CLOUDFLARE | PARTNER NETWORK

ACE
CLOUDFLARE | PARTNER NETWORK
Accredited Configuration Engineer

Implementing Cloudflare

Implementing Cloudflare's Integrated Global Cloud Platform

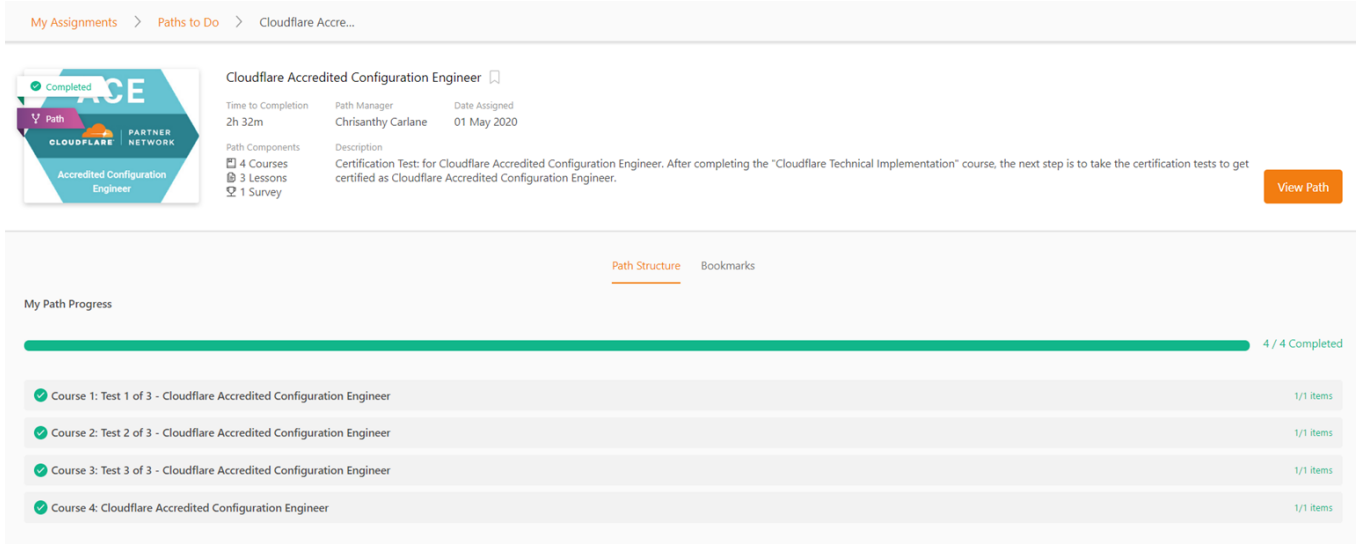
Agenda

Implementing Cloudflare
Technical Architecture Review
Implementation Overview
Onboarding Steps Workshop
Configuration: User Administration
Implementation Detail: DNS,SSL
Useful Tooling for Cloudflare
Product Extensions Onboarding Overview

Instructor

Chrisanthy Carlane
Partner Technical Enablement

ACE Exam Overview



CLOUDFLARE

Cloudflare ACE Training Webinar

Lab Handbook Online: https://ace-training.cf/

Prerequisite

You need a Partner Demo Account to follow today's lab.
Open your browser and login at
https://dash.cloudflare.com/

Make sure you got 1 Enterprise domain quota.
If you don't have one, please request before proceeding.

Time: < 1 min

Cloudflare ACE Training Webinar

Lab Handbook Online: https://ace-training.cf/

Prerequisite

We will use one external service: Freenom.
It is to have a free domain we will onboard on Cloudflare.
Please get your account and one domain at Freenom:
(Not needed if you already have your domain for testing)

https://www.freenom.com/

Time: 5 ~ 20 min (depending on Freenom's performance)

Cloudflare ACE Training Webinar

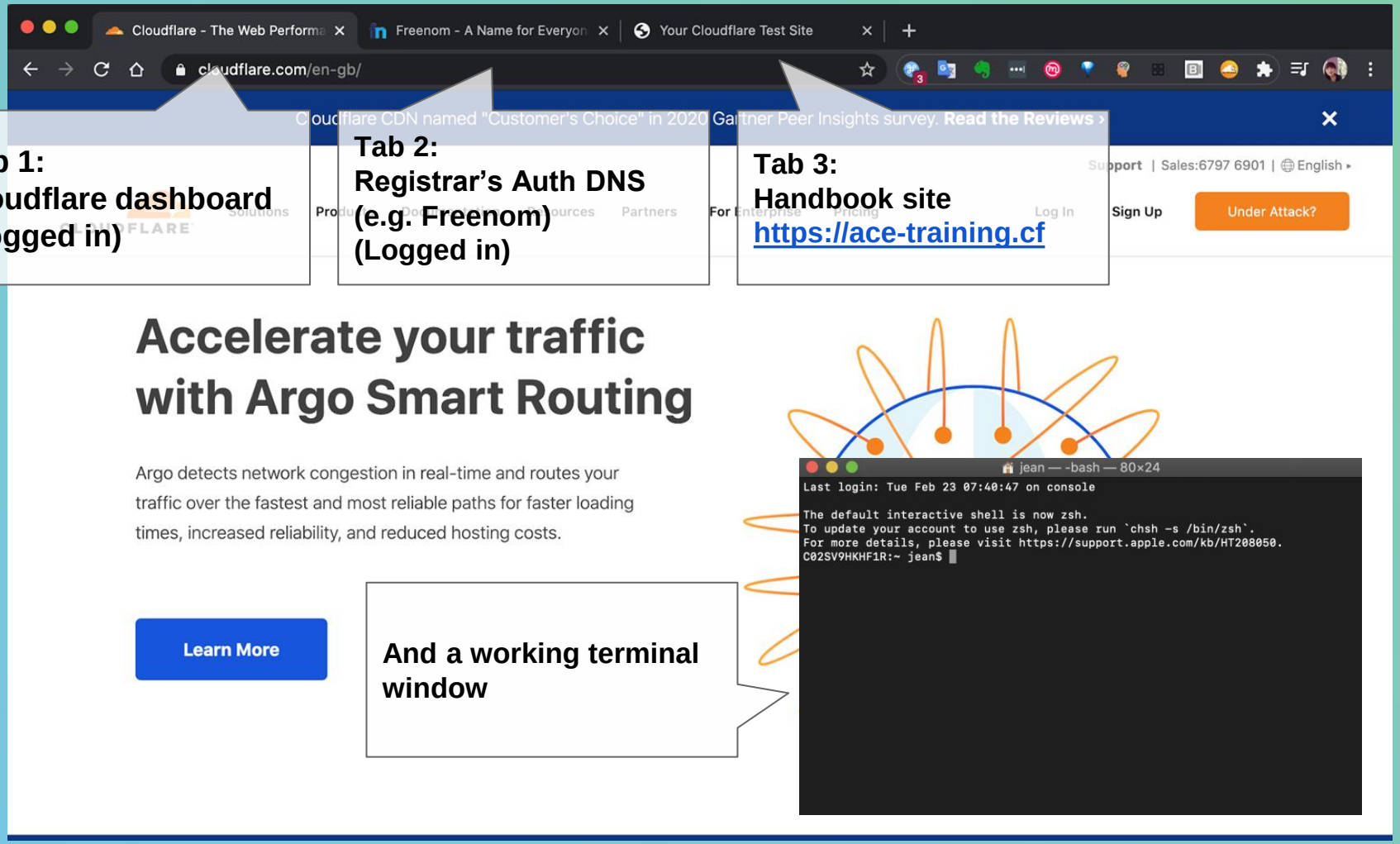
Lab Handbook Online: https://ace-training.cf/

Prerequisite

Please make sure you have terminal-friendly environment (MacOS, Linux) so we can play together with some basic terminal commands such as dig, curl etc.

Time: 5 ~ 15 mins

Prerequisite is also illustrated at the handbook: https://ace-training.cf

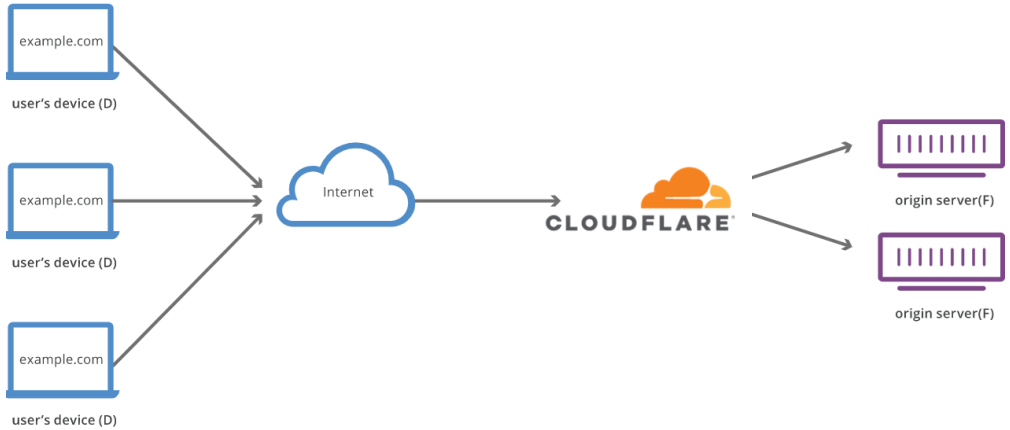

Cloudflare - The Web Performa
Freenom - A Name for Everyon
Your Cloudflare Test Site
cloudflare.com/en-gb/
Cloudflare CDN named "Customer's Choice" in 2020 Gartner Peer Insights survey. Read the Reviews ›
Sales:6797 6901
English
Solutions
Partners
For Enterprise
Pricing
Log In
Sign Up
Under Attack?
Accelerate your traffic with Argo Smart Routing
Argo detects network congestion in real-time and routes your traffic over the fastest and most reliable paths for faster loading times, increased reliability, and reduced hosting costs.
Learn More
jean — -bash — 80×24
Last login: Tue Feb 23 07:40:47 on console
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
C02SV9HKHF1R:~ jean$
Tab 1: Cloudflare dashboard (Logged in)
Tab 2: Registrar's Auth DNS (e.g. Freenom) (Logged in)
Tab 3: Handbook site https://ace-training.cf
And a working terminal window

Cloudflare is an integrated global cloud network that provides performance, security, reliability and platform solutions.

// Technical Architecture Review

What You Should Already Know

- Cloudflare is an integrated, global cloud platform made up of over 200 datacenters.
- Our platform provides security, reliability, performance and platform solutions
- Cloudflare acts as a reverse proxy using Anycast DNS to route customer traffic



Cloudflare offers a complete security and performance suite

SECURITY

- Firewall
- IoT Security
- Bot Management
- SSL/TLS
- DDoS Protection
- Secure Origin Connection
- Zero Trust Security
- Rate Limiting

PERFORMANCE

- Cache
- Mobile Optimization
- Intelligent Routing
- Image Optimization
- Content Optimization
- Mobile SDK

RELIABILITY

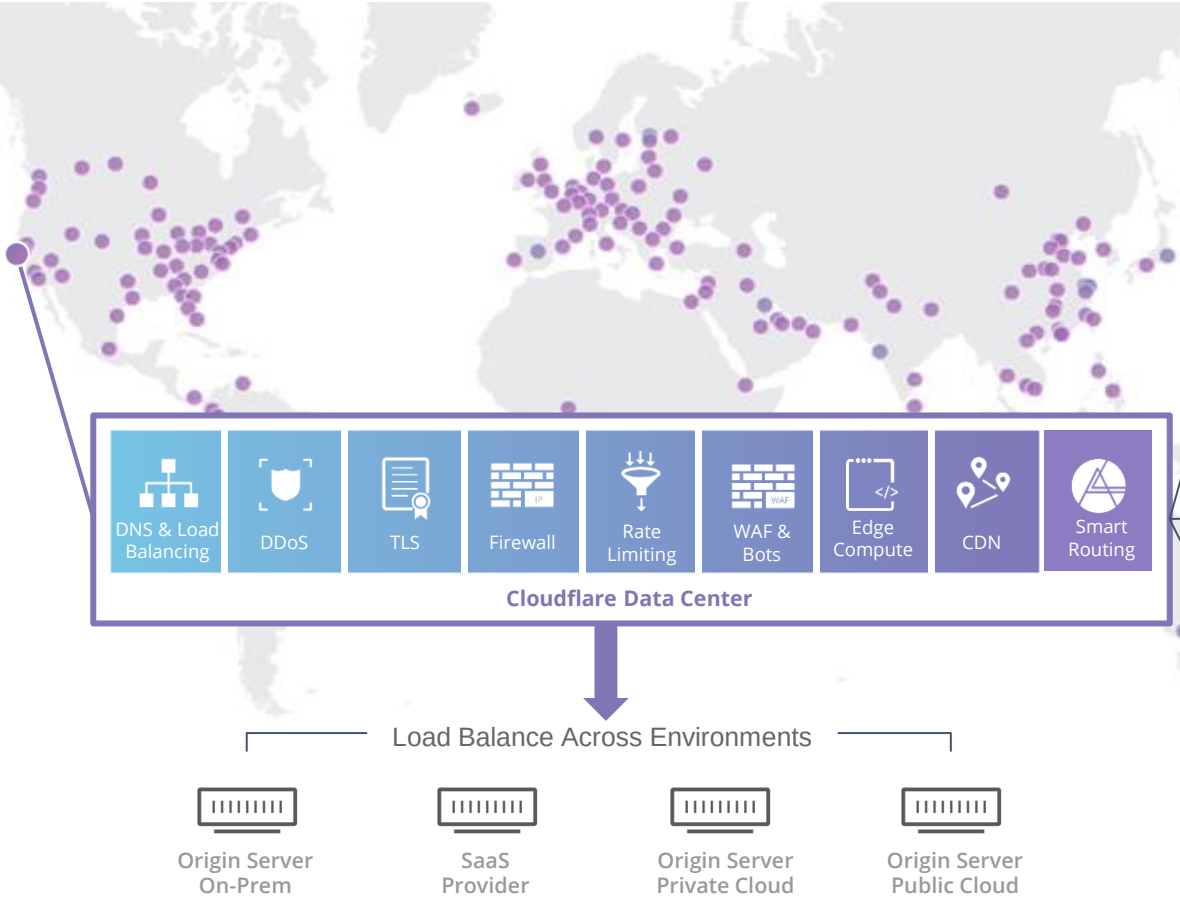
- Load Balancing
- Domain Name System (DNS)
- Anycast Network
- DNS Resolver
- Virtual Backbone
- Always Online

PLATFORM

- Serverless Compute
- Cloudflare Apps
- Analytics

CLOUDFLARE

In an integrated, scalable architecture across 200+ datacenters



Scalable global network with a modern, unified architecture across all datacenters

Integrated stack of security, performance and reliability services

Rapid onboarding, easy configurations

Cloudflare services can be activated via a **simple DNS change.** Customer applications can be protected in just a few minutes.

// Implementation Overview

Implementation Steps

Scoping	Setup	Configuration	Staging	Deployment
Review applications and customer needs	Create accounts, users, and basic settings	Configure accounts and individual applications	Functional Testing	Production changes
DNS Decisions • *Authoritative* • *Subdomain Only / partial cname setup*	*Create Account*	*Configure DNS records*	*DNS Response*	*Final DNS Changes* • *Nameserver or CNAME*
SSL Options	*Add Applications*	*Add TLS Certificates*	*Client IP Restoration & Header Confirmation*	
Plan Selection	*Add License*	*Configuration Best Practices* • *Admin* • *Security* • *Performance*	*Configuration review and tuning*	
Add-On Requirements		*Configure Add Ons (if required)*	*Rollback Planning*	

Scoping: DNS Decision

Customers need to decide their preferred method of connecting to Cloudflare.

Full, Authoritative (How-To Full)

Cloudflare's robust, global and fast Anycast DNS network becomes your authoritative DNS provider.

This is our most common, preferred option.

Pros:

- Cloudflare protects the apex domain.
- Leverages Cloudflare's network for DNS which is very fast, highly available, and resilient to DNS based attacks.
- One-click enablement of DNSSEC authentication.

Cons:

- Changing the authoritative provider is not always possible for organizations.

Partial, Subdomain-only(How-To CNAME)

You keep your primary DNS provider and link individual subdomains to Cloudflare via CNAME or NS record.

Pros:

- Requires limited change and allows only a single subdomain to be sent through Cloudflare.

Cons:

- We cannot protect your apex domain
- An attacker may overwhelm your authoritative DNS provider which will cause all DNS functions to fail including the CNAME to Cloudflare.

Scoping: SSL Options

Customers need to decide how their traffic will be encrypted.

Upload custom SSL certificates

You can upload a custom SSL certificate to Cloudflare

- Fastest and most common
- Cloudflare presents your existing certificate to your users
- Keys are never stored on-disc, only decrypted on demand
- Using your own certificate can allow you to go live immediately (You can always migrate later).

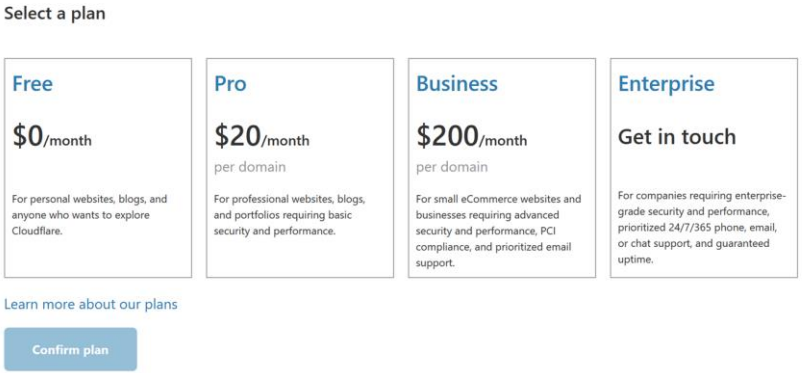
Cloudflare issued SSL certificates

Cloudflare can provide a SSL as a managed service with either completely free, Universal certificates or paid, Dedicated certificates from our our CA partners.

- Automatic validation and renews
- Cloudflare managed keys, CSRs, and renewals automatically with no involvement necessary from an end-customer
- Ownership of your domain must be verified by our CA Partner via the Domain Control Validation process (DCV). How to verify manually.

Scoping: Plan Selection

Choose the proper plan for the domain via dashboard or provisioning API. Reseller partners will have the necessary licenses.



Example - Create Zone Subscription

```
curl -X POST https://api.cloudflare.com/client/v4/zones/<zone id>/subscription -H 'Content-Type:
application/json' -H 'x-auth-email: <x-auth-email>' -H 'x-auth-key: <x-auth-key>' -d
'{"rate_plan": {"id": "<rate plan identifier>"}}'
```

Scoping: Add-On Requirements

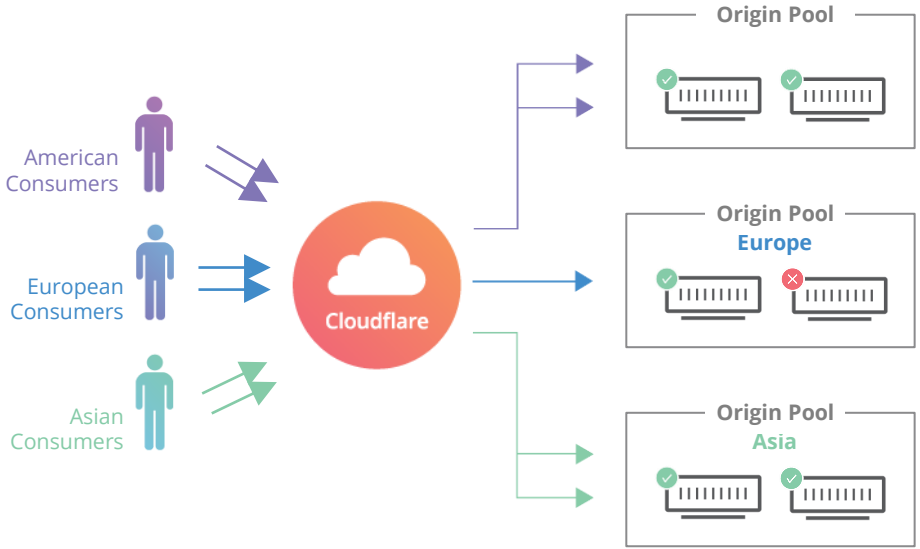
TCP/UDP Protocols Spectrum extends the power of Cloudflare to protect custom TCP and UDP ports and protocols (if required). Applications are configured within the Spectrum application.

- MQTT, Email (SMTP), Passive FTP, Gaming

Load Balancing / Global Traffic Management

Cloudflare load balancing provide global and local load balancing with health checks,global geo-routing, session affinity, and weighted load balancing across on-prem or cloud-based origins.

Multiple origins and load balancer paths are configured in the Traffic application.

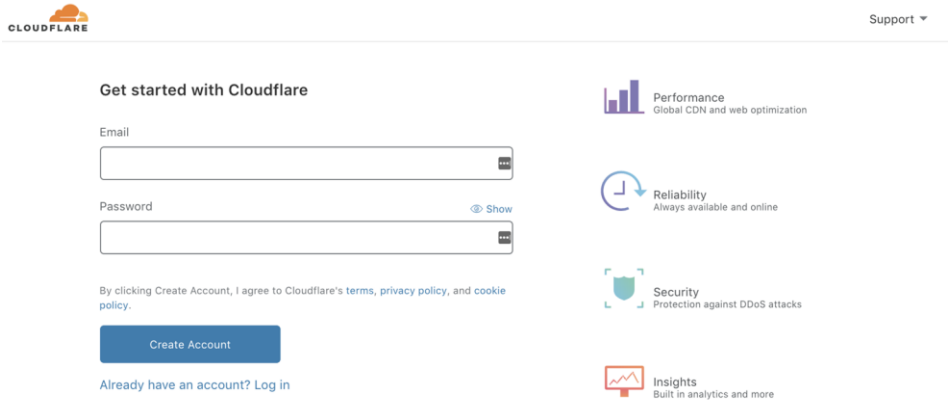


ACE - Lab - Onboarding-A

1. Go to freenom.com and create your account.
2. Get a free domain at “services - Register new domain”.
3. **Go to Cloudflare web dashboard www.cloudflare.com**
4. **Access “Partners Partner Demo Account”.**
5. **Click “Add a site” and register your new domain.**
6. **Select Enterprise Plan.**
7. **Finish the guide.**

Setup: Account creation

- To create a Cloudflare account and user you will need an email address and password.
- Once an account is created, additional users can be invited and granted individual roles.
- User accounts can be provisioned programmatically at scale via client API : https://api.cloudflare.com/

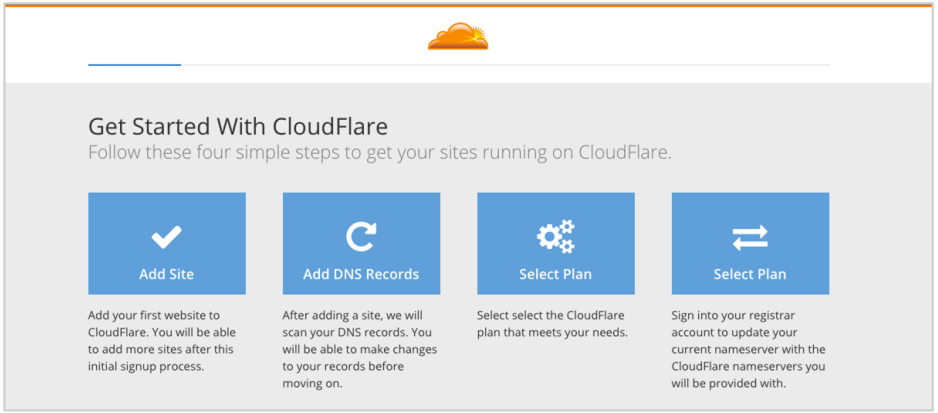


- Role-Based Access for Users
- 2FA Support
- SSO Support

Setup: Add your first application

Websites and applications can be added via the dashboard and programmatically via the API or Terraform.

These can be staged and tested before any production traffic is sent to Cloudflare.



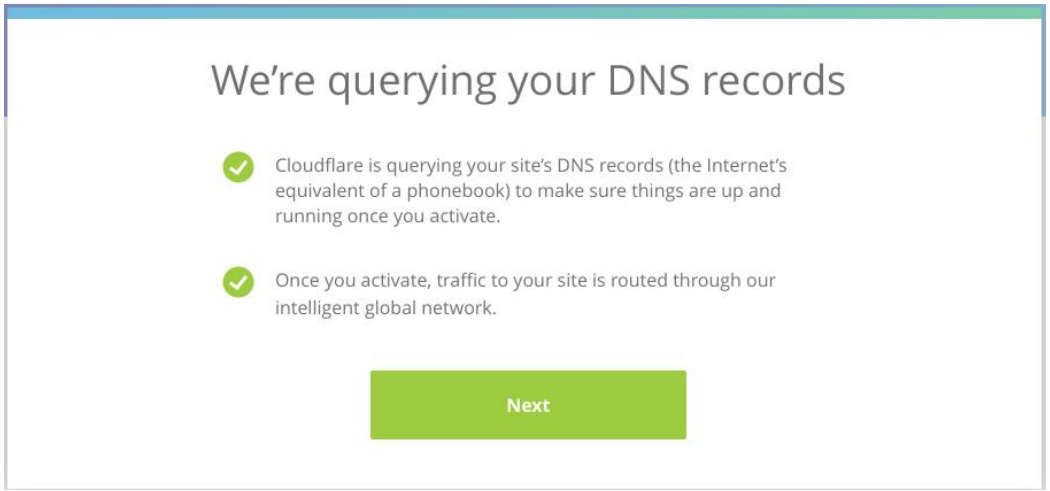

```
curl -X POST "https://api.cloudflare.com/client/v4/zones" \
     -H "X-Auth-Email: user@example.com" \
     -H "X-Auth-Key: c2547eb745079dac9320b638f5e225cf483cc5cfdda41" \
     -H "Content-Type: application/json" \
     --data '{"name":"example.com","account":{"id":"01a7362d577a6c3019a474fd6f485823"
```

Setup: Configuring DNS (Full setup)

To prevent any downtime, there should be complete parity between DNS systems before changing over to Cloudflare's authoritative DNS.

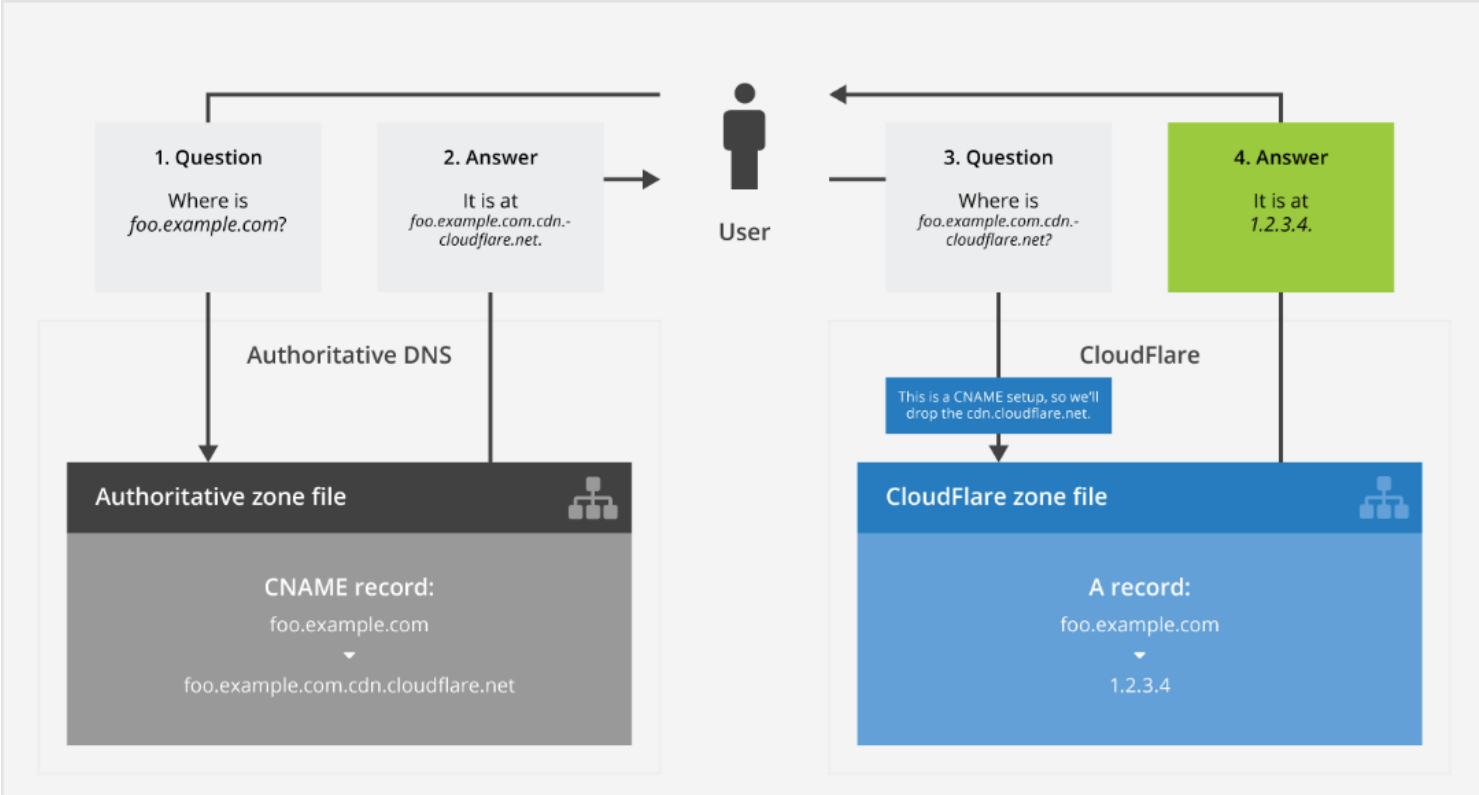
There are a few ways to ensure parity:

1. Cloudflare will scan for common records.
1. Users can add and edit records via dashboard and API.
1. Users can upload a zone file.



Customers requiring TCP/UDP support will need add those applications and ports via the Spectrum tab.

Setup: Configuring DNS (Partial/cname)



ACE - Lab - Onboarding-B

1. **Go to Cloudflare dashboard - Overview.**
2. **Find “Advanced Options -- Convert to CNAME DNS Setup” at the bottom of the screen.**
3. **Read the warning and click “Convert”**
4. **Find TXT record for the zone validation, then go to Freenom dashboard.**
5. At Freenom, access “My domains - Manage Domain - Manage Freenom DNS” and add TXT record you were given.
6. **Check the TXT record propagation at https://dnschecker.org. and confirm Cloudflare account validation.**

Setup: Configuring SSL (Upload)

Your customer should have decided how they want to encrypt their edge traffic.

Business & Enterprise accounts can upload their own SSL cert via dashboard or API.

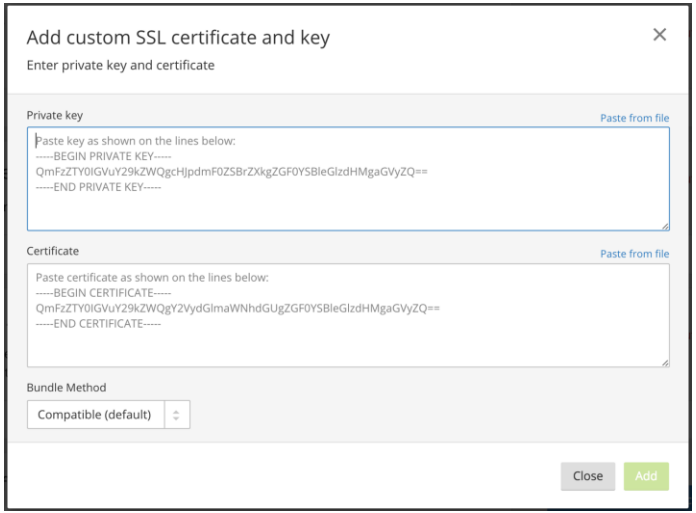
Most customers prefer Cloudflare's free and paid SSL options for a cost effective, fully managed SSL solution, eliminating the burden of generating private keys, creating certificate signing requests (CSR), renewing certificates, and other maintenance tasks.

1. Universal SSL

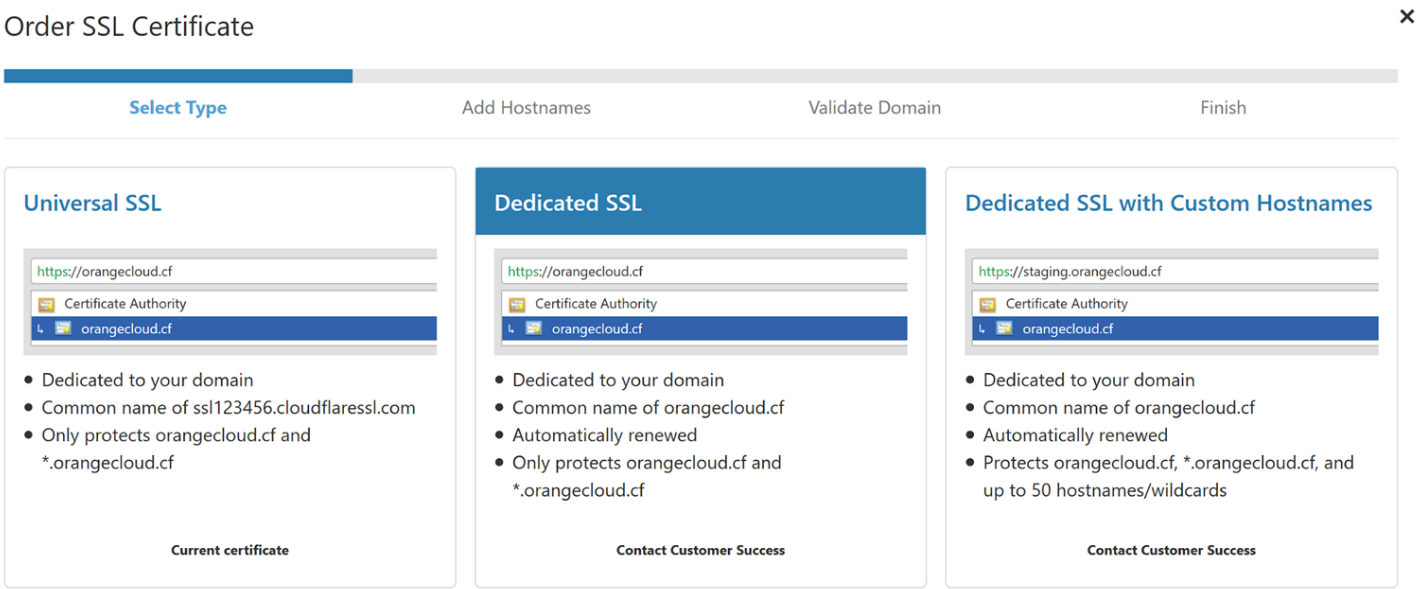
   Free, automatic wildcard certificates

1. Dedicated SSL

   Paid, dedicated certificates at $5 or $10



Setup: Configuring SSL (Cloudflare-issued)



ACE - Lab - Onboarding-C

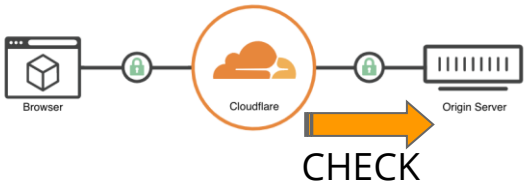
1. Go to Cloudflare dashboard.
2. Access Traffic - Health Checks.
3. Configure health checks.
   Today's origin: 35.234.81.115
   (You can 'bring your own origin' if you want.)

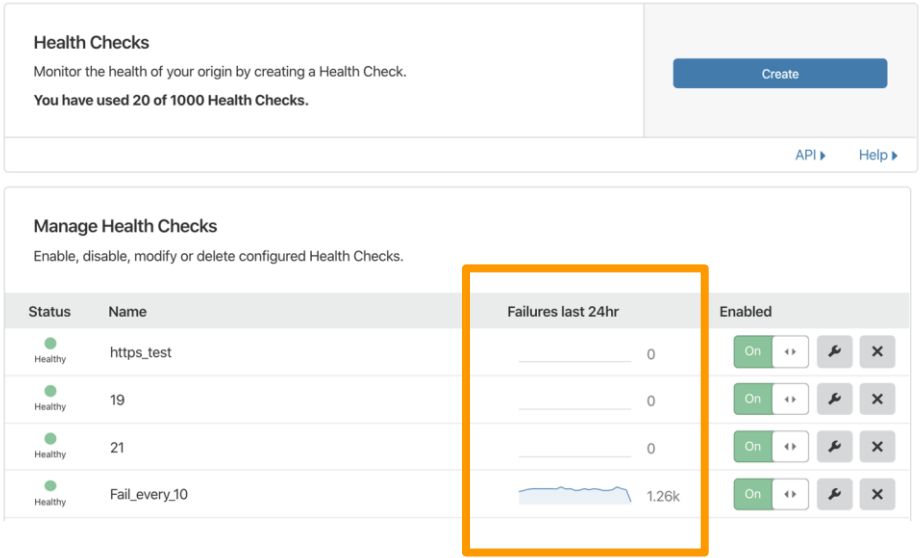
Set up origin health checks

Set up a criteria of health checks and get alerted when origin server is unreacheable from Cloudflare edge.

(under Traffic - Health Checks)

[Standalone Health Checks]



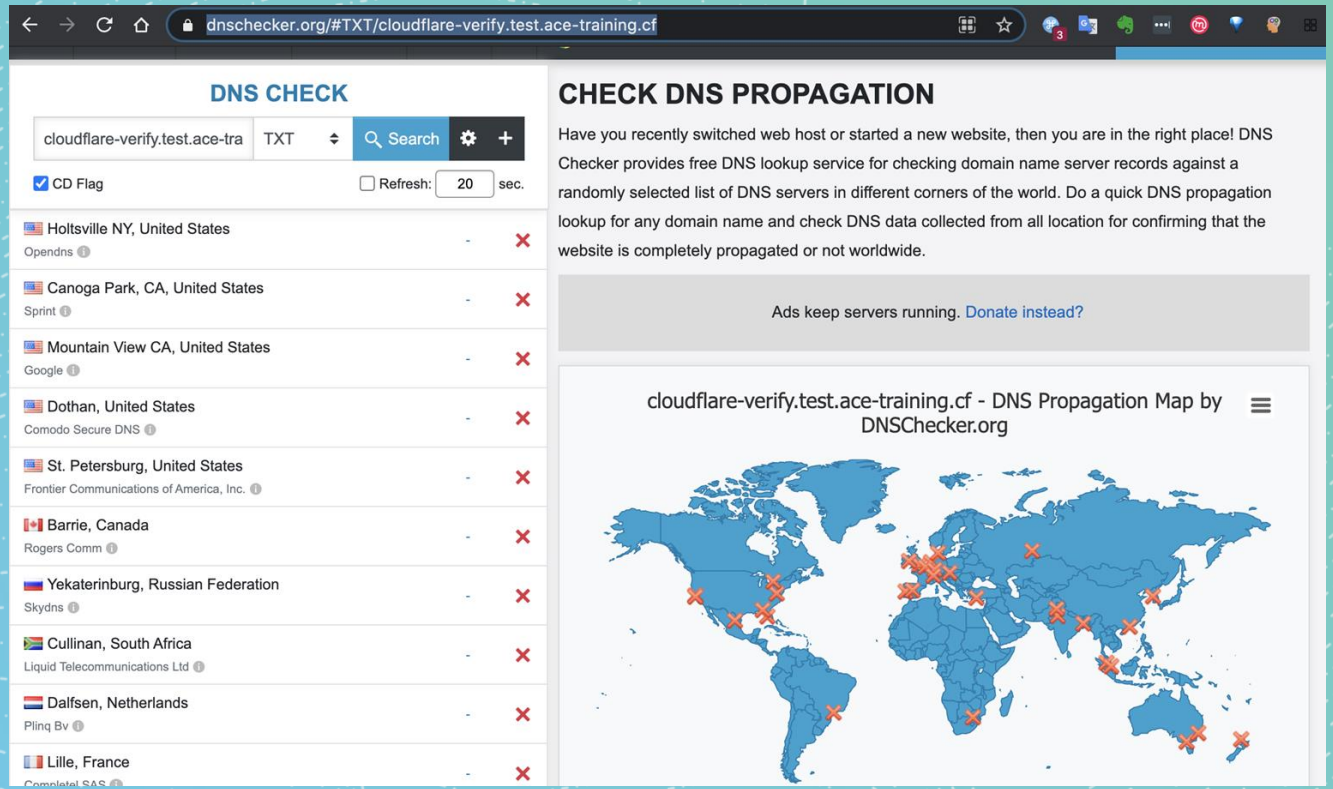


CLOUDFLARE

Not provisioning?
Not showing active?

You sure you put the correct TXT record?
https://dnschecker.org

If correct,
give CF some time.



ACE
CLOUDFLARE PARTNER NETWORK
Accredited Configuration Engineer

ACE - Lab - Onboarding-D

1. Go to Cloudflare dashboard - DNS.
2. configure: ‘staging’ and enter 35.234.81.115 with A record type.
3. Go to Freenom DNS.
4. enter ‘staging’ and enter staging.<yourdomain.cf>.cdn.cloudflare.net CNAME record type.
   staging.<yourdomain.cf> --[CNAME]--> staging.<yourdomain.cf>.cdn.cloudflare.net
5. Check the CNAME record propagation at https://dnschecker.org.

Staging: DNS Response

Local testing

HTTP(s) and Websocket traffic can be pushed through Cloudflare from your local machine by altering your host file with a valid Cloudflare IP. (How to alter your host file).

Development domain testing

A stand-alone development domain is recommended to allow testing before moving production traffic through Cloudflare.

Subdomain Testing

A development subdomain works as well. It is also possible to CNAME a subdomain to your production traffic if your server is configured to properly handle a different host header.

Orange-cloud — Active proxy

Record resolves to Cloudflare IP address for HTTP(s) and Websocket traffic.

Grey-cloud — Inactive Proxy

Record resolves to the configured IP address. Non-HTTP(s) traffic should be grey-clouded

What records are appropriate to orange-cloud? - Knowledge Base

ACE - Lab - Onboarding-F

1. Use your terminal or POSTMAN to send below two requests, and compare the difference in HTTP response headers.
   a. curl –svo /dev/null/ http://35.234.81.115/
   b. curl –svo /dev/null/ http://staging.<yourdomain.cf>
2. Are you able to connect to HTTPS to both sites? Think of a reason about why you can or can't.

Staging - Header Confirmation example

```
curl -svo /dev/null http://whiskytango.us/img/sg50/IMG_0191.jpg
*   Trying 104.16.41.188...
* Connected to whiskytango.us (127.0.0.1) port 80 (#0)
> GET /img/sg50/IMG_0191.jpg HTTP/1.1
> Host: whiskytango.us
> User-Agent: curl/7.43.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 21 Jun 2016 17:53:47 GMT
< Content-Type: image/jpeg
< Content-Length: 222670
< Connection: keep-alive
< Set-Cookie: __cfduid=d64e283e5e56319b47401dd2cf2327e5c1466531627; expires=Wed, 21-Jun-17 17:53:47 GMT; path=/; domain=.whiskytango.us; HttpOnly
< Last-Modified: Tue, 18 Aug 2015 09:05:34 GMT
< ETag: "55d2f55e-365ce"
< CF-Cache-Status: HIT
< Expires: Tue, 21 Jun 2016 21:53:47 GMT
< Cache-Control: public, max-age=14400
< Accept-Ranges: bytes
< Server: cloudflare-nginx
< CF-RAY: 2b69526f25e34408-SFO-DOG
<
{ [839 bytes data]
* Connection #0 to host whiskytango.us left intact
```

Server HTTP Response

Cache Status

CloudFlare RayID

Prepare your origin network

Preparing your network

- Configure firewalls to prevent access to your servers, load balancers, and other infrastructure from non-Cloudflare IP addresses
    - This means allowlisting Cloudflare IPs in your Access Control List to prevent rate-limiting or false positives from any intrusion detection systems.
- Prevents attackers from recording/recognizing the “fingerprints” of your hardware when probing your IPs

Set up Cloudflare Standalone Health Checks

- At Cloudflare dashboard, set up Cloudflare standalone health checks to verify the origin server responds to Cloudflare data center’s HTTP(S)/TCP requests.
- You can find it at Traffic/Health Checks. Select the relevant region as per the business requirement.
- Proceed to the next step only after the health checks are marked as Healthy .

Prepare your origin network

Review HTTP headers and cookies added by Cloudflare

- Cloudflare passes all HTTP headers as-is from the client to the origin and adds additional headers as specified here. Review the headers and make sure the origin server will work as expected.
- Cloudflare uses HTTP cookies to maximize network resources, manage traffic, and protect our Customers' sites from malicious traffic and the details are described here. Review the cookies and make sure the origin server will work as expected.
- Whenever in doubt, run a local/staging test at the step 7 and verify there's no problem.

Restoring original user IP addresses (optional)

- HTTP requests will be coming from Cloudflare, instead of the actual users. Cloudflare adds "CF-Connecting-IP" and standard "X-Forwarded-For" headers to all request
- Nginx, Apache, and IIS configs to switch the logged IP are available.
- You can find out how to easily restore the originating IP address here!

Staging - Rollback Planning

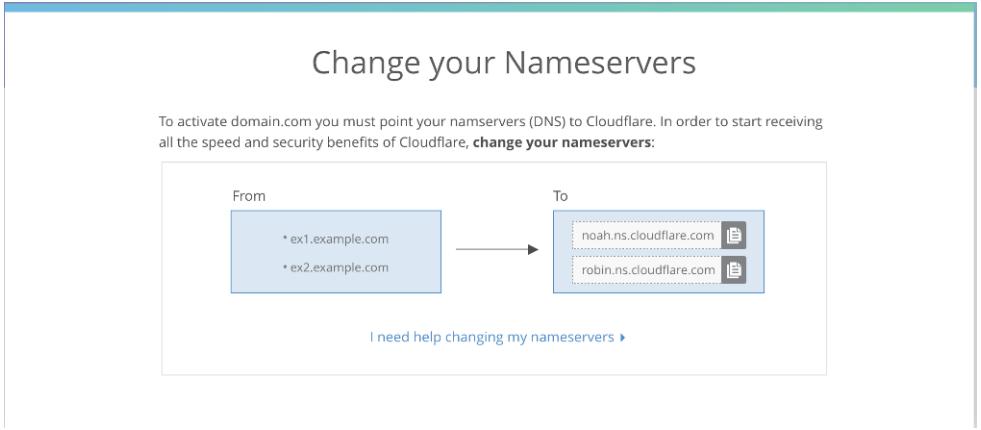
Although everyone expects things to go smoothly. Below are some options in case you need to roll back customer traffic quickly and safely.

Option	What it will do	Activation Time
Disable Specific Features	If specific capabilities are causing issues with your application, they can be disabled on a selective basis. For example, Caching can be disabled on a per-path basis.,	5-30 seconds
Grey Cloud DNS Records	Grey-clouding a DNS record will remove all proxying from that particular record. We will only provide DNS service for the record. This will solve for proxy-related issues such as non-HTTP protocols, SSL conflicts, or redirect loops.	5-30 seconds
Pause the Domain	Pausing the domain will remove all proxying from the Cloudflare service. We will act simply as a DNS provider. This will solve for any proxy-related issues such as SSL conflicts or redirect loops.	5-30 seconds
Rollback Nameservers	Although most drastic, this solution will return the application to its default state. It will not be using Cloudflare DNS or Cloudflare's proxy service. This is useful to solve DNS and proxy issues. Recommendation: For cautious customers, DNS TTLs can be set very low to ensure a rollback happens quickly.	5 minutes - hours (depends on DNS TTLs)

Cutover: Changing nameservers

At this point:

1. The account and application are on Cloudflare's system.
2. All DNS records match your current configuration and are properly orange-clouded.
3. Any SSL certificates are uploaded.
4. Traffic has been functionally tested.
5. Rollback plans are in place.
6. You can now safely change your the authoritative nameservers at the client's registrar. (Or change CNAME records for a CNAME setup)



Changing Nameservers Knowledge Base

DNS Propagation Tools
https://www.whatsmydns.net/
https://dnschecker.org/

ACE - Lab - Onboarding-E

1. Activate Cloudflare for production "www" host.

ACE - Summary so far

- Major steps in Cloudflare onboarding
  - Scoping - What products you need?
  - Setup - Create CF account, add your domain.
  - Configuration - DNS, SSL etc.
  - Staging - Compatibility test vs origin (*important!)
  - Deployment - Push prod traffic.

ACE - Summary so far

- Major customer decisions in onboarding
  - DNS
    - Prod traffic? Full setup.
    - POC/Trial? CNAME setup.
  - SSL
    - Easier life? Cloudflare provisioned cert.
    - Specific requirements? Custom cert (BYOCert).
  - Plan (Enterprise)
  - Do you need Spectrum?
    - Non-web (TCP/UDP based) service to onboard?
    - Web app with non-standard ports?
  - Do you need Load Balancing?

ACE - Summary so far

- Key concerns in onboarding?
  - Changing DNS
    - Any Downtime?
  - SSL Transition
    - Auto-renew with customer's own branding?
  - Application Downtime
    - Why we need origin compatibility test?
  - Staging/Testing Traffic
    - Always recommend non-production (staging) for POC
    - Recommend to keep staging host for ongoing test

Agenda

	Implementing Cloudflare
	Technical Architecture Review
	Implementation Overview
	Onboarding Steps Workshop
You Are Here →	Configuration: User Administration
	Implementation Detail: DNS,SSL
	Useful Tooling for Cloudflare
	Product Extensions Onboarding Overview

// Configuration: Administration

Implementation Steps - Configuration

Scoping	Setup	Configuration	Staging	Deployment
Review applications and customer needs	Create accounts, users, and basic settings	Configure accounts and individual applications	Functional Testing	Production changes
DNS Decisions • *Authoritative* • *Subdomain Only*	*Create Account*	*Configure DNS records*	*DNS Response*	*Final DNS Changes* • *Nameserver or CNAME*
SSL Options	*Add Applications*	*Add TLS Certificates*	*Client IP Restoration & Header Confirmation*	
Plan Selection	*Add License*	***Configuration Best Practices*** • *Admin* • *Security* • *Performance*	*Configuration review and tuning*	
Add-On Requirements		*Configure Add Ons (if required)*	*Rollback Planning*	

Easily Administer Accounts, Users & Domains

Multi-Tenant

Support multiple accounts and provide a group of users role-based permissions to better control the administration of your domains. Each user has their own role and limited API key. Learn More

- Super Administrator
- Analytics Admin
- DNS Admin
- Crypto (SSL/TLS), Caching, Performance, Page Rules, and Customization
- Firewall Admin
- Raw Log Access
- Cache Purge

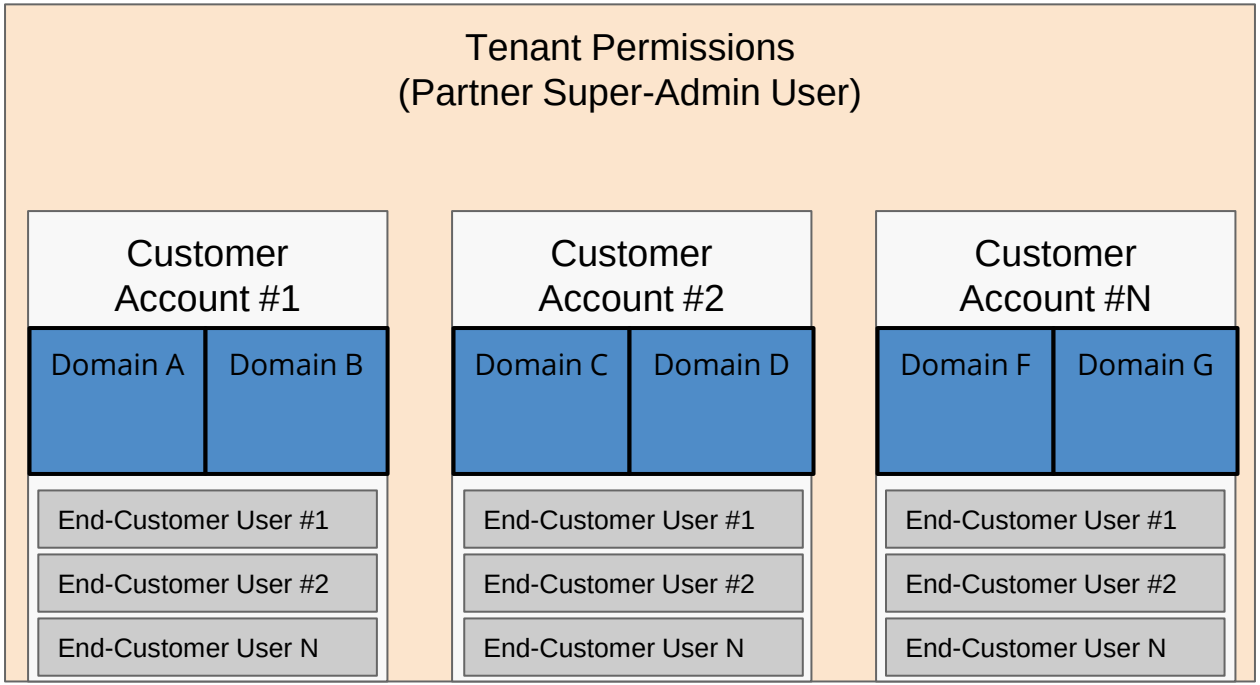
SSO Support

Cloudflare supports SSO providers (SAML providers)

Enforce 2FA

Ensure your entire dashboard is secure by enforcing 2-factor authentication for your organization.

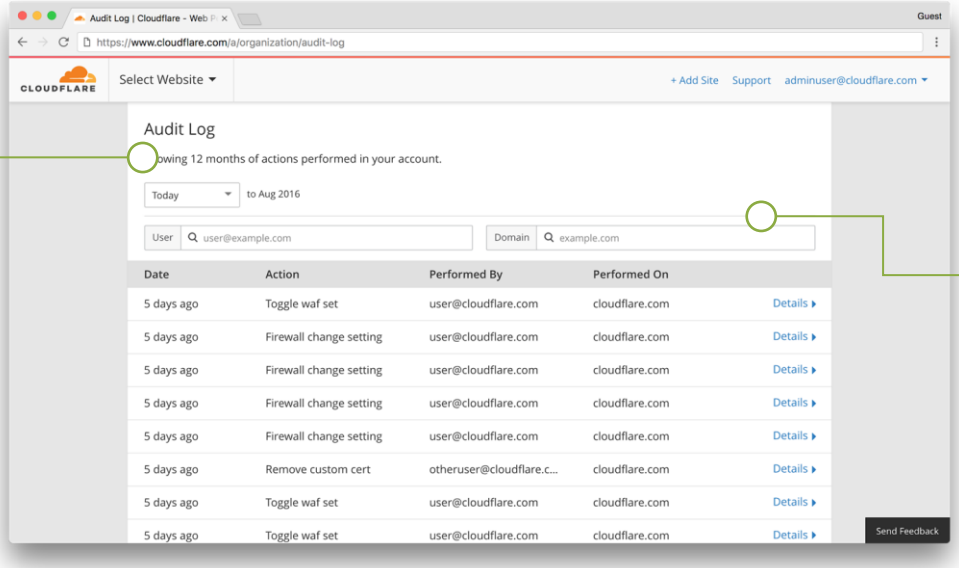
Access to all resources to manage customers



Note: A fully-managed Cloudflare experience may not end up inviting end-customers to accounts.

Quickly And Easily Review Changes Made To Your Account And Domains

Quick Log Review
Easily review audit logs and drill down to detailed information from the dashboard.



Customizable Filters
Whether for compliance reviews or change monitoring, easily pare down logs by the desired field including: date, user and domain.

API Log Export
Export logs via API for further filtering, inspection and monitoring using any log analysis tool

Simple Configuration Change Review
Make compliance reviews and monitoring configuration changes easy with Audit Logs

CLOUDFLARE

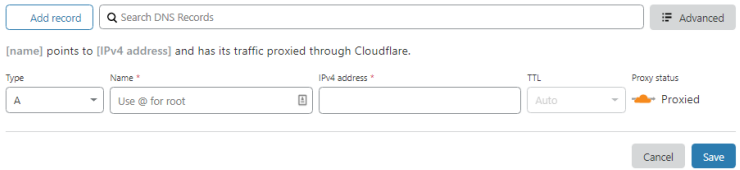
Cloudflare runs one of the largest managed DNS services answering requests for over **38% of all managed DNS traffic** in the world.

// Implementation Detail: DNS + SSL

Manage your DNS records with ease.

DNS Records

Configure your domain name system by adding, deleting, and editing your records as necessary. Records without an orange or grey-cloud cannot be proxied. Upload or export zone files in BIND format.

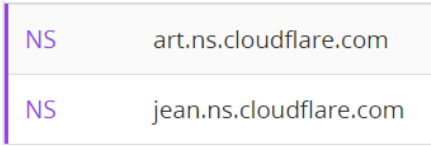


DNSSEC

Ensures that your website's traffic is safely directed to the correct servers, so that a connection to a website is not intercepted by a man-in-the-middle.

Nameserver Options

- Default Cloudflare Nameservers
- Custom Nameservers (ns1.example.com)
- Shared Custom Nameservers



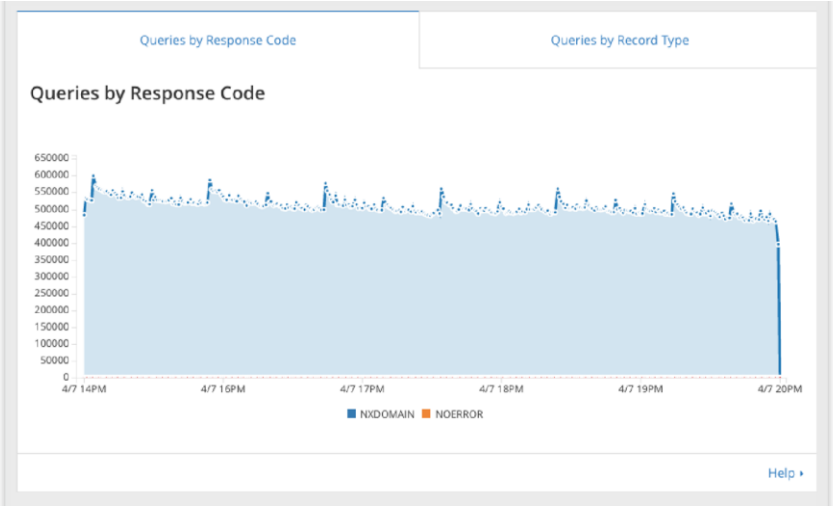
Secondary DNS, Analytics & More

Secondary DNS

Cloudflare Secondary DNS service complements our authoritative DNS with the ability to automatically pull DNS records via zone transfers. This allows customers to work with multiple DNS vendors.

DNS Analytics

Gain valuable insight into DNS traffic. Understand and visualize data through metrics such as query count, response time, response codes, data centers, and more.



Related Products

- DNS Flood Mitigation
- Cloudflare Reliability
- DNSSEC
- Registrar
- DNS Firewall

CLOUDFLARE | PARTNER NETWORK

ACE - Exercise - DNS

Let's verify… "why Cloudflare DNS"

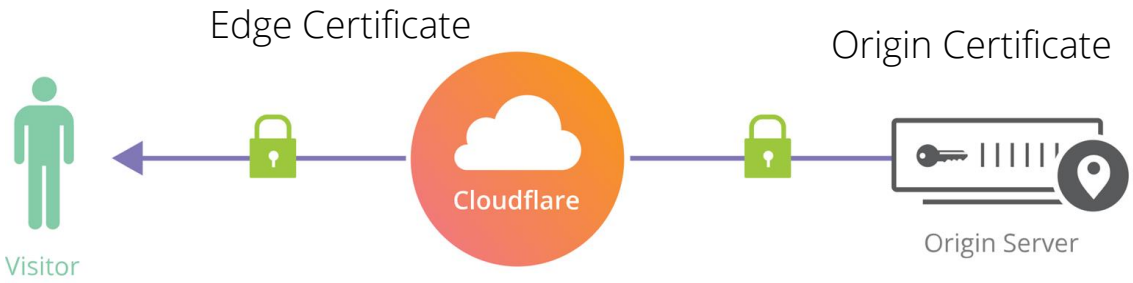
1. Go to https://www.solvedns.com/dnsspeedtest/
2. Test any non-cloudflare domain
   (e.g. freenom.com)
3. Test any domain using Cloudflare DNS (Full setup)
   (e.g. cloudflare.com)

This can show a rough result of as-is and to-be when your prospective customer moves to Cloudflare's DNS.

Encrypting as much web traffic as possible to **prevent data theft** and other tampering is a critical step toward building a safer, better Internet.

// Cloudflare One-Click SSL

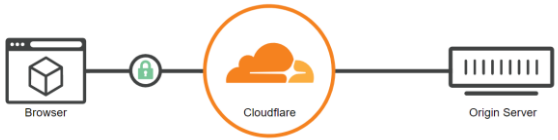
As a reverse proxy, there are now two connections to encrypt



TLS Settings

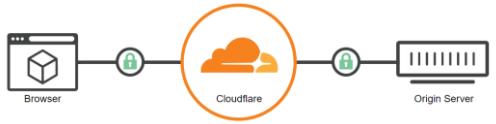
Flexible

- Edge to origin not encrypted
- Self-signed certificates are not supported



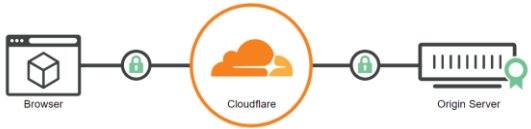
Full

Edge to origin certificates can be self-signed



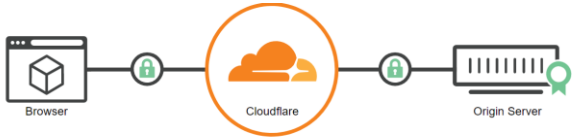
Full (strict)

- RECOMMENDED
- Encrypts end-to-end
- Requires a trusted CA or Cloudflare Origin CA certificate

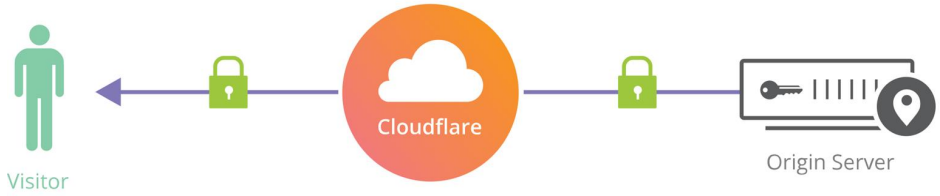


Strict (SSL-only Origin Pull)

- Same as Full (strict)
- Request to the origin must always be encrypted (Enterprise only)



Many options to encrypt traffic end-to-end



Cloudflare Provisioned	**Universal SSL Pack** Keep HTTPS easy with free and automatic wildcard certificates. • SHA2 ECDSA; SHA2 RSA Cloudflare will lazy-load the right certificate for each browser! **Advanced Cert Manager, Dedicated SSL** Secure multiple levels of subdomains with your own certificates.	**Origin CA** A Cloudflare-issued certificate can be provided to encrypt traffic from our edge to your origin. • Cloudflare-managed Key and CSR (ECDSA, RSA) • Upload your own CSR
Custom Certificates	**Upload Custom Certificates** Business and Enterprise customers can serve their own certificates from Cloudflare's edge. They can even select which data center regions the private key is stored and served from with Geo Key. Or, customers can keep their private key with our Keyless SSL offering.	**Keep the origin certificate** Serve your certificate for traffic from our edge to your origin.

Advanced Certificate Manager

Create an Advanced Certificate

Certificate Authority

DigiCert

Certificate Hostnames

You may enter up to 50 hostnames or wildcards (48 remaining):

jeann.net | *.jeann.net ×

Validation method

TXT Validation (recommended)

Certificate Validity Period

- (•) 1 year
  auto renewal 30 days before expiration
- ( ) 3 months
  auto renewal 30 days before expiration
- ( ) 1 month
  auto renewal 7 days before expiration
- ( ) 2 weeks
  auto renewal 3 days before expiration

Custom Certificates (Customer Uploaded)

- Customer uses their own certificates.
- Usually used with **Extended Validation Certificate**
- Customer must manage renewal of certificate on expiry (email reminder)
- All Enterprise licenses receive one Custom SSL upload slot
- Can entitle more slots for additional cost.
- Customer uploads certificate and private key.
- Highest priority certificate.

https://support.cloudflare.com/hc/en-us/articles/200170466-How-do-I-upload-a-custom-SSL-certificate-Business-or-Enterprise-only-

Upload Custom Certificates

POST Create SSL Configuration permission needed: #ssl:edit

FREE ✖ PRO ✖ BUSINESS ✔ ENTERPRISE ✔

Upload a new SSL certificate for a zone

```
POST zones/:zone_identifier/custom_certificates
```

Required **parameters**

Name /type	Description /example	Constraints
certificate *string*	The zone's SSL certificate or certificate and the intermediate(s) `"-----BEGIN CERTIFICATE-----\nMIIDtTCCAp2gAwIBA`	
private_key *string*	The zone's private key `"-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCA`	

Enter private key and certificate

SSL Certificate — Paste from file

Paste certificate as shown on the lines below:
-----BEGIN CERTIFICATE-----
QmFzZTY0IGVuY29kZWQgY2VydGlmaWNhdGUgZGF0YSBleGlzdHMgaGVyZQ==
-----END CERTIFICATE-----

Bundle Method

Compatible (recommended)

Private key — Paste from file

Paste key as shown on the lines below:
-----BEGIN PRIVATE KEY-----
QmFzZTY0IGVuY29kZWQgcHJpdmF0ZSBrZXkgZGF0YSBleGlzdHMgaGVyZQ==
-----END PRIVATE KEY-----

Private Key Restriction Beta

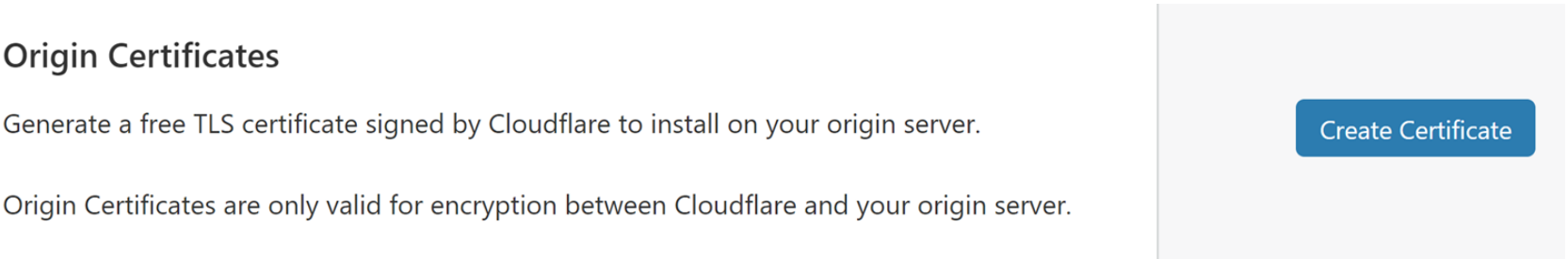
Specify the region below where your private key can be held locally for optimal TLS performance. HTTPS connections to any excluded data center will still be fully encrypted, but will incur some latency while Keyless SSL is used to complete the handshake with the nearest allowed data center.

Distribute to all Cloudflare data centers (optimal performance)

Origin CA Details

- Allows customers to use FULL (Strict) validation of origin **without buying their own certificate**.
- Cloudflare Certificate Authority issues CSR and signs certificate.
  Customer can optionally use their own CSR.
- Not trusted by any client other than CF edge servers.
- Long expiry times.
- Intermediate and Root certificate chain available on support KB where needed.

  https://support.cloudflare.com/hc/en-us/articles/218689638-What-are-the-root-certificate-authorities-CAs-used-with-Cloudflare-Origin-CA-



ACE - Exercise - SSL

Once you onboarded, HTTPS is already available for your site.

1. Check the current available SSL certificate information
2. Automatically redirect http:// requests to https://
3. Order an **Advanced Certificate** with your preferred custom hostnames, validity period, certificate authority.
4. Upload your own certificate in the dashboard.

This lab show how easy SSL is with Cloudflare

Implementation Best Practices & Reference

1. **Always prepare Customer Onboarding Checklist before onboarding a customer**
2. **Review Cloudflare Implementation Documentation**
3. **Review 2020 Cloudflare Enterprise Best Practices**

Cloudflare's IP reputation database identifies and blocks new and evolving threats across all **25+ million applications** on the network.

// Useful Tools

Common Tools

Tool	How its used	Example
dig	Dig is command line tool similar to nslookup that is used to run DNS queries and check DNS records for a given domain/website.	dig cloudflare.com +short
cURL	cURL is a command line tool used to transport data using the URL syntax.	`curl -svo /dev/null http://www.cloudflare.com/`
MTR/ Traceroute	Network based command line tools used to measure performance/latency on a particular path to a given host/destination.	mtr -rwc 30 IPADDRESS/HOSTNAME traceroute IPADDRESS/HOSTNAME
HAR Files	A HAR file is a recording of HTTP requests ran from a web browser. Here is an example of a recording being done from within Chrome's dev tools:	Generating a HAR file

3rd party tools: Chrome Browser + Postman

Tool	How its used	Example
Claire	Claire adds an unobtrusive icon to your browser that turns orange when you are browsing a website that uses Cloudflare.	Chrome Webstore
Dr.Flare	Get insights of your Cloudflare website. Provides an easy way to see benefits with Cloudflare.	Chrome Webstore
Postman Tools	Postman is an API client that makes API calls easier to make by giving the user a full Graphical User Interface. With Collections you can upload all of the formatting for all of our API calls so that it's plug and play.	Cloudflare Postman Collection

ACE - Exercise - Useful Tools

Try the following:

1. dig yourdomain.cf
2. curl -svo /dev/null/ https://yourdomain.cf
3. curl -svo /dev/null/ http://www.yourdomain.cf/ --connect-to ::35.234.81.115
4. mtr www.yourdomain.cf
5. mtr 35.234.81.115

Example DIG Outputs

```
dig londinium.xyz

; <<>> DiG 9.8.3-P1 <<>> londinium.xyz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48929
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;londinium.xyz.                 IN      A
```

DNS Records

```
;; ANSWER SECTION:
londinium.xyz.          4       IN      A       104.16.19.212
londinium.xyz.          4       IN      A       104.16.17.212
londinium.xyz.          4       IN      A       104.16.18.212
londinium.xyz.          4       IN      A       104.16.16.212
londinium.xyz.          4       IN      A       104.16.15.212

;; Query time: 613 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Mar 20 17:56:25 2017
;; MSG SIZE  rcvd: 111
```

DNS Resolver

```
dig +trace londinium.xyz

; <<>> DiG 9.8.3-P1 <<>> +trace londinium.xyz
;; global options: +cmd
.                       169743  IN      NS      a.root-servers.net.
.                       169743  IN      NS      b.root-servers.net.
.                       169743  IN      NS      c.root-servers.net.
.                       169743  IN      NS      d.root-servers.net.
.                       169743  IN      NS      e.root-servers.net.
.                       169743  IN      NS      f.root-servers.net.
.                       169743  IN      NS      g.root-servers.net.
.                       169743  IN      NS      h.root-servers.net.
.                       169743  IN      NS      i.root-servers.net.
.                       169743  IN      NS      j.root-servers.net.
.                       169743  IN      NS      k.root-servers.net.
.                       169743  IN      NS      l.root-servers.net.
.                       169743  IN      NS      m.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 117 ms
```

Root DNS

```
xyz.                    172800  IN      NS      x.nic.xyz.
xyz.                    172800  IN      NS      y.nic.xyz.
xyz.                    172800  IN      NS      z.nic.xyz.
xyz.                    172800  IN      NS      generationxyz.nic.xyz.
;; Received 287 bytes from 193.0.14.129#53(193.0.14.129) in 30 ms
```

TLD Nameservers

```
londinium.xyz.          3600    IN      NS      dawn.ns.cloudflare.com.
londinium.xyz.          3600    IN      NS      matt.ns.cloudflare.com.
;; Received 86 bytes from 185.24.64.42#53(185.24.64.42) in 11 ms
```

Cloudflare Nameservers

```
londinium.xyz.          5       IN      A       104.16.18.212
londinium.xyz.          5       IN      A       104.16.16.212
londinium.xyz.          5       IN      A       104.16.19.212
londinium.xyz.          5       IN      A       104.16.17.212
londinium.xyz.          5       IN      A       104.16.15.212
;; Received 111 bytes from 2400:cb00:2049:1::adf5:3b83#53(2400:cb00:2049:1::adf5:3b83) in 6 ms
```

DNS Records

CLOUDFLARE

Using cURL

Here are some example **cURL** commands used to check server responses:

```
curl -svo /dev/null http://www.example.com/

curl -svo /dev/null --user-agent "USERAGENTSTRING" http://www.example.com/

curl -svo /dev/null --header "Host: www.example.com" http://ORIGINIP/

curl -svo /dev/null --header http://www.example.com --resolve www.example.com:80:ORIGINIP
```

More detailed instructions here Using cURL with Cloudflare

CLOUDFLARE

Sample CURL commands

To simulate how Cloudflare proxying works before change NS

- `curl http://domain.com --resolve domain.com:<port>:<Cloudflare IP>`
- `curl -svo /dev/null https://domain.com --resolve domain.com:443:104.18.159.80`
- `curl -svo /dev/null https://domain.com/assets/03c8cc1c.png --resolve https://domain.com/assets/03c8cc1c.png:104.16.50.144`

CLOUDFLARE

Sample Curl Response

```
curl -svo /dev/null http://whiskytango.us/img/sg50/IMG_0191.jpg
*   Trying 104.16.41.188...
* Connected to whiskytango.us (127.0.0.1) port 80 (#0)
> GET /img/sg50/IMG_0191.jpg HTTP/1.1
> Host: whiskytango.us
> User-Agent: curl/7.43.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 21 Jun 2016 17:53:47 GMT
< Content-Type: image/jpeg
< Content-Length: 222670
< Connection: keep-alive
< Set-Cookie: __cfduid=d64e283e5e56319b47401dd2cf2327e5c1466531627; expires=Wed, 21-Jun-17 17:53:47 GMT; path=/; domain=.whiskytango.us; HttpOnly
< Last-Modified: Tue, 18 Aug 2015 09:05:34 GMT
< ETag: "55d2f55e-365ce"
< CF-Cache-Status: HIT
< Expires: Tue, 21 Jun 2016 21:53:47 GMT
< Cache-Control: public, max-age=14400
< Accept-Ranges: bytes
< Server: cloudflare-nginx
< CF-RAY: 2b69526f25e34408-SFO-DOG
<
{ [839 bytes data]
* Connection #0 to host whiskytango.us left intact
```

Server HTTP Response

Cache Status

CloudFlare RayID

Using MTR/Traceroute

MTR/Traceroutes are network based command line tools used to measure performance/latency on a particular path to a given host/destination.

Here are examples of both commands:

```
mtr -rwc 30 IPADDRESS/HOSTNAME
```

```
traceroute IPADDRESS/HOSTNAME
```

CLOUDFLARE

Example MTR Output

```
mtr -rwc 30 8.8.8.8
Start: Wed Jun 22 02:39:52 2016
HOST: beaker.local                    Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- unknown.maxonline.com.sg        6.7%    30   23.4  37.3   8.8 425.7  78.6
  2.|-- unknown.maxonline.com.sg       13.3%    30   16.1  28.5   9.7 165.8  39.0
  3.|-- 172.21.13.65                    3.3%    30   90.1  42.9   9.8 477.4  86.5
  4.|-- 172.20.7.174                    3.3%    30   28.4  31.6  10.2 169.9  37.6
  5.|-- 203.117.37.205                 10.0%    30   11.3  34.4  11.3 128.6  29.6
  6.|-- 203.117.36.41                  10.0%    30   23.6  25.9  10.2  60.5  14.2
  7.|-- 203.117.34.34                  10.0%    30   18.1  36.2  13.0 185.6  41.7
  8.|-- 72.14.196.189                  13.3%    30   13.6  23.6  10.9 111.8  19.6
  9.|-- 209.85.254.177                  3.3%    30   14.9  27.5  11.4 106.3  22.8
 10.|-- 72.14.234.109                   6.7%    30   13.0  38.8  13.0 160.6  39.9
 11.|-- google-dns-a.google.com         3.3%    30   31.2  36.4  10.6 208.5  47.2
```

CLOUDFLARE

Cloudflare is an integrated global cloud network that providers performance, security, reliability and platform solutions.

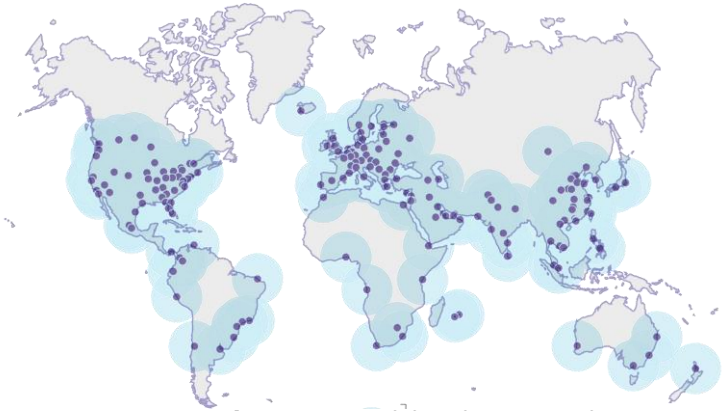
// Add-On Implementation Overview

Non-DNS Product Extensions

Cloudflare Magic Transit - BGP-based protection for Layer 3 & 4

Cloudflare For Teams - Web Gateway

Our **battle-tested network** stack, in front of **your data center**



59+ Tbps DDoS mitigation capacity

DDoS protection
59+ Tbps network capacity
Near-instant TTM

Network firewall
Granular Allow/Deny rules
for IP ranges

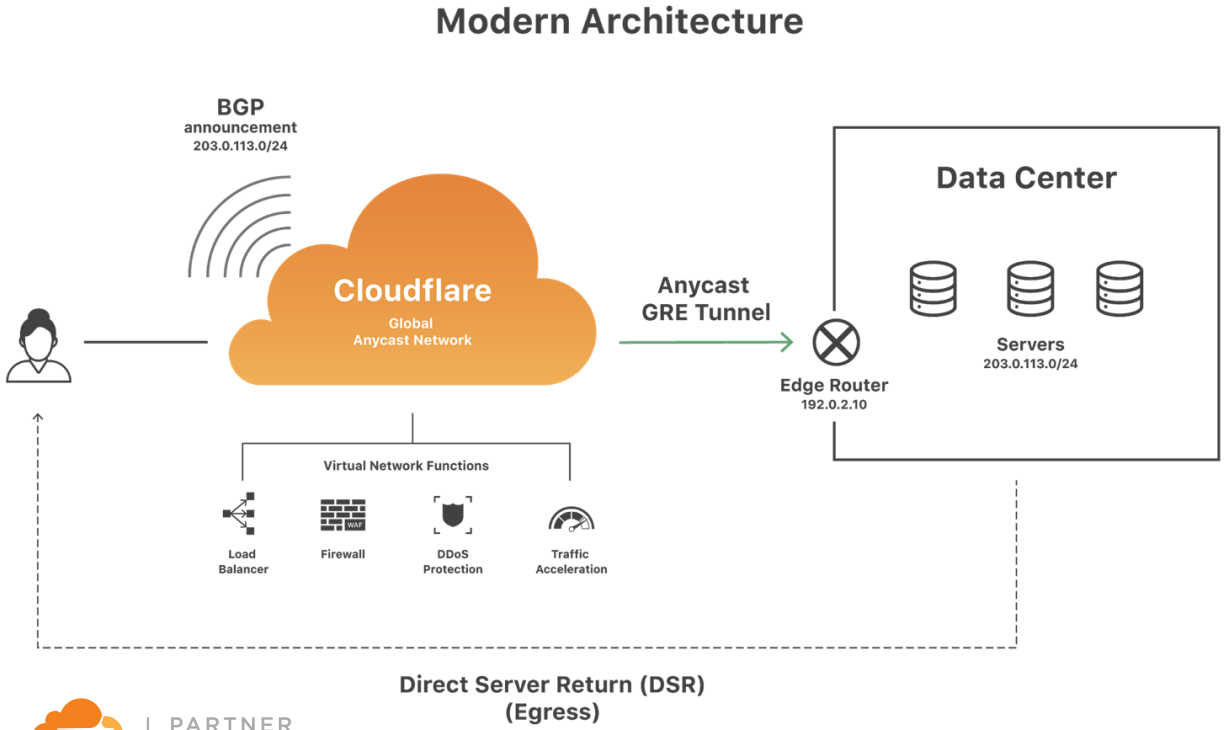
LAYER 3 - IP
(MAGIC TRANSIT)

CLOUDFLARE DATA CENTER

CUSTOMER DATA
CENTER

CLOUDFLARE | PARTNER NETWORK

How it works



Connect:
Using BGP route announcements customer network traffic is ingested by Cloudflare

Protect and Process:
All traffic inspected for attacks automatically and immediately

Accelerate:
Clean traffic is routed back to the customer network over Cloudflare. Anycast GRE tunnels deliver traffic to the customer network

Cloudflare for Teams

Access

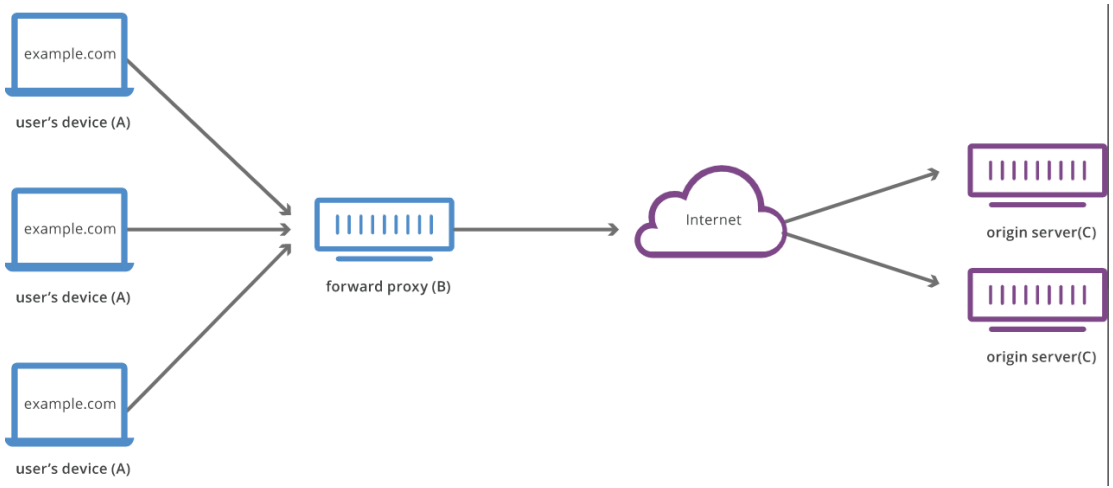
Zero Trust security for any internal apps built on top of Cloudflare's global network.

Gateway

A secure web gateway that's faster and less cumbersome to manage and use.

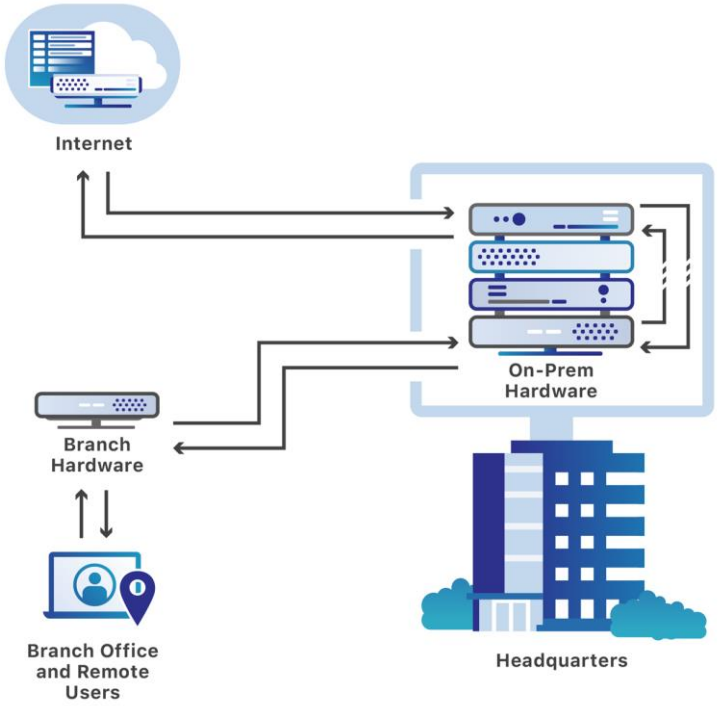
Cloudflare Gateway

- Gateway is a **full forward-proxy** to secure devices, users and networks from security threats like malware, phishing, ransomware etc.

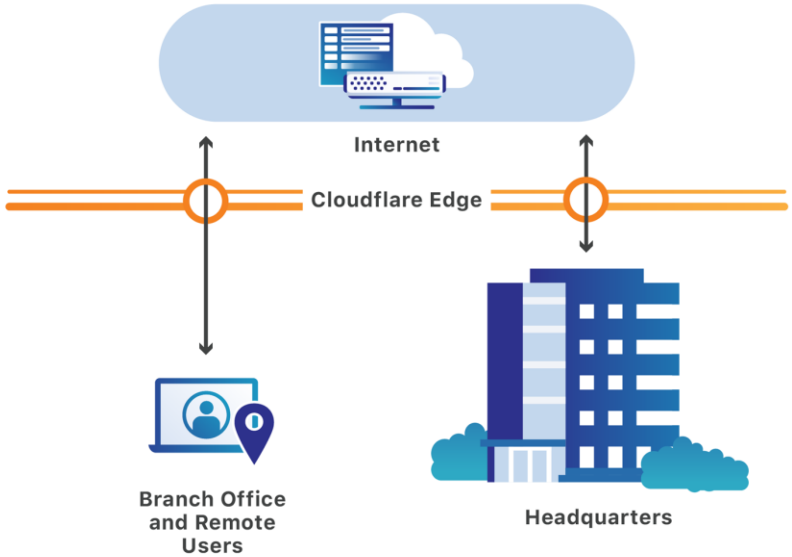


Cloudflare for Teams

Legacy Problem



Cloudflare Solution



Technical Resources

1. Cloudflare Implementation Documentation
2. 2020 Cloudflare Enterprise Best Practices
3. Cloudflare University (partners-only)
4. Partners Asset Library
5. Product documentations - https://developers.cloudflare.com/
6. Knowledgebase - https://support.cloudflare.com/hc/en-us
7. Learning Center (public) - https://www.cloudflare.com/learning/


THANK YOU
See you at
“Optimizing Cloudflare” !