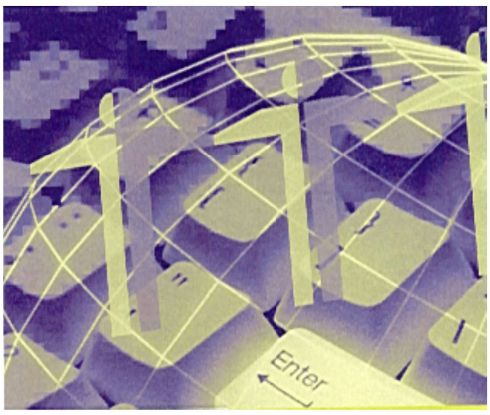


Uptimestar – DDoS Mitigation That Keeps Your Datacenter Running

A White Paper

appthings™

Executive Summary/Key Takeaways

Mounting a DDoS attack is cheap; entire botnets can be rented at low cost on the dark web. Attacks easily overwhelm a data center with traffic that is orders of magnitude higher than the data center can handle. Increasing data center capacity with load-balancing and/or scrubbing is expensive but ultimately does not protect from even larger attacks. The better solution is to intercept attacks "at the Edge", closer to the attackers, before they reach and bring down the data center. Uptimestar provides this solution with a horizontally scalable array of edge nodes that each combine DNS, firewall and a proxy. It can protect from total loss of business during a DDoS attack and from permanent brand damage.

Problem Description

Distributed Denial-of-service (DDoS) attacks can easily damage your business. When a data center shuts down, no business transactions can happen, the loss of sales is immediate. Damage to reputation may last for a long time. On Christmas Day 2014, both Sony's and Microsoft's online gaming networks were brought to a halt by a hacker group named Lizard Squad. Neither Sony or Microsoft were able to avoid outages, even though they had prior notice from the hackers.

If even a huge technology player like Microsoft is unable to protect itself, who can? Some CIOs believe that DDoS simply can't be stopped. Others spend a LOT of money on perceived solutions and vendor offerings.

For years, CIOs have been struggling to find real solutions to DDoS attacks. Part of the problem is that it is very cheap to mount a DDoS attack. Entire botnets can be rented at low cost on the dark web; there is no lack of infected devices in the world that can be used for attacks.

Traditional attempts to defend against these attacks are, however, very expensive, and offer limited success. On June 21, 2017, Microsoft's Skype offering had outages for several days. In a tweet, the hacker group CyberTeam claimed responsibility for the DDoS attack on Skype.

Traditional solution attempts

One classic solution attempt is to increase the capacity of the data center with bigger hardware and load balancing. Bigger hardware, however, is progressively more expensive. When a data center can handle 1M requests per minute (RPM), it's easy for an attacker to generate 10M RPM. This means that you have to "overdimension" your data center by orders of magnitude in relation to legitimate traffic – a VERY expensive proposition. Finally, a load balancer is still a single point of entry that can be overwhelmed with a sufficiently large attack.

Some solutions attempt to redirect traffic identified as an attack to "scrubbing servers", that are supposed to filter such traffic. Conceptually, these are simply costly extensions to a data center that become ineffective given a sufficiently large attack – outages still occur.

A classic approach to handle a large data center load is to redirect users to regional servers that are dedicated to handle the load for that region (e.g. http://india.mycorp.com). This is commonly used when live-video streaming large events. Content that does not change frequently can be cached on those regional servers. Unfortunately, devices that attack a known data center can't be forced to follow redirects to regional servers. Even with such redirects in place, outages still occur.

"Show me a 50-foot wall, and I'll show you a 51-foot ladder."

It appears that this applies to the world of DDoS as well as to border security. A better approach – one that looks 'beyond the wall' – is needed.

The Uptimestar Architecture

A better solution is to intercept the attack 'at the Edge', near the Internet Service Providers (ISPs) used by the attacker. In practice, this translates into a geo-distributed array of Uptimestar 'Edge' nodes. These are server proxies, strategically installed to be close to the larger ISPs (and their users) in the world. Each node is designed to contain an attack to itself (see 'How Uptimestar Nodes Work' below for more detail).

Why do airplanes have two engines? The risk of complete system failure is lower when system components are arranged in parallel rather than "in series". As long as not all engines fail, the system does not fail as a whole. By having separate Uptimestar nodes (=engines) near different ISPs (=on different wings), a fault-tolerant system is created.

By metering and possibly throttling the traffic they proxy, the Uptimestar edge nodes ensure that the data center safe load is not exceeded. A node under DDoS attack possibly shuts down, but traffic to the data center handled by other nodes that are not under attack is maintained. As a result, the attack is regionally or locally contained, and the data center stays operational and available for all other customers. This is a much better outcome than in traditional solutions, where the data center shuts down and all traffic is affected.

How Uptimestar Nodes Work

A typical request flow is as follows: An end-user in Poland requests a page URL with your domain name. To resolve the domain name, his/her ISP's 'caching DNS' obtains the IP endpoint from the Uptimestar authoritative DNS that is part of an Uptimestar node positioned near the ISP in China. The IP address returned points to the same Uptimestar node near that ISP. With that information, the end-user browser now establishes a connection to the Uptimestar node, which functions as a proxy for the data center. The proxy sends its own request to the data center and returns the response to the user.

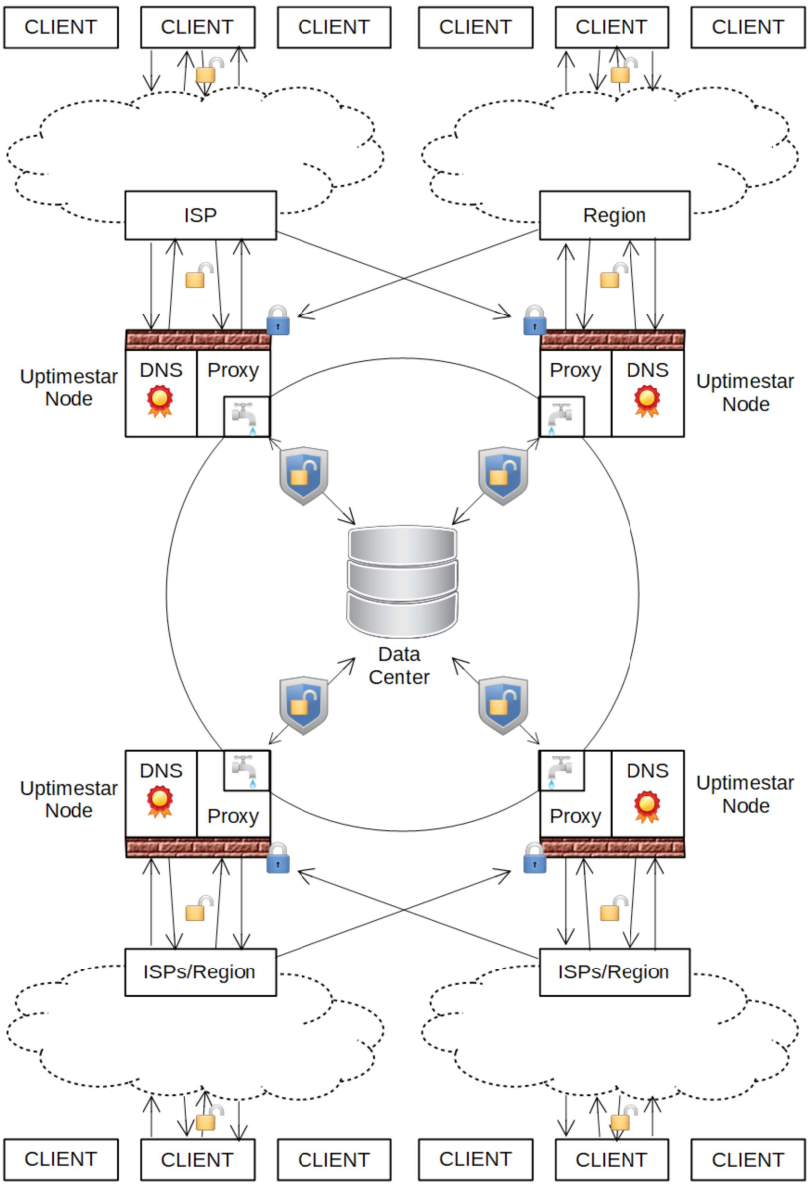
Uptimestar nodes near other ISPs in the same region and Uptimestar nodes in other regions of the world work the same way for users of those ISPs and in those regions.

All Uptimestar proxies implement limits of how many requests per minute they are allowed to send to the data center. They communicate with each other to ensure that the total amount of requests to the data center do not exceed the limit the data center is known to support. Additional rules, such as limits per region, can also be applied.

What happens if someone launches a DDoS attack? If it originates from the same ISP in Poland, the Uptimestar node will fail (and our end-user from that ISP be affected). However, traffic to the data center routed through

other Uptimestar nodes that are not under attack will NOT be affected. This is much better than in a scenario without Uptimestar, where the data center itself will fail and all traffic and business for ALL end-users stops.

With the failure of a node during a DDoS attack, its authoritative DNS will also become unresponsive. Uptimestar ensures that the DNS system will not simply route additional requests from the Attacker's ISP to other Uptimestar nodes (and eventually cause a DDoS failure there). To avoid this 'spillover', each Uptimestar node has a firewall that is configured to make its DNS (and proxy) invisible for traffic that does not originate in their territory (which may be a region and/or ISP).



Delivery Options

Uptimestar is offered as a shared service (SAAS), a dedicated service, and a software subscription; this allows us to provide the highest service levels to enterprise as well as multi-tenant clients.

The number of Uptimestar nodes per service is configurable and can vary per subscriber. Subscribers to the dedicated service can opt for 'insurance', which dynamically adds nodes from the shared service pool of nodes to provide additional capacity during an attack.

Dynamically adding nodes effectively turns DDoS into a no-win game of "whack-a-mole", where an attacker keeps being confronted with new nodes that provide service in lieu of the ones currently under attack. The result is more and better service to users even during sophisticated attacks.

Please contact us to discuss how we can help you with the service that is best suited to your specific needs.

About The Uptimestar Chief Architect

Victor Cekvenich ("Vic") has unique experience that culminates in Uptimestar. He has worked with Ethernet networks, very large databases and the challenges of optimizing their performance. He worked for Akamai on one of their trickiest issues: scaling live high-resolution video streaming, such as for the World Cup South Africa and the China Olympics. He has been working almost exclusively on DDoS for the last four years.

Vic is JDJ trainer of the year. He began his career in software in 1990. He has previously done software engineering work for Tivo, NASA, CSC and Ziff-Davis, among many others. Vic has a BSC in Computer Science from CUNY.

About Appthings

Appthings is a software and IT consultancy shop based in California. Its principals have served demanding clients such as CNBC, NASA and the

Swiss Supreme Court. Integrators and solution providers such as Deloitte Consulting, SAP, Ordina and TrackX have relied on our training, architecture, design and development services to deliver to Fortune 500 companies as well as government clients.

We have successfully delivered software solutions used by Merck Pharma MSD, Tetra-Pak, Tyson Foods, Lombard Odier Darier Hentsch (a premier Swiss private bank), the Dutch Federal Forensic Office and many others. Other consulting clients include Procter & Gamble, the Swiss Federal Police and Louis Vuitton Moet Hennessy (LVMH).

Contact Information

For more information, please contact:
Wolfgang Gehner
Red Cap Development, LLC
El Segundo, CA 90245
USA
Tel: +1 (951) 897-4008

E-mail: wgehner@appthings.io
www.appthings.io

