activereach helps keep the Internet working

Introduction

Our client is a leading DNS provider offering management and registration of a number of global top level domains.

The company was looking to set up new service clusters within alternate hosting centres and wanted to make sure that the new infrastructure being put in place could cope with both the maximal expected load, and a DNS based DDoS attack, before the service went live. The DDoS attack testing service was commissioned to ensure that the relevant mitigation, reporting, and monitoring tools in place worked.

Due to the fact that the systems tested are considered part of Internet infrastructure, the potential cost to the business in terms of reputational damage and loss of revenues was very high.

activereach was selected as the supplier of choice to provide two 90 minute DDoS tests.

The task

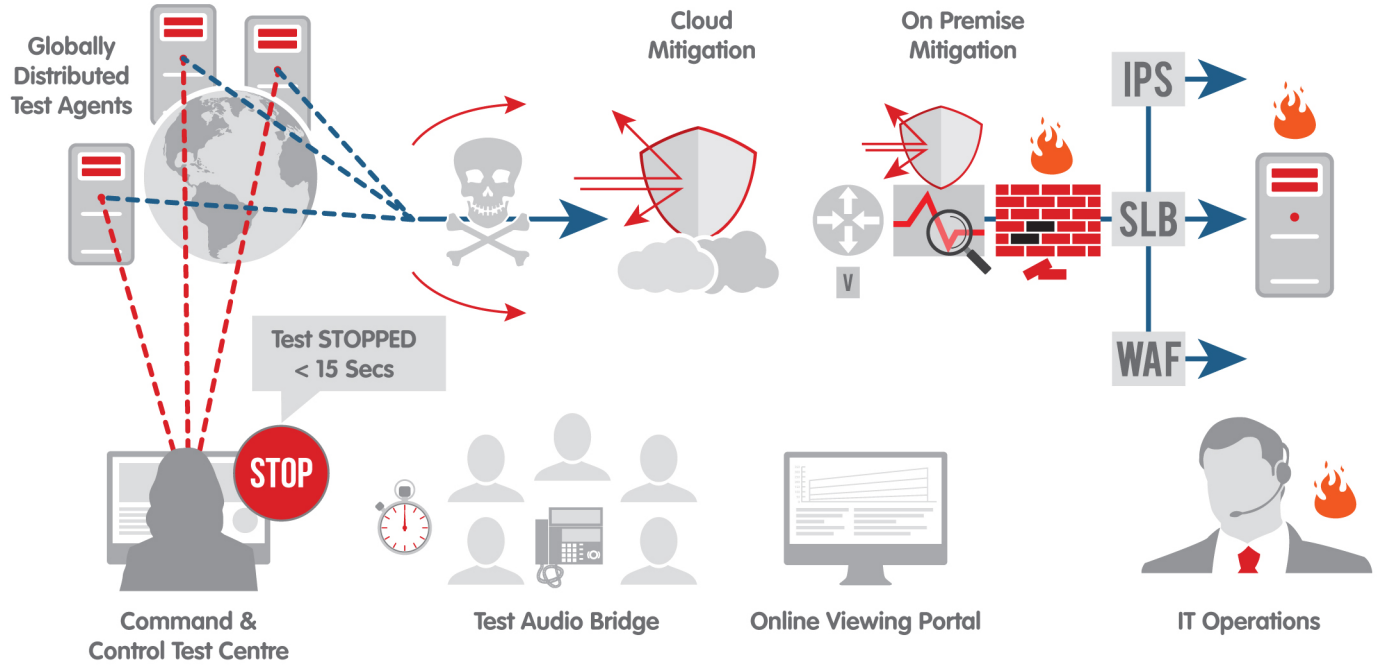
Once NDAs and commercial agreements were completed, activereach engineers conducted a detailed technical consultation phase. This phase establishes a number of key test parameters.

There was both load balancer and server rate limiting in place to restrict the number of requests that can be made over a period of time. This was removed before the tests were conducted so that stress tests could also be run.

Key Test Parameters

1. Required compliance to code of best practice
2. Test objectives
3. Systems, people and risk assessment review
4. DDoS attack types and parameters

The Testing Platform In Operation



The test

The original attack vector was 500,000 DNS queries per second to FQDNs supplied in a text file, with a mix of UDP based record lookups using normal and DNSSec based queries.

On the test date, all key stakeholders connected to a live web conference allowing clear communication with the activereach operations team and visibility of the DDoS attack test portal. At any time during the test the customer had the ability to activate the emergency stop procedure, halting the test within seconds.

The volumetric tests showed how many requests per second the infrastructure could handle. The types of requests sent were also varied to see how the latency and end user response rates altered under system load.

Subsequent to the initial tests, a further round of testing was undertaken to other smaller data centres to confirm the capacity of those sites to load and attack.

Results

The system put in place by the client largely passed the test (though unexpected responses were seen and subsequently investigated with the debugging information supplied through the tests). The overall success meant that the customer had surety that the infrastructure could deal with the likely attack vectors with no loss to business systems.

Metrics & Reporting: A copy of the web conference feed together with details of the test schedule was provided to the end user as no data is kept during the real time tests.

Changes Implemented: Due to the scoping of the project and the tests that were run, the customer considered themselves prepared for possible DDoS attacks and were additionally able to engineer their systems to provide greater protection during valid heavy loading.

Commercial Value: The investment in systems and servers for the new data centre has been fully validated. The two-stage testing sequence alleviated uncertainties regarding security posture, load and system configurations.

Head of Information Security at the DNS Provider, commented:

"activereach were very thorough in the scoping of the project and the way they conducted themselves was very professional.

We greatly benefited from the test and the confirmation that our deployments carried minimal risk even when under significant load."

activereach Ltd.
4 Cliveden Office Village, Lancaster Road, High Wycombe, Bucks. HP12 3YZ.
Tel: 0845 625 9025 / Fax 01494 980 255 / Email: contactus@activereach.net