corero [NETWORK SECURITY]

SCG Be More Connected

SCG CONNECTED CASE STUDY _

SCG Connected Expands Business Security Solutions with DDoS Protection from Corero Network Security

Southern Communications Group (SCG Connected) is a rapidly growing, award-winning business with over 50 years of experience connecting people and technology. SCG Connected continues to expand their services to now include telephony, broadband, mobile, and cloud solutions to support the needs of businesses of all sizes across the United Kingdom. The company has realized a 12-fold increase in revenue over the past decade from a strategy of organic growth and acquisitions fueled by its commitment to customer service and innovation.

The Challenge

Moving from a traditional ISDN/PSDN voice provider to next-generation voice over IP (VoIP) has positives and negatives, and one of the negatives is that it expands the threat surface significantly. Additionally, voice is highly sensitive to line overload, which makes it an attractive target for DDoS attacks.

As the Chief Technical Officer at SCG Connected, Matt Wring's role is to develop and deploy platforms that deliver differentiated, value-add solutions to business customers, the majority of which use voice services, not only internet. DDoS protection is one of the company's key criteria for advanced security and threat protection to their customers. However, DDoS attacks are complex to address for several reasons.

Wring explained how building quality of service (QoS) profiles is not an option with broadband and using firewalls to filter traffic creates VoIP jitter. There's also the challenge of protecting the service chain and the different ways in which DDoS attacks can disrupt service availability.

4 Key Reasons SCG Connected Chose Corero

1. Packet Sampling
2. Juniper Integration
3. Feature-rich APIs
4. Multi-tenant capabilities built-in

VoIP expands the threat surface significantly so any part of the service chain can be interrupted. To maintain service availability, SCG Connected needs to be able to protect the entire service chain so that customers can continue to make calls no matter what.

According to Wring, "We can't have the quality of our voice service impacted by a DDoS attack, but we also have to consider the impact of a DDoS attack on the service chain. The customer doesn't care if it's the phone, the switch, the firewall, the router, the line, or the hosted platform that is impacted. It's about service availability. If they can't make a call, they look to us to solve the problem."

The distributed element of a DDoS attack also comes into play. "Usually a threat actor isn't going to directly attack a smaller business, but they will install a bot on their server in order to use the server's compute power to distribute DDoS attacks, and that impacts the line and voice traffic," Wring said.

> "The ability for us to protect customers regardless of the circuit type and before the traffic ever gets to them and stop the distribution aspect is really important."
>
> **- Matt Wring, Chief Technical Officer, SCG Connected**

The effectiveness of the DDoS protection solution to defend against malicious traffic comprehensively and quickly without impacting the quality of service is paramount. However, as an acquisitive business, SCG Connected had additional requirements. They also needed a solution that could scale and was flexible enough to accommodate future acquisitions without a huge jump in cost.

Why Corero

Wring learned about Corero through conversations with industry peers. After product demonstrations, discussions with existing Corero customers, and an R&D project which included simulated traffic testing, four key aspects surfaced that convinced Wring and his team that the Corero SmartWall ONE™ platform was the way forward.

> "Everything we do as a technical team has to fit into three criteria: simplify, standardize, and automate – and that's what Corero does."
>
> **- Matt Wring, Chief Technical Officer, SCG Connected**

1. **Packet sampling.** Corero SmartWall ONE monitors traffic at the ingress point, inspects packets directly, and surgically blocks malicious traffic and allows good traffic to flow uninterrupted. "We wanted a product that didn't do traditional firewall stateful sampling that interrupts traffic because that won't work for us," said Wring. "Corero's approach to sampling doesn't interfere with time-sensitive traffic, so our customers can continue to make phone calls uninterrupted."

2. **Integration with Juniper infrastructure.** SCG Connected uses the Juniper MX platform at the core of their network because of its versatility and capabilities. "Since Corero integrates with Juniper, we didn't have to put another device in line which would add another hop, more jitter, and more cost," said Wring.

3. **Feature-rich APIs.** SCG Connected has a core service program and multiple point programs that need to synchronize data with the core program. Trying to maintain data fidelity manually is error prone and requires additional headcount that is hard to find, so the use of APIs to automate the process is important. According to Wring, "Corero's feature-rich APIs allow us to do this data synchronization across the myriad systems we have with fewer resources and at scale, without having to manipulate the Corero platform."

4. **Multi-tenant capabilities built in.** Corero makes it easy to provide DDoS protection-as-a-service with a highly customizable service portal for per-tenant onboarding and management. Additionally, per-tenant views allow customers to see their own customizable dashboards and receive alerts and reports with more details about the attacks they are being defended from.

The Benefits

SCG Connected has two main driving principles behind the platforms they build: Try to get as close to the factory gate as possible and build with customer service in mind.

Corero's DDoS protection-as-a-service offering aligns to these principles which has allowed the business-to-business communications provider to realize significant benefits.

- **Revenue generation:** According to Wring, "The integration of Corero SmartWall ONE on the Juniper platform allows us to get DDoS protection into the core of our network, add value, and then sell it to more customers which adds margin – that's a force multiplier."
- **Differentiation:** The deployment strategy also allows SCG Connected to differentiate in two ways – by offering premium DDoS protection-as-a-service, and at a fraction of the price of other service providers. "Instead of paying hundreds of dollars per month, customers can pay tens of dollars which adds immense value to their service," added Wring.
- **Customer service at scale:** The more vendor types introduced into a technology stack the more training required and the greater the risk of service degradation. "Standardizing on the Juniper MX platform and managing Corero through an API stack simplifies operation, and that leads to consistency of service delivery as we scale, which is one of our key criteria," says Wring.
- **Long-term partnership:** Looking to the future, as SCG Connected continues to enhance its DDoS attack protection service they plan to leverage Corero's managed services capabilities and deep domain and engineering expertise to help them build additional offerings.

> "We see our partnership with Corero as a long-term relationship. We leaned heavily on the pre-sales team to help us deliver immediate value to our customers, but Corero also has the level of in-life support and through-life development capabilities to help us continue to productize and deliver next-generation services."
>
> **- Matt Wring, Chief Technical Officer, SCG Connected**

Corero SmartWall ONE Highlights

- Surgically and automatically removes DDoS attack traffic before it reaches critical systems, eliminating downtime and ensuring optimal performance and maximum availability.
- Mitigates the impact of a wide range of DDoS attacks, from simple volumetric floods to sophisticated state exhaustion attacks, at Layers 3 through 7.
- Delivers line-rate, in-line DDoS attack protection in a solution that scales to terabits per second of protected throughput.
- Provides comprehensive forensic-level analysis before, during, and after attacks.
- Ensures that legitimate traffic is not impacted by false positives.
- Inspects every inbound packet header and payload data, surgically removing DDoS packets without disrupting the delivery of legitimate network traffic.
- Quickly defends against new and complex DDoS attacks by using Smart-Rules that adapt in real-time, ensuring continuous protection without downtime.
- Detects and mitigates attack traffic in real time instead of the minutes or tens of minutes required by traditional DDoS protection solutions.