Smart Defense
Learn how to use intelligent mitigation techniques against today's application DDoS attacks.

PRESENTED BY:
Manuel Haehr
Senior Systems Engineer
L7 Behavioral DDOS Protection: an advanced, phased approach

Multiple Layers of Protection

Start of Attack
Identify Attackers
Advanced Attacks
Persistent Attacks

Rate Limit to Protect the Server
Detect and Block Bots and Bad Actors
Create and Enforce Dynamic Signatures
Analyze Application Stress and Continually Tune Mitigations.

Even basic attacks can take an unprotected server down quickly.

Persistent attackers will adjust tools, targets, sources and attack volume to defeat static DOS defenses.

The F5 approach protects the server from the first moment of the attack and then analyzes the attack tools, sources and patterns to refine mitigations.

These sophisticated protections maximize application availability while minimizing false positives.
High-level overview

- Learn what’s the typical behavior (statistical site model)
- Detect attack (service impact / service health)
- Find the behavior anomaly - what is changed in global behavior (anomaly detection)
- Find who created / contributed to the anomaly (bad actors)
- Generate list of rules that describe attacking traffic and don’t affect the good one (attack signatures)
- Mitigate attack (multilayer defense from DDoS Attack).
Multi-Layer Defense

Bad IPs
- Shun List (SW/HW) block traffic from bad IP addresses

Accelerated Signatures
- HTTP block requests that match the attack signatures
- TCP slowdown requests from bad IP addresses

Bad IPs
- HTTP block/rate limit requests from bad IP addresses

Signatures
- HTTP block requests that match the attack signatures

Connections
- Limit the number of concurrent connections from bad IP addresses

Global
- If necessary, basing on the server’s health rate limit all requests / limit the number of all concurrent connections

CONSERVATIVE MITIGATION

STANDARD MITIGATION

DDoS Attack
Legitimate Users

DDoS Attackers

Stress Evaluator

Signature: (http.request.method eq GET) and (http.uri_file hashes like /) and (http.referer hashes like http://10.0.2.1/none.html) and (http.accept contains application) and (http.accept_encoding_header_exists eq true) and (http.headers_count eq 10) and (http.browser_type eq chrome)

Per SrcIP

Stress Triggers

Signature Generation and enters "Attack" state

Signal metering

Good Data

Attack Data

Bad Actor Detection

Mitigations

Selective Drops

Rate Limit

Bad Actor Mitigation

Signature-based Mitigation

Global Mitigation

Financial Services

E-Commerce

Subscriber
Frequency (PPS)

Load (PPS)

Browser Types
- Safari
- Firefox
- IE / Cortana
- Opera
- Chrome

Server Health

Max (Chrome)

Min (Chrome)

Current Value

Threshold
Legitimate Users

DDoS Attackers

Stress Evaluator

Signature

Per SrcIP

Stress Triggers

Signature Generation and enters "Attack" state

Bad Actor Detection

Mitigations

Selectives Drops

Rate Limit

Bad Actor Mitigation

Signature-based Mitigation

Global Mitigation

Financial Services

E-Commerce

Subscriber

( http.request.method eq GET ) and
( http.uri_file hashes like / ) and
( http.referer hashes like http://10.0.2.1/none.html ) and
( http.accept contains application ) and
( http.accept_encoding_header_exists eq true ) and
( http.headers_count eq 10 ) and
( http.browser_type eq chrome)
Grafana Dashboard
Thank You

www.f5.com