



Managed Security (Day 2)

Introduction and Deployment of Cloudflare's Security Solutions

Agenda

Cloudflare Security Services (ASA)

WAF

Firewall Rules

Bot Management

Rate Limiting

Spectrum

Summary of Security Services

Instructors

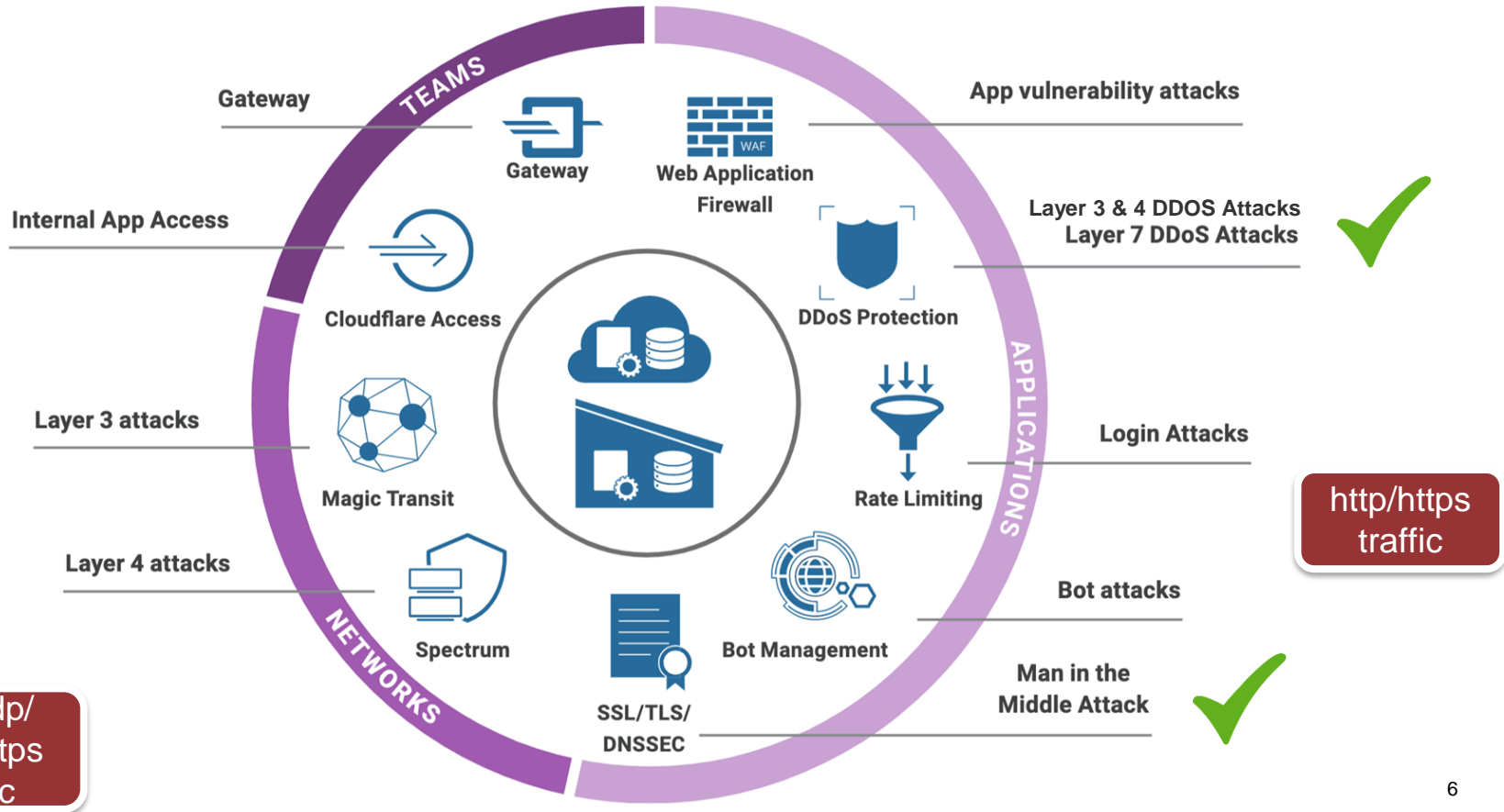


Chrisanthy Carlane
Partner Tech Enablement
ccarlane@cloudflare.com



Declan Carlin
Partner Solution Engineer
EMEA
declan@cloudflare.com

Cloudflare Security Portfolio



// WAF

WAF Fun Facts

- Cloudflare WAF processing times is $<0.3\text{ms}$
- WAF configuration change takes about 30 seconds to update globally vs other competitor which may take 15 min – a few hours for the change to activate
- Cloudflare WAF blocks more than 57 billion cyber threats per day, equal to 650k blocked HTTP requests per second (as of Q4 2020)

Reference: <https://www.cloudflare.com/static/media/pdf/cloudflare-datasheet-waf.pdf>

Cloudflare Firewall Overview - WAF Detail

- Advanced 'Layer 7' inspection of traffic.
- WAF checks Request URI (start-line), HTTP headers and body for **Anomalies** and **Signatures**.
- WAF 'module' scans every request in <1ms.
- Comprises three packages:
 - **OWASP ModSecurity Core Ruleset**
 - **Cloudflare Ruleset**
 - **Firewall Rules**
- Often a requirement of customers looking to maintain/achieve PCI compliance.

The diagram illustrates the structure of an HTTP request. It shows the following components from top to bottom:

- start-line:** A red box highlights the text `POST / HTTP/1.1`. An arrow points from the label 'start-line' to this box.
- HTTP headers:** A series of header lines: `Host: localhost:8000`, `User-Agent: Mozilla/5.0 (Macintosh;...)... Firefox/51.0`, `Accept: text/html,application/xhtml+xml,..., */*;q=0.8`, `Accept-Language: en-US,en;q=0.5`, `Accept-Encoding: gzip, deflate`, `Connection: keep-alive`, `Upgrade-Insecure-Requests: 1`, `Content-Type: multipart/form-data; boundary=-12656974`, and `Content-Length: 345`. A vertical label 'HTTP headers' is positioned to the right of these lines.
- empty line:** A blue box highlights an empty line. An arrow points from the label 'empty line' to this box.
- body:** A dashed box highlights the text `-12656974` followed by `(more data)`. An arrow points from the label 'body' to this box.

Cloudflare Firewall Overview - Cloudflare Managed Rules

- Rules that were created by CF engineering.
- Specific to known vulnerabilities that impact specific CMS's, languages and software libraries.
- CVE = Common Vulnerability Exploit.
- **Signature based** detection system.
- New rules commonly pushed to 'Cloudflare Specials' rule group.
- Simpler to toggle single rules to Simulate mode for 'learning mode'.

```
POST / HTTP/1.1
Host: localhost:8000
User-Agent: Mozilla/5.0 (Macintosh;... )... Firefox/51.0
Accept: text/html,application/xhtml+xml,..., */*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-12656974
Content-Length: 345

-12656974
(more data)
```

The diagram illustrates the structure of an HTTP request. It is divided into four main sections by horizontal lines and arrows on the right side:

- start-line:** Indicated by a red box around the first line, `POST / HTTP/1.1`.
- HTTP headers:** Indicated by a vertical label on the right, this section includes the lines from `Host: localhost:8000` to `Content-Length: 345`.
- empty line:** Indicated by a blue box around the blank line following the headers.
- body:** Indicated by a dashed box around the final two lines, `-12656974` and `(more data)`.





Cloudflare Firewall Detail - OWASP ModSecurity Ruleset

- Open-Source project maintained by [SpiderLabs](#).
- ModSecurity is an Apache plugin that we recompiled in lua.
- It is an anomaly-based detection system targeting top-10 web vulnerabilities as released by OWASP.
- Every rule has an associated threat score (not advertised to customers) based on severity.
- If a request exceeds a threat score of 25 (High Sensitivity), 40 (Medium) or 60 (Low) the WAF will trigger.
- Supports **Block**, **Challenge** and **Simulate** modes.
- Individual rules/anomalies can only be **on** or **off** and are grouped by attack category type (SQLi, XSS etc.)

New WAF with updated OWASP Ruleset

Web Application Firewall (WAF)

The Web Application Firewall protects your application by analyzing characteristics from each request and determining how the request should be completed.

| Name | Description | Enabled |
|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|  Cloudflare OWASP Core Ruleset | Cloudflare's implementation of the Open Web Application Security Project, or OWASP ModSecurity Core Rule Set. Cloudflare routinely monitors and updates this policy with updates from OWASP based on the latest version available from the official GitHub repository. |  Configure |
|  Cloudflare Managed Ruleset | Created by Cloudflare security engineers, Cloudflare Managed Rules is designed to provide fast and performant protection for your applications. It is updated and improved on a frequent basis to cover new vulnerabilities and to improve false positive rates. |  Configure |

<https://blog.cloudflare.com/new-cloudflare-waf/>

Recommended Reading

<https://support.cloudflare.com/hc/en-us/articles/200172016-Understanding-the-Cloudflare-Web-Application-Firewall-WAF-#4vxxAwzbHx0eQ8XfETjxiN>

<https://blog.cloudflare.com/new-cloudflare-waf/>

// Firewall Rules

Cloudflare Firewall Detail - Firewall Rules**

- Firewall Rules gives you the ability to proactively inspect incoming site traffic and automatically respond to threats. You define expressions that tell Cloudflare what to look for and specify the appropriate action to take when those criteria are satisfied. It is a simple concept, but like the Wireshark Display Filter language that inspired our own expression language, it is extremely powerful and allows organizations to rapidly adapt to a constantly evolving threat landscape.

When incoming requests match...

| Field | Operator | Value | | |
|-------------|-------------|--------------------|-----|----|
| Country × ▾ | equals ▾ | United Kingdom × ▾ | And | × |
| And | | | | |
| Select... ▾ | Select... ▾ | | And | × |
| Or | | | | |
| Select... ▾ | Select... ▾ | | And | Or |
| | | | | × |

Expression Preview

[Edit expression](#)

```
(ip.geoip.country eq "GB")
```

**** Add-on features available**

Cloudflare Firewall Detail - Expression Editor

- Advanced users will appreciate the Expression Editor (shown below), which trades the visual simplicity of the builder for the raw power of the Cloudflare Firewall Rules Language. It offers access to advanced features, such as grouping symbols, for constructing highly sophisticated, targeted rules.

When incoming requests match...

[Use expression builder](#)

```
((http.request.uri.path contains "/xmlrpc.php") or (http.request.uri.path contains "/wp-login.php") or (http.request.uri.path contains "/wp-admin/" and not http.request.uri.path contains "/wp-admin/admin-ajax.php" and not http.request.uri.path contains "/wp-admin/theme-editor.php"))) and ip.geoip.country ne "MY")
```

Then...

Choose an action

Block ▼

Test rule

<https://developers.cloudflare.com/firewall/cf-firewall-language/fields>

Cloudflare Firewall Detail - Rule Order

- By default, Cloudflare evaluates firewall rules in list order, where rules are evaluated in the order they appear in the Rules List. When list ordering is enabled, the Rules List allows you to drag and drop firewall rules into position, as shown below.

Firewall

Manage access by IP, country, or query rules

Firewall Rules

Control incoming traffic to your zone by filtering requests based on location, IP address, user agent, URI, and more.

You have used 4 of 1000 active Firewall rules.

Create a Firewall rule

SEARCH

STATUS

ACTION

Q Search description...

All

All

IP Ordering

| | Action | Description | |
|---|--------------|------------------------------|----|
| 1 | Allow | Remote workers IP Address | On |
| 2 | Challenge | Test rule IP Address | On |
| 3 | JS Challenge | Spam comments IP Address | On |
| 4 | Block | Private pages URI Path | On |

1-4 of 4

Help

Cloudflare Firewall Detail - Testing Rules

- To help customers in the Enterprise plan understand the potential impact of a new firewall rule, Cloudflare built Rule Preview. With the click of a button, Rule Preview allows you to test a firewall rule against a sample of requests drawn from the last 72 hours of traffic. Rule Preview is built into the Create Firewall Rule and Edit Firewall Rule panels so that you can test a rule as you edit it. For more, see [Preview rules](#).

Then...

Choose an action

Block

Test rule

Specific filter expressions could affect how known good bots, e.g. Googlebot, access your site. Details on how to avoid this can be found here: [Firewall Rules Documentation](#).



Cancel

Save as Draft

Deploy

Lab - Writing a Firewall Rule



You can configure Firewall Rules not only from the Cloudflare Firewall app and the Cloudflare API but also through Terraform (see [Getting Started with Terraform](#)). However, the Firewall Rules panel in the Firewall app provides the most intuitive interface for building, deploying, and managing firewall rules.

TASK:

- Generate a Firewall Rule that blocks your particular User Agent.
- Review the event in the Firewall Events tab.

Quiz:

What is the difference between Firewall Rules and IP Access Rules?

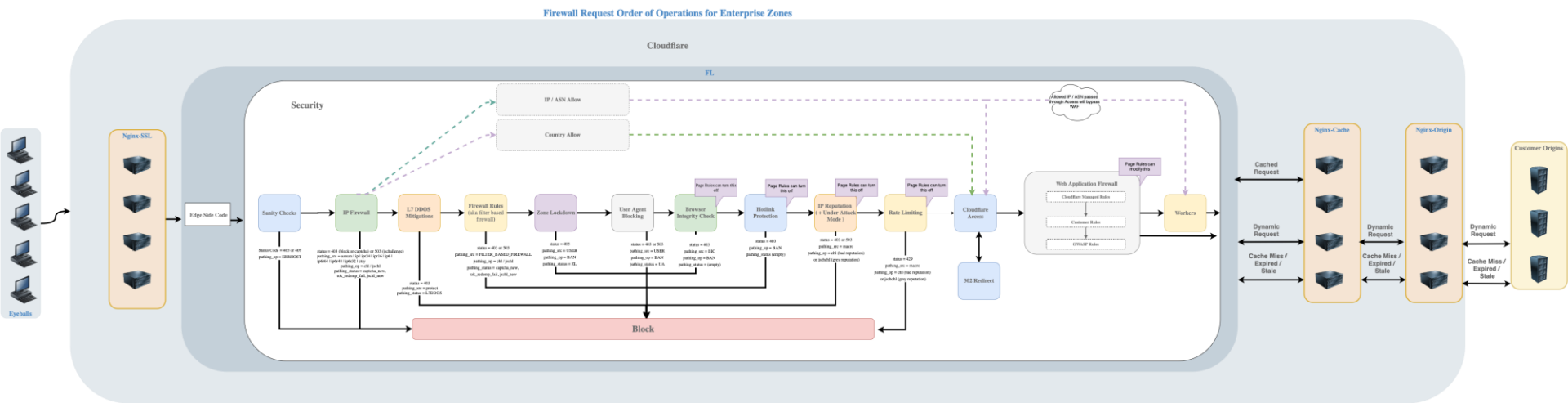
Quiz:

What are the differences between Firewall Rules and IP Access Rules?

Answer:

- IP Access Rules is triggered first before Firewall Rules
- IP Access Rules can span across individual zones, all zones for a user or all zones in an organization
- Spectrum uses IP Access Rules to whitelist/blacklist IP/ASN/Country

Cloudflare Security – Order of Operations for ENT zones





Common Firewall Rules Use Case

Only accept requests over ports 80 and 443

Overview - By default, Cloudflare allows requests over a number of different ports. Firewall Rules allows you to restrict which ports have access to your application.

In this example, requests that do not come over ports 80 or 443 will be blocked, and Cloudflare will return a 403 error.

For a list of ports that Cloudflare allows by default, see [Identifying network ports compatible with Cloudflare's proxy](#) on the Cloudflare support site.

| Expression | Action |
|-------------------------------------------------------------------------------------|--------------|
| <code>http.host eq "www.example.com" and not cf.edge.server_port in {80 443}</code> | <i>Block</i> |



Common Firewall Rule Use Case

Limit access to only those users with a specific cookie

Cookies are a great tool for securing a sensitive area, such as a development environment, since you can share a cookie with trusted individuals and then filter requests so that only users that have the cookie are allowed access. The example below uses two rules. In the first, we look for a specific cookie key, `devaccess`, with individual values for three authorized users: *james*, *matt*, and *michael*. We specify our host and set the action to *Allow*. The second rule blocks all access to our development domain. Since the *Allow* action has precedence over *Block*, requests that satisfy Rule 1 will be granted access; all other requests will be denied.

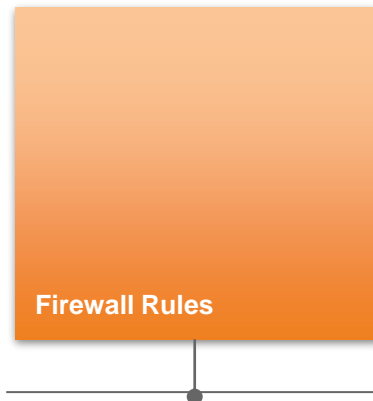
| Execution order | Expression | Action |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 1 | (http.cookie contains "devaccess=james" or http.cookie contains "devaccess=matt" or http.cookie contains "devaccess=michael") and http.host eq "dev.www.example.com") | <i>Allow</i> |
| 2 | http.host eq "dev.www.example.com" | <i>Block</i> |

Takeaways – WAF & Firewall Rules



WAF checks Request URI (start-line), HTTP headers and body for **Anomalies** and **Signatures**

WAF changes take about 30 seconds to update globally



Multiple Security features to be consolidated into Firewall Rules

Provides flexibility to customer to build their own rules

//Cloudflare Bot Solutions

Use Cases

- Credential Stuffing & Account Takeover
- Inventory Hoarding
- Content Scraping
- Credit Card Stuffing
- Content Spam
- API Abuse

How Bots Evade Detection:

- Rotate IP addresses
- Manipulate HTTP request attributes
- Navigate at human speeds
- Run additional stealth plug-ins

Cloudflare Bot Solutions Differentiator

- Network intelligence
- No added latency
- No external processing
- Ease of deployment
- No training period for ML/Heuristics
- Single pane of glass, service consolidation



(Super) Bot Fight Mode

(Super) Bot Fight Mode

- Bot Fight Mode and Super Bot Fight Mode use the same underlying technology that powers our Bot Management product.
- Capability:
 - Protect entire domains without endpoint restrictions
 - Cannot be customized, adjusted, or reconfigured via Firewall Rules
 - Although these products are designed to fight malicious actors on the Internet, they may challenge API or mobile app traffic.
 - For more granular control, upgrade to [Bot Management for Enterprise](#).

<https://blog.cloudflare.com/super-bot-fight-mode/>

Generating Bot Scores - Modules

1) Heuristics → (bot score = 1)

Considering user agent, SSL negotiation (fingerprints on TLS handshake of different technologies), fingerprints of HTTP/2 patterns

2) Machine-learning model → (bot score = 2-99)

Considering SSL mode, request headers, cookies to build signature.

Applied to historical data, if I issue a captcha on the response to this request, how likely is this signature to pass?

2a) Session cookie → (2-99)

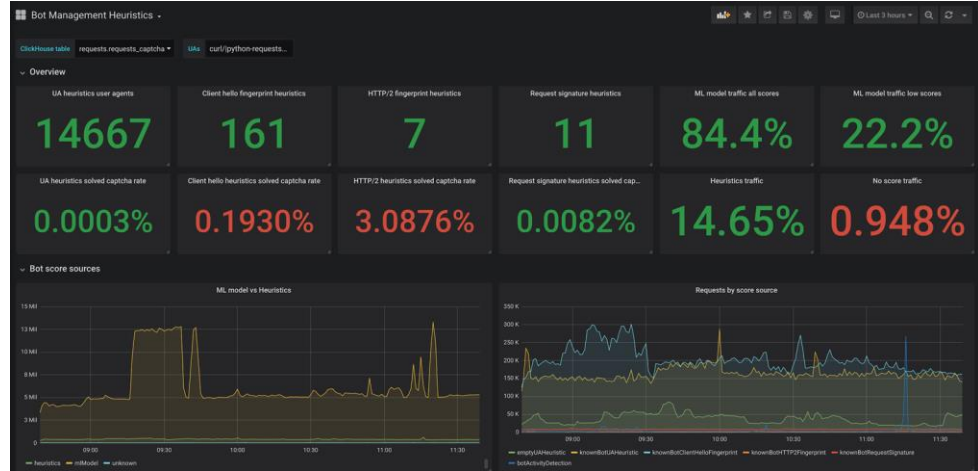
Adjust score based on previous ML scores from the same session over 30 mins

3) Behavioral analysis → (bot score = 1)

Baseline of traffic calculated per IP, looking at: requests/sec, ratio of user/request, ratio of request/path, etc.

1) Detection mechanism: Heuristics

- Heuristics types:
 - *User agent*
 - *ClientHello fingerprint*
 - *HTTP2 fingerprint*
 - *Request signature*
 - Inference time: **10 μ s!**
- [Heuristics dashboard](#)



2) Machine Learning + Bot Management Cookie

Cloudflare will issue a cookie, measure a single user's request pattern and apply it to the machine learning data - this “smooths out” the trust score and reduces false positives across a single user session.

```
__cf_bm=b8e553ba7ed77b87df308407a4277475cd2fb96b-1551227705-1800-  
AeFJuTHW9l9va/FP5xh1qzHEfYgwHo7DxtZDAj5rjZryoOLpMrJuk+NFMcF61C62oy/acHI0wLqCs1C
```

- Hash of IP and Zone ID
- Expires after 30 minutes
- Duration refreshed for each subsequent request while the cookie is live.
- Cookie will not function until the zone is active.

3) JavaScript Detections

- Enabled by Default
- To identify headless browsers and other malicious fingerprints
- Performs a lightweight, invisible JavaScript injection on the client side of any request
- Action: blocks, challenges, or passes requests to other engines
- To adjust your settings, open the Bot Management Configuration page from Firewall > Bots > Configure Super Bot Fight Mode

Dashboard

Configure Super Bot Fight Mode

Definitely automated

Definitely automated traffic typically consists of bad bots. Select an action for this traffic.

Allow



Likely automated

Likely automated traffic can include bad bots, along with other traffic. Select an action for this traffic.

Allow



Verified bots

Verified bots are unique good bot identities validated by Cloudflare. Select an action for verified bots for this traffic.

Allow



Static resource protection

Enable if static resources on your application need bot protection.

Note: Static resource protection can also result in legitimate traffic being blocked.



JavaScript Detections

Use lightweight, invisible JavaScript detections to improve Bot Management. [Learn more.](#)



Bot Management

Bot Management*

- Detecting automated vs non-automated traffic
- Bot score :
 $1(\text{bot}) < \text{bot}/\text{human} < 100(\text{human})$
- Configured in FW Rules
- Additional Fields will be available:
 - **Verified Bot**
 - **Bot Score**
 - **Serve Static Resource**
- Bot Scores exposed in FW Events and Cloudflare Logs for further analysis

Rule name
Give your rule a descriptive name
Bot Management BM<30

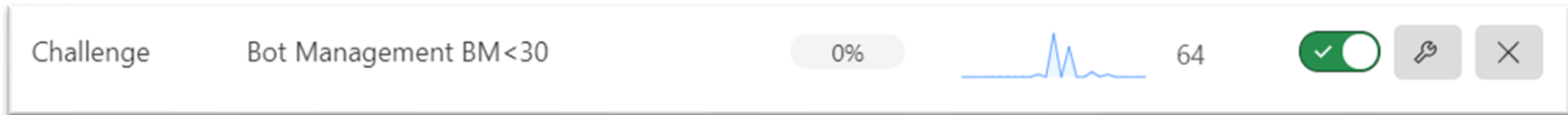
When incoming requests match...

| Field | Operator | Value | |
|----------------------|-----------|--------------------------|----------|
| Bot Score | less than | 30 | And X |
| And | | | |
| Serves Static Res... | equals | <input type="checkbox"/> | And X |
| And | | | |
| Verified Bot | equals | <input type="checkbox"/> | And Or X |

Expression Preview [Edit expression](#)

```
(cf.bot_management.score lt 30 and not cf.bot_management.static_resource and not cf.bot_management.verified_bot)
```

* Add-on feature



Super Bot Fight Mode vs ENT Bot Management

| | Super Bot Fight Mode (BIZ) | Bot Management |
|---------------------------------------------------|----------------------------|----------------|
| Block/challenge bots | ✓ | ✓ |
| ML, Heuristics, and JS | ✓ | ✓ |
| Analytics | ✓ | ✓ |
| Firewall Rules | | ✓ |
| Logs | | ✓ |
| Behavioral Analysis | | ✓ |
| False positive support | | ✓ |
| Use on specific paths / user agents | | ✓ |
| Choose <i>type</i> of action (JS challenge, etc.) | | ✓ |
| Use bot score in Workers | | ✓ |

4) Anomaly Detection

- Used to be called Behavioral Analysis Detection (BAD)
- Optional detection engine that uses a form of unsupervised learning
- Cloudflare records a baseline of your domain's traffic and uses the baseline to intelligently detect outlier requests.
- User agent-agnostic
- Not recommended for API Traffic
- Contact Cloudflare Account team to enable this feature

Bot Management - Variables

Bot Management variables

After activating Bot Management, new variables are available in FW Rules to detect automated traffic:

- **Bot Threat Score:** The score Bot Management generates for the request (1 to 99).
- **Verified Bot:** A boolean value that is true if the request comes from a good bot (allowed by Cloudflare).
- **Serves Static Resource:** An identifier to match file extensions for many types of static resources.

Bot Management - Logs

Viewing Bot Management in logs

If you are exporting your raw HTTP request logs using either [LogPull](#) or [LogPush](#), you will have access to the following two log fields related to Bot Management:

- **BotScore**: The bot score assigned to this request. Valid range: [1-99].
- **BotScoreSrc**: Underlying detection engine or *source* on where the bot score is calculated.
Possible values: [*Not Computed* | *Heuristics* | *Machine Learning* | *Behavioral Analysis* | *Verified Bot*]
- **(new) BotTags**: Provides Information on Bot Category.
Possible values: [*api* | *google* | *bing* | *googleAds* | *googleMedia* | etc.]

Sample of Bot Event

25 Aug, 2020 11:39:23

Challenge

United States

104.131.54.149

Firewall rules

| | |
|--------------|-----------------------------------------------------------------------------------------------------------------------|
| Ray ID | 5c8249209e2df01d |
| Method | GET |
| HTTP Version | HTTP/1.1 |
| Host | login.orangecloud.cf:80 |
| Path | /adminer-3.3.4.php |
| Query string | <i>Empty query string</i> |
| User agent | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1 Safari/605.1.15 |
| IP address | 104.131.54.149 |
| ASN | AS14061 DIGITALOCEAN-ASN |
| Country | United States |

| | |
|--------------|------------------------------------------------------------------------------------------------------------------|
| Service | Firewall rules |
| Rule ID | 590b6e25779f46ceb4425f00e2e7722b |
| Rule name | Bot Management BM<30 |
| Expression | (cf.bot_management.score lt 30 and not cf.bot_management.static_resource and not cf.bot_management.verified_bot) |
| Action taken | Challenge |

| | |
|------------|------------|
| Bot score | 1 |
| Bot source | Heuristics |

 [Export event JSON](#)

Bot Score - Firewall Rules

Protecting a wordpress login form page from credential stuffing:

```
(http.request.uri.path contains "wp-login.php"  
and cf.bot_management.score lt 30  
and not cf.bot_management.verified_bot)
```

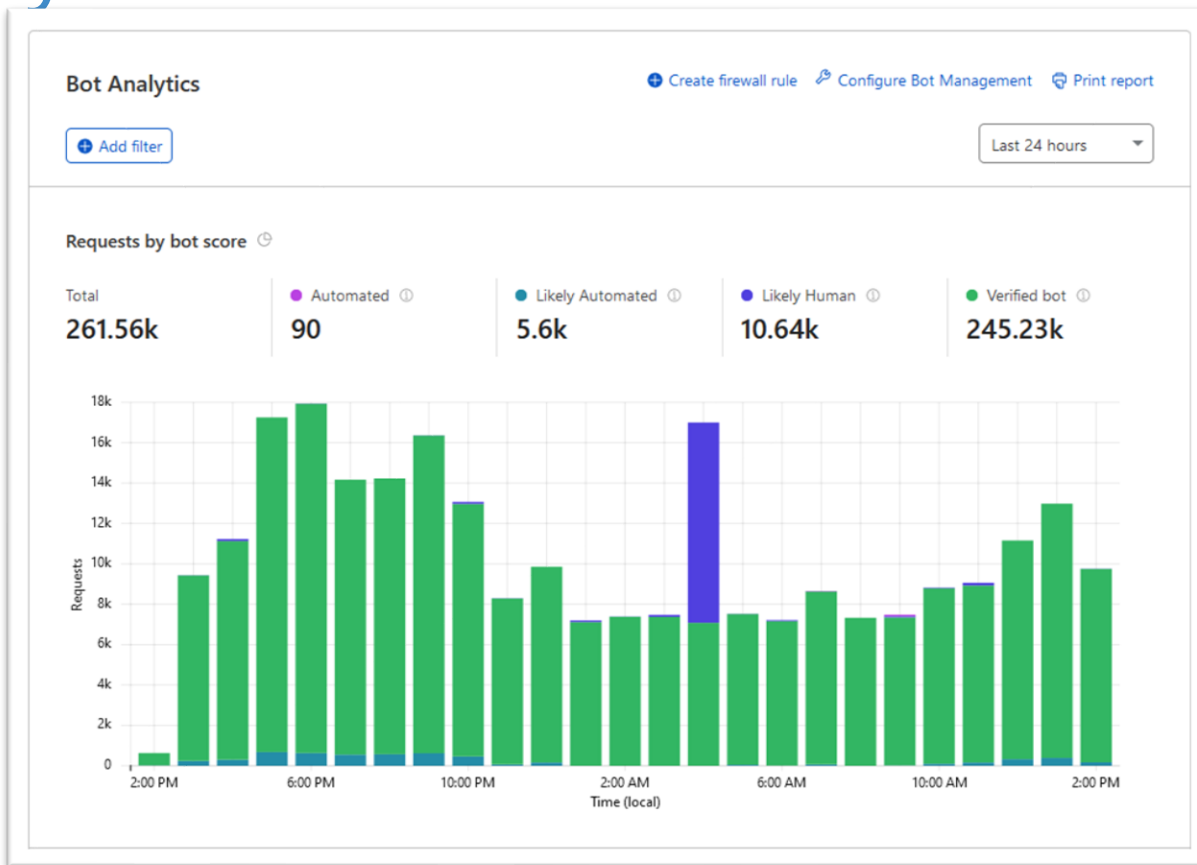
Why the threshold of 30?

The current model performs on average the best at 30 for web traffic, so we catch the highest ratio of true positives to false positives.

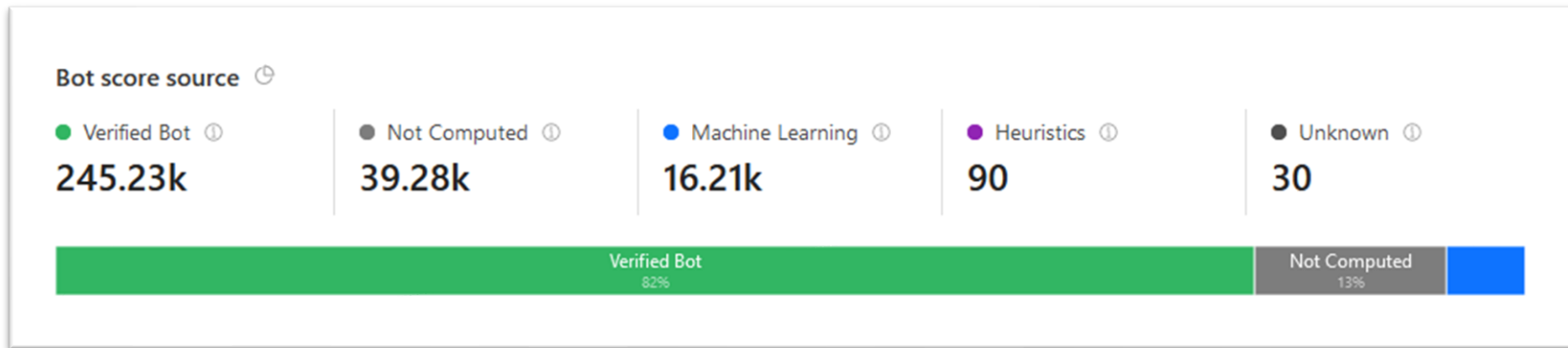
When incoming requests match...

| Field | Operator | Value |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|----------------------|
| <div><div></div><div>Threat Score</div><div>Verified Bot</div><div>Bot Threat Score</div><div>Bot JS Score</div><div>Serves Static Resource</div></div> | <div>Select...</div> | <div></div> |
| Choose an action | | |
| <div>Block</div> | | <div>Test rule</div> |

Bot Analytics



Bot Analytics



Details about Bot Traffic and Action (Challenge/Block) can be found at Firewall Events



Lab - Writing a Bot Management Rule

When incoming requests match...

| Field | Operator | Value | | |
|----------------------|------------------|-------------|-----|----|
| Bot Score | less than | 30 | And | × |
| And | | | | |
| Serves Static Res... | equals | Off | And | × |
| And | | | | |
| Verified Bot | equals | Off | And | × |
| And | | | | |
| User Agent | does not cont... | curl/7.58.0 | And | Or |
| | | | × | |

Expression Preview

[Edit expression](#)

```
(cf.bot_management.score lt 30 and not cf.bot_management.static_resource and not cf.bot_management.verified_bot and not http.user_agent contains "curl/7.58.0")
```

Then...

Choose an action

Challenge (Captcha)

Test rule

Cancel

Save

Create a bot management rule like the example above.

Takeaways – Bot Management



Integrated with Firewall Rules

Bot scoring identification:

$1(\text{bot}) < \text{bot/human} < 100(\text{human})$

No learning period

(Super) Bot Fight Mode vs Bot Management
for Enterprise value differentiator

Quiz:

What detection mechanism does Cloudflare use to assess bots?

Quiz:

What detection mechanism does Cloudflare use to assess bots?

Answer:

- Heuristics (User Agent, SSL Handshake, HTTP2 fingerprint)
- Machine Learning Modelling with Bot Management Cookie
- Behavioral Anomaly Detection (Baseline vs Outlier Traffic Detection)
- JavaScript Detections (identifies headless browsers and other malicious fingerprints)

Quiz:

Why is it recommended to start off with BotScore value of 30 or less?

Quiz:

Why is it recommended to start off with BotScore value of 30 or less?

Answer:

Scores below 30 are commonly associated with bot traffic

// Rate Limiting

Rate Limiting*

- Configurable L7 volumetric attack mitigation.
- Once enabled applies to **all** zones in an account.
- Each PoP keeps a count of # of HTTP requests received from a single IP (default) over a time period.
- HTTP 429 Response with error page, custom text or JSON if defined threshold is exceeded.
- Support for clients behind NAT feature.
- **Measures only requests to origin. Cached requests are ignored.**
- URL patterns can include wildcards but not query strings.
Specific 'verbs' and/or response codes are supported.
- Specific URLs can be bypassed. Rules are not ordered - most aggressive counter that matches URL will apply.

Error 1015

Ray ID: 41968452dfd97f0c • 2018-05-11 17:55:30 UTC

You are being rate limited

What happened?

The owner of this website (secure.jamesaskham.us) has banned you temporarily from accessing this website.

```
< HTTP/2 429
< date: Fri, 11 May 2018 17:56:04 GMT
< content-type: text/html; charset=UTF-8
< retry-after: 65
< set-cookie: __cfduid=d1667fdd39845cbd00577ac22601fbfd11526061364; expires=Sat, 11-May-19 17:56:04 GMT
; path=/; domain=.secure.jamesaskham.us; HttpOnly; Secure
< cache-control: no-cache
< x-frame-options: SAMEORIGIN
< expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
< server: cloudflare
< cf-ray: 419685289eaa7f06-SFO-DOG
<
{ [1050 bytes data]
* Closing connection 0
* TLSv1.2 (OUT), TLS alert, Client hello (1):
} [2 bytes data]
```

* Add-on feature

Lab - Write a Rate Limiting Rule



Task

1. Log into your Cloudflare account.
2. Select the domain to protect.
3. Click the **Firewall** app and then the **Tools** tab.
4. Click **Protect your login** under **Rate Limiting**.
5. Enter **Rule Name** and **Enter your login URL** in the **Protect your login** dialog that appears.
6. Click **Save**.
7. The **Rule Name** appears in your **Rate Limiting** rules list.

Quiz

How can you measure the number of requests to configure when creating Rate Limiting Policy?

Quiz

How can you measure the number of requests to configure when creating Rate Limiting Policy?

Answer

- Create a Rate Limiting Policy with some number in Simulate mode, and adjust accordingly based on the monitored result
- Allow 10-30% buffer to accommodate traffic spike
- Adjust according to your server capacity

// Spectrum

Spectrum*

- For apps with custom ports
- TCP/UDP/HTTP/HTTPS/*Minecraft/SSH/RDP*
- Protection -> IP Firewall, DDOS
- HTTP/HTTPS traffic will benefit from performance and security features, too
- How customers using Spectrum: protect Game applications, custom mobile apps, mail servers, etc
- Proxy Protocol is required to get source IP
 - Some services you run may require knowledge of the true client IP. In those cases, you can use a proxy protocol for Cloudflare to pass on the client IP to your service.

<https://developers.cloudflare.com/spectrum/getting-started/proxy-protocol/>

* Add-on feature

Application Type

Choose the type of application. The application type determines the protocol by which data travels from the edge to your origin.

TCP

Domain

Your application will be associated with a DNS name on your Cloudflare zone.

(optional) subdomain



.orangecloud.cf

Edge IP Connectivity

Choose which types of IP addresses will be provisioned for this subdomain. IPv4 will result in A records, IPv6 in AAAA records.



IPv4 + IPv6



IPv4 Only



IPv6 Only

Edge Port

Enter the Cloudflare edge port. One or more anycast addresses at Cloudflare's edge will represent your service. We'll listen for incoming connections to these addresses on this port. Connections to these addresses are proxied to your origin. For TCP and UDP applications, you can also specify a range, e.g. 22-23. In that case, the origin port should also be a range with the same difference.

25565

Origin

You can designate an IP or a Cloudflare Load Balancer as your origin.



Origin IP



Load Balancer

Enter the IP and port of your service. Your service must use the same transport protocol as the edge port.

IP

Port

25565

Edge TLS Termination

When enabled, Cloudflare will encrypt traffic for your application at the edge. TLS may not be used with UDP applications.



Off

IP Access Rules

If enabled, access rules with a Block or Allow action will be enforced for this Spectrum application.



Off

Proxy Protocols

Enable the protocol version that your origin supports, if any. This relays the client's original IP and port information to your origin. It is only supported for TCP and UDP.

Off

BYOIP (Bring Your Own IP) with Spectrum*

- When creating a Spectrum application, Cloudflare normally assigns an arbitrary IP from Cloudflare's IP pool to Spectrum application
- BYOIP with Spectrum allows you to use your own IP addresses when connecting to your application
- Cloudflare supports min. /24 for IPv4 and /48 for IPv6
- BYOIP is an Add-On Feature on top of Spectrum

<https://developers.cloudflare.com/spectrum/about/byoip>

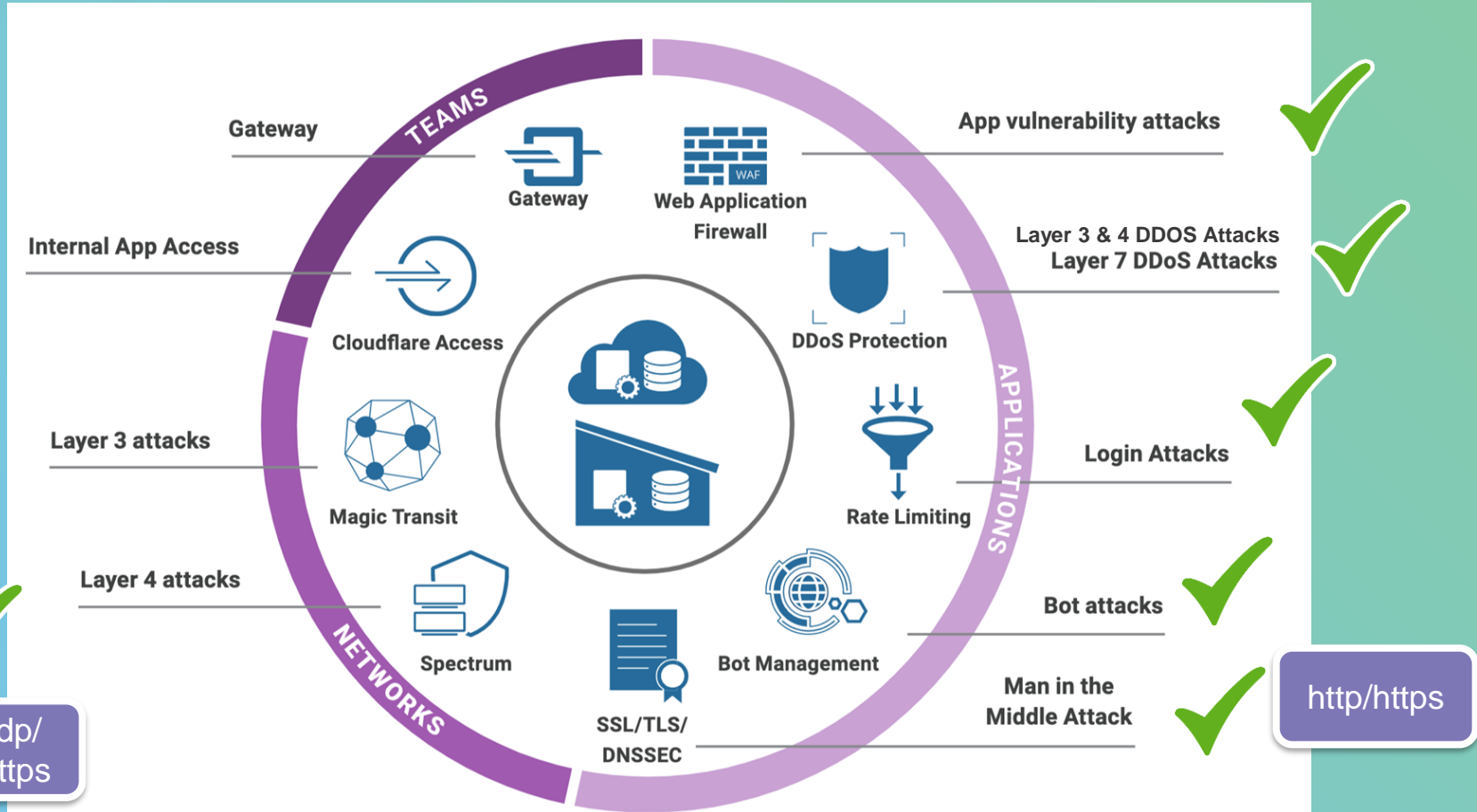
Lab – Create a Spectrum App



Task

1. Log into your Cloudflare account.
2. Select the domain to protect.
3. Click the **Spectrum** app and then **Create An Application button**.
4. Choose **TCP** as your Application Type.
5. Choose how you want the clients to connect to your app by configuring **Domain** (URL endpoint for the app), **Edge IP Connectivity**, **Edge Port**, **Edge TLS** setting, e.g SSH server port 22
6. Choose how you want to connect to your origin by configuring Origin IP or LB and origin port
7. For this lab, you can keep **IP Access Rules** and **Proxy Protocol** to **OFF**
8. Click **Add** and test accessing your application

End of Day 2 Summary



See you on Day 3 for these topics:

- Cloudflare Performance Services
- Advanced Caching & Tuning
- Argo Smart Routing & Tiered Caching
- Browser Insight
- Image Resizing
- Stream and Stream Delivery
- Performance Analytics
- Updates on Cloudflare Speed Week 2021

Knowledge Check

- Can I control WAF rules independently for my staging and production environments hosted at **uat.application.com** and **prod.application.com**?
- Where can I find the 'Cloudflare Specials'?
- The Firewall Events tab is unusable as there are so many events. What advice would you give to an Enterprise customer?
- A prospective customer is worried that malicious bots are scraping their site for content and brute forcing login pages. What are some Cloudflare tools that might be used to combat this?