DDOS: DDo’s and DDon’ts

DrupalCon 2016

Agenda

- What is DDoS
- Detecting DDoS Attacks
- DDoS Prevention
- Improving Performance
- Questions

Glossary

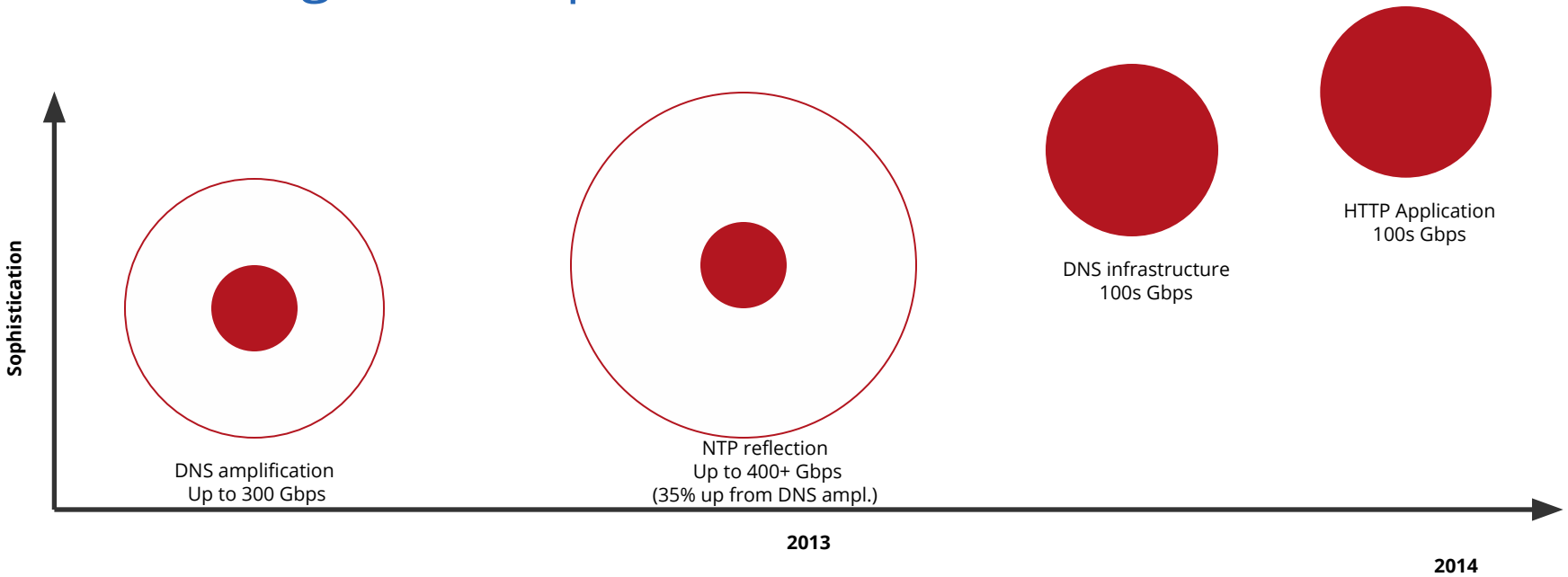
- **DDoS** - Attempt to make a server or network resource unavailable to Internet users
- **WAF** - Web Application Firewall, filter that applies a set of rules to an HTTP conversation
- **DNS** - Domain name system answers queries with IPs
- **OSI** - Open System Interconnection Model
  - **Layer 3 & 4** - Network and Transport layers (IPv4 & IPv6, TCP, UDP)
  - **Layer 7** - Application layer (Chrome, Firefox)
- **CDN** - system of distributed servers that deliver content to a user based on the location of the user, the origin of the webpage and a content delivery server

Ransom Notes


Send BITCOIN
&AWAIT FURTHER
INSTRUCTIONS

History of DDoS

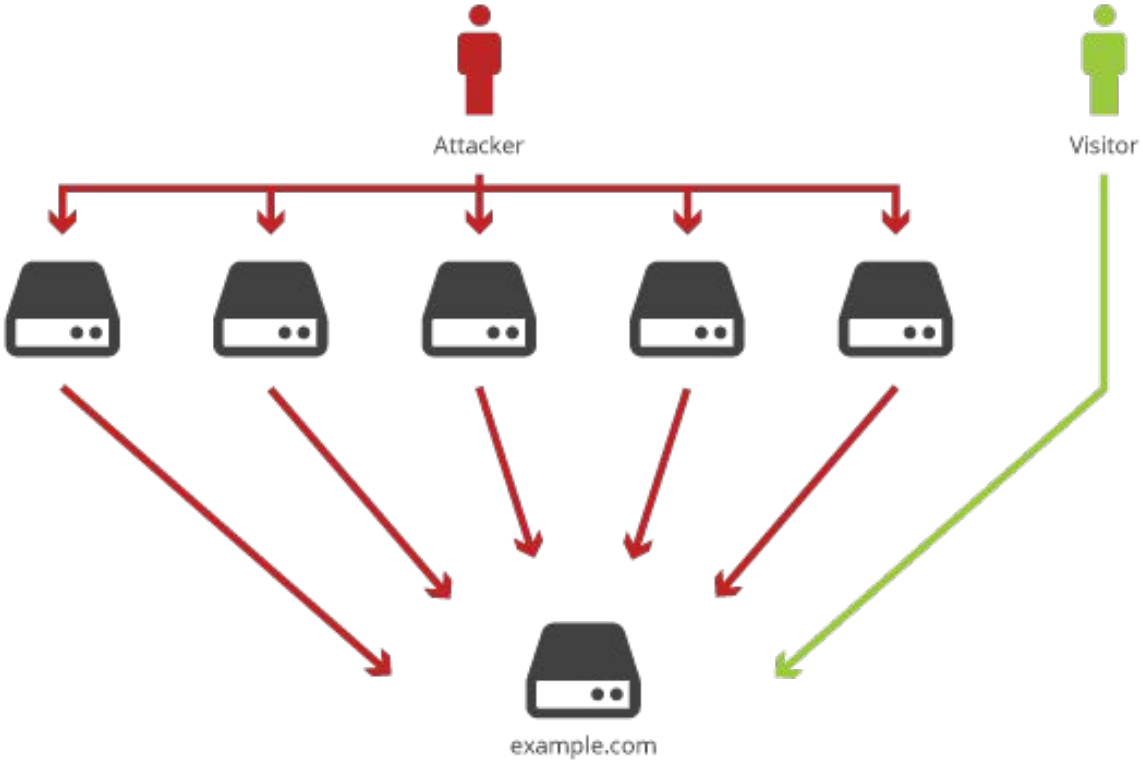
The Evolving Landscape of DDoS Attacks



ATTACK TYPE	TREND
• Volumetric Layer 3 / 4	⬇
• DNS Infrastructure	⬆
• HTTPS application	⬆
• Origin: 100s of countries	⬆

More sophisticated DDoS mitigation and larger surface area to block volumetric attacks has forced hackers to change tactics. New DNS infrastructure and HTTP layer 7 attack signatures that mimic human-like behavior are increasing in frequency.

Layer 3 / 4 Attacks

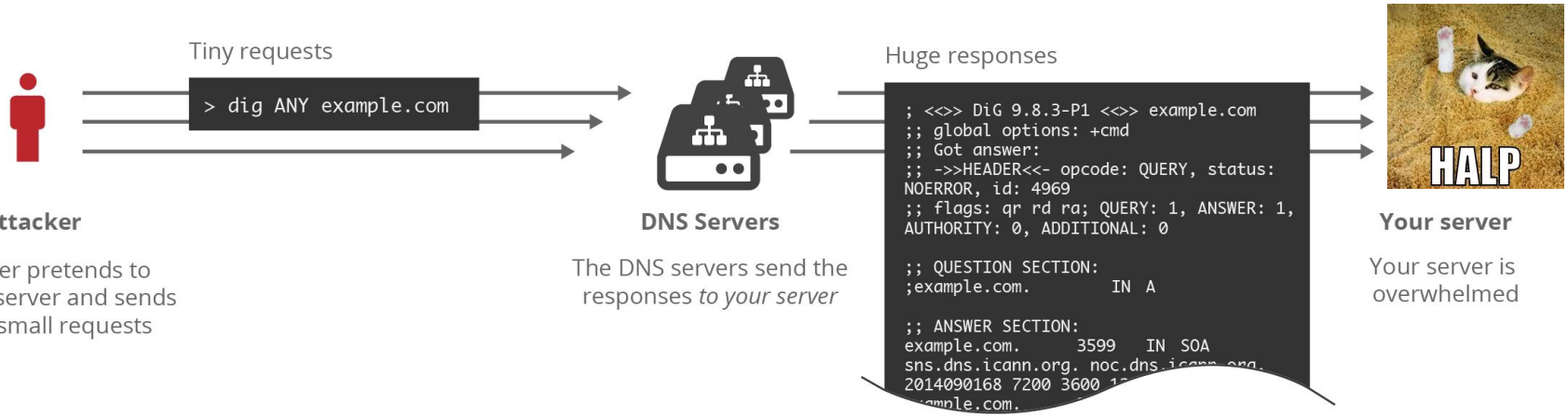


CLOUDFLARE

DNS / NTP Amplification attack

UNPROTECTED

Attackers pretending to be your server make tiny requests to thousands of DNS or NTP servers. Those servers return huge responses to your server, knocking it offline.



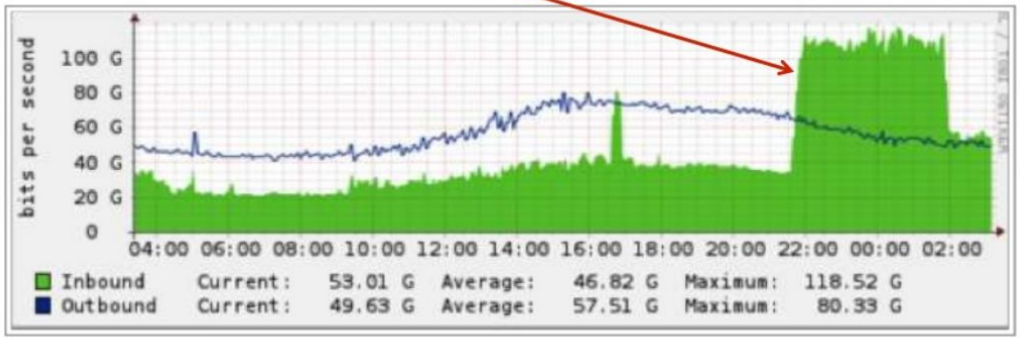
CLOUDFLARE

Exhausts network connection

DNS amplification attacks in action

Wednesday, March 20th

“Instant on”



~75Gbps attack

CLOUDFLARE

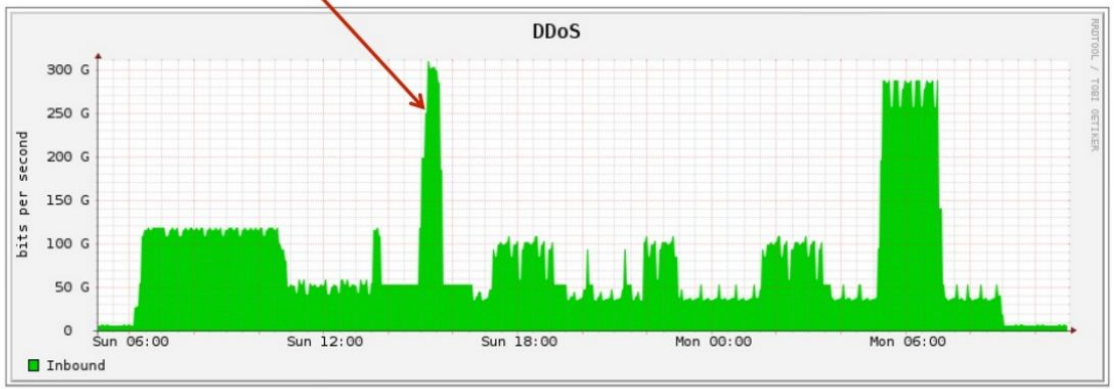
DNS amplification attacks in action

3 days later...

DNS amplification attacks in action

Sunday, March 24th thru 25th

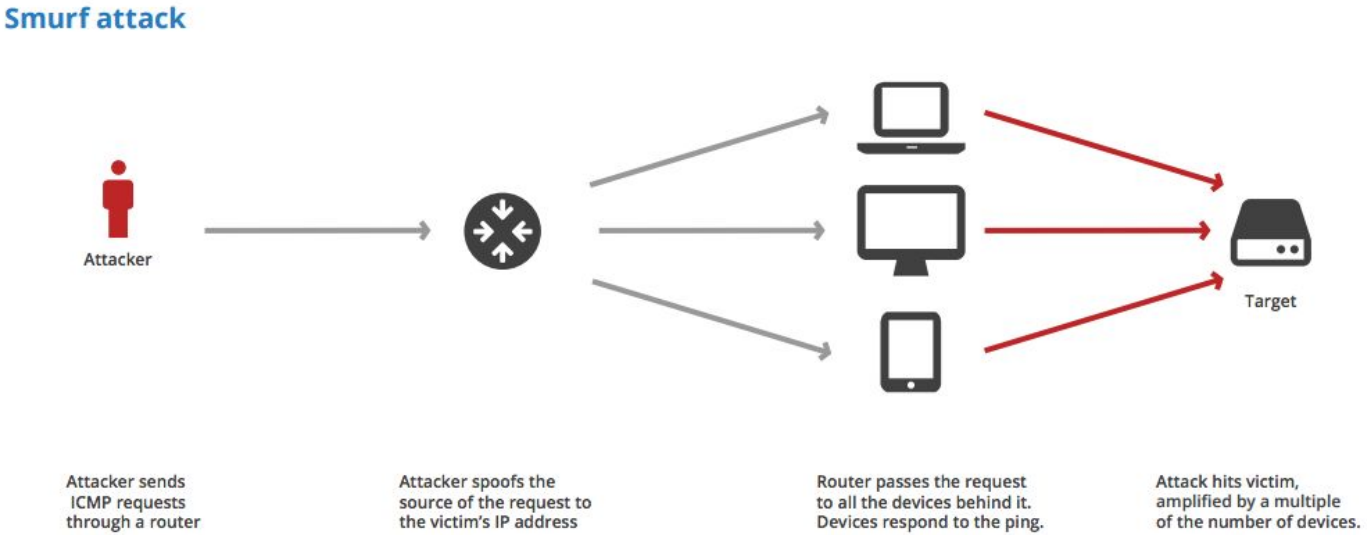
"Instant on"



Peaks of the attack reached 309Gbps

CLOUDFLARE

SMURF attacks



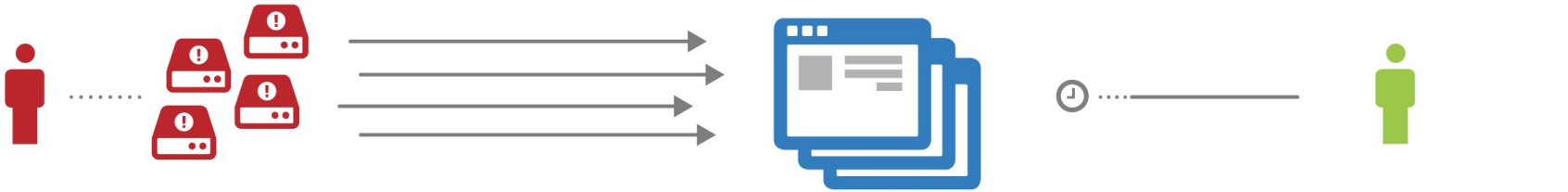
SMURF attacks are largely a thing of the past. For the most part, network operators have configured their routers to disable the relay of ICMP requests sent to a network's broadcast address.

CLOUDFLARE

Layer 7 attacks

UNPROTECTED

Attackers use millions of compromised machines to launch a sophisticated attack that mimics real users and overloads the slow points in your web property.



Network of compromised machines

Network of compromised machines controlled by attackers using advanced software

Your software or website

Mimics the patterns of real users and takes advantage of your software
e.g. requests photos over and over

Your visitors

Good users are stuck waiting because your CPU is overloaded

CLOUDFLARE

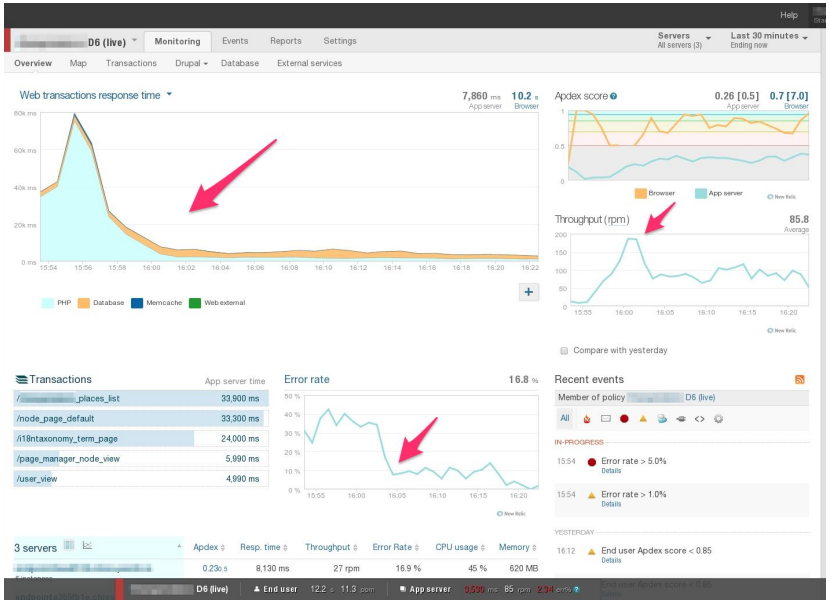
Exhausts CPU

Layer 7: Drupalgeddon / SQL Injection

CLOUDFLARE

Detecting DDoS Attacks

What an attack looks like...




```
 Id        Date            Severit   Type
Message

 3161818   16/Jun 16:45    notice
spambot          Blocked registration:
email=supplyweqz@gmail.com,ip=120.
43.21.95

 3161817   16/Jun 16:45    notice    user
Login attempt failed for JulianHut.

 3161794   16/Jun 16:44    notice    user
Login attempt failed for Julianml.
```

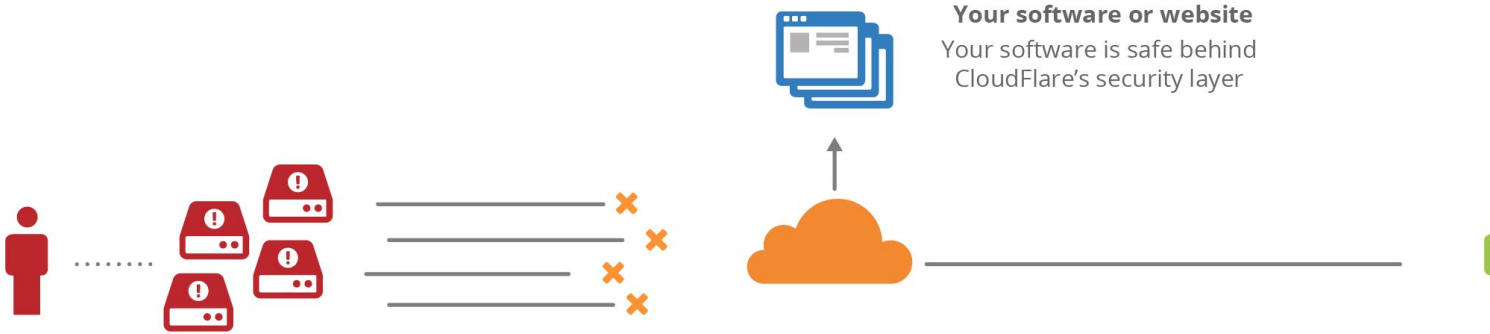
CLOUDFLARE

DDoS Prevention

Common Spam Traffic Defense Methods

- CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart
- Timegate (Time Difference)
- Honeypot
- Content analysis
- Visitor reputation

WAF: Web Application Firewall



Your software or website

Your software is safe behind CloudFlare's security layer

Network of compromised machines

Network of compromised machines controlled by attackers using advanced software

CloudFlare

The attacks mimic the patterns of real users but are blocked by CloudFlare

Your visitors

Good users are let through, and are accelerated by CloudFlare

CLOUDFLARE

CloudFlare Drupal WAF Rules

D0000 - Block Large Requests to xmlrpc.php for Drupal CMS

D0002 - Block requests with odd array arguments

D0001 - Block Requests to xmlrpc.php for Drupal CMS

URIs:

/xmlrpc.php -- most common

/?q=node&destination=node

/blog/xmlrpc.php

/user/login/

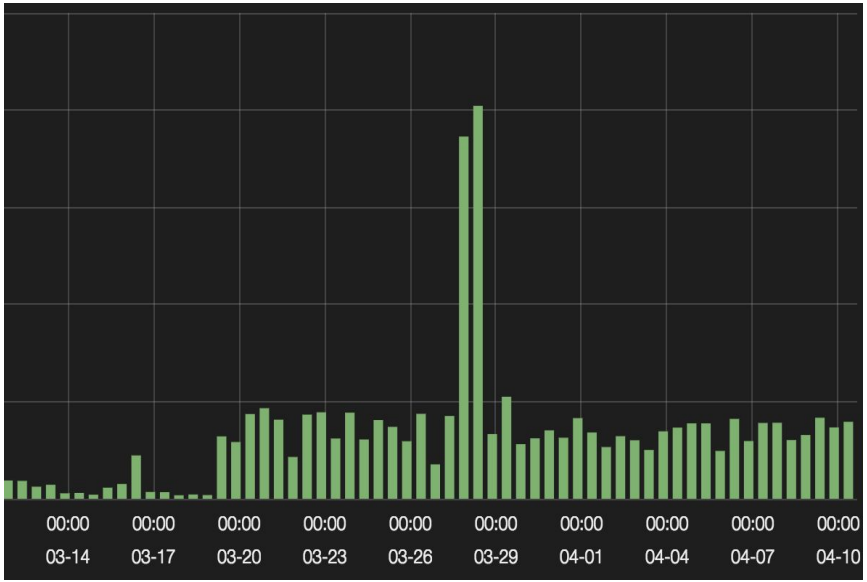
HTTP Method:

POST -- most common

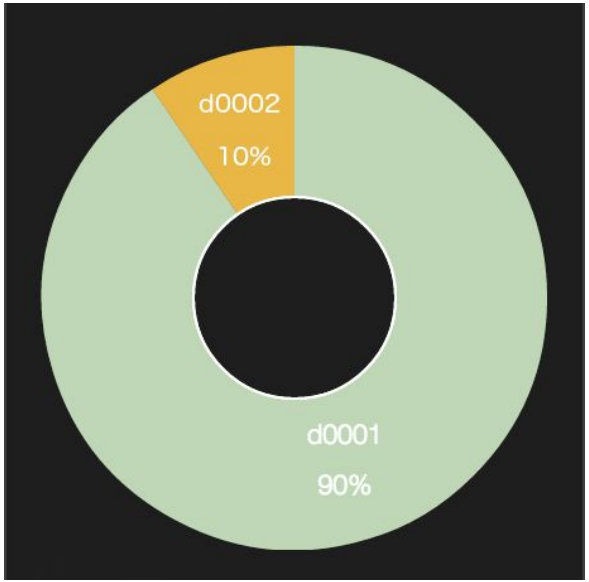
GET

CloudFlare Drupal WAF Triggers

Frequency of Triggers over 30 Days



Percentage of trigger by WAF Rule



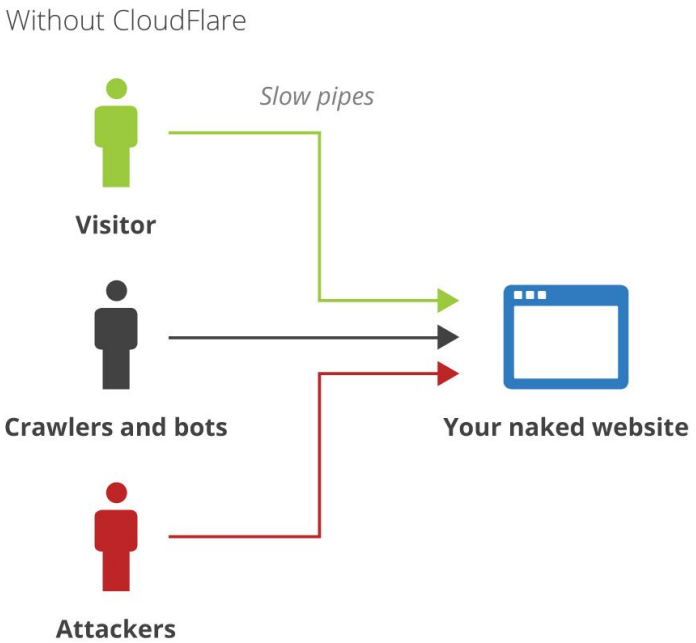
CLOUDFLARE

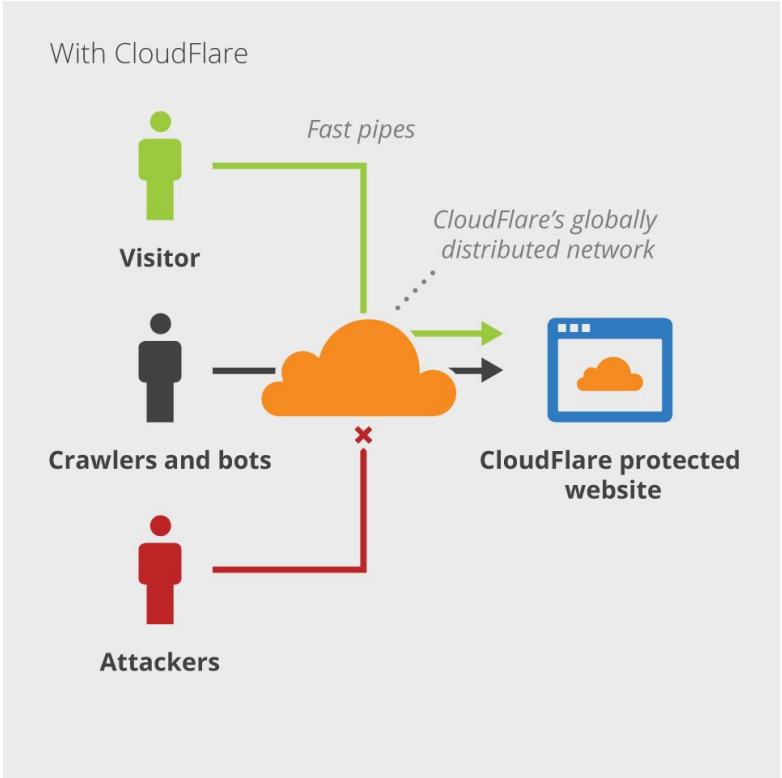
Improving Performance: CDN

CDN

CLOUDFLARE

CDN





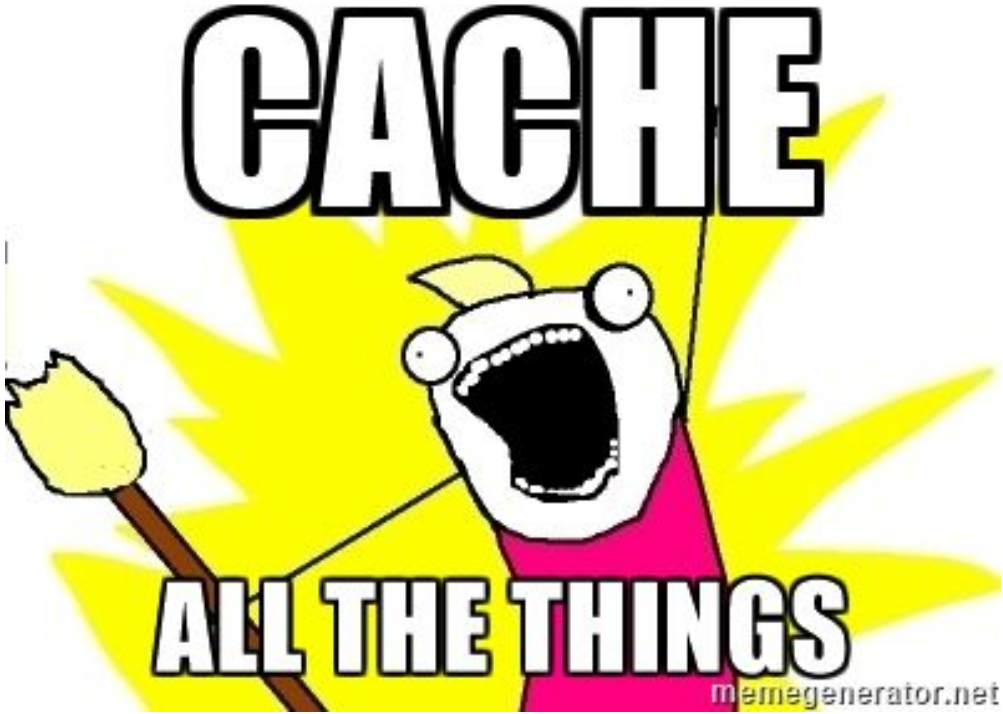
CLOUDFLARE

CDN: Anycast network

- **Global:** 28 data centers in over 15 countries
- **Secure:** built into every layer and every protocol
- **Robust:** every node can perform any task. Anycast HTTP routing
- **Reliable:** built-in redundancy, load balancing, and high-availability

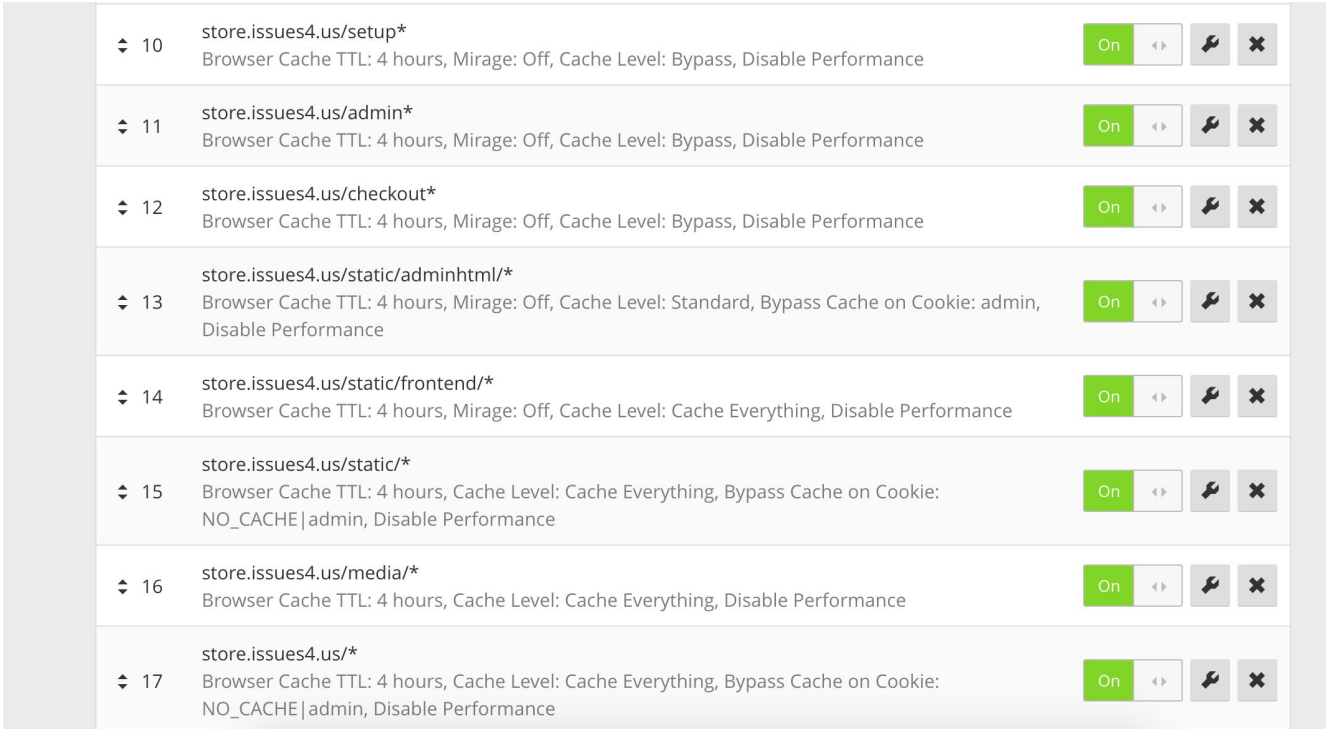
CLOUDFLARE

CDN: Caching



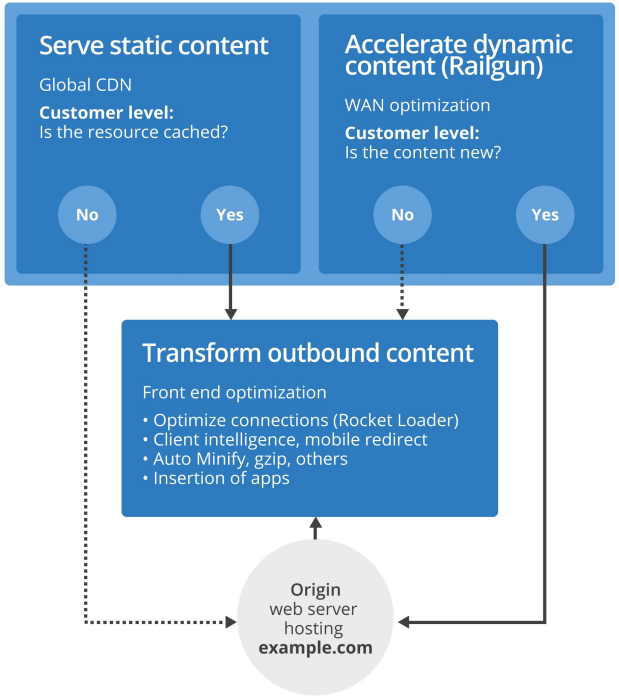
CLOUDFLARE

Page Rules for Drupal



CLOUDFLARE

CDN Performance boost



- **Improve Performance**: CloudFlare caches static content by default (JS, CSS, images). Custom caching options
- **Accelerate Dynamic Content (Railgun™)**: WAN optimization tool to compress and accelerate dynamic pages. Up to 99.6% compression ratio & 7.3x performance gain
- **Edge Side Code**: deploy powerful logic that alters HTTP requests and responses on the fly, without added latency
- **Front End Optimization**: auto-minify, image optimization, JS bundling
- **Client Intelligence:** optimization for network and device type

CLOUDFLARE


THANKS FOR WATCHING MY PRESENTATION
ANY QUESTIONS???
memegenerator.net

CLOUDFLARE