IMPROVING CONNECTICUT'S CYBERDEFENSE OF DDOS ATTACKS

Keeping the Threats Away from CT Systems

CEN enables Fast-Flood detection to reduce the time for Distributed Denial of Service (DDoS) detection and mitigation, and delivers improved reporting to its member-customers.

State of CT

Submitter: Mark Raymond, CIO

Category: Cybersecurity

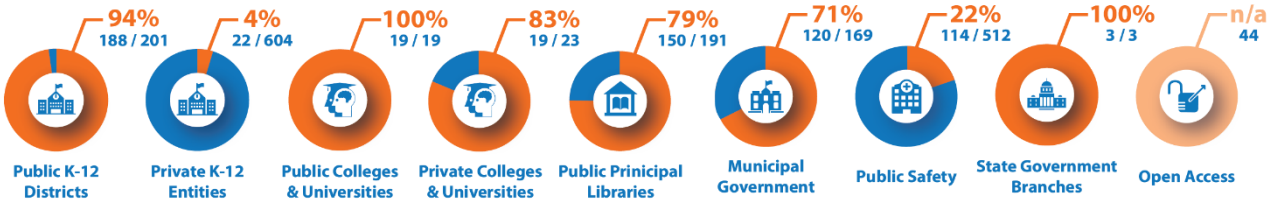
Executive Summary

The State of Connecticut, though the Connecticut Education Network, delivers advanced cyber defense at scale through its Distributed Denial of Service (DDoS) detection and mitigation services protecting Connecticut's community anchor institutions. DDoS attacks are malicious attempts to disrupt normal internet and network traffic to the target system(s) and can create costly downtime if not properly dealt with. DDoS attacks are impossible to defend with conventional cyber security products and require specialized services to properly address.

The Connecticut Education Network's DDoS fast-flood enhancement project improved DDoS protections for CT based community anchor institutions (CAIs) and further delivered on the value proposition of what is means to connect to the Connecticut Education Network.

CEN

The Connecticut Education Network (CEN) is an internet service provider delivering advanced network and value-added services to CAIs and open-access constituents throughout the state of Connecticut. CEN operates an all-fiber, statewide, open-access, multi-gigabit, low latency, high performance network connecting 679 member institutions, including all three branches of State Government, over two-thirds of municipalities, most of the public K-20 education community, and thousands of individual CAIs throughout the state.



CEN Member Institution Count by Vertical

The network connects roughly 1.9M citizens, over 50% of the state population, and serves as a platform for workforce development, economic development, and directly supports digital citizenry throughout The State. CEN is a mission-based, member driven organization and as such, operates in cost recovery (non-profit) model, and relies on advice and counsel from its member advisory councils to tailor services to their needs. https://ctedunet.net/

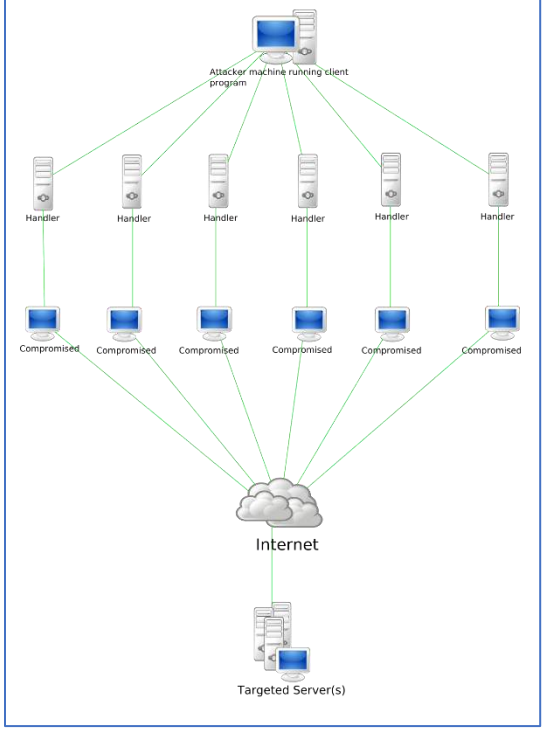
The Challenge

The threat of DDoS attacks are always looming and attacks can happen at random or even as targeted events. While it is impossible to know how many attacks went undetected, it is known that an average of more than three attacks per day were occurring prior to the initial project being started in 2019.

DDoS attacks overwhelm target systems, servers, or services with enormous amounts of network traffic generated by compromised hosts acting like zombies under the control of a malicious actor. DDoS attacks are initiated by bad-actors for any number of reasons and attacks can easily

overwhelm traditional cybersecurity products, such as next-generation firewalls, when targeting devices under their protection or even as the specific target to render inoperable.

Diagram of DDoS Attack



DDoS attacks are the fourth most popular cyberattack in 2021 according to *Crowdstrike*, a popular cybersecurity company. Not only do DDoS attacks take down services, but it can also create a situation where another breach in security can go relatively undetected.

If you look at the cyber-attacks that have impacted the nations infrastructure over the last few years, such as the attack in the 2021 attack on the Colonial Pipeline, the 2021 attack on the water treatment plant in Oldsmar, Florida or the 2020 attack on healthcare facilities in the US and the UK, you realize the impact of an attack is more than financial. These attacks can have dire consequences.

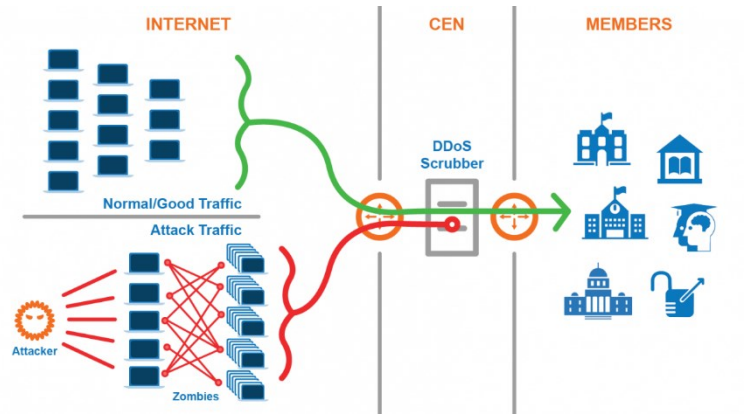
In a recent study done by Deloitte, a low-end cyber-attack costing $34 per month could return $25,000 a month, while a more sophisticated attack costing several thousand dollars could return as much as a million dollars a month.

Connecticut needed a way to rapidly identify and respond to attacks and needed to alert key personnel with details so a proper assessment of damage could be conducted. Since most agencies in the state of Connecticut use CEN, it made most sense to make the service available at scale for all CAIs to benefit.

The Project

In response to the growing threat of Distributed Denial of Service (DDoS) attacks, Connecticut needed to adapt. CEN shouldered the responsibility and initiated a project to implement a series of functional and technical improvements to its existing DDoS service to improve its efficacy, overall protections, and streamline notification to members. The project name was 'DDoS Fast-Flood Enhancements' (https://ctedunet.net/ddosfastfloodenhancement/).

The goals of the project was to allow for faster recognition (detection) and remediation (mitigation) of DDoS attacks, and improve initial notification and in summary reporting when it was over. The baseline for average auto detection was 30 seconds and average auto mitigation was 90 seconds. The targets were to reduce the average times of each by at least half. Upon initiation and post attack, the service also needed to improve reporting of the entire incident to affected member. Manual reporting had been slow and heavily reliant on human resources, so a more automated approach was desired.



The implementation of DDoS Fast-Flood enhancement was created by a cross functional team of stakeholders at CEN comprised of IT security, Network Operations, Business Operations, and advisory council members.

The implementation was a pilot program involving thirty member organizations of assorted sizes and types. The pilot lasted 7 months during which new features were introduced and existing policies were tuned. Ongoing feedback from the organizations participating in the pilot were utilized to measure service efficacy and improvements.

CEN designed a solution that would be able to scale, allows real time monitoring and detection, automated to block, mitigate without human intervention & report as well as allowing flexibility in customizations around policy, rules, and thresholds. The service provides 24 x 7 support as well as cost competitive enterprise service.

Detection and Mitigation Deep Dive

The need to keep services up for our members led to innovations and improvements. Part of the DDoS mitigation service is to redirect IP addresses to the central scrubbers so they can separate and drop malicious traffic at the TCP/IP level. The rules of the public Internet dictate that you can only route a /24 or 256 IP address block at a time under normal circumstances. CEN's service is unique as it leverages on-network appliances that allow for more granular segmentation of IP addresses down to a single IP to be redirected into the scrubbers to then segment good from bad traffic. This allows for more surgical and precise scrubbing of malicious traffic and simply leaves the other IP addresses in the block alone as they are not otherwise involved. Like a police officer directing traffic, it stops or redirects the malicious traffic and keeps the roads clear for everyone else.

Below is an example of what the size of the traffic looks like during an actual DDoS attack on a 10Gbps attached public school district in early 2022. The red indicates all bad traffic coming (dropped) from the attacker. The green indicated legitimate traffic (allowed) destined for the district.

While the bad traffic is being stopped, the user's traffic in green continued uninterrupted.

The dip represents a moment where the bad guys may have thought they could fool the system to thinking the attack was over, but this is a security system that operates 24x7 and 'never sleeps.' CEN mitigates 250-1000 DDoS attacks per year on average.

Communication

Another important part of the DDoS service is notification, so local member IT staff know right away that something is happening and to have cybersecurity personnel on standby if needed. Notifications are automatically sent out to impacted members and CEN staff when an attack starts, and another summary report is sent when the attack ends. Notifications are automated / scripted and sent to primary technical contacts. IT administrators receive the reports to improve communication and allocate time to the issues at hand. If for some reason the DDoS attack is impacting local service, there is a phone number to call and initiate dialog with CEN Tier 3 engineers on how to further troubleshoot and reduce impacts. Being able to time block attacks allows for a targeted assignment of resources to investigate any possible damage such as simultaneous attacks or troubleshooting of problems during the time. The reports can be used as evidence of cybercrime when reporting incidents to federal, state and/or local authorities. In addition, through the enhancement project and feedback through continued member engagement process, CEN developed a checklist of items for local IT administrators to consider and implement to lessen the impact of any residual DDoS traffic that may get through the CEN DDoS scrubbers, as well as methods to potentially pinpoint individual attackers when they may be initiated from within their own local network. The checklist has been shared with members broadly.

Impact / Value

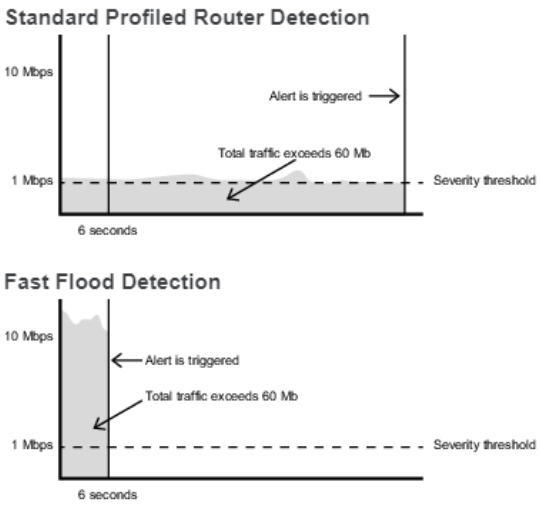
Whether it is a government agency, a small business, when an attack occurs, the ramifications can affect every aspect of our society. While cyber-attacks are a regular thing in the news, being under an attack is usually a chaotic experience for all involved. Taking down services is the goal of these bad actors. Users, not knowing why their systems are slowed, bombard their IT support with questions, external constituents cannot get to online resources they need, and leadership wants answers. It often takes teamwork and communication to mitigate user impact to solutioning and not to mention fixing for the attack.

The reason that the DDoS Fast Flood enhancement denial of service attacks matters to member institutions fall into five key areas:

- Downtime –How quickly and effectively does the solution perform in the Member environment.
- Reputation – If a company's services are not available or terribly slow, consumers may decide to leave and work with a more reputable supplier.

- Legal issues – Companies can be held liable and could be subject to legal or regulatory issues which are very time consuming.
- Monetary loss – Companies can experience significant monetary loss due to the downtime associated with a DDoS attack.
- Compliance – Some companies or Government entities are held responsible for data protection and security. Attacks can also impact company requirements to pass internal and external audit activities.

With the above in mind, the target project goals were met to reduce the recognition (detection) and remediation (mitigation) of DDoS attacks, and improve initial notification and in summary reporting when it was over. Detection went from an average of 30 seconds to as little as 1 second, and average auto mitigation went from 90 seconds to as little as 30 seconds. These improved times allow next-generation firewalls to better withstand the now minimal traffic bursts that get through while the CEN DDoS scrubbers initialize and start cleaning traffic. Previously any next-generation firewall or border appliance would struggle to keep up and eventually lock up even though the CEN service system was already faster than most commercial offerings.



Automated messaging pulls reports and emails them to the primary contact within 2-5 minutes of an attack, and provides a summary report of activities about 10-15 minutes after the attack. These improved times help save valuable time and resources of what would otherwise be a devastating experience.

When the pilot was completed, the implementation resulted in an improved and more value-added offering for CEN members as part of Internet service delivery. The entirety of the CEN member base benefits as does the 1.9 million citizens that connected through the member institutions in public and private k-12 education, public and private higher education, libraries, municipalities, and branches of State government. The CEN DDoS aggregated mitigation service helps that state avoid approximately $30M annually when compared to individually acquired commercial alternatives.

Fast Flood Cost

CEN's primary focus has been and continues to be meeting the needs of Connecticut's community anchor institutions including education, health care, and research organizations, municipal and state government facilities, public libraries, and businesses.

Project implementation costs were minimal and in the form of licensing and soft costs for time of engineering personnel and convening members. The overall impact on the users has been incredibly positive as service outages resulting from DDoS attacks are now negligible.

The DDoS detection, mitigation, and notification service is 'free' to members and is included as part of Internet service delivery available through CEN. The 'always-on' service is available 24x7 and

includes off hours escalations as needed. The project scope included many organizations in the pilot as CEN is mission driven and member led. The members provide advice and council to further improve service.

Ongoing

Unfortunately for us all, the battle with cyber criminals is never over. Using state of the art analytics, the cyber security teams can see a change from frequency of attacks to size of attacks. In the past 4 years the number of known attacks has been reducing, however the size of the attacks that has been mitigated has increased sixfold. This is akin to bad guys sending trains instead of cars.

Year	Number of TMS Mitigations	Volume of Traffic Passed by TMS	Volume of Traffic Dropped by TMS	Volume of Largest TMS Mitigation	Rate of largest TMS Mitigation	Duration of Longest TMS Mitigation
2023*	152*	6.8 TB	26.49 TB	16.63 TB	25.26 Gbps	0d 23h 45m
2022	242	40.36 TB	22.93 TB	18.32 TB	29.75 Gbps	58d 7h 42m
2021	537	25.41 TB	59.74 TB	6.00 TB	38.42 Gbps	150d 2h 20 m
2020	844	20.84 TB	45.83 TB	6.49 TB	19.99 Gbps	86d 10h 47m
2019	978	2.18 TB	12.04 TB	3.74 TB	20.03 Gbps	2d 17h 54m

* Through May 1, 2023; projected annual count will be 608

CEN continues to add capacity and fine tune the DDoS Detection and Mitigation with Fast-Flood service. We recently upgraded hardware, increased licensed capacity, are in-process of upgrading physical connectivity, and are always tuning policies. In addition, CEN is streamlining contingency planning with third parties to ensure the ability to address any level of DDoS attack should local appliances be overwhelmed.

In conclusion, CEN's response to the growing threat of Distributed Denial of Service attacks, Connecticut was able to adapt. CEN implemented, Fast Flood DDoS improvements as a series of changes which automatically and painlessly addresses attacks and notifies agencies. The service is included at no additional cost to its members. The overall impact to the users has been incredibly positive as service outage resulting from DDoS attacks are now down to nearly zero.