corero

CASE STUDY

Santa Rosa Communications

Deploys Smartwall to protect customers deep in the heart of Texas

Santa Rosa Communications is a regional ISP serving several communities across Texoma, with an established territory covering Northern Texas and Southern Oklahoma. The company provides residential services such as phone, Internet and television, as well as business-grade voice, Wi-Fi and IT services.

With roots in the rural Texas telephone business since the 1950s, Santa Rosa Telephone Cooperative has provided communication services for many years in Wilbarger County. In 1999, the company began construction of its fiber optic network in Seymour, Texas. In 2006, the team began offering fiber-to-the-home technology to provide customers with access to ultra-fast Internet speeds; and, in 2019, the company experienced continued growth through the acquisition of two other companies: Pinnacle Network Solutions and PCnet, a managed service provider based in Wichita Falls.

CORERO SMARTWALL AT A GLANCE

- Surgically removes DDoS attack traffic automatically, before it reaches critical systems, ensuring optimal performance and maximum availability.
- Delivers line-rate, in-line DDoS attack protection, from 1 Gbps to 100 Gbps per rack unit, in a solution that scales to terabits per second of protected throughput.
- Prevents several attacks, from simple volumetric floods, to sophisticated state exhaustion attacks at Layers 3 through 7.
- Delivers comprehensive visibility for analysis and forensics – before, during and after attacks.

CHALLENGE

The increasing number of Distributed Denial-of-Service (DDoS) attacks were causing trouble throughout the network.

Transient problems led to investigations that revealed legacy systems being easily overwhelmed by the DDoS attacks. This led to poor experiences for customers, downtime, and lots of wasted effort during troubleshooting, with no real resolution, says Seth Tabor, CTO at Santa Rosa.

The growing DDoS attacks experienced would vary in size, intensity and duration. The company would see commodity attacks in the 1-2 Gbps range, on average, a few times a day. In some instances, they would be hit by up to 10 attacks in a single day. Midsize attacks, in the 2-8 Gbps range, would occur almost weekly; and larger attacks would happen every two to four weeks, on average. Tabor said the attacks would last about 15 minutes on average, although they did experience some hour-long attacks reasonably frequently, and multi-hour attacks occasionally.

In response to the growing number of attacks, the only available action the Santa Rosa team could take, was to blackhole the traffic, dropping both malicious and legitimate traffic. Being forced into blackholing (RTBH) also prevents legitimate traffic from getting through, resulting in customer downtime and, ultimately, considerable dissatisfaction.

> "That helped, but was far from the solution we wanted for our customers," says Tabor. "That could offer some protection, but it sacrificed the victim. It was automatic, but it was not ideal. Once the target was black-holed, we could not see the attack, so after the timer expired we would allow the traffic to flow again, and often find ourselves having to black-hole it again."

VALUE-ADDED OFFERING

Santa Rosa has enjoyed additional benefits through the Corero deployment. The ability to perform full scrubbing helped the company land several significant new enterprise customers during 2020. "The fact that we scrub all traffic is a key selling point for the business side," says Tabor.

> "Customers are benefiting, because they must no longer suffer frequent DDoS attacks if they were targeted, or worse, because they happened to be collateral damage, when another customer was attacked," he adds. "The Internet is so important to almost everyone now, so when our Internet service works well, very nearly all the time, it really lets customers do what they want in their lives and businesses."

THE SOLUTION

In early 2020, Santa Rosa decided enough was enough and set about looking for a proper solution to the growing impact of DDoS. After researching the market, they chose and deployed the Corero SmartWall, implementing full inline, always-on, scrubbing for all traffic. "We wanted to protect our entire network and all customers," says Tabor. "We chose inline for simplicity and unobtrusive reactions."

The company now surgically mitigates DDoS inline at every transit peer, effectively scrubbing all inbound Internet traffic. Tabor says the company does still blackhole, or swing to cloud scrubbing, for the very large attacks which would result in transit saturation, but these are much less common.

> "Since we started scrubbing all transit peers, DDoS-related trouble is very rare," says Tabor. "Customer satisfaction is up, and any trouble that remains a mystery, or is directly attributable to DDoS, is way down." The company has also reduced costs through the implementation, by reducing the number of trouble tickets and dispatches.

The team loves how reliable and "hands off" the Corero system is, as well as the visibility and how customers can easily investigate the anatomy of an attack. But there's an even more favorite feature for Tabor: "At the end of the day, the fact it can solve so many problems for us, without intervention, is fantastic!"

"We love the visibility and how we can investigate components of an attack. However, at the end of the day, the fact it can solve so many problems for us without intervention is fantastic."

— Seth Tabor, CTO at Santa Rosa Communications

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