œil rapide à ce qui rend Cloudflare si précieux : - **Gestion DNS** : Cloudflare fournit des services DNS rapides et fiables, garantissant que votre site web est toujours accessible. - **CDN** : Il accélère votre site en mettant en cache le contenu plus près de vos visiteurs. - **Sécurité** : Cloudflare offre une protection contre les attaques DDoS, un chiffrement SSL/TLS et des outils pour bloquer le trafic malveillant. - **Facilité d'utilisation** : Et mieux encore, Cloudflare propose un plan gratuit parfait pour les petits sites web et blogs.

Passons maintenant aux détails.

Étape 1 : Configurer le DNS sur Cloudflare

Le DNS (Domain Name System) est comme l'annuaire téléphonique de l'Internet - il traduit votre nom de domaine (par exemple, `example.com`) en une adresse IP que les serveurs peuvent comprendre. Lorsque vous utilisez Cloudflare, vous gérerez vos enregistrements DNS via leur plateforme, qui offre une vitesse et une sécurité supplémentaires.

Comment configurer le DNS Cloudflare :

1. **Inscription à Cloudflare** : Si vous n'avez pas encore de compte, rendez-vous sur le site web de Cloudflare et inscrivez-vous pour un compte gratuit.
2. **Ajouter votre domaine** : Une fois connecté, cliquez sur "Ajouter un site"et entrez votre nom de domaine (par exemple, `example.com`). Cloudflare analysera vos enregistrements DNS existants.
3. **Revoir les enregistrements DNS** : Après l'analyse, Cloudflare vous montrera une liste de vos enregistrements DNS actuels. Vous pouvez les examiner pour vous assurer que tout est correct.
4. **Changer vos serveurs de noms** : Pour utiliser le DNS de Cloudflare, vous devez mettre à jour les serveurs de noms de votre domaine auprès de votre registrar de domaine (par exemple, GoDaddy, Namecheap). Cloudflare vous fournira deux serveurs de noms (par exemple, `ns1.cloudflare.com` et

`ns2.cloudflare.com`). Connectez-vous au tableau de bord de votre registrar, trouvez les paramètres des serveurs de noms pour votre domaine et remplacez les serveurs de noms existants par ceux de Cloudflare.

5. **Attendre la propagation** : Les modifications DNS peuvent prendre jusqu'à 24 heures pour se propager, mais c'est généralement beaucoup plus rapide. Une fois terminé, votre domaine utilisera le DNS de Cloudflare.

Note importante : Assurez-vous de copier les serveurs de noms exactement comme fourni par Cloudflare. Des serveurs de noms incorrects peuvent rendre votre site indisponible.

Étape 2 : Gérer les enregistrements A sur Cloudflare

Un enregistrement A est un type d'enregistrement DNS qui mappe votre domaine (ou sous-domaine) à une adresse IPv4. Par exemple, il indique à l'Internet que `example.com` doit pointer vers `192.0.2.1`. Cloudflare rend facile l'ajout, la modification ou la suppression d'enregistrements A.

Comment gérer les enregistrements A :

1. **Connectez-vous à Cloudflare** : Allez sur votre tableau de bord Cloudflare et sélectionnez le domaine que vous souhaitez gérer.
2. **Accéder à DNS** : Cliquez sur l'onglet "DNS"dans le menu supérieur.
3. **Ajouter un enregistrement A** :
   - Cliquez sur "Ajouter un enregistrement."
   - Sélectionnez "A"dans le menu déroulant de type.
   - Entrez le nom (par exemple, `www` pour `www.example.com` ou laissez-le vide pour le domaine racine).
   - Entrez l'adresse IPv4 que vous souhaitez pointer.
   - Choisissez si vous souhaitez proxyer l'enregistrement via Cloudflare (plus à ce sujet ci-dessous).
   - Définissez le TTL (Time to Live). Pour les enregistrements proxyés, il est par défaut à 300 secondes.
   - Cliquez sur "Enregistrer."
4. **Modifier un enregistrement A** : Trouvez l'enregistrement A existant dans la liste, cliquez sur "Modifier", faites vos modifications et cliquez sur "Enregistrer."
5. **Supprimer un enregistrement A** : Cliquez sur "Modifier"à côté de l'enregistrement, puis sur "Supprimer."Confirmez la suppression.

Proxyé vs. DNS uniquement : - **Proxyé (Nuage Orange)** : Le trafic passe par Cloudflare, activant les fonctionnalités CDN, sécurité et performances. - **DNS uniquement (Nuage Gris)** : Le trafic va directement à votre serveur, contournant les protections de Cloudflare. Utilisez ceci pour les enregistrements qui n'ont pas besoin des fonctionnalités de Cloudflare (par exemple, les serveurs de messagerie).

Astuce rapide : Cloudflare prend également en charge les enregistrements AAAA pour les adresses IPv6. Le processus de gestion est le même que pour les enregistrements A.

Étape 3 : Interdire les régions IP sur Cloudflare

Cloudflare vous permet de bloquer le trafic provenant de pays ou régions spécifiques, ce qui peut aider à réduire le spam, les bots et les attaques malveillantes. Cette fonctionnalité est particulièrement utile si vous remarquez un trafic indésirable provenant de certaines zones.

Comment interdire les régions IP :

1. **Connectez-vous à Cloudflare** : Allez sur votre tableau de bord Cloudflare et sélectionnez votre domaine.
2. **Accéder à la sécurité** : Cliquez sur l'onglet "Sécurité", puis sélectionnez "WAF"(Web Application Firewall).
3. **Créer une règle** :
   - Cliquez sur "Créer une règle de pare-feu."
   - Donnez un nom à votre règle (par exemple, "Bloquer des pays spécifiques").
   - Définissez la règle pour bloquer le trafic en fonction du pays du visiteur. Par exemple :
     - Champ : "Pays"
     - Opérateur : "est dans"
     - Valeur : Sélectionnez les pays que vous souhaitez bloquer.
   - Choisissez l'action : "Bloquer."
   - Cliquez sur "Déployer."
4. **Surveiller le trafic bloqué** : Vous pouvez voir les requêtes bloquées dans l'onglet "Sécurité"sous "Événements."

Note importante : Utilisez cette fonctionnalité avec précaution. Bloquer des régions entières peut empêcher involontairement des utilisateurs légitimes d'accéder à votre site. Il est préférable de surveiller votre trafic et de ne bloquer des régions que si vous êtes sûr que c'est nécessaire.

Conseils supplémentaires et bonnes pratiques

- **Utilisez le plan gratuit de Cloudflare** : Il est parfait pour les petits sites web et inclut des fonctionnalités essentielles comme la gestion DNS, le CDN et la sécurité de base.

- **Proxyez vos enregistrements** : Pour des performances et une sécurité optimales, proxyez vos enregistrements A et AAAA via Cloudflare chaque fois que possible.
- **Configurer SSL/TLS** : Cloudflare propose des certificats SSL gratuits pour chiffrer le trafic entre vos visiteurs et votre site. Vous pouvez l'activer dans l'onglet "SSL/TLS".
- **Explorer le cache** : Le cache de Cloudflare peut considérablement accélérer votre site. Consultez l'onglet "Cache"pour le configurer.
- **Surveiller votre site** : Utilisez les analyses de Cloudflare pour garder un œil sur le trafic, les menaces et les performances.

Conclusion

Cloudflare est un outil puissant qui peut améliorer la vitesse, la sécurité et la fiabilité de votre site web. En suivant les étapes de ce guide, vous pouvez facilement configurer le DNS, gérer les enregistrements A et interdire les régions IP pour protéger votre site. Rappelez-vous : - **Configuration DNS** : Mettez à jour vos serveurs de noms correctement pour éviter les temps d'arrêt. - **Enregistrements A** : Utilisez-les pour mapper votre domaine à l'adresse IP de votre serveur et envisagez de les proxyer pour des avantages supplémentaires. - **Blocage de régions IP** : Utilisez cette fonctionnalité avec parcimonie pour éviter de bloquer des utilisateurs légitimes.

Cloudflare propose bien d'autres fonctionnalités, comme le chiffrement SSL/TLS, le cache et les outils de sécurité avancés. Une fois à l'aise avec les bases, explorez ces options pour tirer encore plus parti de la plateforme.