Project Summary: Automated DDoS Protection on the NetVM Platform

Overview

Robust protection against Distributed Denial of Service (DDoS) attacks is not cheap. Most DDoS defense strategies involve powerful networking hardware and well-trained network engineers. While larger companies can afford this (or outsource it to another company), smaller businesses are not always able to afford the cost. This project will lower the cost of DDoS defenses by providing an automated solution; by targeting DDoS traffic with automated algorithms running on cheap commodity servers, businesses will be able to more quickly and easily deal with DDoS attacks, saving businesses money, time, and downtime.

Subtopic name: IT6- Networking Technology

Intellectual Merit

This Small Business Innovation Research Phase I project will find an automated method of classifying and defending against various classes of Distributed Denial of Service (DDoS) traffic. The system will sit between an internal network and a larger one (e.g. a business' internal network and the Internet) with the ultimate goal of reducing the effectiveness of DDoS attacks on the internal network.

The system will monitor IP traffic as it enters the internal network and rate all incoming network connections using various heuristics. Very suspicious connections that are highly reminiscent of a DDoS attack will be blocked; moderately suspicious connections will be throttled; unsuspicious connections will pass through the system untouched.

Broader/Commercial Impact

Most defenses against DDoS attacks are expensive. While commercial CDNs and large businesses such as CloudFlare, Akamai, and Google are able to afford the resources required to defend against DDoS's, the financial burden is higher for smaller businesses. This system will lower the cost of in-house DDoS defenses by providing an automated solution that can run on typical commercial-grade server hardware. This system will run on NetVM, a high-performance software-defined networking platform that runs on run-of-the-mill commercial-grade servers. This reduces the cost of the system by allowing clients to take the same class of servers that run their business-critical applications and use them to protect their network from attack.