CASE STUDY

CNI DEFENDS DDoS ATTACKS WITH CORERO SMARTWALL SOLUTION

>summary

TYPE OF SERVICE PROVIDER
Premier Operations Support and Development Center for next-generation Broadband Service Providers; Regional Backbone Provider in Ohio and Michigan. Wholesale ISP, Transport Provider

SCALE
Protects 200Gbps of transit

SOLUTION
Corero SmartWall® NTD1100

DEPLOYMENT MODEL
Inline, at the network perimeter

COMMERCIAL MODEL
Value-add (no charge) to end customers

Established in 1993, CNI is an Internet Service Provider that was formed through a collaboration of 17 Ohio independent local exchange companies (ILECs). CNI has since grown to 21 ILECs and one electrical cooperative, and it now serves communication providers throughout the United States. CNIprovides IPPBX Voice Services, Cloud Connectivity, DWDM Services, Dedicated Internet Access, and wide-area network (WAN) transport services to meet the needs of businesses and service providers throughout its coverage area.

CNI is committed to operating its network and service with integrity, and to early adoption of new and innovative voice, video, and Internet access and data applications.

>the challenge

CNI's network is targeted by more than 1,000 DDoS attacks per month, that very greatly in duration; most are under 15 inutes, some are around a minute, and some last as long as an hour and forty-five minutes. The attack volumes range from 200 Mbps to 15 Gbps. Prior to deploying the Corero DDoS mitigation solution, CNI attempted to manually block DDOS attacks, but that approach was time-consuming, labor-intensive, and not vary effective. The only alternative was black-holing/null-routing attacked customers, which would have been unacceptablebecause that approach blocks them completely, including their legitimate traffic.
"We needed a proactive, automated approach to protect our customers from DDoS attacks," said Randall Plaisier, CNI's Chief Technology Officer.

>the solution

CNI has two SmartWall® Threat Defense System appliances, connected at 100Gbps, to ensure that only clean traffic gets into the CNI network. The appliances are deployed inline at the network perimeter to provide real-time attack mitigation and network resilience. Both appliances have built-in bypass functionality that allows them to be deployed effectively at the edge of their network, without data continuity risks in the event of system maintenance or a failure.

> *"We looked at many solutions and ultimately chose Corero's SmartWall because we liked the way it reviews and scrubs data, and the fact that it has an optical bypass option in the event of maintenance or failure," said Plaisier. CNI has been a Corero customer since 2017.*

>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 distributed denial of service attack protection, from 1Gbps to 100Gbps per rack unit, in a solution that scales to Terabits per second of protected throughput.
- Prevents the impact of attacks ranging from simple volumetric floods, to sophisticated state exhaustion attacks, at layers 3 to 7.
- Delivers comprehensive visibility for analysis and forensics, before, during and after attacks.

- No need to blackhole or null route all traffic to a DDoS target
- Negligible false positives impacting legitimate traffic
- Maximum levels of service availability are maintained for users, even in the face of a DDoS event
- DDoS attacks are automatically mitigated locally at each of their PoPs, avoiding the need to backhaul traffic across the network for mitigation
- Increased staff efficiency resulting from the automatic and accurate protection
- Increased user satisfaction resulting from the speed and accuracy of protection

>the results for Clouvider

Corero has improved Clouvider's business on two fronts: they're better able to retain existing customers, and they can more easily acquire new customers. It's a competitive differentiator for Clouvider; *"We definitely stopped losing customers; we can retain customers now because we offer top-notch DDoS protection. And, we're also gaining new customers because they had previous experience with Corero's solution and were satisfied with it."*

Because Corero automatically mitigates 99+% of bad traffic, Nowicki says *"I no longer have to respond to alarms saying that we have an attack in progress, or that one of our security analysts can't identify the pattern to then apply the appropriate manual mitigation."* Clouvider's support team members are also happy with the Corero solution because they spend significantly less time working on attack mitigation, due to the automated functionality of the Network Threat Defense appliance that is part of the SmartWall solution. They've seen a 90% reduction in the number of support tickets for attack outages.

About CNI

CNI is an Ohio-based company, formed through a collaboration of 17 Ohio independent local exchange companies (ILECs). After over 25 years of service, CNI has grown its ownership base to 21 ILECs and one electrical cooperative. While still based in Ohio, we have extended well beyond our local service providers to communication providers located throughout the United States. CNI's provides the highest quality communication offering to local providers is found to be an early adopter of new and innovative voice, video, and Internet access and data applications. CNI has added Quality of Service (QoS) and Quality of Experience (QoE) metrics to its traditional voice and IP service offerings. CNI, operates a 24/7/365 Network Operations Center (NOC) and Call Center.

About Corero Network Security

Corero Network Security is dedicated to improving the security and availability of the Internet, through the development of innovative DDoS mitigation solutions. We are the leader in real-time, high-performance, automatic DDoS attack protection, with comprehensive attack visibility, analytics and reporting. Deployed on-premises, hybrid, and in the cloud, we protect thousands of organizations world-wide, across many verticals. The Corero SmartWall® Threat Defense System (TDS) family of solutions utilizes modern DDoS mitigation architecture to automatically and surgically remove DDoS attack traffic, while allowing good user traffic to flow uninterrupted. For more information, visit www.corero.com.

US HEADQUARTERS info@corero.com **EMEA HEADQUARTERS** info_uk@corero.com

corero.com