CASE STUDY
Suffern Schools

Suffern Schools Fend Off DDoS Attack, Add Secondary Route Ensuring Secure Connectivity

BACKGROUND

It could have been a catastrophic day for Suffern Schools' IT department. Instead, it was a day that started with a sobering electronic alert and ended well.

The Suffern Central School District is headquartered in Hillburn, a village in New York's Rockland County area. The district is made up of seven schools: five elementary schools (Pre-K - 5), one middle school (6 - 8) and one high school (9 - 12), which was named a high performing school by the New York State Department of Education.

With 94% of its graduating high school class attending a 2- or 4-year university, academic success is highly valued within the local community. The district offers Project Based Learning, tech labs, and what it calls "21st century workspaces" providing modern tech-based resources for students to thrive.

These resources all rely deeply upon electronic communication and the Internet in order to function.

CHALLENGE

With a limited IT budget and the recent cost of migrating the district's apps and data to the cloud, Suffern Schools was on the fence about adding yet another expense to its budget in the form of a DDoS mitigation tool. After all, to date, it hadn't experienced a DDoS attack. However, having seen the reputation damage and disruptions from a neighboring school district that had suffered an attack, the district decided to explore its options.

Additionally, Suffern was faced with a frequent challenge: its fiber connection passes through a wooded one-mile road and during snowstorms or wind storms, plows or downed trees would often cut the fiber line, leaving students and staff with no connectivity for lengthy periods of time.

(CONTINUED)

EXECUTIVE SUMMARY

INDUSTRY: EDUCATION

LOCATION: HILLBURN, NY

CHALLENGE:

- With the ongoing threat of DDoS attacks, and in light of an attack that occurred at another school system in Western New York, Suffern School District was vulnerable and concerned about the impact a DDoS attack would have on its 4,000 students
- With a recent migration to the cloud for most of the district's applications and data, and a growing dependence on SaaS applications, it became increasingly important for Suffern to ensure optimum Internet connectivity and no downtime to allow uninterrupted Internet access for students and staff
- IT Director Eric Coronado wanted to avoid both massive disruptions to online learning as well as the bad press and negative publicity associated with a DDoS attack

SOLUTION:

- Suffern School District decided to invest in FirstLight's DDoS Protection and Mitigation to guard against DDoS attacks and the potential disruption and negative publicity that would ensue
- Given the increased dependence on SaaS applications, Suffern had a second Internet POP connection installed in the event that if one Internet pathway were to go down, a second redundant pathway could be used

RESULTS:

- In the midst of a DDoS attack, FirstLight's DDoS Protection and Mitigation solution detected an attack, alerted the IT department, and allowed legitimate traffic to flow while blocking illicit traffic until the attack ceased
- The process was so seamless that the school didn't notice it was being attacked until it received an electronic alert
- During a recent fiber cut, Suffern's primary Internet connection went down; Suffern's secondary Internet pathway kicked in with no interruption – unbeknownst to the IT department until an automated notification alerted them of the fiber cut
- Unlike a neighboring school district, Suffern's DDoS attack and fiber cut incident had no impact on students or administration, and avoided any bad publicity or reputation damage
- With its Internet connectivity secured against DDoS attacks and outages, the Suffern School District is better positioned to ensure that its student body has continuous and protected access to its cloud and SaaS providers, various online learning tools, and connectivity for a growing number of connected devices

SOLUTION

Based on FirstLight's extensive security solution portfolio and deep bench of experts, the School District realized the value of partnering with FirstLight and moved forward with its DDoS Protection & Mitigation solution. Ideally, a DDoS solution should be in place for a few months in order to create a baseline for what is considered "normal" traffic vs. unusual and heavy traffic patterns – the hallmarks of a DDoS attack. In January, the solution was installed on the district's network and monitored regular, ongoing Internet traffic. With that data, the detection tool was activated and sometime during the first week of school, traffic suddenly exploded as a DDoS attack took place.

DDoS Protection allows legitimate web traffic to continue, while stopping suspicious traffic that is likely part of an attack.

> ***"When I received that attack notification, I remember thinking, 'Wow! It actually worked.' The attacker realized the attack wasn't effective and the attack stopped."***

"One morning, I received an alert from the FirstLight Systems IP address, informing me that I was being attacked," explained Eric Coronado, Director of Technology at the Suffern Central School District. "I had never received an email like that before, so I called our FirstLight account executive asking if this message was legitimate. We logged into the DDoS portal – although I had no issues connecting to the portal via my Internet connection – and discovered an attack was being mitigated in real time."

"When you buy health insurance or auto insurance, it's an ongoing expense, but a necessary one – and one you hope you never need," says Coronado. "The last thing I wanted was to be in the news because of a DDoS attack," he added. "When I received that attack notification, I remember thinking, 'Wow! It actually worked.' The attacker realized the attack wasn't effective and the attack stopped."

As for the ongoing issue of cut Internet lines during storms, the school district added a secondary geo-diverse point of presence (POP) so that if its primary Internet connection went down, it could rely on a separate redundant FirstLight connection for backup, maintaining connectivity without disruption.

RESULTS

Today, the Suffern School District is confident that it is safe from DDoS attacks, and its IT staff carefully monitors the portal to gauge any potential future attacks.

The district continues to make smart investments in its infrastructure, knowing its connectivity is more secure than ever. Suffern recently migrated most of its IT infrastructure to the cloud, with reliance on the Internet critical for the 4,000 students and seven campus buildings that make up the district. Since most of its data and applications, like Google and Microsoft, are nestled in the cloud, access to the cloud is essential. "I need to spend a good part of my budget on making sure the Internet is as reliable as possible," Coronado explained.

When Suffern's primary FirstLight Internet connection suffered a recent outage, the new PoP connection kicked in after several seconds. If it wasn't for a system notification informing him of the issue, he would have been oblivious to the problem. "When the primary connection dies, the router changes the pathway to the secondary circuit, and often it's unnoticeable," said Coronado.

"Thank goodness we had it, because if we didn't, we'd be down for several days, and we'd be in the news," he concluded.