CLOUDFLARE | PARTNER NETWORK

ASA

CLOUDFLARE | PARTNER NETWORK

Accredited Services Architect

Managed Security

Introduction and Deployment of Cloudflare's core Security Solutions

Agenda

Accredited Services Architect - Security
Cloudflare Security Solutions
DNS + DNSSEC
DDOS Mitigation Methods
Firewall Actions
Firewall Services Layer : IP Access Rules, IP Lists, Zone Lockdown, User Agent Block, Browser Integrity Check, Security Level

Instructor

Chrisanthy Carlane
Partner Tech Enablement
ccarlane@cloudflare.com

Declan Carlin
Partner Solution Engineer
EMEA
declan@cloudflare.com

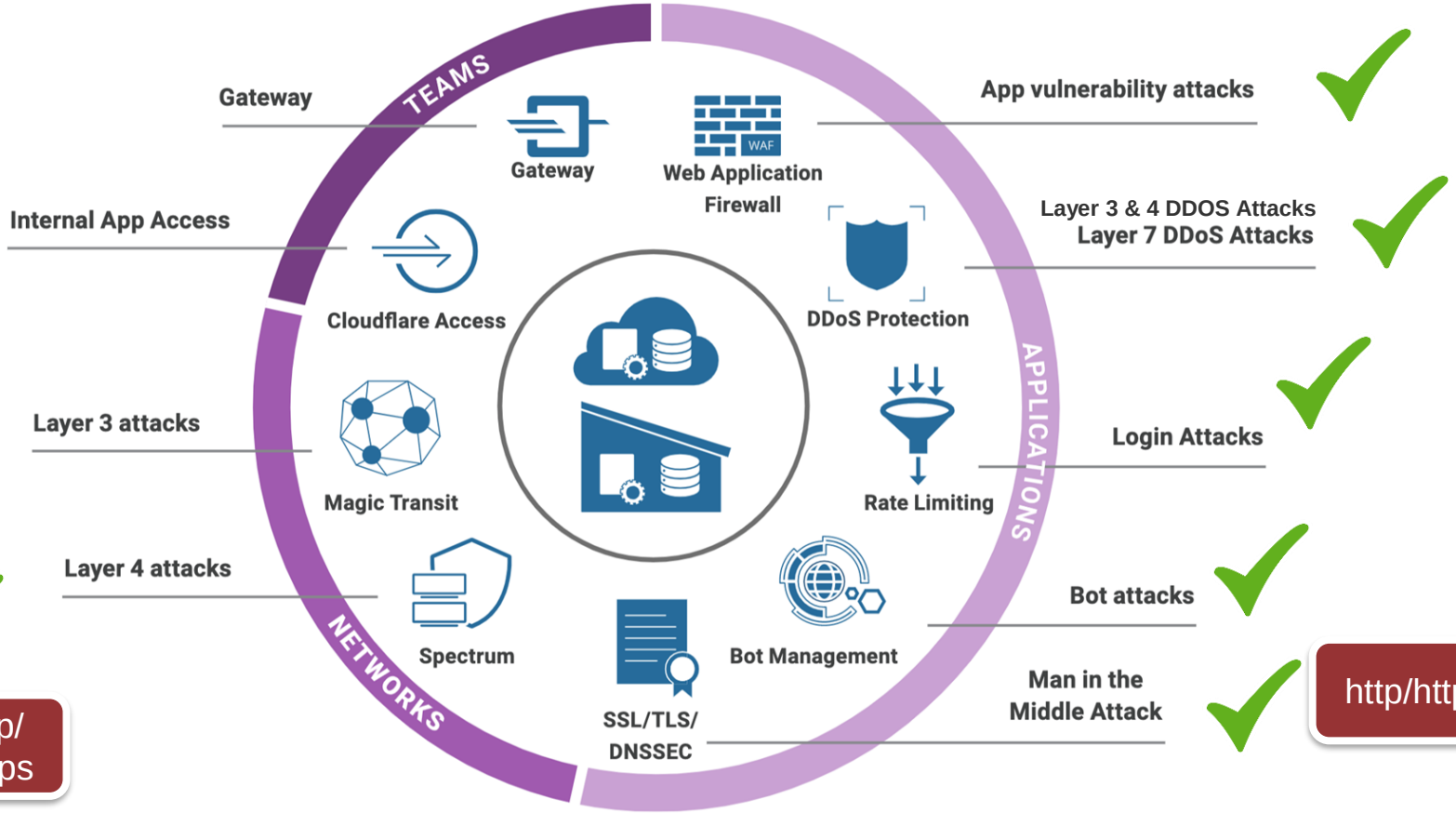
What you should already know from Accredited Configuration Engineer Training

- Core Product Implementation Steps
- DNS/SSL Configurations
- Security Best Practices
- Performance Best Practices
- Basic Troubleshooting

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

// Security Solutions

Cloudflare Security Portfolio



tcp/udp/
http/https

http/https

Cloudflare services across the OSI stack

7	Application Layer	**HTTP, DNS** • Authoritative DNS • CDN • Argo • Load Balancing • WAF • Bot Management • Video Streaming
6	Presentation Layer	
5	Session Layer	**TCP/UDP** • Spectrum • Argo • Load Balancing
4	Transport Layer	
3	Network Layer	**IP, GRE, any packet/protocol** • Magic Transit
2	Datalink Layer	**Physical interconnects** • Network Interconnect (CNI)
1	Physical Layer	

CLOUDFLARE

Cloudflare Security Services

DNS/DNSSEC
Secure and reliable DNS.

DDoS Protection
Enterprise-class DDoS

SSL/TLS
Easy to provision and manage SSL, including dedicated certificates.

(Covered in ACE)

Layer 7
Granular controls to detect and mitigate abusive traffic: WAF, Rate Limiting & more

Bot Mitigation
Identify and block malicious bot traffic.

Out of Scope

Orbit
Secure and authenticated connection between an IoT device and origin.

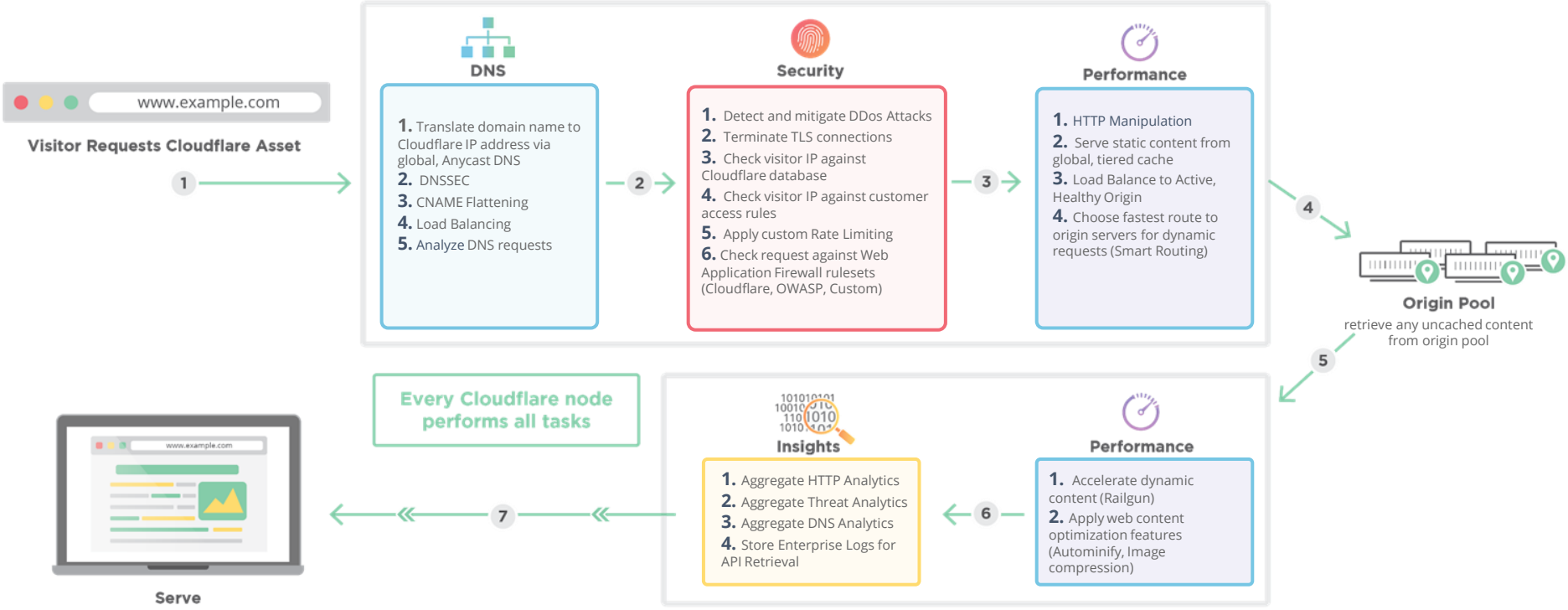
Spectrum
Protect TCP applications and ports from volumetric DDoS attacks and data theft.

Access
Secure, authenticate, and monitor user access to any domain, application, or path on Cloudflare.

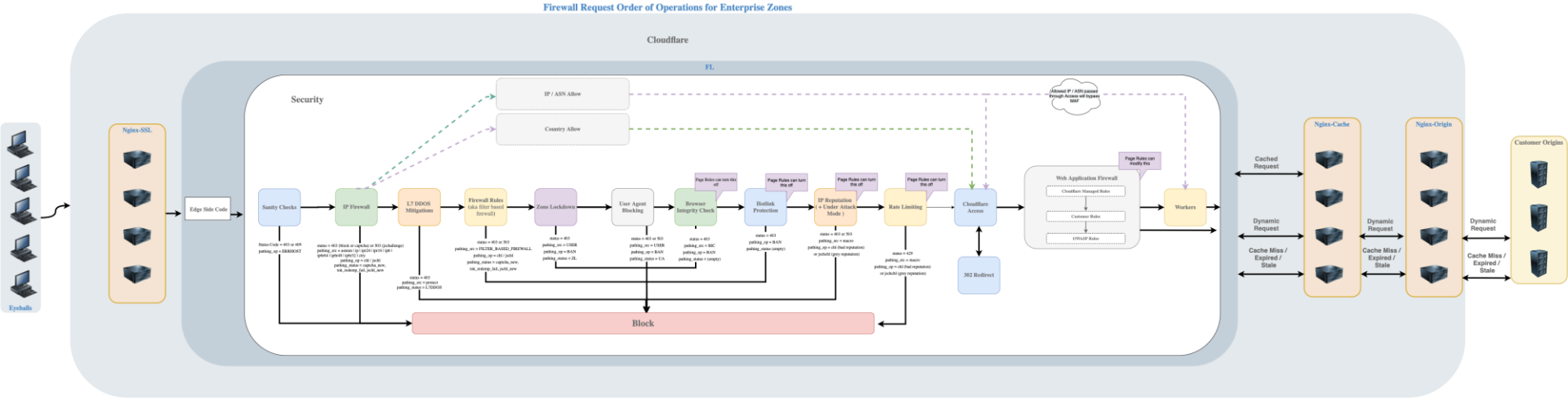
Argo Tunnel
Creates an encrypted tunnel between an application's origin server and the nearest data center without opening a public inbound port.

Workers
Runs JavaScript Service Workers to customize and configure apps on the edge.

Review: Life Of A Request



Cloudflare Security – Order of Operations for ENT zones

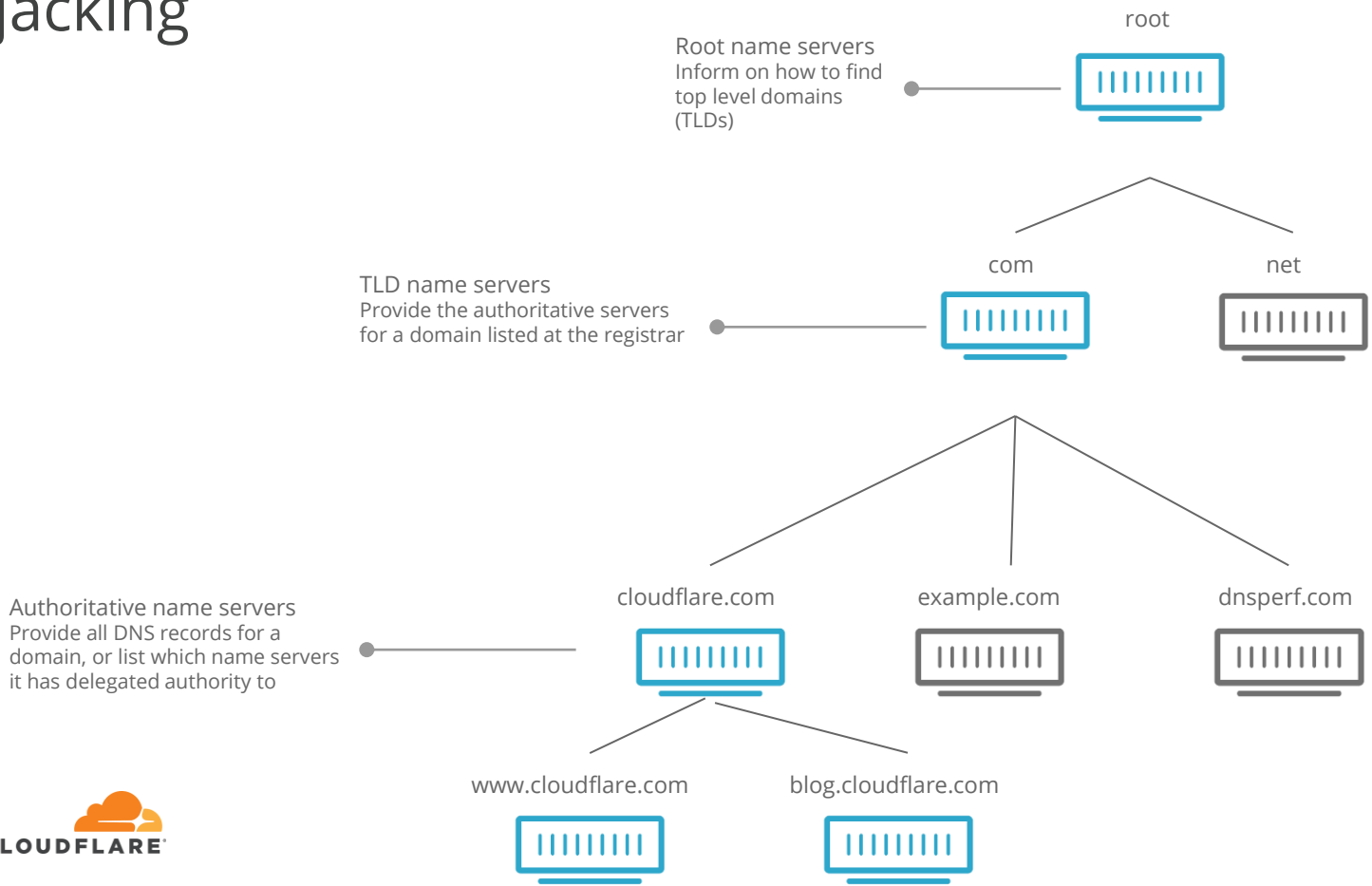


CLOUDFLARE

Cloudflare has one of the largest managed DNS providers in the world with over 38% of all DNS responses being served.

// DNS + DNSSec

DNS - Distributed, decentralized, & vulnerable to hijacking



CLOUDFLARE

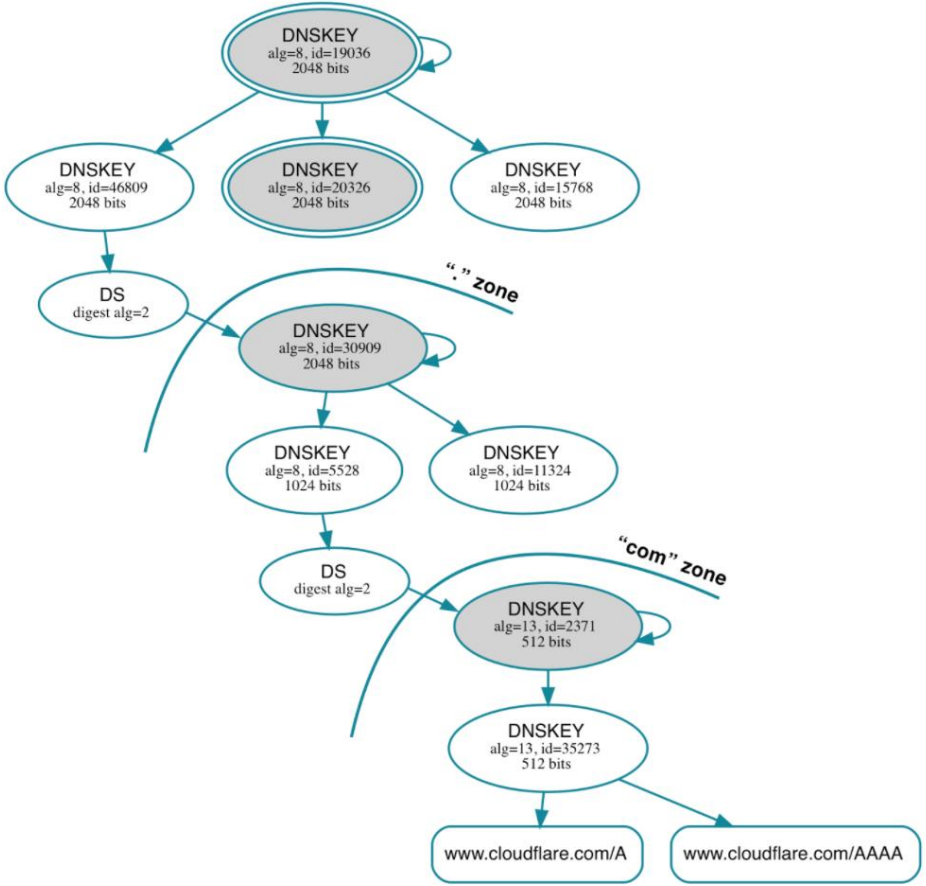
DNSSEC (DS) Records

- DNS Security records allow your authoritative nameservers to digitally sign the response they sent to your client, and for your client to verify the response it received was from the expected authoritative nameserver.

- This fixes the problem of spoofing responses from name servers, which can allow hackers to redirect queries for a given domain to another IP address, in order to steal data or spread malware.

DNSSEC adds a few new DNS record types:

RRSIG - Contains a cryptographic signature
DNSKEY - Contains a public signing key
DS - Contains the hash of a DNSKEY record
NSEC and **NSEC3** - For explicit denial-of-existence of a DNS record
CDNSKEY and **CDS** - For a child zone requesting updates to DS record(s) in the parent zone.



Enabling DNSSEC in Cloudflare DNS

Step 1 - Enable DNSSEC in Cloudflare DNS

By enabling DNSSEC first in the Cloudflare dashboard, you're asking Cloudflare to generate the data necessary for adding a delegation signer (DS) record to your domain at the registrar.

> Cloudflare's chosen cipher suite (Algorithm 13, also known as ECDSA Curve P-256 with SHA-256), is not supported by some registrars. Note that some registrars support a different set of verification algorithms depending on the TLD. If your registrar or TLD registry doesn't support Algorithm 13, see What if my registrar or TLD doesn't support DNSSEC?

Step 1: To obtain the Cloudflare DS record data:

1. Log in to the Cloudflare dashboard.
2. Ensure the website for the DS record you need is selected.
3. Click the **DNS** app.
4. Scroll down to the **DNSSEC** panel.
5. Click **Enable DNSSEC.** You will see a dialog informing you that your configuration is pending until the DS record is added at your registrar.
6. Next, click to expand the **DS Record** dropdown in the **DNSSEC** panel.
7. Copy the DS record information displayed as you will need it for Step 2 below

Step 2 - Add the DS record to your registrar

DNSSEC migration note: https://cloud.google.com/dns/docs/dnssec-config#migrating

Learn More: https://support.cloudflare.com/hc/en-us/articles/360006660072-Understanding-and-Configuring-DNSSEC-in-Cloudflare-DNS

Quiz:

Can you implement Cloudflare DNSSEC with CNAME setup?

Quiz:

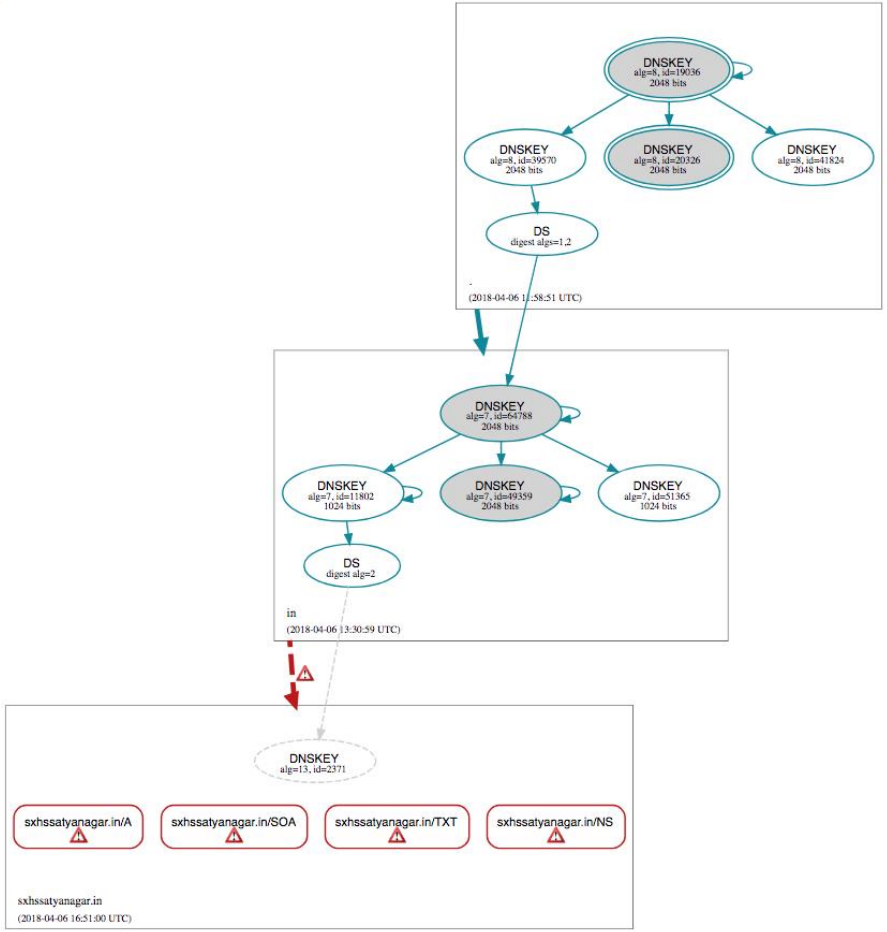
A customer intends to implement Cloudflare DNSSEC with CNAME setup? What’s your recommendation?

Answer:

You can’t use Cloudflare DNSSEC with CNAME setup.

You need to use Full Setup to use DNSSEC.

DNSSEC Troubleshooting Resources

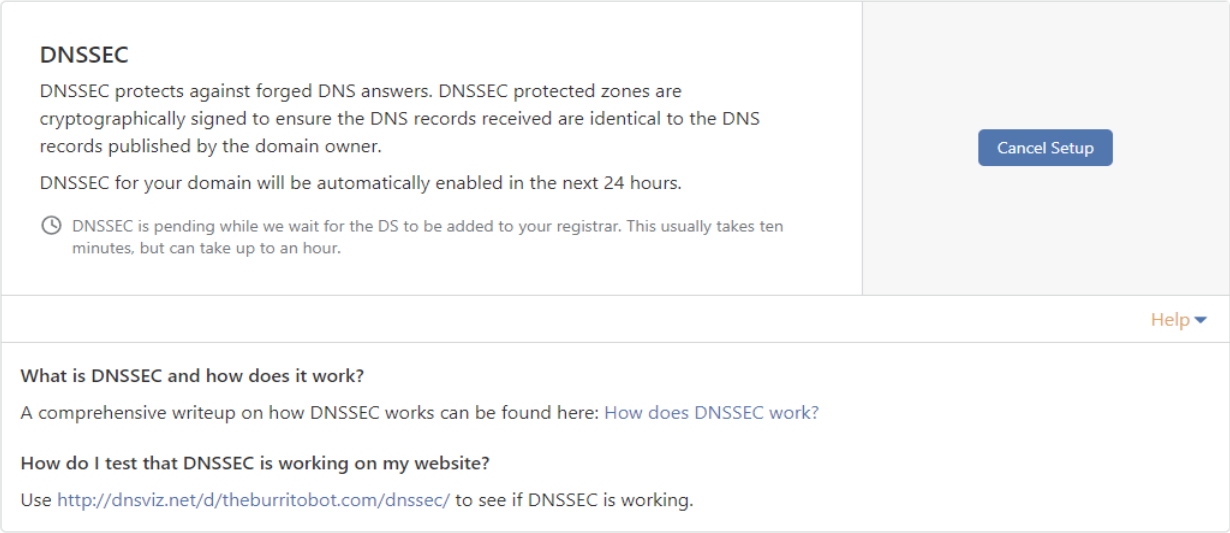



```
$ dig a cloudflare.com +dnssec

;; ANSWER SECTION:
cloudflare.com.          378     IN      A
                 198.41.214.162
cloudflare.com.          378     IN      A
                 198.41.215.162

cloudflare.com.          378     IN      RRSIG
                 A 13 2 600 20180829201022 20180827181022 35273
cloudflare.com.
8VD0d38J9gAHStzF4t97bI59kJsO9GG5gwSP8rXDdO6YCcp/ot9WDLQf
IhG0gVSKK/u05OeuxCAJ+1fSwxWT/w==
```

- Tools: https://DNSViz.net & https://dnssec-analyzer.verisignlabs.com/
- Dig +trace +dnssec

Lab - Reviewing DNSSec in the Dashboard and using dig

- Try dig commands from https://support.cloudflare.com/hc/en-us/articles/360021111972



CLOUDFLARE

Lab - DNSSec output for Cloudflare.com and brokendnssec.net

- Go to dnsviz.net
- Enter Cloudflare.com as domain name and observe the output
- Enter brokendnssec.net as domain name and observe the output

Takeaways - DNSSEC

Introduction

DNSSEC is an extra layer of security that resolves DNS hijacking concerns

Cloudflare uses Algorithm 13, which may not be supported by all registrars.

Implementation

The DS records can be found in the Cloudflare DNS tab for copy/pasting into your registrar

Troubleshooting

DNSViz.net is a simple tool to diagnose DNSSEC issues.

Dig and trace can also be used to determine what DS records are being sent.

Cloudflare has over 67 Tbps of network capacity to dilute, absorb, and mitigate the world's largest attacks.

// DDoS

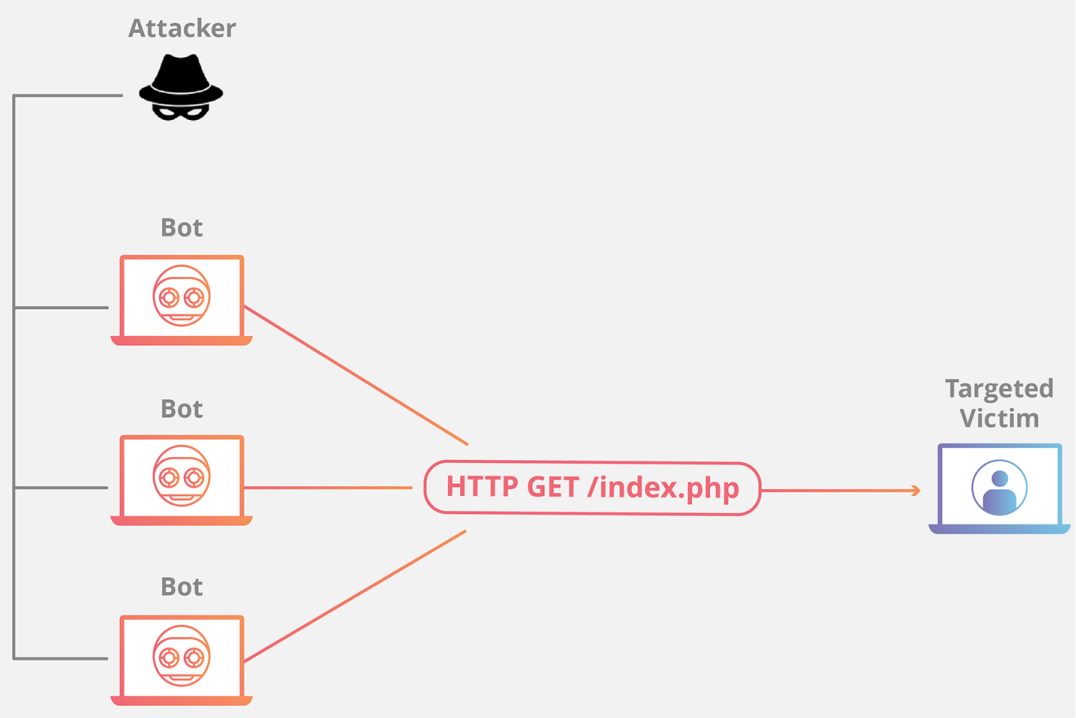
Introduction to DDoS Attacks

Problems

- Disrupt normal traffic
- Impact service

Solutions

- Dilute attacks
- Firewalls (WAF)
- Rate Limiting
- IP Reputation
- I am under attack mode (IAUM)

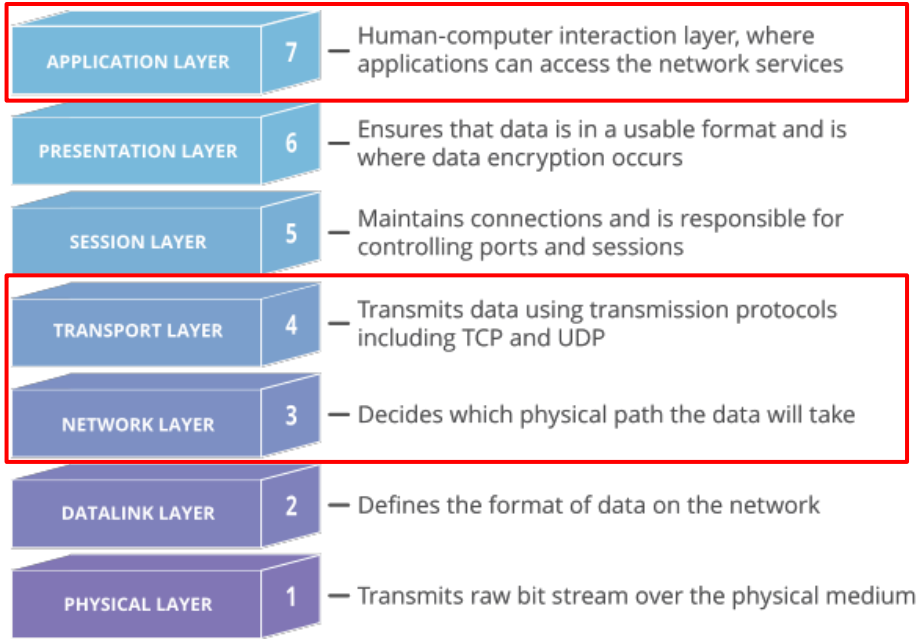


CLOUDFLARE

DDoS attack layers

Types

- Application
  - HTTP flood
- Protocol attacks
  - SYN flood
- Volumetric
  - DNS Amplification



OSI Model

CLOUDFLARE

Layer 3 / 4 Attack Details

Are

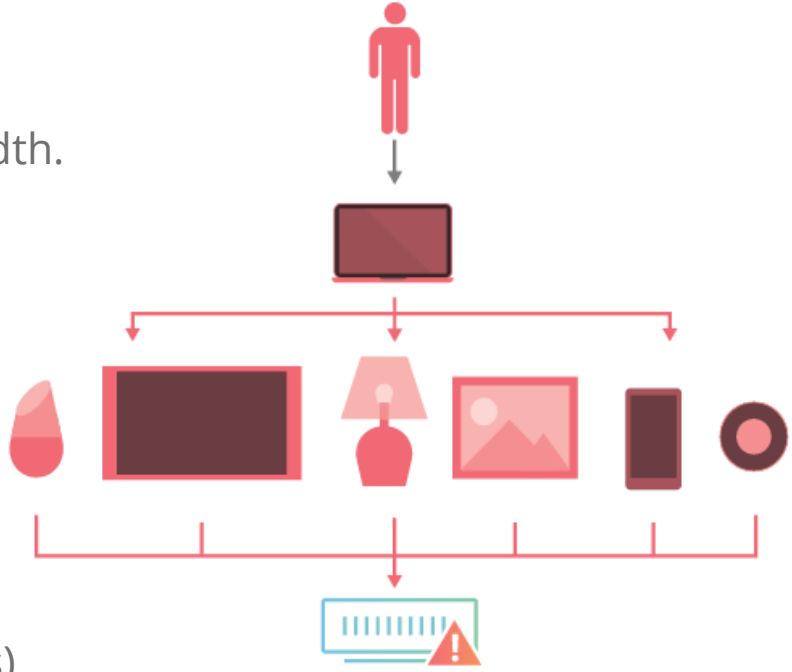
- Volumetric
- Target network infrastructure
- Degrade performance and consume bandwidth.

Most common:

- SYN floods
- UDP floods
- DNS (reflection or amplification) attacks.

Mitigations:

- Mitigated automatically by Gatekeeper
- Rarely noticed by customers
- Spectrum (for L4 attacks to custom port apps)



CLOUDFLARE

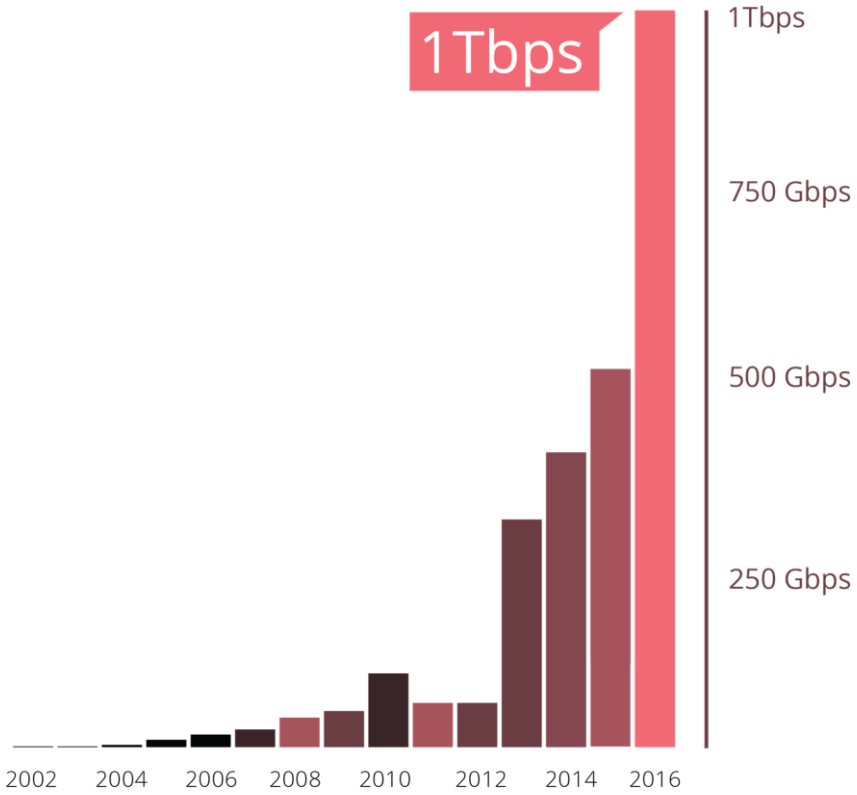
Layer 7 Attacks (application layer)

Types:

- GET/POST floods
- XSS
- SQLi attacks
- more...

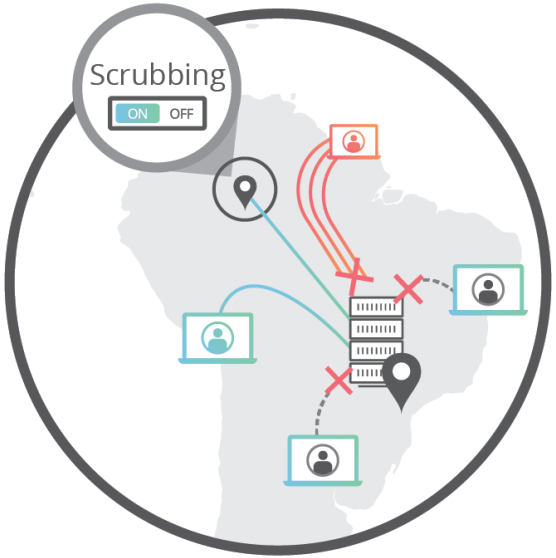
Layered Mitigations:

- Rate Limiting
- Firewall
- I'm Under Attack Mode (IAUM)
- Bot Management



CLOUDFLARE

Industry On-Demand vs. Cloudflare Always On



Industry Legacy Scrubbing

- Long propagation times (up to 300 sec)
- Asynchronous routing
- Adds significant latency
- Typically requires manual intervention and regular testing (config drift)

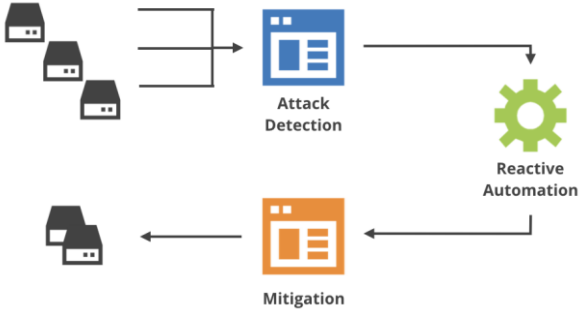
Always-On

- Zero propagation time
- Synchronous routing
- No added latency; ongoing perf. improvements
- Immediate, automated mitigation, with no “cutover” required

Gatebot & Gatekeeper

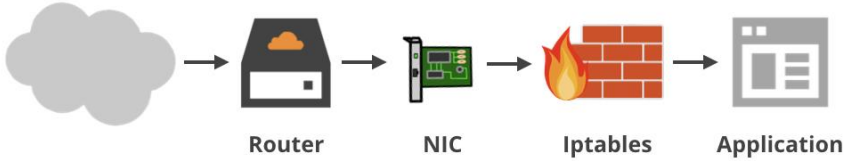
Gatebot(global)/DosD(local) - samples traffic, creates signatures that allow for automatic or manual mitigation

1. attack detection
2. reactive automation
3. mitigations



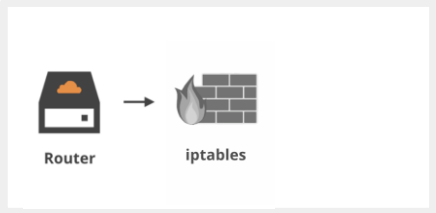
Gatekeeper - manages firewall mitigation for L3/L4 packet floods

- Gatekeeper - tool creates firewall rules, writes to database
- gatesetter - daemon that polls the database, updates the firewall

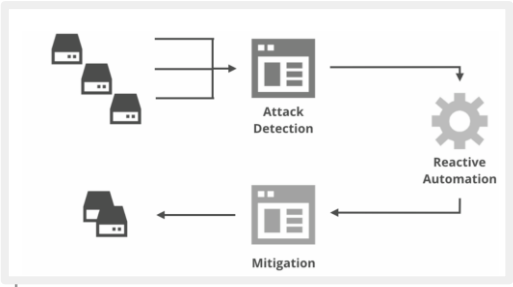


CLOUDFLARE

Cloudflare DDoS - Technical Advantage

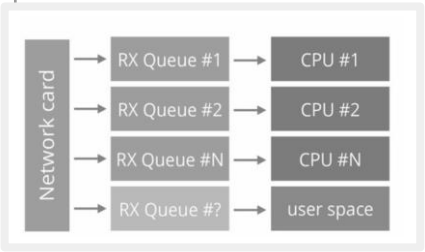


Dynamically Managed iptables
Dynamically drop packets that hit Cloudflare Network cards. Our custom stack of high-performance filters enables us to scale to block high-volumes of network traffic.



Auto Mitigation
Aggregates all traffic to develop automatic mitigation heuristics which dramatically reduces the need for humans to intervene to block traffic.

CPU Efficiency
Sustain larger attacks by bypassing kernel and offload to the user space. This allows millions of packets per second per server to be processed.



DDOS Attacks and Trends

Attacks

7 Days

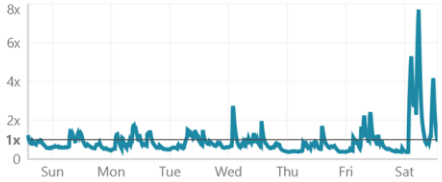
Network-level DDoS Attacks

Learn More

Distribution of Layer 3/4 DDoS attacks by different attack types.

ICMP	TCP	UDP	GRE
0%	62%	38%	0%

Change in Layer 3/4 DDoS attack volume over the selected time period. Learn how to secure your websites, applications, and networks against DDoS attacks.



Application-level Attacks

Learn More

Distribution of Layer 7 attacks by mitigation techniques deployed to block them.

Firewall	WAF	DDoS	Other
6%	2%	91%	0%

Quarterly DDOS Attack Trends (https://blog.cloudflare.com/ddos-attack-trends-for-2021-q1/)
Internet Traffic Trends (https://radar.cloudflare.com/)

DDOS Further Reading

https://blog.cloudflare.com/no-scrubs-architecture-unmetered-mitigation/

https://blog.cloudflare.com/how-cloudflares-architecture-allows-us-to-scale-to-stop-the-largest-attacks/

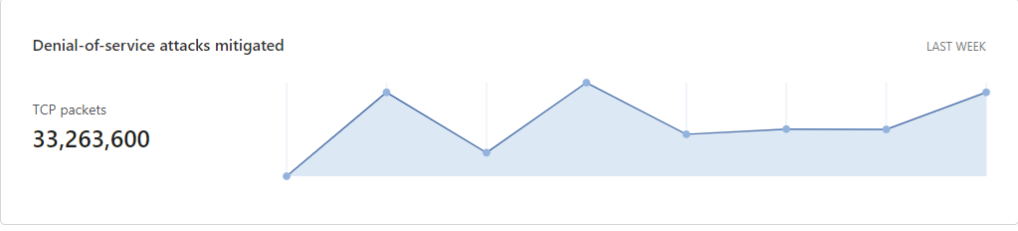
https://blog.cloudflare.com/moobot-vs-gatebot-cloudflare-automatically-blocks-botnet-ddos-attack-topping-at-654-gbps/

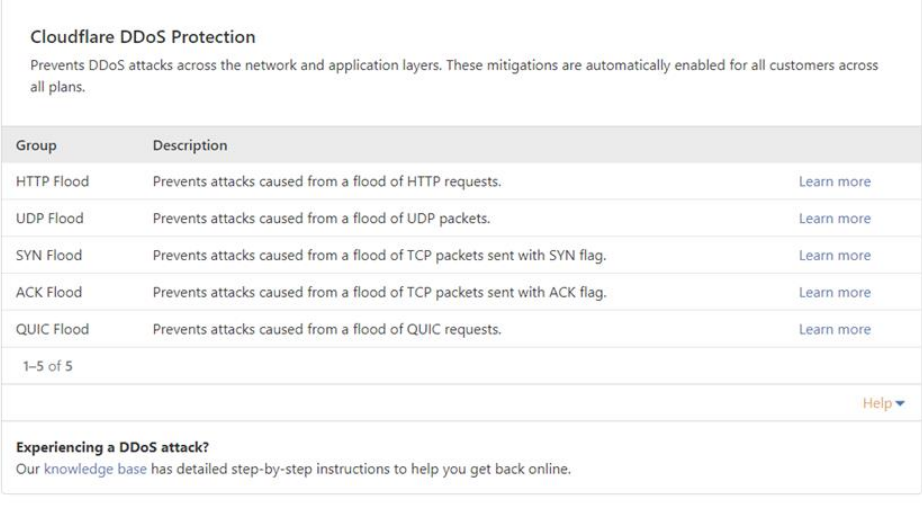
https://blog.cloudflare.com/rolling-with-the-punches-shifting-attack-tactics-dropping-packets-faster-cheaper-at-the-edge/

https://blog.cloudflare.com/announcing-flowtrackd/

CLOUDFLARE

Lab - Explore DDoS Analytics and Protections





Cloudflare DDoS Protection

Prevents DDoS attacks across the network and application layers. These mitigations are automatically enabled for all customers across all plans.

Group	Description	
HTTP Flood	Prevents attacks caused from a flood of HTTP requests.	Learn more
UDP Flood	Prevents attacks caused from a flood of UDP packets.	Learn more
SYN Flood	Prevents attacks caused from a flood of TCP packets sent with SYN flag.	Learn more
ACK Flood	Prevents attacks caused from a flood of TCP packets sent with ACK flag.	Learn more
QUIC Flood	Prevents attacks caused from a flood of QUIC requests.	Learn more

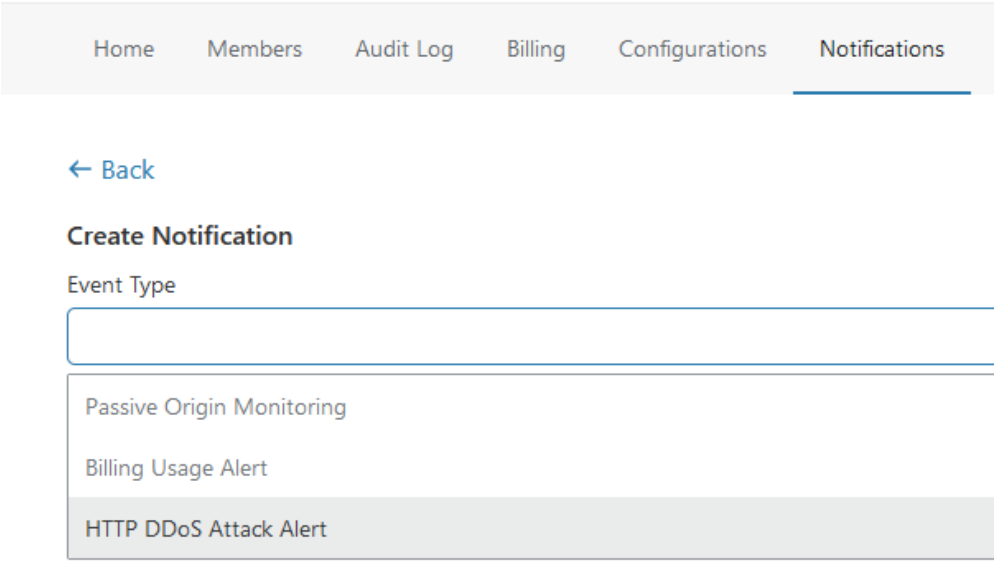
1–5 of 5

Help

Experiencing a DDoS attack?

Our knowledge base has detailed step-by-step instructions to help you get back online.

Lab - Explore DDoS Alerting



Takeaways - DDoS

Introduction

SYN and UDP Floods are most common

Cloudflare has over 67Tbps+ of capacity

Implementation

All DNS proxied records are protected from Layer 3, 4, and 7 attacks

Troubleshooting

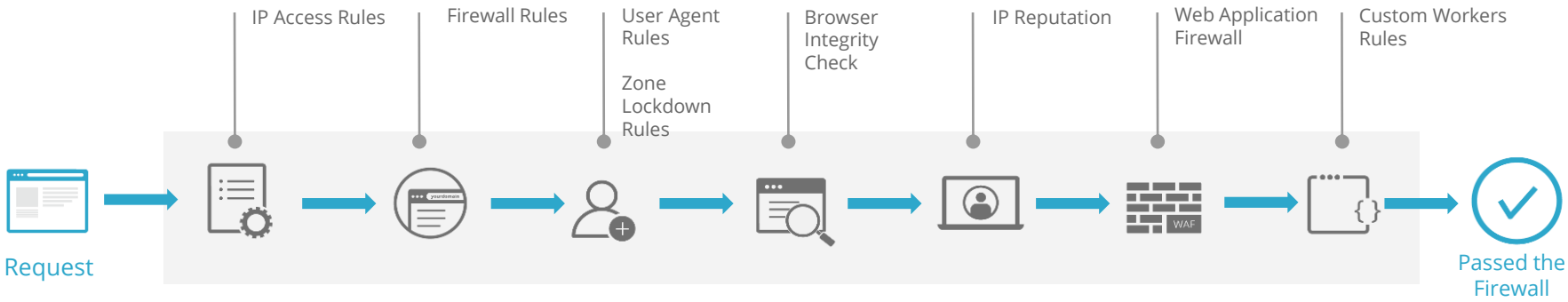
Analytics are available on the Firewall events pages

Cloudflare also has a BGP-based solution known as Magic Transit for securing entire networks: https://www.cloudflare.com/magic-transit/

Cloudflare Firewall includes an IP Firewall, Managed Rulesets, and the ability to write custom rules.

// Firewall

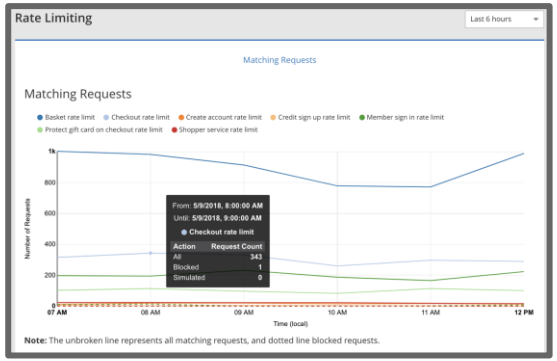
Cloudflare Firewall Services Layer



When a request hits the Cloudflare edge network, it goes through a series of security checks and features

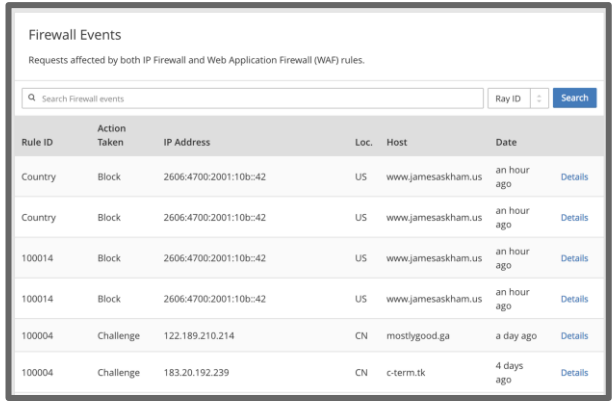
Security Event Logging & Locations

Analytics -> Threats & Rate Limiting



https://support.cloudflare.com/hc/en-us/articles/204191238-What-are-the-types-of-Threats-

Firewall -> Overview



https://developers.cloudflare.com/firewall/

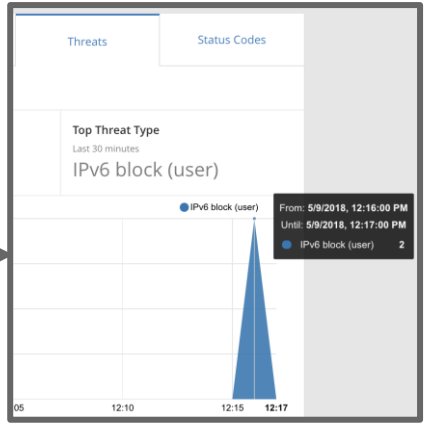
Log Share


```
{
  "ClientIP": "2606:4700:2001:10b::42",
  "ClientRequestHost": "www.jamesaskham.us",
  "ClientRequestURI": "/",
  "EdgePathingOp": "chl",
  "EdgePathingSrc": "user",
  "EdgePathingStatus": "captchaNew",
  "EdgeResponseStatus": 403
}
```

Firewall Actions: Blocks

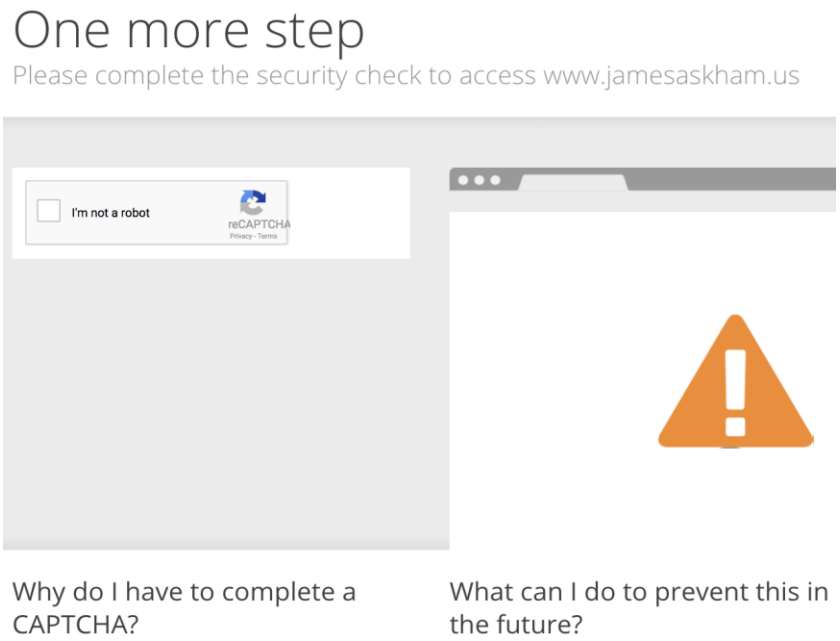
- Count as ‘Cached Request’ and ‘Cached Bandwidth’
- Logged as 403 Status Code
- Logged in Analytics and ELS only
- Country Blocks DO appear in Firewall Events.

IP Block



Firewall Actions: Captcha Challenge

- IP Firewall CAPTCHA same presentation as IP Reputation, WAF and Country challenge pages.
- Ensures visitor is not a bot.
- First CAPTCHA presents picture challenge using hCaptcha.
- Page is logged as a 403 in Status Codes.
- Counts as ‘Cached Bandwidth’ and a ‘Cached Request’
- Only logged in ELS. “Human Challenged” event in Analytics if failed
- Can generate a CAPTCHA with ‘cf-setopt-chl’ header value of ’1’.

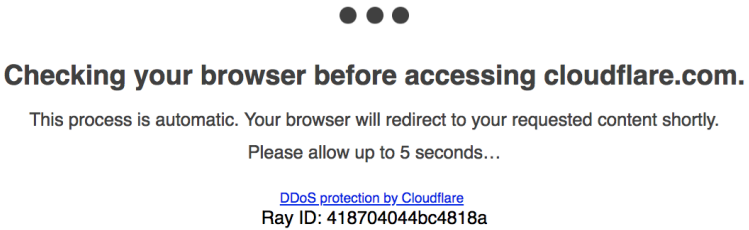


Firewall Actions: Javascript Challenge

JavaScript Challenge

- Same in presentation as the I'm Under Attack Mode (IUAM).
- Prevents bots from accessing a webpage.
- Validates real browser user without human interaction.
- Not perfect, smart attackers can bypass with smart bots.
- Counts as a 503 response, cached bandwidth, cached request.

  Browser Challenged in Analytics.
- Also referred to as an **Interstitial Page**
- Will break any non-browser connectivity (API, XHR etc.)
- Rate Limiting product is becoming a more popular alternative but requires more configuration.



Firewall Actions: Whitelist + Simulate/Log

Whitelist

- Allowing IPv4, IPv6, IP range, Country will **disable all CF security features** for that visitor, includes:
  - IP Reputation
  - Browser Integrity Check
  - WAF
  - UA Block
  - Rate Limiting
  - Scrape Shield features

NOTE: Exception: allowing a Country will NOT bypass WAF.

- IP Access Whitelist Rules should NOT be specifying allow access to the site for ONLY these visitors. Zone Lockdown is a better tool for that use case.

Simulate/Log - the request is allowed through but is logged in the Security Events

IP Access Rules

- Inspects source IP address in header of inbound IP packets. Layer 3 of OSI.
- Rules can be applied to individual zones, all zones for a user or all zones in an organization
- The Tor network is stored as a country and can be applied
- Can **Block**, **Captcha challenge**, **JavaScript challenge** and **Whitelist** clients.
- Rules can be one of:
  - IPv4 ("ip" in SQL)
  - IPv6 ("ip6" in SQL)
  - IPv4 CIDR ("ipr" in SQL)
  - IPv6 CIDR ("ipr6" in SQL)
  - Country ("ctry" in SQL)
  - ASN ("asn" in SQL)
- Limits on number of access rules per plan/user

CLOUDFLARE

https://support.cloudflare.com/hc/en-us/categories/200275228-Firewall

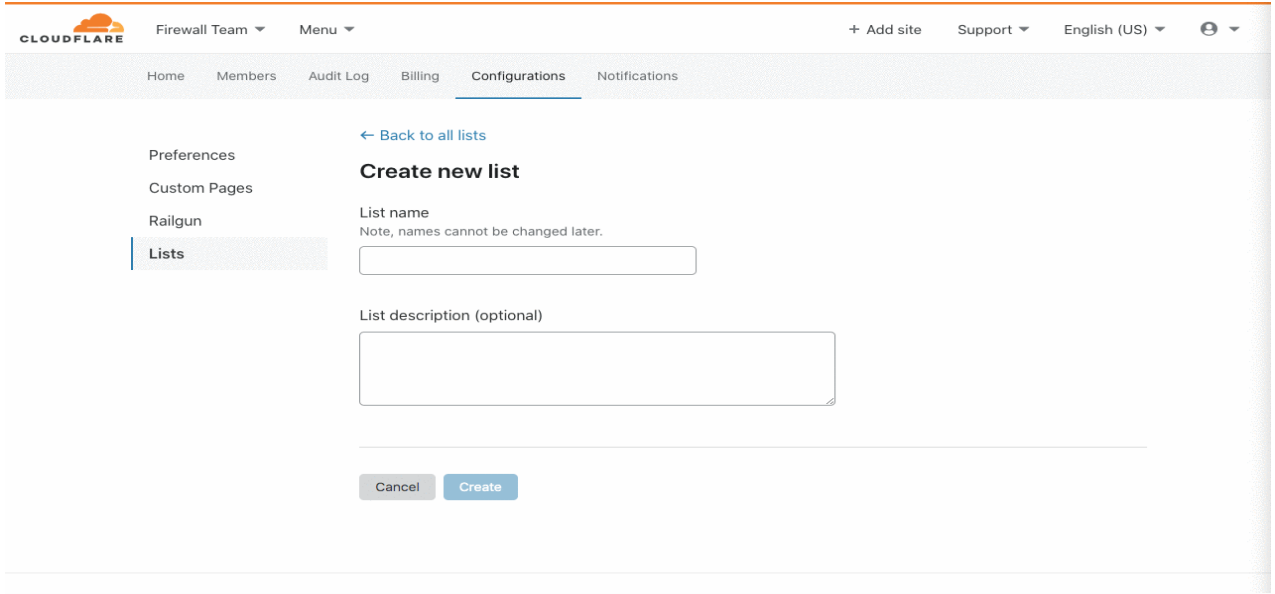
Lab - Writing an IP Access Rule

TASK:

1. Find your current country of origin and block that country within your Cloudflare lab domain using an IP Access Rule.
2. Attempt to access the domain and confirm the result.
3. Unblock your country of origin.

IP Lists

IP lists make it easier to create and re-use IPs for creating firewall rules.



https://support.cloudflare.com/hc/en-us/categories/200275228-Firewall

Lab – Create IP Lists

TASK:

1. Create IP Lists containing your own IP
2. Create a Firewall Rules to challenge all access to your demo site from the IP Lists
3. Check if the rules take effect

Firewall > Tools: Zone Lockdown =>To be migrated to FW Rules

Zone Lockdown specifies a list of one or more IP addresses, CIDR ranges, or networks that are the only IPs allowed to access a domain, subdomain, or URL. **Zone Lockdown** allows multiple destinations in a single rule as well as IPv4 and IPv6 addresses. IP addresses not specified in the **Zone Lockdown** rule are denied access to the specified resources.

For multiple overlapping **Zone Lockdown** rules, set a **Priority** under **Advanced Options** of the **Zone Lockdown** configuration. The lower the number, the higher the priority. Higher priority rules take precedence.

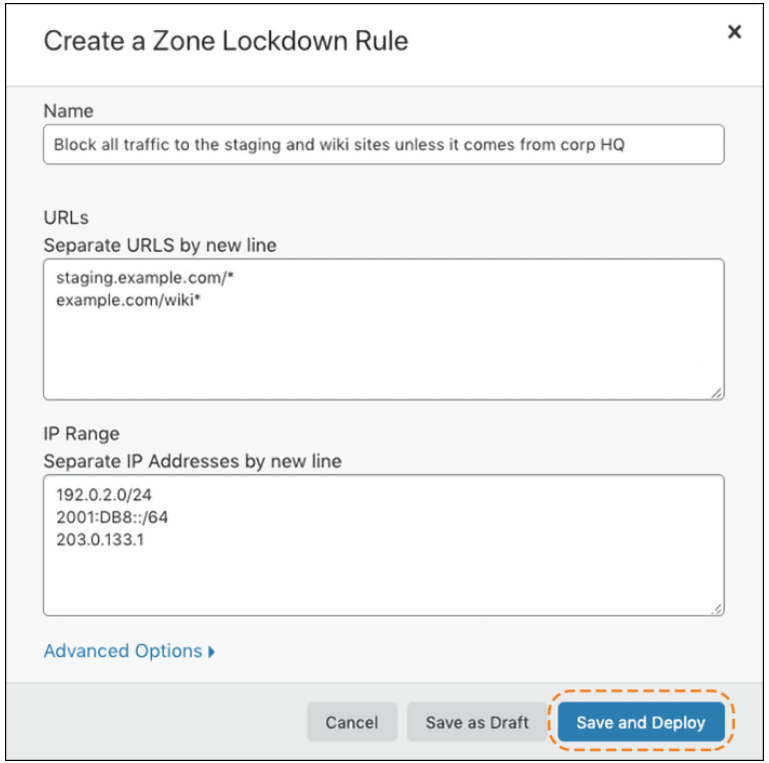
Error 1106 Ray ID: 3a1664f1d3468c5e • 2017-09-20 17:09:45 UTC

Access denied

What happened?

The owner of this website (example.com) has banned your IP address (2606:4700:2001:10e::c).

Cloudflare Ray ID: **3a1664f1d3468c5e** • Your IP: 2606:4700:2001:10e::c • Performance & security by Cloudflare



Firewall > Tools: User Agent Block => To be migrated to FW Rules

User Agent Blocking (UA) rules block specific browser or web application **User-Agent** request headers. UA rules apply to the entire domain instead of individual subdomains. UA rules are applied **after Zone Lockdown** rules, so permitting an IP address via **Zone Lockdown** skips UA rules.

You can also choose how to handle a matching request with the same list of actions as you have in the IP Firewall (Block, JS Challenge, Captcha Challenge, and Allowlist). Note that User-Agent blocking applies to your entire zone, so you cannot specify sub-domains as you can with Zone Lockdowns.

1. Log in to your Cloudflare Account.

2. Select the appropriate Domain.

3. Select the **Tools** tab within the Cloudflare **Firewall** app.

4. Click **Create Blocking Rule** under **User Agent Blocking.**

5. Enter the **Name/Description.**

6. Select an applicable **Action** of either *Block*, *Challenge* (captcha), or *JS challenge*.

7. Enter the **User Agent**. For example, to block the *Bad Bot* web spider:

BadBot/1.0.2 (+http://bad.bot)

8. Wildcards (*) are not supported.

9. Click **Save and Deploy.**

Firewall Tools: Browser Integrity Check

The Cloudflare **Browser Integrity Check (BIC)** operates similar to Bad Behavior and looks for common HTTP headers abused most commonly by spammers and denies access to your page. It also challenges visitors without a user agent or with a non-standard user agent such as commonly used by abusive bots, crawlers, or visitors.

BIC is enabled by default via the **Settings** tab of the Cloudflare **Firewall** app. You can disable the **BIC** using a Firewall BYPASS rule. Also, use a Page Rule to selectively enable or disable this feature for certain sections of your website. For example, disable **BIC** for your API traffic.

Firewall Tools: IP Reputation + Security Level

Security Level uses the IP reputation of a visitor to decide whether to present a Captcha challenge page. Once the visitor enters the correct Captcha, they receive the appropriate website resources. IP Reputation is collected from Project Honeypot. Cloudflare sets **Security Level** to *Medium* by default.

Security Level	Threat Scores	Description
Essentially off	greater than 49	Only challenges IP addresses with the worst reputation.
Low	greater than 24	Challenges only the most threatening visitors.
Medium	greater than 14	Challenges both moderate and the most threatening visitors.
High	greater than 0	Challenges all visitors that exhibit threatening behavior within the last 14 days.
I'm Under Attack!	N/A	Only for use if your website is currently under a DDoS attack.

Lab – Create Challenge/Block for specific UA

TASK:

1. Create a Firewall Rules to challenge/block all access from specific User Agent
2. Create a Firewall Rules to only allow/JW challenge access to a specific URL from your IP Address

End of Day 1 Summary

- Cloudflare Security Services Sequence
- DNS & DNSSEC
- DDOS Attack Mitigations
- Firewall Services Layer : IP Access Rules, IP Lists, Zone Lockdown, User Agent Block, Browser Integrity Check, Security Level
- Firewall Actions: Whitelist, Block, Challenge, JS Challenge, Simulate/Log

See you on Day 2 for these topics:

- WAF
- Firewall Rules
- Bot Management
- Spectrum
- Rate Limiting

Hands-on Lab Setup

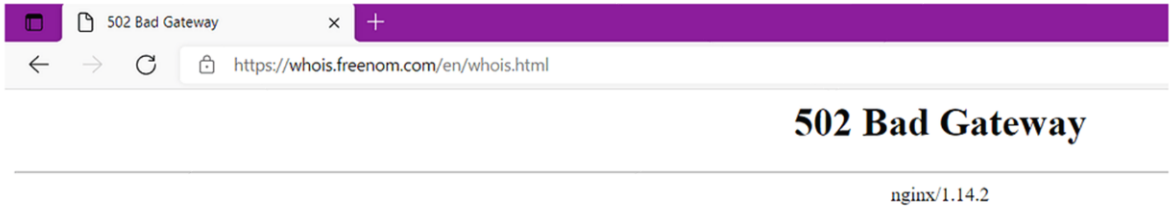
Common Issue with Freenom.com

erictung MVP '21 17d

This has been discussed quite a few times recently.

The answer is still the same: issue with Freenom WHOIS.

Even the Freenom WHOIS website is not accessible, I'm not really sure why you still need to blame Cloudflare where the issue is coming from Freenom:

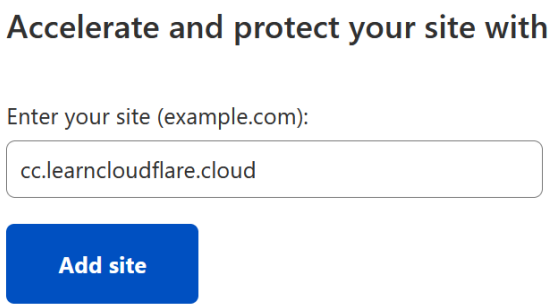


Solution

Problem when adding my freenom domain to cloudflare

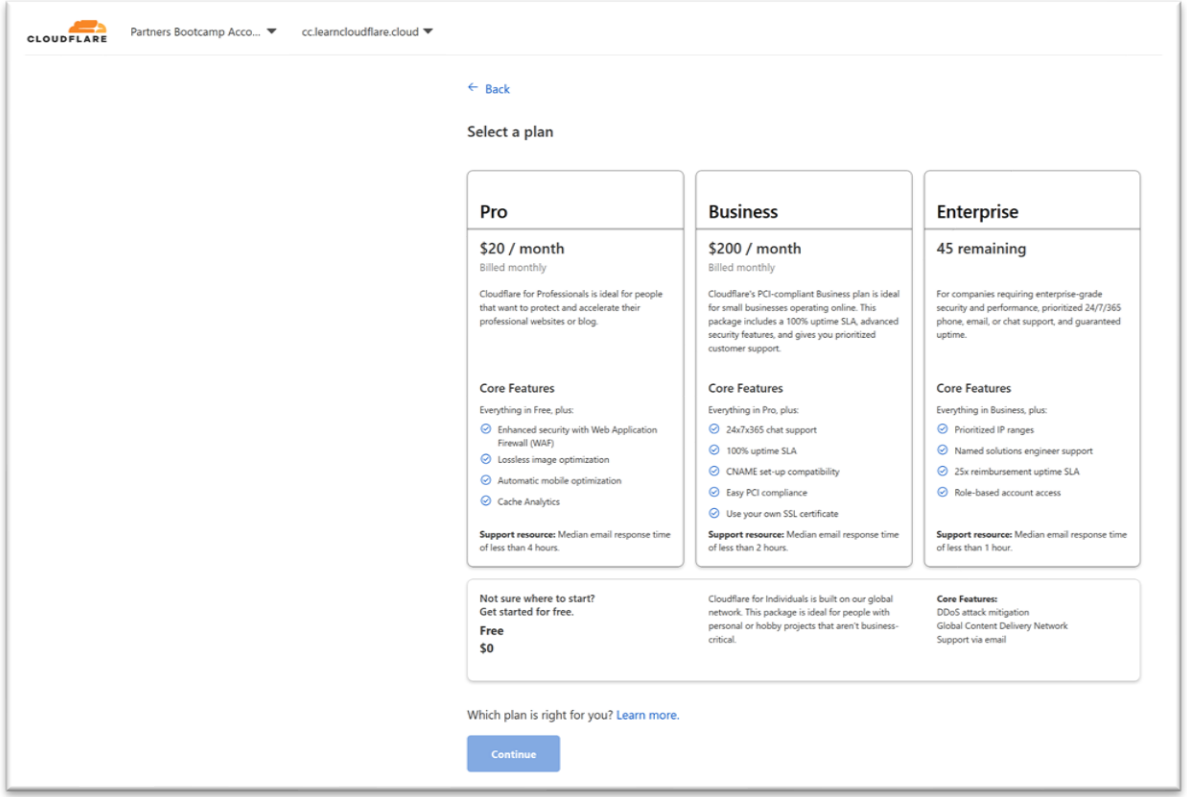
Steps to add Subdomain Support

1. Click **+ Add Site** button on the top right of Account Home
2. Enter **<your name>.learncloudflare.cloud** as your site



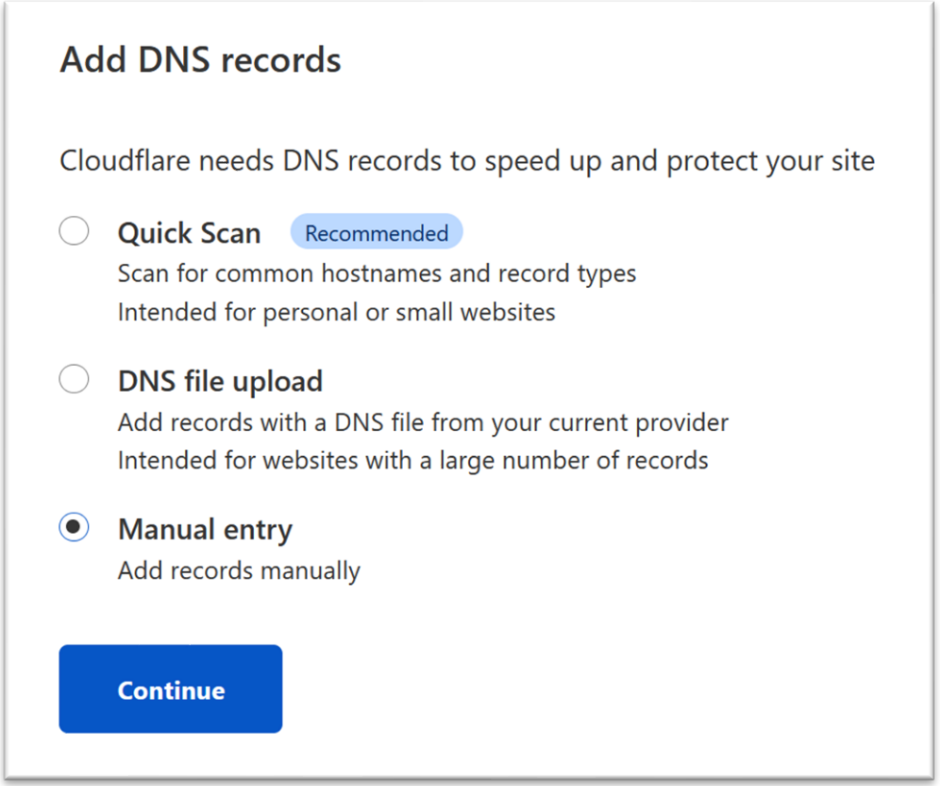
Steps to add Subdomain Support

3. Choose Enterprise plan for this training purpose



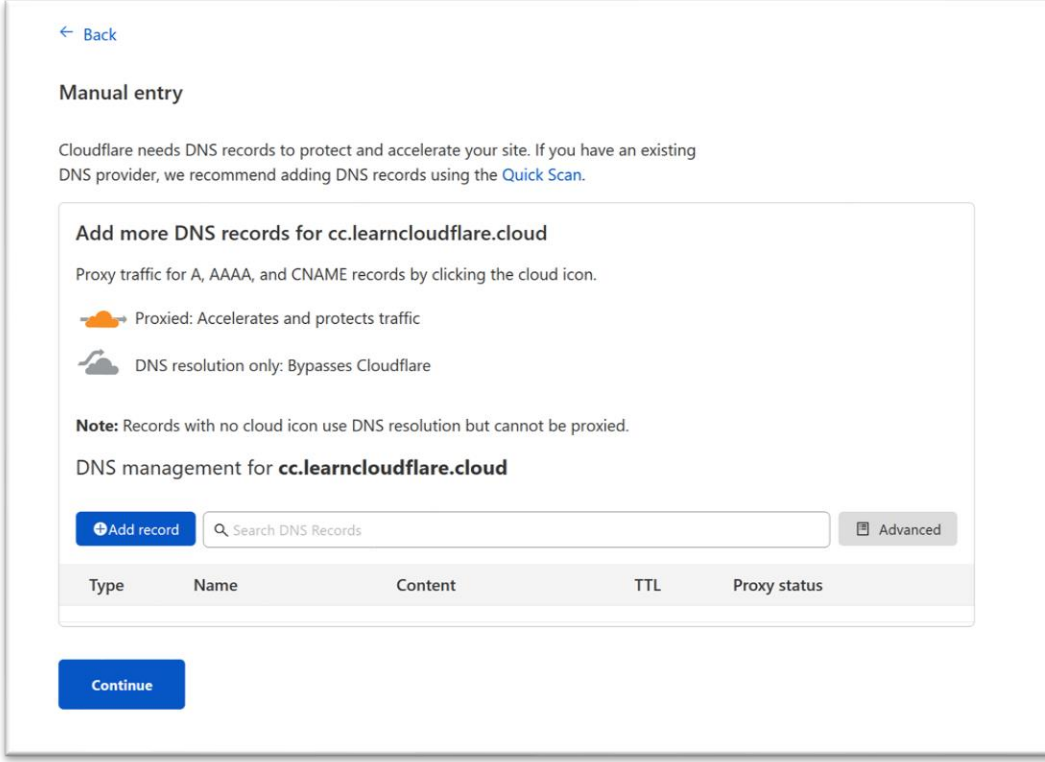
Steps to add Subdomain Support

4. Choose **Manual entry** for this training purpose



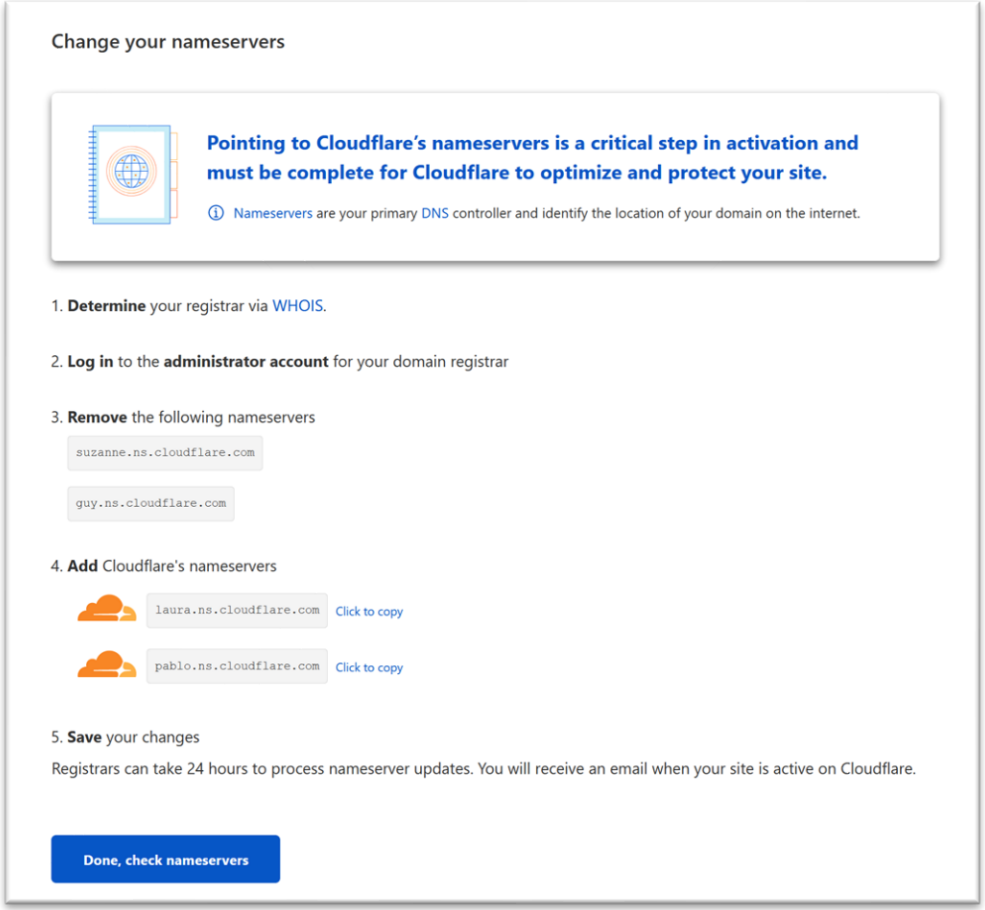
Steps to add Subdomain Support

5. Click **Continue**



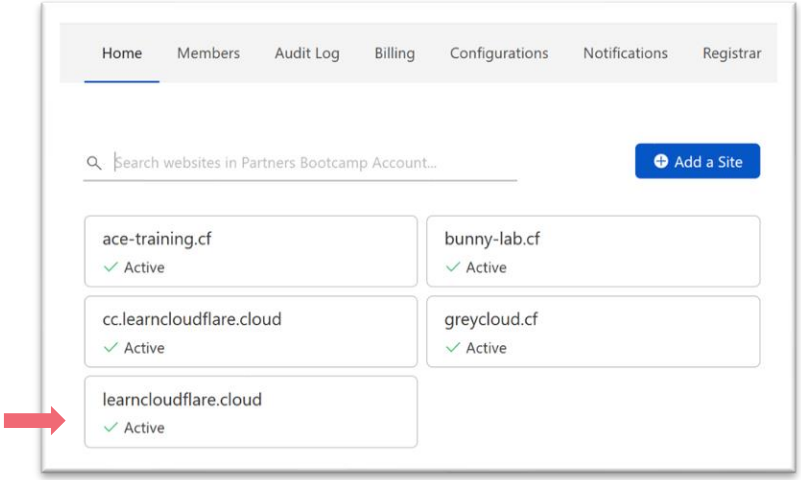
Steps to add Subdomain Support

6. Click **Done, check nameservers**



Steps to add Subdomain Support

7. Go to the **learncloudflare.cloud** domain dashboard **DNS** app



Steps to add Subdomain Support

8. Add **2 NS records** provided in the previous step
9. Check that the Subdomain is marked as **Active** in Account Home

DNS management for **learncloudflare.cloud**

Add record | Search DNS Records | Advanced

Type	Name	Content	TTL	Proxy status	
[redacted]					
[redacted]					
NS	cc	pablo.ns.cloudflare.com	Auto	DNS only	Edit
NS	cc	laura.ns.cloudflare.com	Auto	DNS only	Edit

cc.learncloudflare.cloud

✓ Active