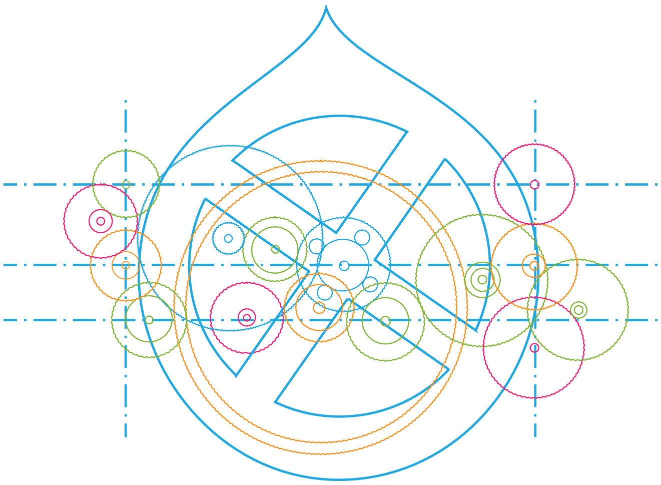
ACQUIA THINK AHEAD.

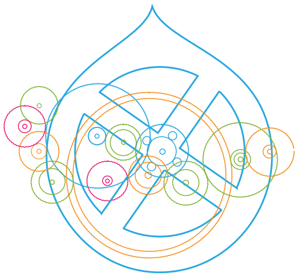
Acquia Cloud Edge Protect

Denial-of-service (DoS) Attacks Are on the Rise and Have Evolved into Complex and Overwhelming Security Challenges



TECHNICAL GUIDE

TABLE OF CONTENTS

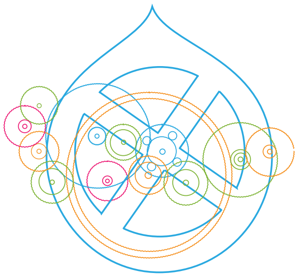


Introduction

Although DoS attacks are not a recent phenomenon, the methods and resources available to conduct and mask such attacks have dramatically evolved to include distributed (DDoS) and, more recently, distributed reflector (DRDoS) attacks—attacks that simply cannot be addressed by traditional on-premise solutions.

Acquia Cloud Edge Protect's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of such threats and can be used to mitigate DDoS attacks of all forms and sizes, including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification, and Layer 7 attacks. This document explains the anatomy of each attack method and how the Acquia Cloud Edge Protect network powered by CloudFlare is designed to protect your web presence from such threats. The following sections provide information on these attacks and how the Acquia Cloud Edge Protect network protects against them.

- Layer 3/4 attacks
- DNS amplification attacks
- SMURF attacks
- ACK attacks
- Layer 7 attacks
- Making DoS a thing of the past



Layer 3/4 Attacks

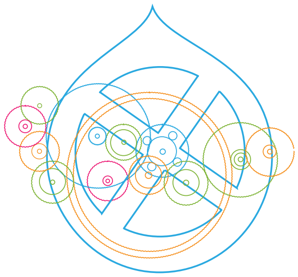
Most DDoS attacks target the transport and network layers of a communications system. These layers are represented as layers 3 and 4 of the OSI model. The so called “transport” layer of the network stack specifies the protocol (for example, TCP or UDP) by which two hosts on a network communicate with one another. Attacks directed at layers 3 and 4 are designed to flood a network interface with attack traffic to overwhelm its resources and deny it the ability to respond to legitimate traffic. More specifically, attacks of this nature aim to saturate the capacity of a network switch, or overwhelm a server’s network card or its CPU’s ability to handle attack traffic.

Layer 3 and 4 attacks are difficult—if not impossible—to mitigate with an on-premise solution. If an attacker can send more traffic than a network link can handle, no amount of additional hardware resources will help to mitigate such an attack. For example, if you have a router with a 10Gbps port and an attacker sends you 11Gbps of attack traffic, no amount of intelligent software or hardware will allow you to stop the attack if the network link is completely saturated.

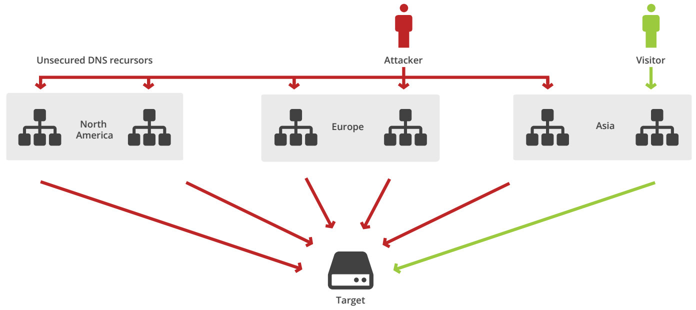
Very large Layer 3/4 attacks nearly always originate from a number of sources. These many sources each send attack traffic to a single Internet location, creating a tidal wave that overwhelms a target’s resources. In this sense, the attack is distributed. The sources of attack traffic can be a group of individuals working together, a botnet of compromised PCs, a botnet of compromised servers, misconfigured DNS resolvers, or even home Internet routers with weak passwords.

Because an attacker launching a Layer 3/4 attack doesn’t care about receiving a response to the requests they send, the packets that make up the attack do not have to be accurate or correctly formatted. Attackers regularly spoof all information in the attack packets, including the source IP, making it look as if the attack is coming from a virtually infinite number of sources. Because packet data can be fully randomized, techniques like upstream IP filtering become virtually useless.

With Acquia Cloud Edge Protect, all attack traffic that would otherwise directly hit your server is automatically routed to Acquia Cloud Edge Protect’s global Anycast network of data centers. Once attack traffic is shifted, we are able to leverage the global capacity of our network, as well as racks-upon-racks of server infrastructure, to absorb the floods of attack traffic at our network edge. This means that Acquia Cloud Edge Protect is able to prevent even a single packet of attack traffic from ever reaching a site protected by Acquia Cloud Edge Protect.

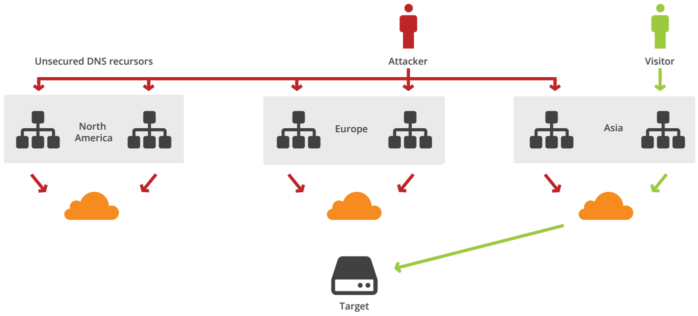


Reflection Attack Before Using Acquia Cloud Edge Protect



An attacker gathers resources, such as botnets or unsecured DNS recursors, and imitates the target’s IP address. The resources then send a flood of replies to the target, knocking it offline.

Reflection Attack After Using Acquia Cloud Edge Protect



An attacker gathers resources, such as botnets or unsecured DNS recursors, and imitates the target’s IP address. The resources then send a flood of replies to the target, but they are blocked by Acquia Cloud Edge Protect’s data centers. Legitimate traffic can still access the web property.

DNS Amplification Attacks

DNS amplification attacks, one form of DDoS, are on the rise and have become the largest source of Layer 3/4 DDoS attacks. Acquia Cloud Edge Protect routinely mitigates attacks that exceed 100Gpbs and recently protected a customer from an attack that exceeded 300Gbps—an attack *The New York Times* deemed the "largest publicly announced DDoS attack in the history of the Internet."

The resolvers then respond to the request, sending the large DNS zone answer to the IP address of the intended victim. The attackers' requests themselves are only a fraction of the size of the responses, allowing the attackers to amplify their attacks to many times the size of the bandwidth resources they themselves control.

An amplification attack has two criterion. First, a query can be sent with a spoofed source address (for example, via a protocol like ICMP or UDP that does not require a handshake). Secondly, the response to the query is significantly larger than the query itself. DNS is a core, ubiquitous Internet platform that meets these criteria, and therefore has become the largest source of amplification attacks.

DNS queries are typically transmitted over UDP, meaning that, like ICMP queries used in a SMURF attack (described below), they are fire-and-forget. As a result, the source attribute of a DNS query can be spoofed and the receiver has no way of determining its veracity before responding. DNS is also capable of generating a much larger response than query. For example, you can send the following (tiny) query (where x.x.x.x is the IP of an open DNS resolver) dig ANY isc.org @x.x.x.x +edns=0 and get back a gigantic response. This is a 64 byte query that results in a 3,223 byte response. In other words, an attacker is able to achieve a 50x amplification over whatever traffic they can initiate to an open DNS resolver.

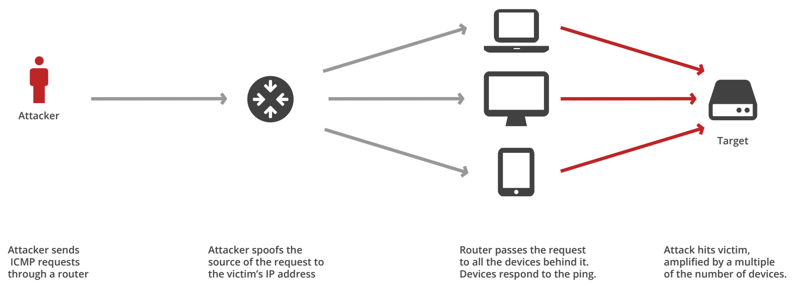
Acquia Cloud Edge Protect's Anycast network was specifically designed to stop massive Layer 3/4 attacks. By using Anycast, we are able to announce the same IP addresses from each of our several worldwide data centers. The network itself load balances requests to the nearest facility. Under normal circumstances this helps us ensure that your site's visitors are automatically routed to the nearest data center on our network to ensure the best performance.

SMURF Attacks

One of the first amplification attacks was known as a SMURF attack. In a SMURF attack, an attacker sends ICMP requests (for example, ping requests) to a network's broadcast address (that is, X.X.X.255) announced from a router configured to relay ICMP to all devices behind the router. The attacker then spoofs the source of the ICMP request to be the IP address of the intended victim. Because ICMP does not include a handshake, the destination has no means of verifying if the source IP is legitimate. The router receives the request and passes it on to all the devices that sit behind it.

Each of these devices then respond back to the ping. The attacker is able to amplify the attack by a multiple equal to the number of devices behind the router. For example, if you have 5 devices behind the router, then the attacker is able to amplify the attack 5x.

Smurf Attack


Attacker
Target
Attacker sends ICMP requests through a router
Attacker spoofs the source of the request to the victim's IP address
Router passes the request to all the devices behind it. Devices respond to the ping.
Attack hits victim, amplified by a multiple of the number of devices.

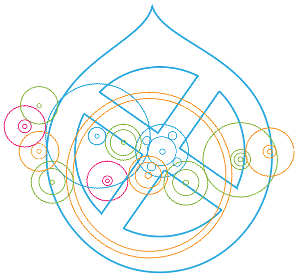
SMURF attacks are largely a thing of the past. For the most part, network operators have configured their routers to disable the relay of ICMP requests sent to a network's broadcast address.

ACK Attacks

To understand an ACK attack, you must delve into the world of TCP. When a TCP connection is established, there is a handshake. The server initiating the TCP session sends a SYN (for synchronize) request to the receiving server. The receiving server responds with an ACK (for acknowledge). After that handshake, data can be exchanged.

In an ACK reflection attack, the attacker sends lots of SYN packets to servers with a spoofed source IP address pointing to the intended victim. The servers then respond to the victim's IP with an ACK creating the attack.

Like DNS reflection attacks, ACK attacks disguise the source of the attack, making it appear to come from legitimate servers. However, unlike a DNS reflection attack, there is no amplification factor, the bandwidth from the ACKs is symmetrical to the bandwidth the attacker has to generate the SYNs. The Acquia Cloud Edge Protect network is configured to drop unmatched ACKs, which mitigates these types of attacks.

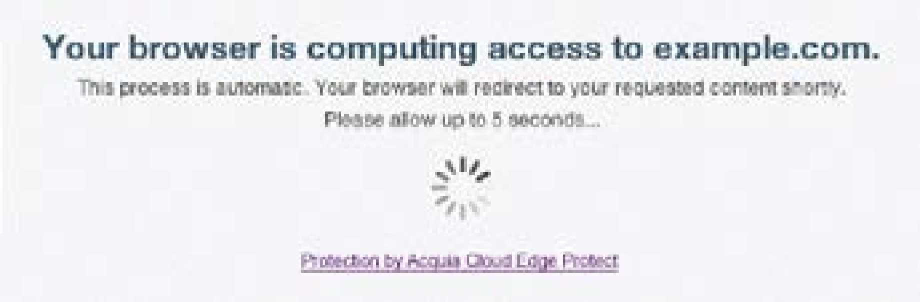


Layer 7 Attacks

A new breed of attacks target Layer 7 of the OSI model, the "application" layer. These attacks focus on specific characteristics of web applications that create bottlenecks. For example, the so-called Slow Read attack sends packets slowly across multiple connections. Because Apache opens a new thread for each connection, and since connections are maintained as long as there is traffic being sent, an attacker can overwhelm a web server by exhausting its thread pool relatively quickly.

Acquia Cloud Edge Protect has protections in place against many of these attacks, and in real-world experiences, we generally reduce HTTP attack traffic by 90 percent. For most attacks, and for most of our customers, this is enough to keep them online. However, the 10 percent of traffic that does get through traditional protections can still be overwhelming to customers with limited resources or in the face of very large attacks. In this case, Acquia Cloud Edge Protect offers a security setting known as "I'm Under Attack" mode (IUAM).

IUAM is a security level you can set for your site when you're under attack. When IUAM is turned on, Acquia Cloud Edge Protect adds an additional layer of protections to stop malicious HTTP traffic from being passed to your server.



Your browser is computing access to example.com.

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

Please allow up to 5 seconds...

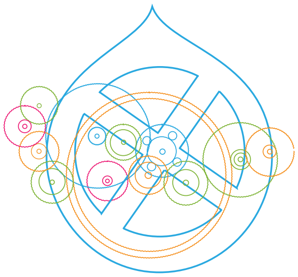
Protection by Acquia Cloud Edge Protect

After verified as legitimate by the automated tests, visitors are able to browse your site unencumbered. JavaScript and cookies are required for the tests and to record that the tests were correctly passed. The page, which your visitors see when in IUAM, can be fully customized to reflect your branding. I'm Under Attack mode does not block search engine crawlers or your existing Acquia Cloud Edge Protect whitelist.

Making DoS a Thing of the Past

As technology advances, DoS attacks will only increase in complexity and magnitude. Traditional on-premise DoS solutions simply can't adapt to the wide range of new attack vectors and are rendered completely ineffective for attacks that exceed an organization's network capacity.

The Acquia Cloud Edge Protect network is designed to mitigate and keep pace with the changing threat landscape. Acquia Cloud Edge Protect, as an operator of one of the largest global networks on the Internet, is able to leverage its aggregate network capacity across 30 points of presence and is able to learn from attacks against any individual customer to protect all customers on our network.



Let's talk

acquia.com | 888.922.7842 | 1.781.238.8600

Acquia® THINK AHEAD.