Los geht’s mit Cloudflare

Cloudflare ist ein beliebter Dienst, der eine Reihe von Tools bietet, um die Leistung, Sicherheit und Zuverlässigkeit Ihrer Website zu verbessern. Ob Sie einen kleinen Blog oder eine große E-Commerce-Website betreiben, die Funktionen von Cloudflare –wie DNS-Verwaltung, Content Delivery Network (CDN) und Sicherheitsschutz –können einen erheblichen Unterschied machen. In diesem Blogbeitrag führen wir Sie durch drei wichtige Aufgaben: Konfiguration von DNS, Verwaltung von A-Einträgen und Sperrung von IP-Regionen. Diese sind entscheidend, um das Beste aus Cloudflare herauszuholen, und sie sind einfacher einzurichten, als Sie vielleicht denken!

Warum Cloudflare verwenden?

Bevor wir in die Praxis eintauchen, lassen Sie uns kurz darlegen, was Cloudflare so wertvoll macht: - **DNS-Verwaltung**: Cloudflare bietet schnelle und zuverlässige DNS-Dienste, die sicherstellen, dass Ihre Website immer erreichbar ist. - **CDN**: Es beschleunigt Ihre Website, indem es Inhalte näher an Ihre Besucher zwischenspeichert. - **Sicherheit**: Cloudflare bietet DDoS-Schutz, SSL/TLS-Verschlüsselung und Tools zum Blockieren von schädlichem Datenverkehr. - **Einfachheit der Nutzung**: Noch besser: Cloudflare bietet einen kostenlosen Plan, der perfekt für kleine Websites und Blogs ist.

Nun gehen wir ins Detail.

Schritt 1: Konfiguration von DNS bei Cloudflare

DNS (Domain Name System) ist wie das Telefonbuch des Internets –es übersetzt Ihren Domainnamen (z. B. `example.com`) in eine IP-Adresse, die Server verstehen können. Wenn Sie Cloudflare verwenden, verwalten Sie Ihre DNS-Einträge über deren Plattform, die zusätzliche Geschwindigkeit und Sicherheit bietet.

So richten Sie Cloudflare DNS ein:

1. **Registrieren Sie sich bei Cloudflare**: Wenn Sie noch kein Konto haben, gehen Sie zu Cloudflare’s Website und registrieren Sie sich für ein kostenloses Konto.
2. **Fügen Sie Ihre Domain hinzu**: Nach dem Einloggen klicken Sie auf „Add a Site“und geben Sie Ihren Domainnamen (z. B. `example.com`) ein. Cloudflare scannt Ihre bestehenden DNS-Einträge.
3. **Überprüfen Sie die DNS-Einträge**: Nach dem Scan zeigt Cloudflare Ihnen eine Liste Ihrer aktuellen DNS-Einträge an. Sie können sie überprüfen, um sicherzustellen, dass alles korrekt aussieht.
4. **Aktualisieren Sie Ihre Nameserver**: Um Cloudflare’s DNS zu verwenden, müssen Sie die Nameserver Ihrer Domain bei Ihrem Domain-Registrar (z. B. GoDaddy, Namecheap) aktualisieren. Cloudflare stellt Ihnen zwei Nameserver (z. B. `ns1.cloudflare.com` und `ns2.cloudflare.com`) zur Verfügung.

Melden Sie sich in das Dashboard Ihres Registrars an, finden Sie die Nameserver-Einstellungen für Ihre Domain und ersetzen Sie die bestehenden Nameserver durch die von Cloudflare.

5. **Warten Sie auf die Ausbreitung**: DNS-Änderungen können bis zu 24 Stunden dauern, um sich auszubreiten, aber es ist in der Regel viel schneller. Sobald dies abgeschlossen ist, verwendet Ihre Domain Cloudflare's DNS.

Wichtiger Hinweis: Stellen Sie sicher, dass Sie die Nameserver genau so kopieren, wie sie von Cloudflare bereitgestellt werden. Falsche Nameserver können dazu führen, dass Ihre Website offline geht.

Schritt 2: Verwaltung von A-Einträgen bei Cloudflare

Ein A-Eintrag ist eine Art DNS-Eintrag, der Ihre Domain (oder Subdomain) auf eine IPv4-Adresse abbildet. Zum Beispiel sagt er dem Internet, dass `example.com` auf `192.0.2.1` zeigen soll. Cloudflare macht es einfach, A-Einträge hinzuzufügen, zu bearbeiten oder zu löschen.

So verwalten Sie A-Einträge:

1. **Melden Sie sich bei Cloudflare an**: Gehen Sie zu Ihrem Cloudflare-Dashboard und wählen Sie die Domain aus, die Sie verwalten möchten.
2. **Navigieren Sie zu DNS**: Klicken Sie auf die Registerkarte „DNS"in der oberen Menüleiste.
3. **Fügen Sie einen A-Eintrag hinzu**:
   - Klicken Sie auf „Add Record."
   - Wählen Sie „A"aus dem Typ-Dropdown-Menü.
   - Geben Sie den Namen ein (z. B. `www` für `www.example.com` oder lassen Sie es leer für die Stammdomain).
   - Geben Sie die IPv4-Adresse ein, auf die gezeigt werden soll.
   - Wählen Sie, ob Sie den Eintrag durch Cloudflare proxyen möchten (mehr dazu unten).
   - Setzen Sie die TTL (Time to Live). Für proxyierte Einträge beträgt der Standardwert 300 Sekunden.
   - Klicken Sie auf „Save."
4. **Bearbeiten Sie einen A-Eintrag**: Finden Sie den bestehenden A-Eintrag in der Liste, klicken Sie auf „Edit", nehmen Sie Ihre Änderungen vor und klicken Sie auf „Save."
5. **Löschen Sie einen A-Eintrag**: Klicken Sie auf „Edit"neben dem Eintrag und dann auf „Delete. "Bestätigen Sie die Löschung.

Proxied vs. DNS Only: - **Proxied (Orange Cloud)**: Der Datenverkehr geht durch Cloudflare, wodurch CDN-, Sicherheits- und Leistungsfunktionen aktiviert werden. - **DNS Only (Gray Cloud)**: Der Datenverkehr geht direkt zu Ihrem Server und umgeht Cloudflare's Schutzmaßnahmen. Verwenden Sie dies für Einträge, die Cloudflare's Funktionen nicht benötigen (z. B. Mailserver).

Schneller Tipp: Cloudflare unterstützt auch AAAA-Einträge für IPv6-Adressen. Der Prozess zur Verwaltung ist derselbe wie für A-Einträge.

Schritt 3: Sperrung von IP-Regionen bei Cloudflare

Cloudflare ermöglicht es Ihnen, Datenverkehr aus bestimmten Ländern oder Regionen zu blockieren, was helfen kann, Spam, Bots und schädliche Angriffe zu reduzieren. Diese Funktion ist besonders nützlich, wenn Sie unerwünschten Datenverkehr aus bestimmten Gebieten bemerken.

So sperren Sie IP-Regionen:

1. **Melden Sie sich bei Cloudflare an**: Gehen Sie zu Ihrem Cloudflare-Dashboard und wählen Sie Ihre Domain aus.
2. **Navigieren Sie zu Sicherheit**: Klicken Sie auf die Registerkarte „Security“, dann wählen Sie „WAF “(Web Application Firewall).
3. **Erstellen Sie eine Regel**:
   - Klicken Sie auf „Create Firewall Rule.“
   - Geben Sie Ihrer Regel einen Namen (z. B. „Block Specific Countries“).
   - Legen Sie die Regel fest, um Datenverkehr basierend auf dem Land des Besuchers zu blockieren. Zum Beispiel:
     - Feld: „Country“
     - Operator: „is in“
     - Wert: Wählen Sie die Länder aus, die Sie blockieren möchten.
   - Wählen Sie die Aktion: „Block.“
   - Klicken Sie auf „Deploy.“
4. **Überwachen Sie den blockierten Datenverkehr**: Sie können blockierte Anfragen in der Registerkarte „Security“unter „Events“anzeigen.

Wichtiger Hinweis: Verwenden Sie diese Funktion vorsichtig. Das Blockieren ganzer Regionen kann versehentlich legitime Benutzer daran hindern, auf Ihre Website zuzugreifen. Es ist am besten, Ihren Datenverkehr zu überwachen und Regionen nur zu blockieren, wenn Sie sicher sind, dass es notwendig ist.

Zusätzliche Tipps und Best Practices

- **Verwenden Sie Cloudflare’s kostenlosen Plan**: Er ist perfekt für kleine Websites und enthält wesentliche Funktionen wie DNS-Verwaltung, CDN und grundlegende Sicherheit.

- **Proxyen Sie Ihre Einträge**: Für optimale Leistung und Sicherheit proxyen Sie Ihre A- und AAAA-Einträge durch Cloudflare, wann immer möglich.
- **Richten Sie SSL/TLS ein**: Cloudflare bietet kostenlose SSL-Zertifikate zur Verschlüsselung des Datenverkehrs zwischen Ihren Besuchern und Ihrer Website. Sie können dies in der Registerkarte „SSL/TLS “aktivieren.
- **Erkunden Sie das Caching**: Cloudflare’s Caching kann Ihre Website erheblich beschleunigen. Schauen Sie sich die Registerkarte „Caching“an, um es zu konfigurieren.
- **Überwachen Sie Ihre Website**: Verwenden Sie Cloudflare’s Analytics, um den Datenverkehr, Bedrohungen und die Leistung im Auge zu behalten.

Fazit

Cloudflare ist ein leistungsstarkes Tool, das die Geschwindigkeit, Sicherheit und Zuverlässigkeit Ihrer Website verbessern kann. Durch die Schritte in dieser Anleitung können Sie DNS konfigurieren, A-Einträge verwalten und IP-Regionen sperren, um Ihre Website zu schützen. Denken Sie daran: - **DNS-Konfiguration**: Aktualisieren Sie Ihre Nameserver korrekt, um Ausfallzeiten zu vermeiden. - **A-Einträge**: Verwenden Sie sie, um Ihre Domain auf die IP-Adresse Ihres Servers abzubilden, und überlegen Sie, ob Sie sie proxyen, um zusätzliche Vorteile zu erhalten. - **IP-Regionen-Blockierung**: Verwenden Sie diese Funktion sparsam, um legitime Benutzer nicht zu blockieren.

Cloudflare bietet viele weitere Funktionen wie SSL/TLS-Verschlüsselung, Caching und erweiterte Sicherheitswerkzeuge. Sobald Sie sich mit den Grundlagen auskennen, erkunden Sie diese Optionen, um noch mehr aus der Plattform herauszuholen.