



# 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](mailto:ccarlane@cloudflare.com)



Declan Carlin  
Partner Solution Engineer  
EMEA  
[declan@cloudflare.com](mailto:declan@cloudflare.com)

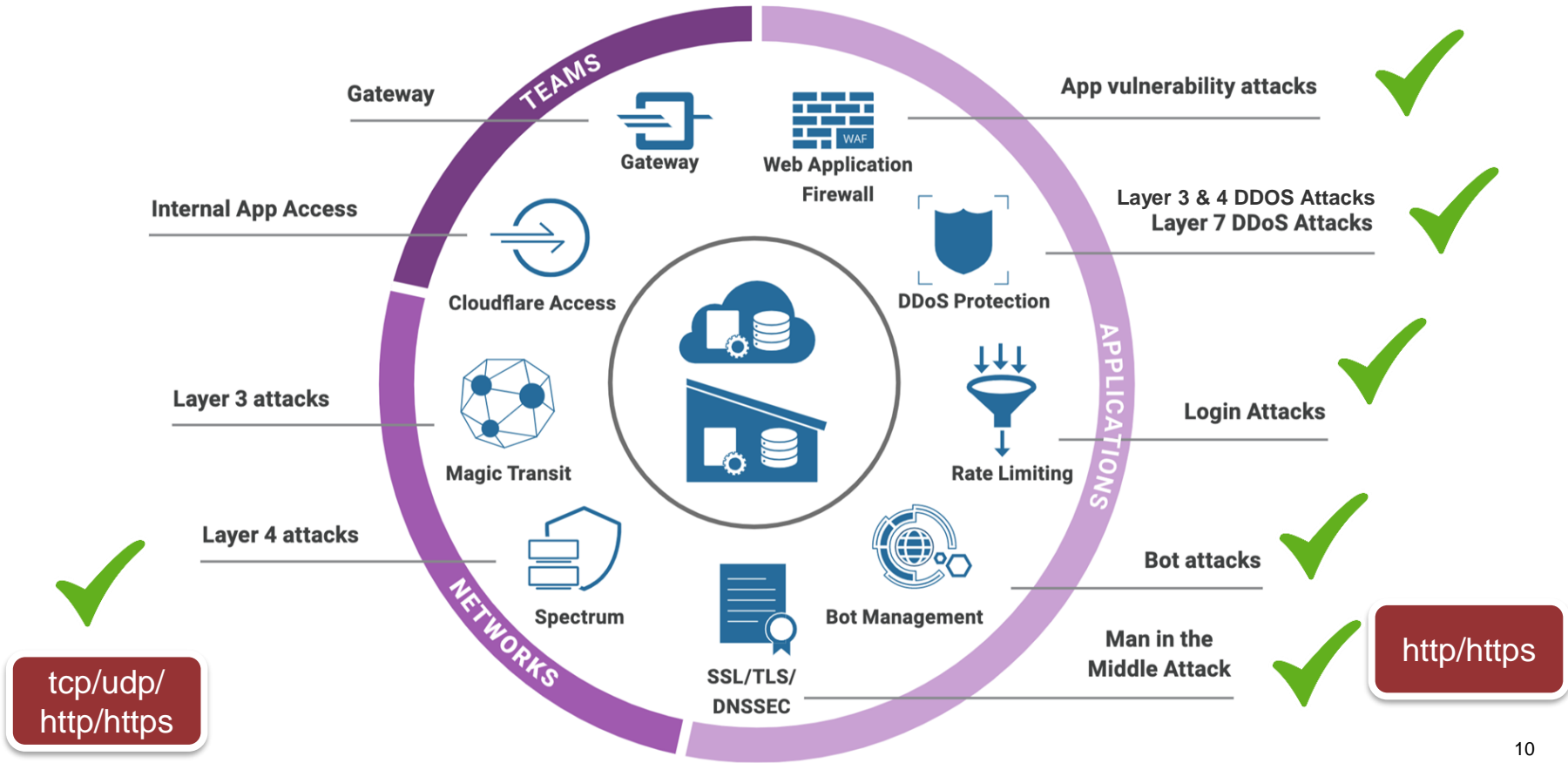
# What you should already know from Accredited Configuration Engineer Training

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

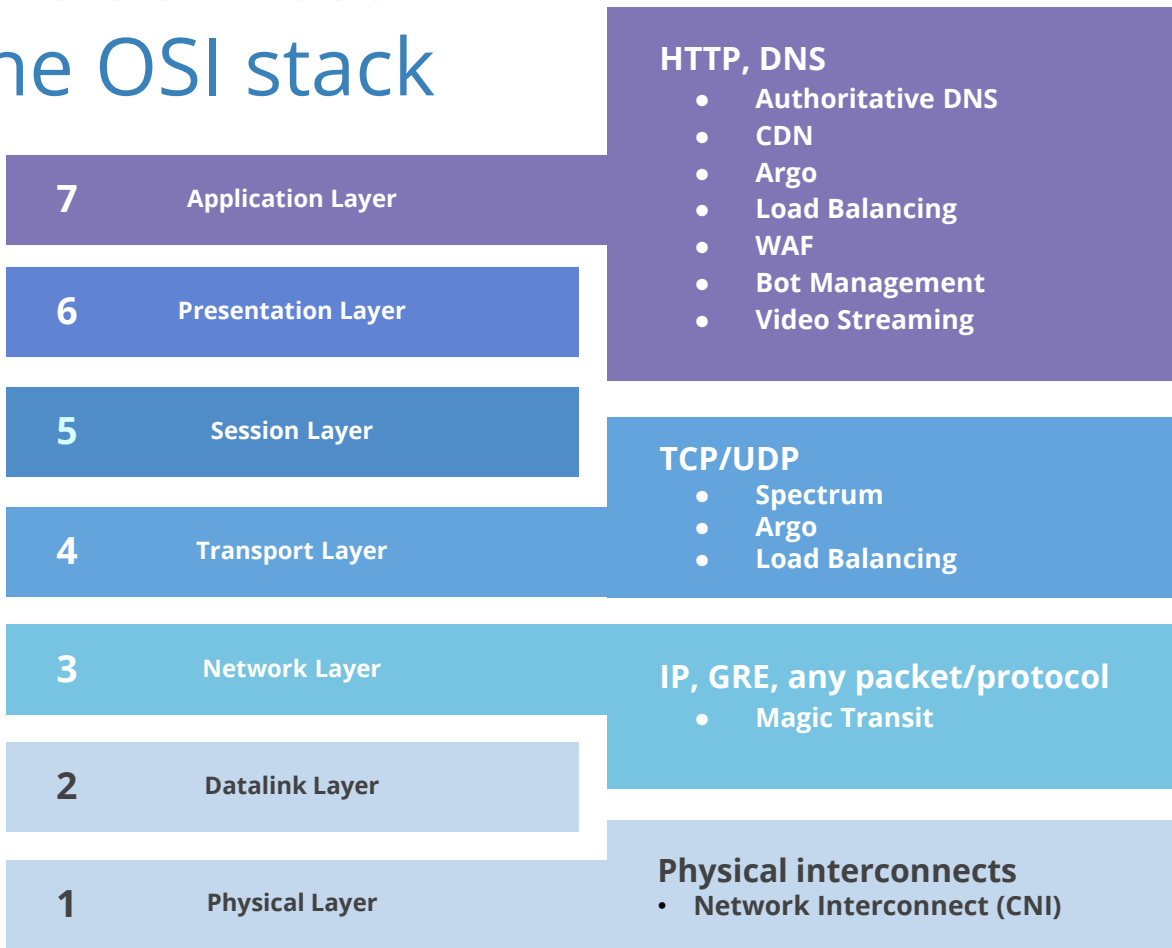
Cloudflare is an integrated global cloud network that provides performance, security, reliability and platform solutions.

## // Security Solutions

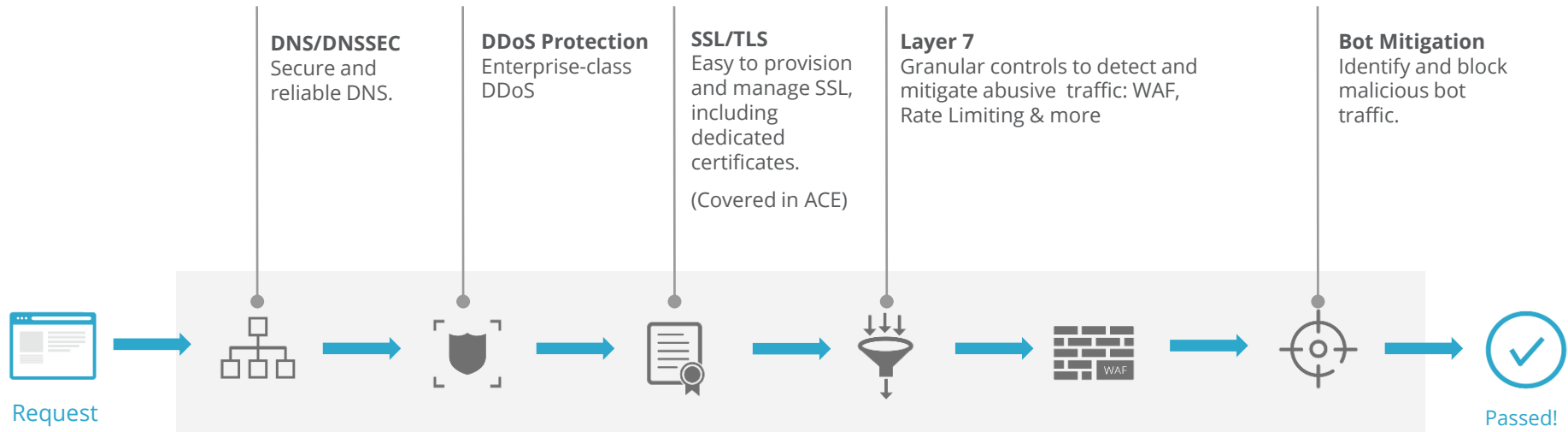
# Cloudflare Security Portfolio



# Cloudflare services across the OSI stack



# Cloudflare Security Services



## 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

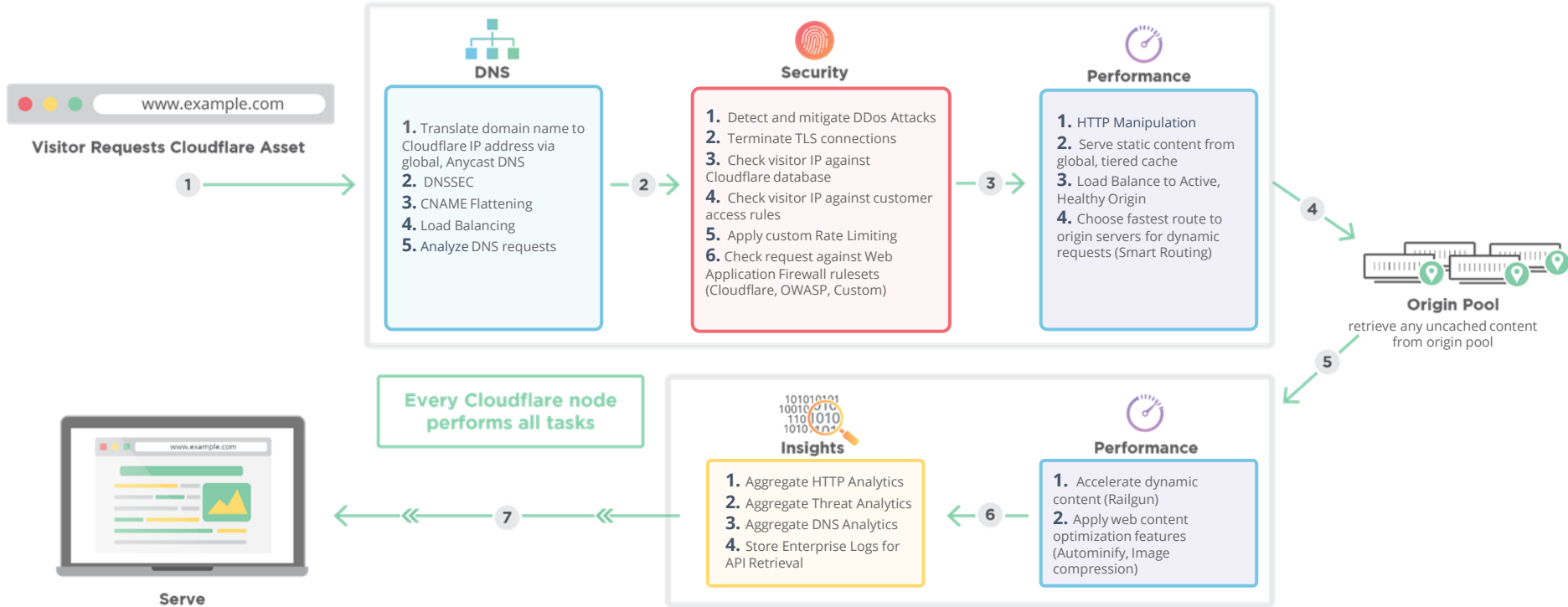
Creates an encrypted tunnel between an application's origin server and the nearest data center without opening a public inbound port.



### Workers

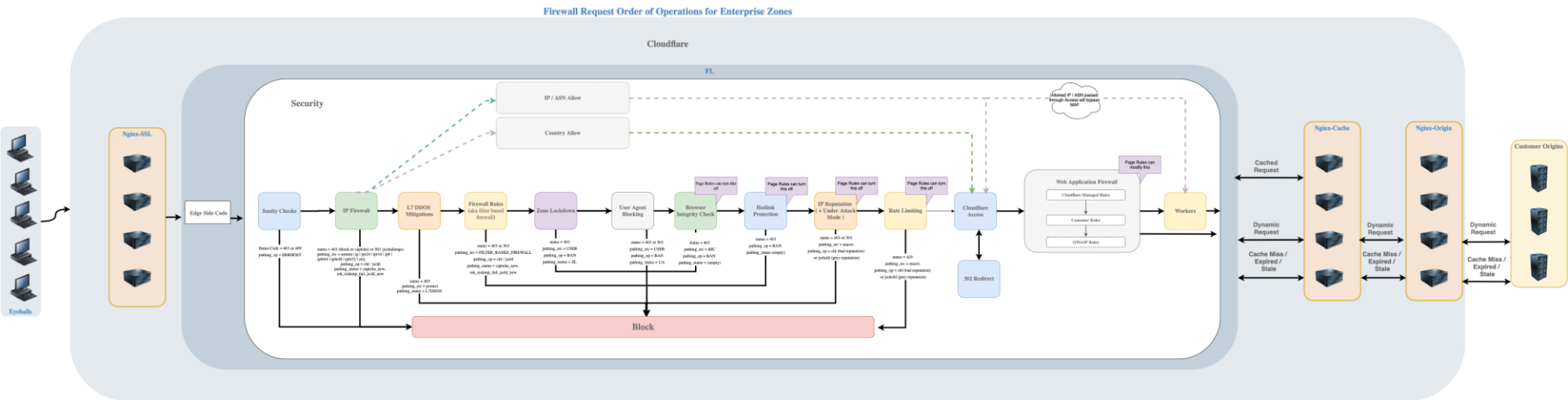
Runs JavaScript Service Workers to customize and configure apps on the edge.

# Review: Life Of A Request





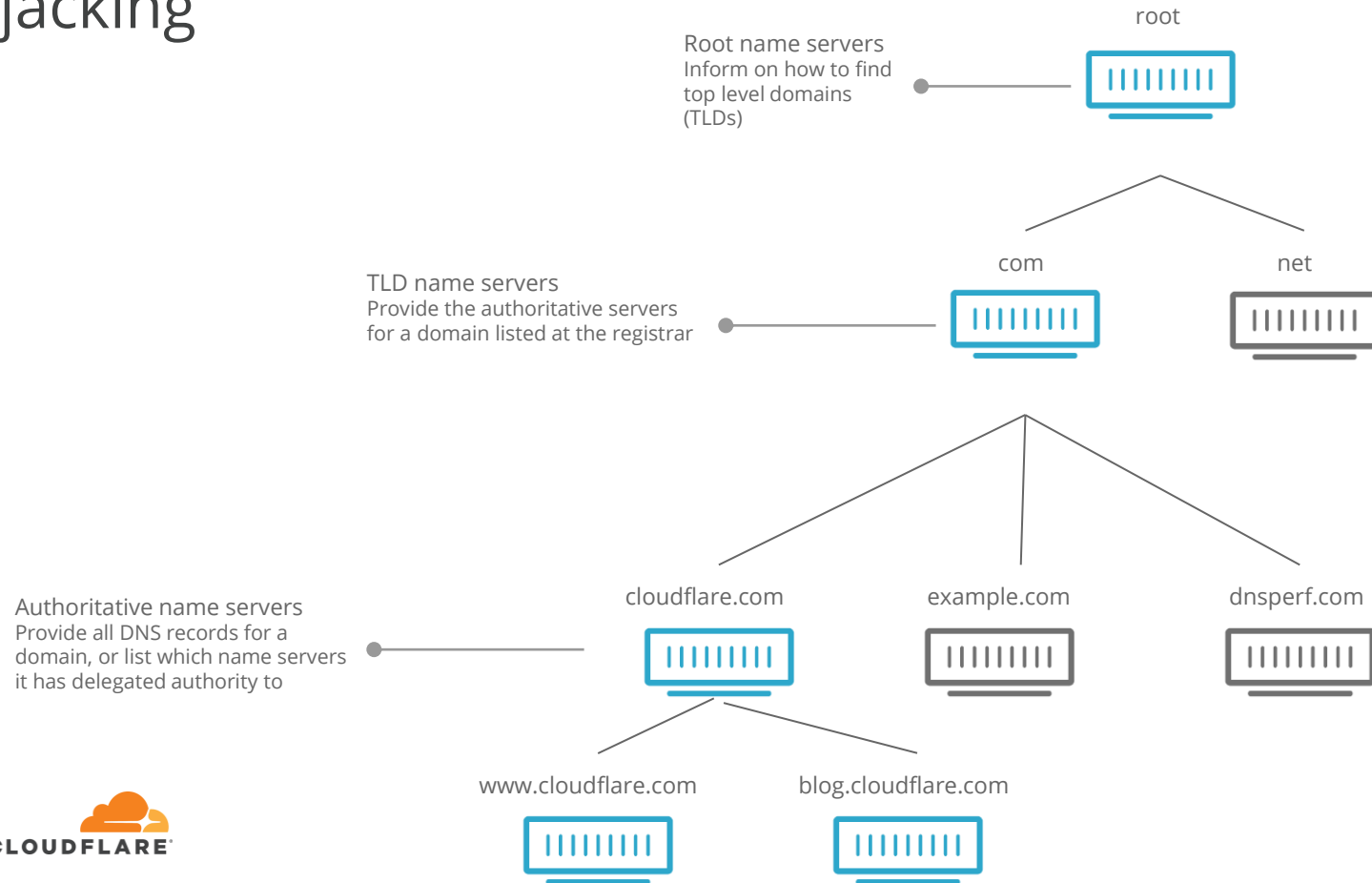
# Cloudflare Security – Order of Operations for ENT zones



Cloudflare 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



# 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:

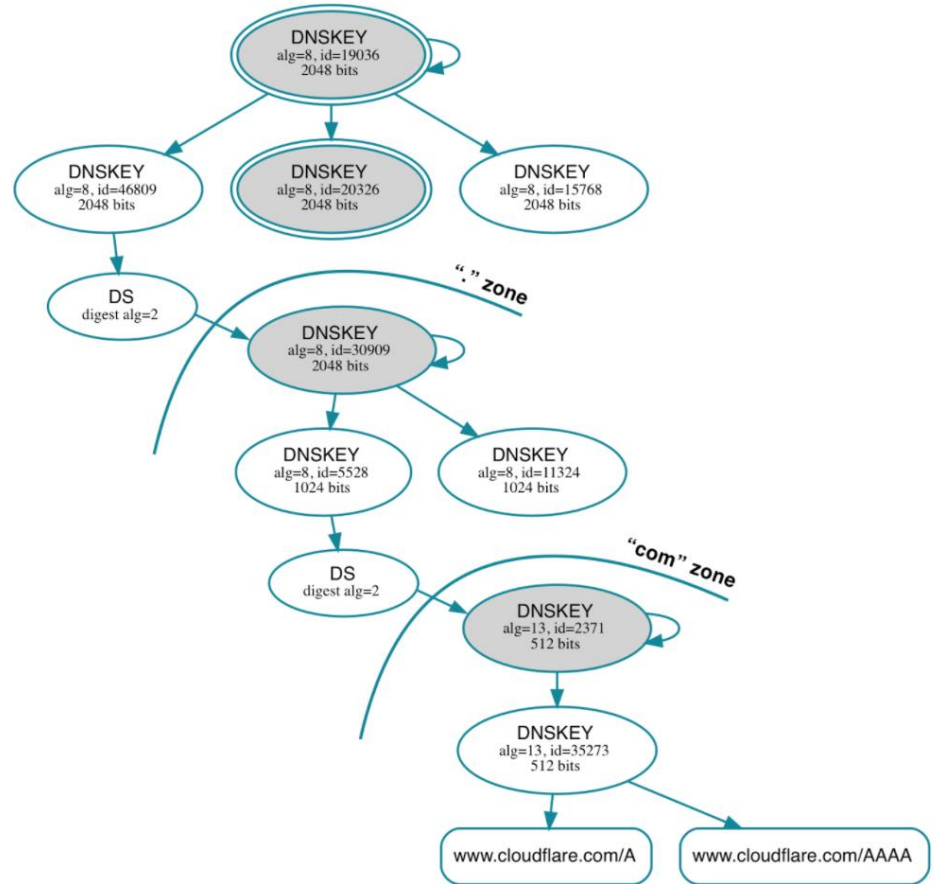
**RRSIG** - Contains a cryptographic signature

**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:

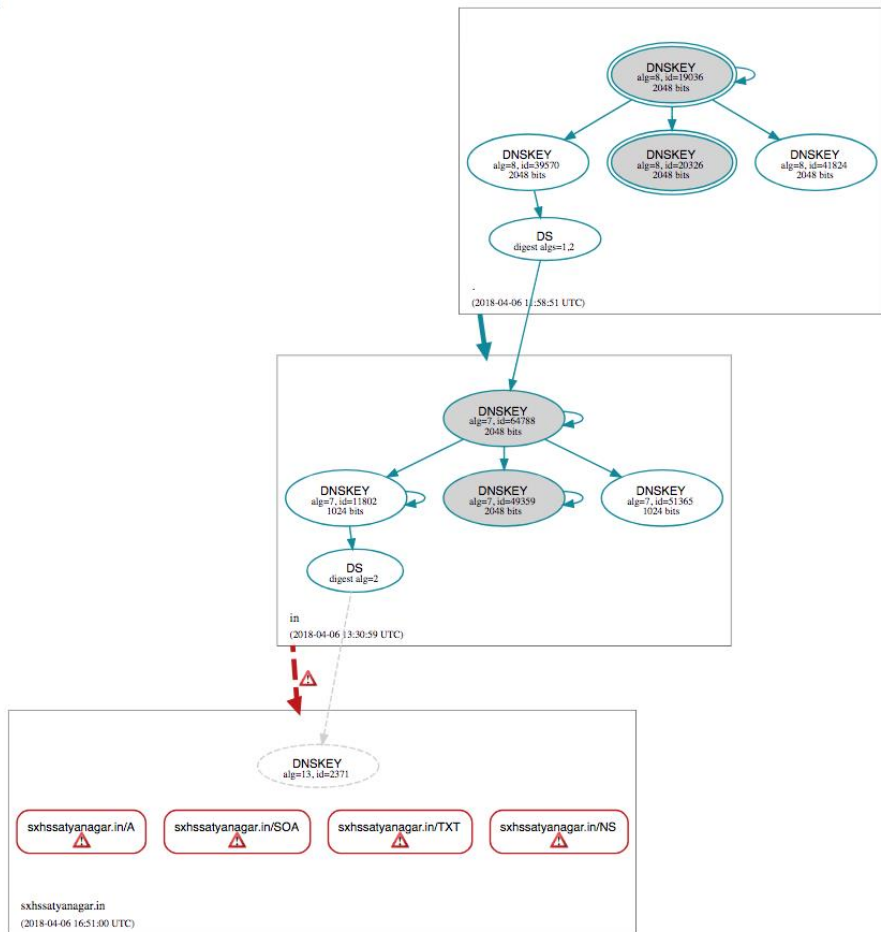
A customer intends to implement Cloudflare DNSSEC with CNAME setup? What's your recommendation?

# 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
lhG0gVSKK/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>

### DNSSEC

DNSSEC protects against forged DNS answers. DNSSEC protected zones are cryptographically signed to ensure the DNS records received are identical to the DNS records published by the domain owner.

DNSSEC for your domain will be automatically enabled in the next 24 hours.

🕒 DNSSEC is pending while we wait for the DS to be added to your registrar. This usually takes ten minutes, but can take up to an hour.

[Cancel Setup](#)

[Help](#) ▼

**What is DNSSEC and how does it work?**

A comprehensive writeup on how DNSSEC works can be found here: [How does DNSSEC work?](#)

**How do I test that DNSSEC is working on my website?**

Use <http://dnsviz.net/d/theburritobot.com/dnssec/> to see if DNSSEC is working.



## Lab - DNSSEC output for Cloudflare.com and brokendnssec.net

- Go to [dnsviz.net](https://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

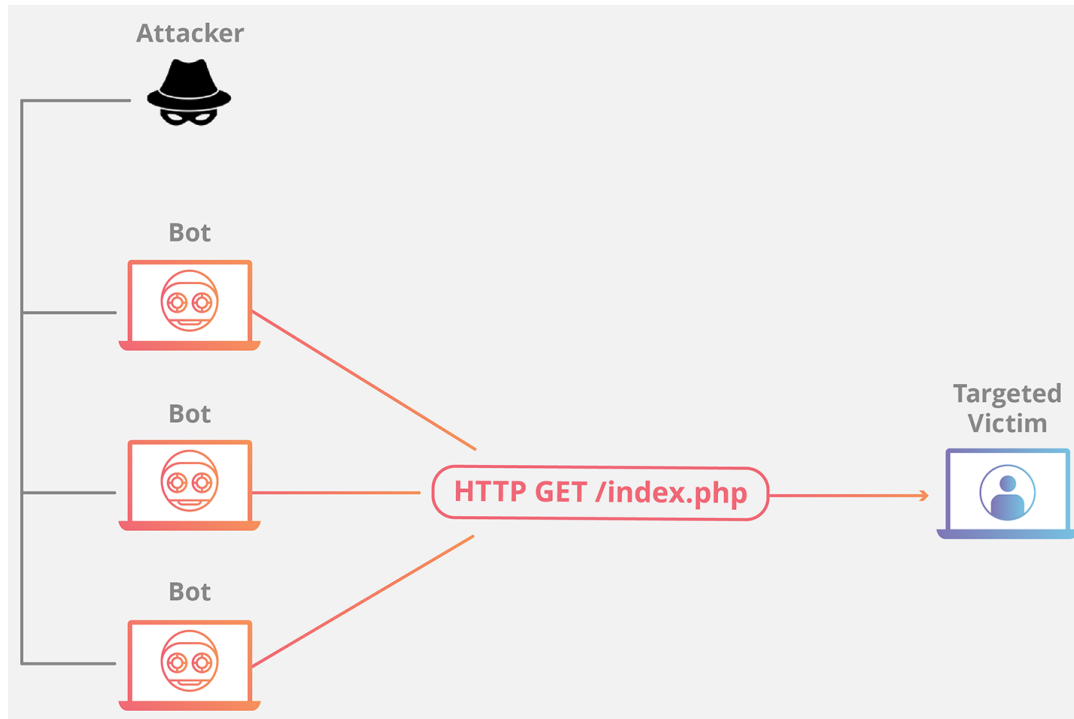


## Problems

- Disrupt normal traffic
- Impact service

## Solutions

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

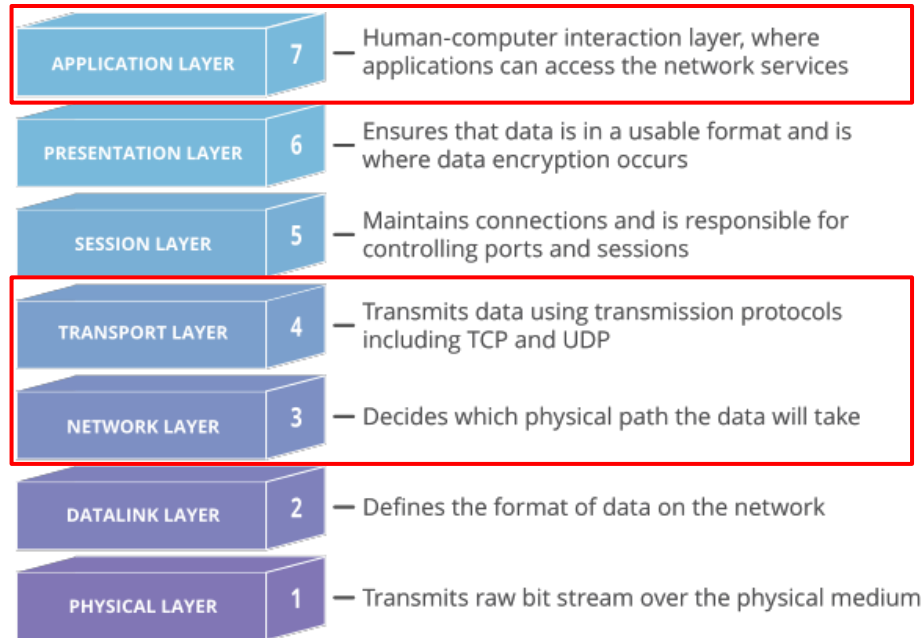


# DDoS attack layers



## Types

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



## OSI Model

# Layer 3 / 4 Attack Details

## Are

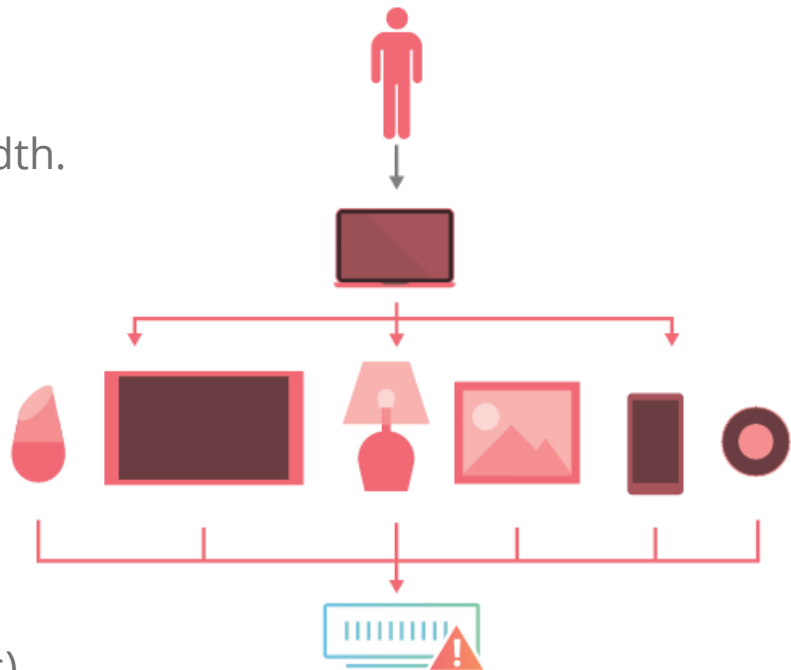
- Volumetric
- Target network infrastructure
- Degrade performance and consume bandwidth.

## 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)



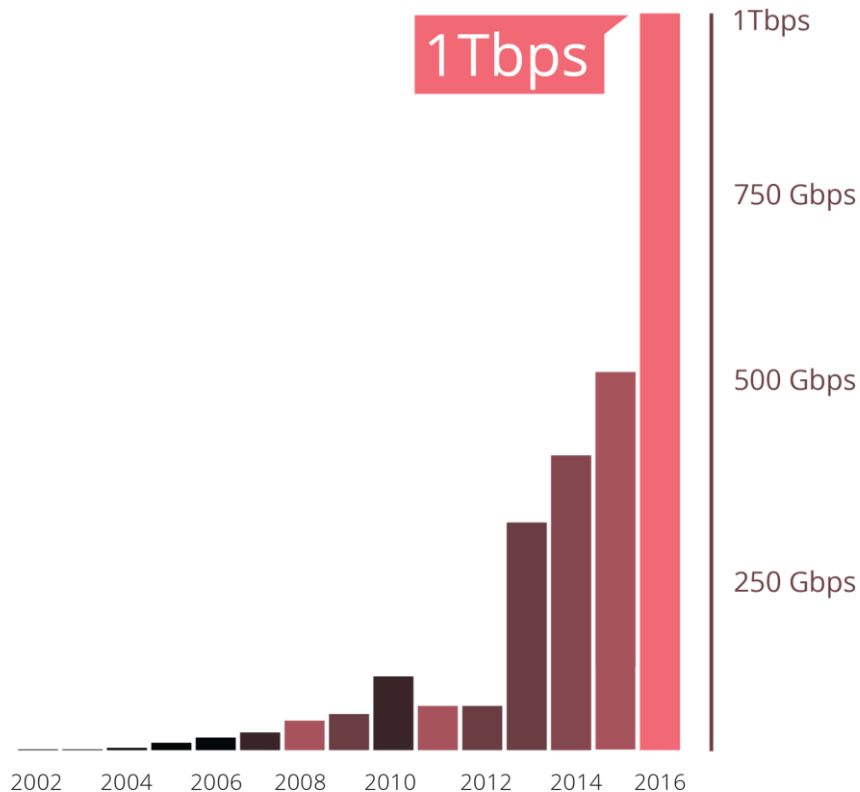
# Layer 7 Attacks (application layer)

## Types:

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

## Layered Mitigations:

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





# 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

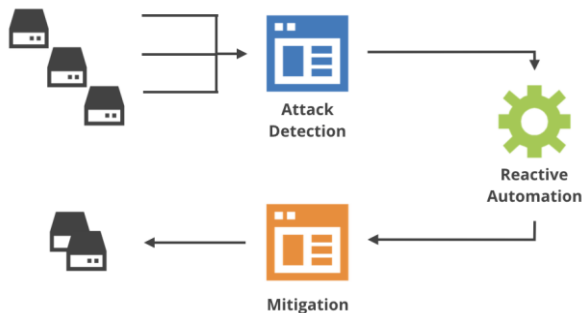
- Zero propagation time
- Synchronous routing
- No added latency; ongoing perf. improvements
- Immediate, automated mitigation, with no "cutover" required

# Gatebot & Gatekeeper



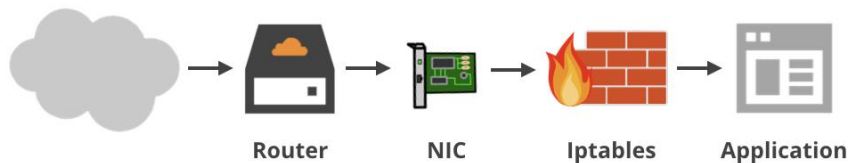
**Gatebot(global)/DosD(local)** - samples traffic, creates signatures that allow for automatic or manual mitigation

1. attack detection
2. reactive automation
3. mitigations

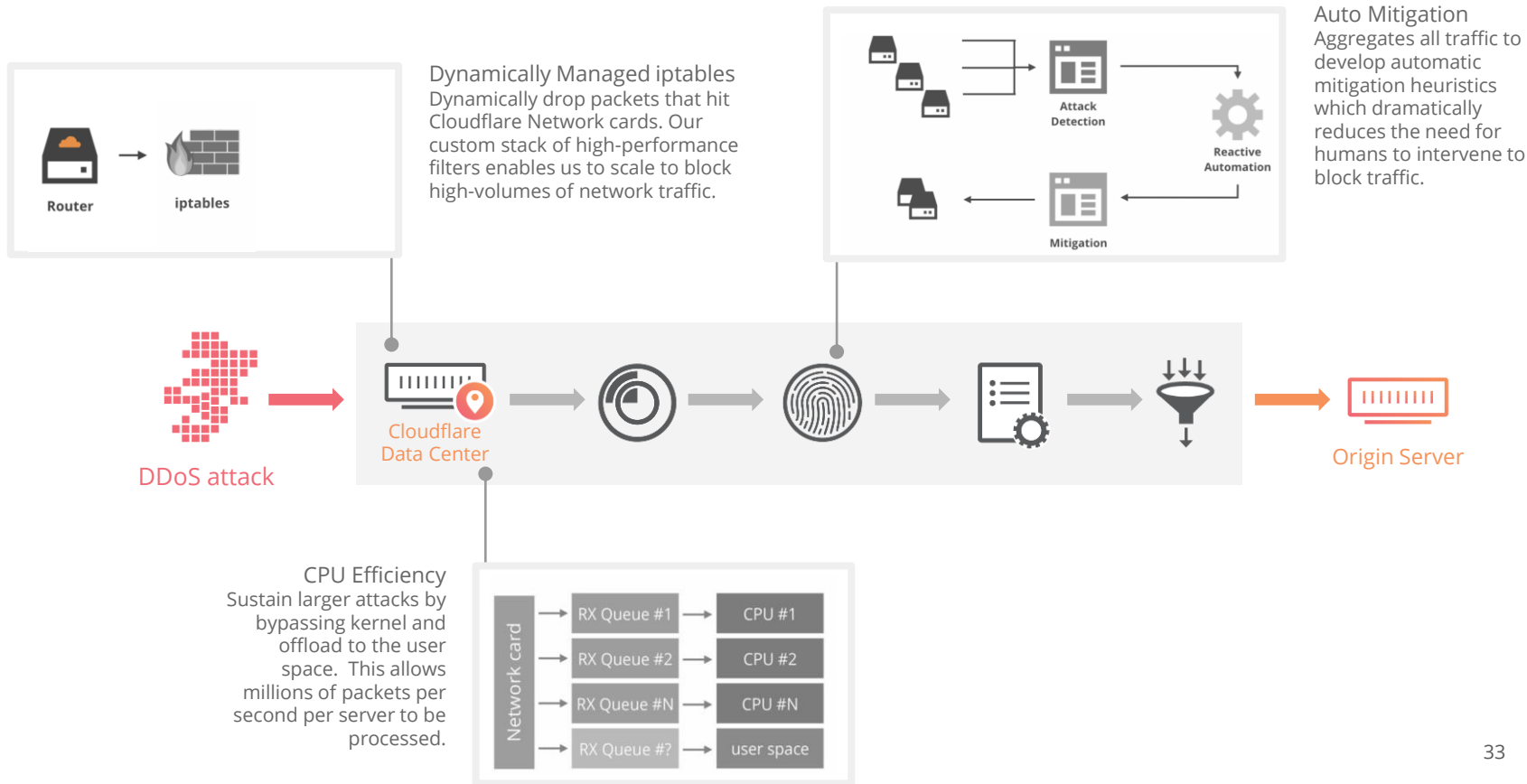


**Gatekeeper** - manages firewall mitigation for L3/L4 packet floods

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



# Cloudflare DDoS - Technical Advantage



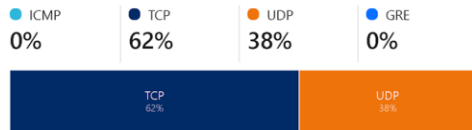
# DDoS Attacks and Trends

## Attacks

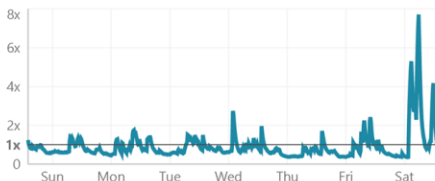
7 Days

### Network-level DDoS Attacks [Learn More](#)

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

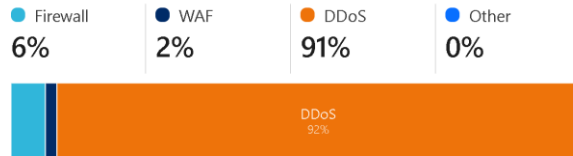


Change in Layer 3/4 DDoS attack volume over the selected time period. Learn how to secure your websites, applications, and networks against [DDoS](#) attacks.



### Application-level Attacks [Learn More](#)

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



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/>

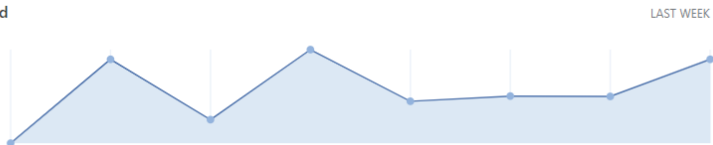
# Lab - Explore DDoS Analytics and Protections



## Denial-of-service attacks mitigated

TCP packets

33,263,600



## 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.	<a href="#">Learn more</a>
UDP Flood	Prevents attacks caused from a flood of UDP packets.	<a href="#">Learn more</a>
SYN Flood	Prevents attacks caused from a flood of TCP packets sent with SYN flag.	<a href="#">Learn more</a>
ACK Flood	Prevents attacks caused from a flood of TCP packets sent with ACK flag.	<a href="#">Learn more</a>
QUIC Flood	Prevents attacks caused from a flood of QUIC requests.	<a href="#">Learn more</a>
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

[Home](#)[Members](#)[Audit Log](#)[Billing](#)[Configurations](#)[Notifications](#)[← Back](#)

## Create Notification

Event Type

Passive Origin Monitoring

Billing Usage Alert

HTTP DDoS Attack Alert

# 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

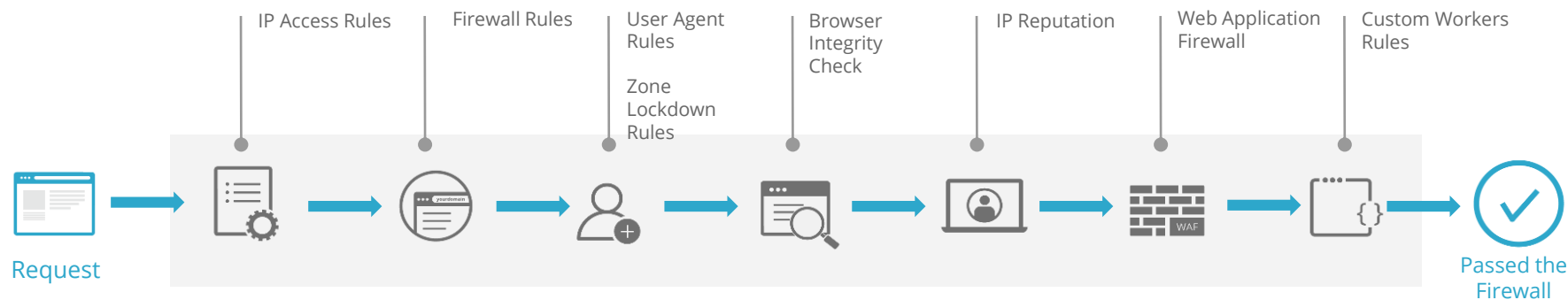
Analytics are available on the Firewall events pages



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

# // Firewall

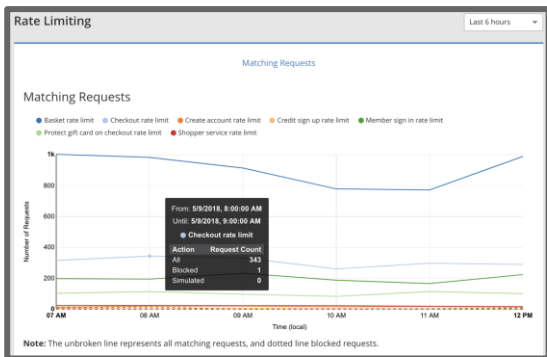
# Cloudflare Firewall Services Layer



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



## Firewall -> Overview

Firewall Events					
Requests affected by both IP Firewall and Web Application Firewall (WAF) rules.					
<input type="text" value="Search Firewall events"/>				Ray ID	<input type="text" value="Search"/>
Rule ID	Action Taken	IP Address	Loc.	Host	Date
Country	Block	2606:4700:2001:10b::42	US	www.jamesaskham.us	an hour ago
Country	Block	2606:4700:2001:10b::42	US	www.jamesaskham.us	an hour ago
100014	Block	2606:4700:2001:10b::42	US	www.jamesaskham.us	an hour ago
100014	Block	2606:4700:2001:10b::42	US	www.jamesaskham.us	an hour ago
100004	Challenge	122.189.210.214	CN	mostlygood.ga	a day ago
100004	Challenge	183.20.192.239	CN	c-term.tk	4 days ago

## Log Share

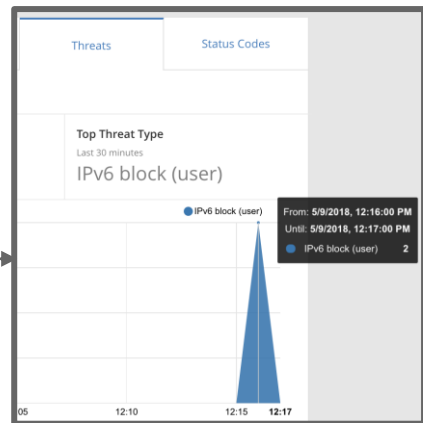
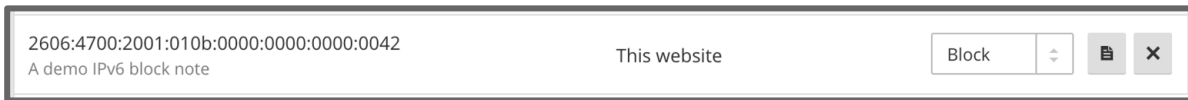
```
{
  "ClientIP": "2606:4700:2001:10b::42",
  "ClientRequestHost": "www.jamesaskham.us",
  "ClientRequestURI": "/",
  "EdgePathingOp": "chl",
  "EdgePathingSrc": "user",
  "EdgePathingStatus": "captchaNew",
  "EdgeResponseStatus": 403
}
```

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

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

# Firewall Actions: Blocks

## IP Block



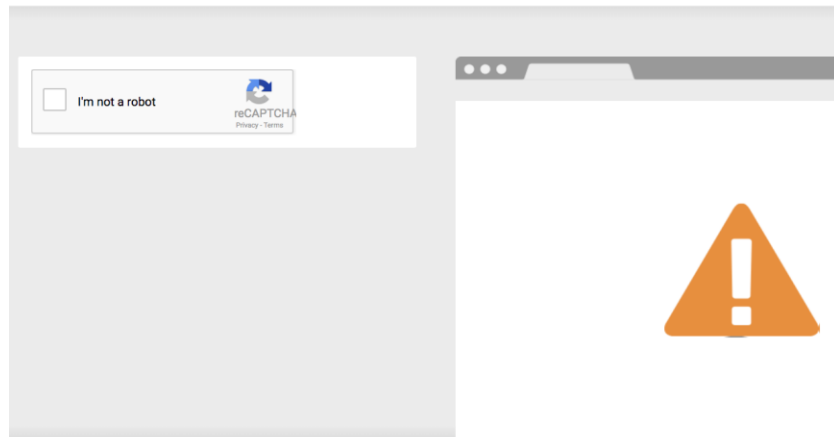
- Count as 'Cached Request' and 'Cached Bandwidth'
- Logged as 403 Status Code
- Logged in Analytics and ELS only
- Country Blocks DO appear in Firewall Events.

# 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'.

## One more step

Please complete the security check to access [www.jamesaskham.us](http://www.jamesaskham.us)



Why do I have to complete a CAPTCHA?

What can I do to prevent this in the future?

# 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.



### Checking your browser before accessing cloudflare.com.

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...

[DDoS protection by Cloudflare](#)  
Ray ID: 418704044bc4818a

# 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](#)



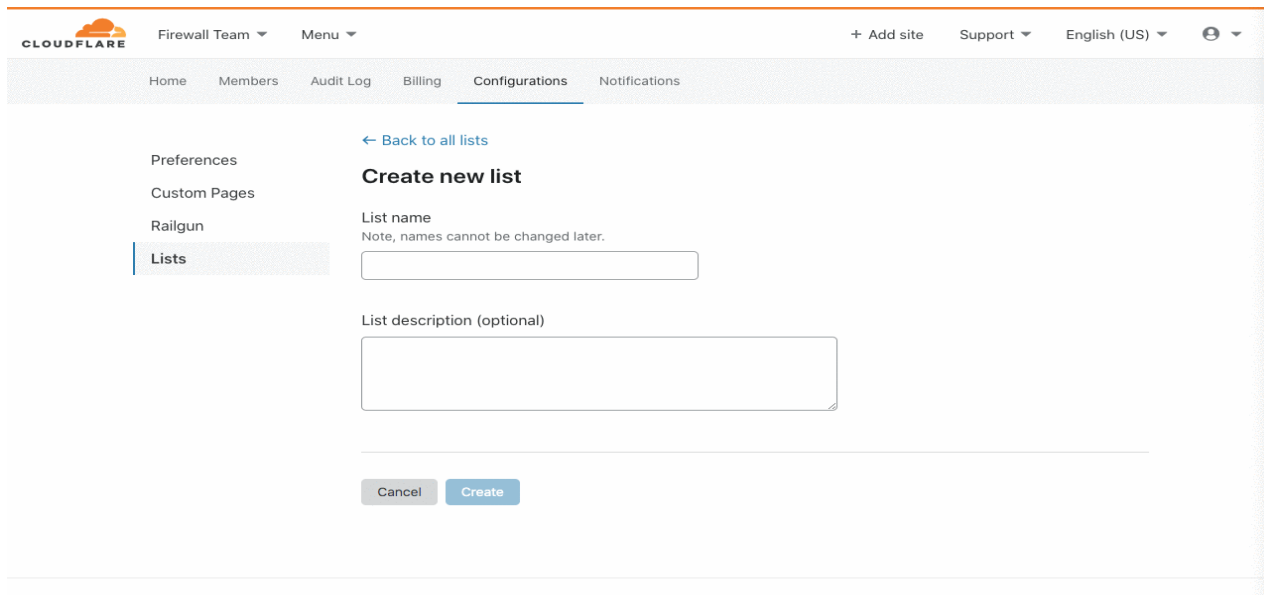


### **TASK:**

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.



The screenshot shows the Cloudflare dashboard interface for creating a new IP list. At the top, the Cloudflare logo is on the left, and navigation links for 'Firewall Team', 'Menu', '+ Add site', 'Support', 'English (US)', and a user profile icon are on the right. Below this is a horizontal menu with 'Home', 'Members', 'Audit Log', 'Billing', 'Configurations' (which is underlined), and 'Notifications'. On the left side of the main content area, there is a sidebar menu with 'Preferences', 'Custom Pages', 'Railgun', and 'Lists' (which is highlighted with a blue bar). The main content area has a heading 'Create new list' with a link '← Back to all lists' above it. Below the heading, there is a 'List name' field with a note 'Note, names cannot be changed later.' and a text input box. Below that is a 'List description (optional)' field with a larger text input box. At the bottom of the form are two buttons: 'Cancel' and 'Create'.

Cloudflare

Firewall Team ▾ Menu ▾

+ Add site Support ▾ English (US) ▾

Home Members Audit Log Billing Configurations Notifications

Preferences

Custom Pages

Railgun

Lists

← Back to all lists

**Create new list**

List name

Note, names cannot be changed later.

List description (optional)

Cancel Create

<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: 3a1664fd3468c5e • 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).

### Create a Zone Lockdown Rule

**Name**

Block all traffic to the staging and wiki sites unless it comes from corp HQ

**URLs**

Separate URLs by new line

staging.example.com/\*  
example.com/wiki\*

**IP Range**

Separate IP Addresses by new line

192.0.2.0/24  
2001:DB8::/64  
203.0.133.1

[Advanced Options](#)

Cancel

Save as Draft

Save and Deploy

# 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 subdomains 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

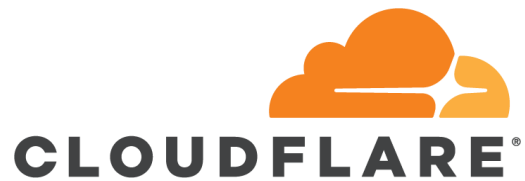


## End of Day 1 Summary

- 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



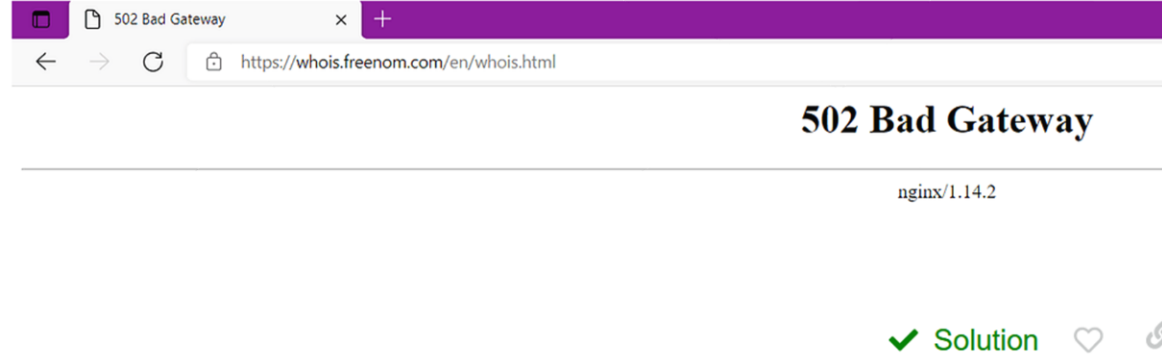
erictung MVP '21

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:



🔗 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

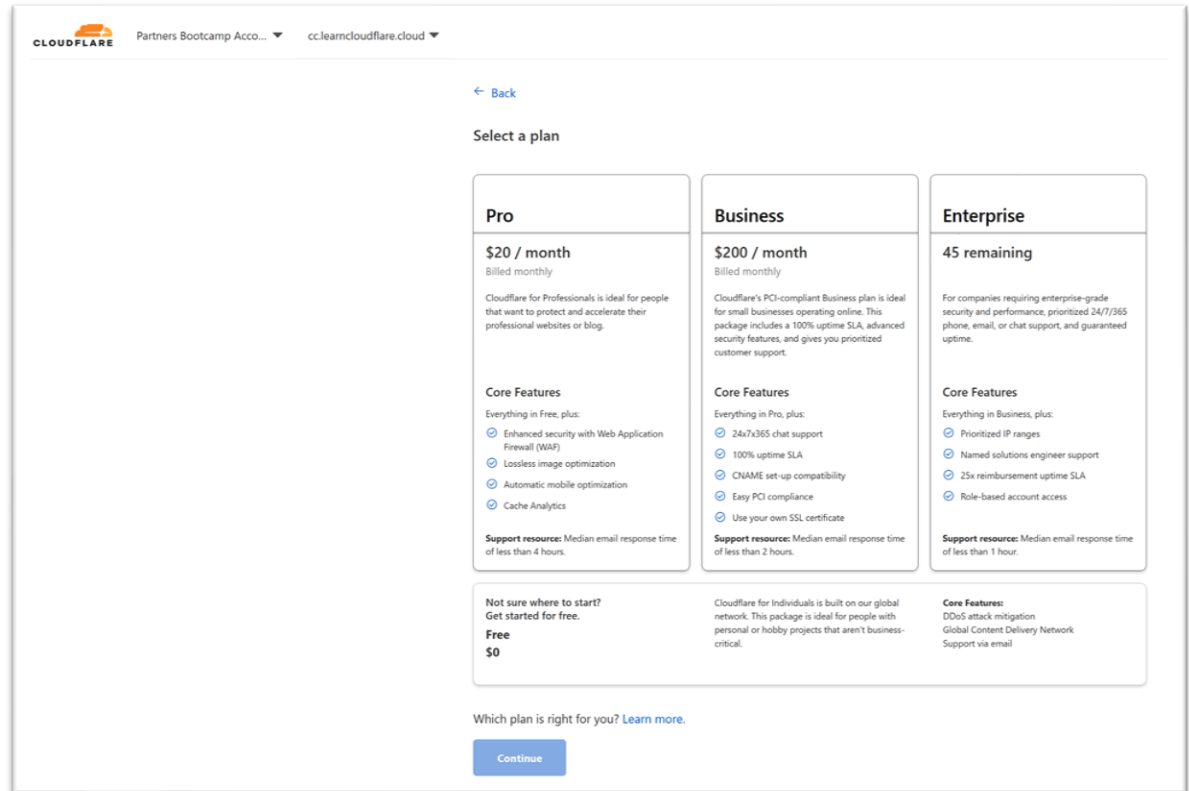
Accelerate and protect your site with Cloudflare

Enter your site (example.com):

**Add site**

# Steps to add Subdomain Support

## 3. Choose Enterprise plan for this training purpose



The screenshot shows the Cloudflare pricing page. At the top, there's a navigation bar with the Cloudflare logo, a dropdown menu for "Partners Bootcamp Acco...", and another dropdown menu for "cc.learncloudflare.cloud". Below the navigation bar, there's a "Select a plan" section. It contains three columns for different plans: Pro, Business, and Enterprise. Each column lists the plan name, price, billing cycle, a description, core features, and support resources. The Enterprise plan is highlighted with a "45 remaining" badge. At the bottom, there's a "Which plan is right for you? Learn more." link and a "Continue" button.

**Cloudflare** Partners Bootcamp Acco... cc.learncloudflare.cloud

[← Back](#)

Select a plan

Pro	Business	Enterprise
<b>\$20 / month</b> Billed monthly	<b>\$200 / month</b> Billed monthly	<b>45 remaining</b>
Cloudflare for Professionals is ideal for people that want to protect and accelerate their professional websites or blog.	Cloudflare's PCI-compliant Business plan is ideal for small businesses operating online. This package includes a 100% uptime SLA, advanced security features, and gives you prioritized customer support.	For companies requiring enterprise-grade security and performance, prioritized 24/7/365 phone, email, or chat support, and guaranteed uptime.
<b>Core Features</b> Everything in Free, plus: <ul style="list-style-type: none"><li>Enhanced security with Web Application Firewall (WAF)</li><li>Lossless image optimization</li><li>Automatic mobile optimization</li><li>Cache Analytics</li></ul>	<b>Core Features</b> Everything in Pro, plus: <ul style="list-style-type: none"><li>24x7x365 chat support</li><li>100% uptime SLA</li><li>CNAME set-up compatibility</li><li>Easy PCI compliance</li><li>Use your own SSL certificate</li></ul>	<b>Core Features</b> Everything in Business, plus: <ul style="list-style-type: none"><li>Prioritized IP ranges</li><li>Named solutions engineer support</li><li>25x reimbursement uptime SLA</li><li>Role-based account access</li></ul>
<b>Support resource:</b> Median email response time of less than 4 hours.	<b>Support resource:</b> Median email response time of less than 2 hours.	<b>Support resource:</b> Median email response time of less than 1 hour.

**Not sure where to start?**  
Get started for free.  
**Free**  
**\$0**

Cloudflare for Individuals is built on our global network. This package is ideal for people with personal or hobby projects that aren't business-critical.

**Core Features:**  
DDoS attack mitigation  
Global Content Delivery Network  
Support via email

Which plan is right for you? [Learn more.](#)

[Continue](#)

# Steps to add Subdomain Support

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

## Add DNS records

Cloudflare needs DNS records to speed up and protect your site

- ☐ **Quick Scan** Recommended  
Scan for common hostnames and record types  
Intended for personal or small websites
- ☐ **DNS file upload**  
Add records with a DNS file from your current provider  
Intended for websites with a large number of records
- ☒ **Manual entry**  
Add records manually

**Continue**

# Steps to add Subdomain Support

## 5. Click **Continue**


[← Back](#)


**Manual entry**

Cloudflare needs DNS records to protect and accelerate your site. If you have an existing DNS provider, we recommend adding DNS records using the [Quick Scan](#).

**Add more DNS records for cc.learncloudflare.cloud**

Proxy traffic for A, AAAA, and CNAME records by clicking the cloud icon.

 Proxied: Accelerates and protects traffic

 DNS resolution only: Bypasses Cloudflare

**Note:** Records with no cloud icon use DNS resolution but cannot be proxied.

DNS management for **cc.learncloudflare.cloud**

[+ Add record](#)

[Advanced](#)

Type	Name	Content	TTL	Proxy status
------	------	---------	-----	--------------


[Continue](#)



# Steps to add Subdomain Support

## 6. Click **Done, check nameservers**

### Change your nameservers




**Pointing to Cloudflare's nameservers is a critical step in activation and must be complete for Cloudflare to optimize and protect your site.**

🔗 **Nameservers** are your primary **DNS** controller and identify the location of your domain on the internet.

1. **Determine** your registrar via [WHOIS](#).
2. **Log in** to the **administrator account** for your domain registrar
3. **Remove** the following nameservers


suzanne.ns.cloudflare.com

guy.ns.cloudflare.com
4. **Add** Cloudflare's nameservers



laura.ns.cloudflare.com

[Click to copy](#)



pablo.ns.cloudflare.com

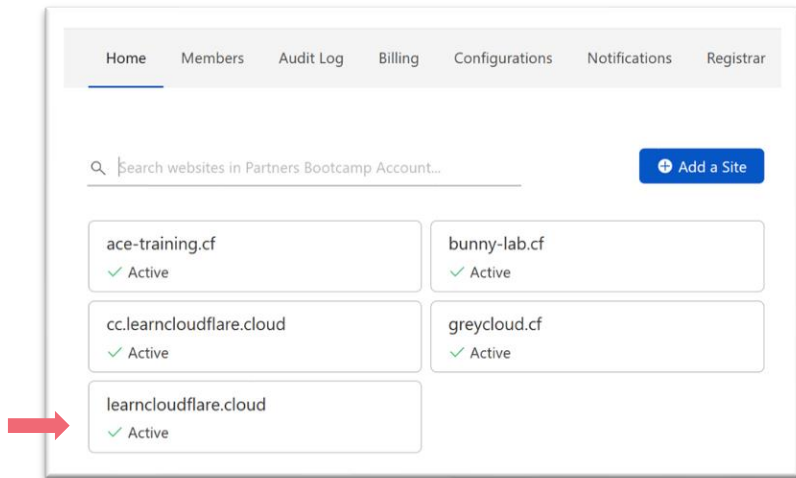
[Click to copy](#)
5. **Save** your changes

Registrars can take 24 hours to process nameserver updates. You will receive an email when your site is active on Cloudflare.

**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

Q

Search DNS Records

📄

Advanced

Type	Name	Content	TTL	Proxy status	
NS	cc	pablo.ns.cloudflare.com	Auto	DNS only	<a href="#">Edit</a> ▶
NS	cc	laura.ns.cloudflare.com	Auto	DNS only	<a href="#">Edit</a> ▶

cc.learncloudflare.cloud

✓ Active