

How creating the ability to easily and quickly test DDoS mitigation moved network DDoS attack defences from reactive to proactive.

Background: Fortune 500 Global Bank

The Problem

Our organization has been targeted by DDoS attacks every few months for the last 5 years. Some are large, but most were small but still impactful. Our cloud protection providers would consider the attacks 'too small' or difficult to block because they were encrypted (SSL). Our on-premise defense systems exhibited failures where they often did not activate and block the attack, or they would leak a significant portion of the attack through. Every DDoS attack that disabled our systems impacts tens of thousands of customers and caused significant load on our telephone support and emergency response teams.



The Solution

A review of our approach indicated that we had a number of 'holes' or 'vulnerabilities' in our layered defense. Redwolf® testing offered an opportunity to sweep all known DDoS attack types from low attack levels. These tests uncovered dozens of areas where configuration settings could be improved. The Redwolf® team was able to craft attacks that targeted specific aspects of our defense architecture. Tests for cloud anti-DDoS systems, firewalls, on-premise DDoS attack mitigation, load balancers and even web servers were created. Redwolf's ability to create a re-usable test-library was excellent as it allowed precise re-testing by both Redwolf® and our own teams via the self-serve testing portal. Our teams were very impressed with the ease-of-use of the self-serve testing portal and it allowed us to perform simple and cost-effective what-if testing of various approaches for mitigation testing.

The Benefit

DDoS Over three test periods within one year our systems went from defending only 25% of the attacks to an 80% success rate. The Redwolf® testing methodology allowed our teams to significantly improve the resilience of our defense systems at a whole instead of piece-meal. Redwolf® testing allowed us to optimize the existing investment and get the most bang-for-the-buck from our anti-DDoS technologies. Above all, the capability improvement is demonstrable vs. theoretical – something not often found in the InfoSec discipline. After the first year of the program the number of DDoS attacks that impacted our systems has fallen to all-time lows. There are still attacks that threaten us, but Redwolf's program can simulate those as well and we are confident that continuing the program will allow our teams to continually and demonstrably improve our defense capabilities in the following year.



The Problem

Serious DDoS attacks with no way to verify mitigation was functional.



The Solution

The ability to easily and quickly test DDoS mitigation using a trusted partner



The Benefit

DDoS maturity moved from being reactive to proactive

Learn how Redwolf® Enterprise level cyber defence testing helps you optimize your network to defend against the latest threats

Contact us at +1.519.2084475 or info@redwolf.com