




CASE STUDY

Columbia Wireless Ends DDoS Problem with Corero's SmartWall



The Internet Service Provider was under assault from DDoS, and losing customers, until it found a way to automatically detect and block the attacks.

Columbia Wireless is a high-speed Internet Service Provider (ISP) delivering connectivity throughout British Columbia, Canada. The family owned and operated company operates 25 mountain-top towers that provide line-of-sight service to residents and commercial customers across the region. Most of the towers are fully powered by solar and wind generation. Columbia is committed to providing a secure, reliable, and fast Internet connection for all of its customers.

CHALLENGE

Increasing DDoS Attacks Led to Lost Business

In November 2018, Columbia Wireless experienced a Distributed Denial of Service (DDoS) attack that saturated its upstream provider links, effectively bringing down its network service for all customers for about one hour in the middle of a business day.

The company had never experienced such an attack before and was caught completely off guard.



Columbia lost some large clients because of this and it earned them a bad reputation for low reliability. Customers even expressed that they thought the company didn't know what it was doing, in the form of emailed responses to the impact of the DDoS attacks.

The impact on the business was significant, with estimates that the company lost an average \$3,000 per month in revenue, just as a result of the lost clients.

Prior to the first attack Columbia Wireless had about 1,400 total customers, around 25% of which are businesses, and this subsequently decreased to 1,250. Plus, there's no way to measure how many prospective customers have stayed away from the ISP because of word about the DDoS attacks and the service outages they created.

Columbia Wireless has never determined the true motive, or source of the attacks. However, the sense is that it was related to an online gaming platform used by some of the company's residential customers who were targeted by other gamers.

When the attacks occurred, the ISP's only recourse was to use a time-consuming, manual process to try and stop the impact. They had many users that were being impacted, and struggled to find the one IP address that was being targeted. With no automated DDoS attack protection in place this was a virtually impossible task.

IT staff had to painstakingly scan its network connections looking for patterns that would indicate the particular IP address that was getting attacked the most. Once identified, they had to enable "blackhole advertisements" of the IP address being attacked, notifying upstream carriers to stop all traffic to that destination.

"That would stop the upstream carrier saturation, so the rest of our network would not lose Internet service", Leslie said, adding... "of course that meant the owner of the attacked IP address was still completely offline for the duration of the attacks".





THE SOLUTION

Corero's SmartWall DDoS Protection Provides Effective Protection

To address the problem of DDoS attacks and the ineffective process it had for dealing with them, in the Spring of 2020, Columbia Wireless deployed Corero's SmartWall DDoS Protection solution.

Among the reasons the ISP selected the platform, over other DDoS offerings, was that Corero is one of the leading and most experienced DDoS solution providers in the market, Leslie says.

The SmartWall family of DDoS protection solutions is designed to mitigate the full range of volumetric attacks while, at the same time, maintaining the availability of the services it's protecting, by not disrupting the delivery of legitimate network traffic.

SmartWall is capable of handling large network-based DDoS attacks or floods, reflective amplified spoof attacks, and attacks that are typically too low to be detected by traditional out-of-band solutions.

Because the protection system works in real-time and is always-on, it identifies and protects against any attacks which target the network on a daily basis. As the majority of DDoS attacks are now relatively small and short in duration but, can still have a big impact on business continuity, companies need this type of dedicated, always-on DDoS protection solution to prevent attacks from doing damage.

SmartWall leverages an innovative and automated, multi-stage detection and mitigation pipeline to ensure the highest possible protection. It ensures that legitimate traffic isn't affected by damaging false positives or any significant increase network latency.

The solution's Deep Packet Inspection capability looks at every bit of every packet header, and well into the payloads too, to deliver comprehensive DDoS attack protection and visibility for Columbia Wireless. Detection and mitigation occurs in seconds, rather than the minutes or tens of minutes needed by traditional DDoS products and cloud services.

Many alternative DDoS solutions on the market rely on off-site, cloud-based scrubbing technologies and take more than 10 minutes to activate the needed mitigation, Leslie says. By that time, an attack might already have done damage in terms of service downtime. SmartWall handles this on premises so the process is much faster, drastically reducing the likelihood of service interruptions, he says.





BENEFITS

Greater Network Visibility and Zero Downtime from DDoS

Corero installed the SmartWall DDoS Protection platform within a matter of hours, and after about a week of testing Columbia Wireless had the system running on live traffic. "I chose Corero to install the SmartWall system" Leslie says. "as I also didn't want to risk a long period of downtime during the implementation - I trusted the Corero team would do it seamlessly."

SmartWall is installed between the ISP's edge routers and its upstream providers' links. "We have a failover optical bypass installed with the Corero SmartWall system also, so that in the event the SmartWall loses power or suffers a failure, it will failover so traffic can still route," Leslie says.

Columbia is providing the DDoS protection capability as a value-added offering. "We wanted to make sure our entire network didn't go down because of one IP on our network having a DDoS attack," Leslie says.

With the SmartWall solution in place, the ISP is now assured of delivering continuous services to its customers. Since the time the company deployed SmartWall, its network has received about 10 DDoS attacks "and Corero has effectively blocked all of them," Leslie says. "We have not had a minute of downtime."

The technology's automated email notification system, Leslie's favorite feature of the solution, keeps him informed about attacks on the Columbia Wireless network. This gives him greater visibility than ever into DDoS attacks and their resolution.

"I have seen the Corero SmartWall email me—in plain English—about an attack that it is in the process of blocking, when it caught the attack, what kind of attack it is, and what the victim IP was on my network," Leslie says. "It also emailed me to let me know when the attack has stopped. I can't believe how many attacks there are that we didn't even notice before."

The system also includes an analytics capability with a graphical interface that lets users view attacks in great detail. "Basically, it's a fully automated system that lets me stop thinking and worrying about the next DDoS attack and get back to life and growing my business," Leslie says, adding "Among the biggest benefits of SmartWall are its ease of use and reliability".

While Leslie has not yet assessed the difference in terms of revenue or reduced costs, he believes Columbia Wireless will see an increase in revenue as clients "start to warm up to the idea that they will not be impacted by DDoS again in the future. It will probably take close to a year with no successful DDoS attacks before my clients start to fully believe in the product."

Ultimately, all Columbia Wireless clients will benefit from the DDoS protected network, because such attacks made up about 75% of the company's overall network outages, and 90% of outages during business hours.

"This will protect our clients and keep them from [inadvertently] attacking others" via DDoS, Leslie says. "It's very powerful. I'll be able to tell clients we have this amazing solution in place and we should no longer have these attacks. This will be our redemption."

US HEADQUARTERS

Corero Network Security Inc.
293 Boston Post Road West, Suite 310
Marlborough, MA 01752
Tel: +1 978 212 1500
Email: info@corero.com

EMEA HEADQUARTERS

Corero Network Security (UK) Ltd.
St Mary's Court, The Broadway,
Amersham, Buckinghamshire, HP7 0UT, UK
Tel: +44 (0) 1494 590404
Email: info_uk@corero.com

