VentraIP Australia Keeps Hosted Customers Online with Corero SmartWall DDoS Protection

VentraIP Australia is Australia's largest privately-owned web hosting and domain name company, with over 100,000 customers, 700+ servers, and 50 locally-based staff in Melbourne. The company primarily serves small to medium businesses looking to register domain names, host a website, or have email hosting served in Australia. VentraIP Australia has two data centers, each with its own network, with multiple transit and peering providers in each location. It has 60Gbps of total capacity in each data center (transit and peering combined).

The Challenge

DDoS attacks have always been a problem for web hosting providers, due to the number of websites they host; there will always be a website someone doesn't like, or a competitor, or any other number of reasons that someone will want to attack a website. "In the past, there were many DDoS attacks, and during each one we would have to call our transit provider, and it was like fighting fire to look into the server and block IPs so that no attack traffic at all reached the server," said Kyle Thorne, Chief Technical Officer, VentraIP Australia.

During the 2017 Christmas holiday period VentraIP Australia was hosting a cryptocurrency website; for some unknown reason a cybercriminal in the United States started targeting the website with a heavy DDoS attack. "The timing was bad because we had just changed transit providers, and our new transit provider was fairly inexperienced and didn't yet have a DDoS mitigation platform (despite telling us they did), so our only option at the time was blackholing IPs," said Thorne. Blackholing IPs obviously isn't a desirable solution when potentially dozens or hundreds of customers are using the same IP address; when that IP doesn't route anywhere, hundreds of websites go offline. Customers submit support tickets, complain, and sometimes move to another hosting provider, if the downtime was too intolerable. The holiday DDoS attack against VentraIP Australia's customer continued for approximately one week, causing many problems for customers on that same server/IP, until eventually VentraIP Australia was able to use the DDoS mitigation services of another company in Australia that filtered the traffic and passed it to VentraIP Australia over a peering link.

The Solution

After that December 2017 incident VentraIP Australia didn't want to rely on another company (either its transit provider, or another host) to filter attack traffic for them. They started researching DDoS mitigation solutions, asked other Australian providers what they use, and for their opinions. Thorne said, "A company we're fairly close with was using NSFocus, who said while it did work, it was expensive, and fairly limited in what it could do, and they themselves were looking at Corero's SmartWall® Network Threat Defense, so we got in contact with the Corero sales team and went forward from there."

One of the many reasons VentraIP Australia chose Corero is because it offers flexible implementation options (in-line, or out of band), and is extremely effective in automatically defending against attacks. "Every other network device had hiccups but we had literally zero problems with Corero," said Thorne.

The Implementation

In May 2018 the company tested two Corero Network Threat Defense appliances, with zero-power bypasses, in its Melbourne network (which carries much less traffic than their Sydney network). They left the solution in monitor mode for one week, then switched it to mitigate mode. After the three-month trial VentraIP Australia added two Corero appliances in Melbourne, as well as the two in Sydney, again leaving them in monitor/detect mode for roughly a week before switching automatic protection on. As a result, VentraIP Australia now has 80 Gigabits per second of automatic real-time DDoS protection across its network.

VentraIP Australia uses Simple Network Management Protocol (SNMP) monitoring on the Corero appliances, and has its own thresholds set for different metrics. They have email groups that get alerted, as well as graphs displayed at its Network Operations Centers so they can immediately know when and how many packets are being blocked during an attack.

Since implementing the Corero SmartWall solution VentraIP Australia hasn't had any period of server/network downtime caused by a DDoS attack. "Every attack has been filtered very quickly, and we haven't heard any feedback or complaints about attacks, which is exactly what we want. That's how we know the Corero appliances are doing their job," said Thorne.

Benefits

It didn't take long to install and configure the Corero solution before VentraIP Australia began realizing the benefits. "There were zero problems for the three months we tested; no legitimate traffic was dropped, and the few attacks that we did have were blocked as expected," said Thorne. Since implementing the Corero solution VentraIP Australia has detected a couple occurrences of outbound attacks from virtual private servers (VPS), which they previously would not have noticed; in such cases not only does the attack not leave VentraIP Australia's network (which is good for their reputation), but it also allows VentraIP Australia to contact those customers and tell them what their VPS is doing and, if it's intentional, suspend them. "There have also been a few attacks to our company websites/customer control panels that, in the past, would have affected hundreds or thousands of customers trying to order or manage products, but thankfully those were unaffected since the Corero SmartWall appliances were installed," said Thorne.

Real-Time Mitigation

One of the key benefits of the Corero SmartWall is its real-time automatic mitigation. "Not having to have someone 'on call' to manually enable mitigation is extremely helpful. We don't have to worry about having one of our network administrators near their computer 24/7. Now that we have automatic alerts, we see attack attempts every few days, and we can see in real time that the attacks are blocked," said Thorne.

Excellent Customer Support

Another significant factor in VentraIP Australia's success and satisfaction, is Corero's excellent, highly-experienced, round-the-clock customer support. "We've had suppliers in the past who don't reply to support tickets for days, and when they do, they are barely helpful. We haven't needed support more than a few times, but when we do the Corero support team replies within a few hours, and are always very helpful," said Thorne.

Competitive Advantage

VentraIP Australia offers the benefits of Corero's SmartWall DDoS protection to all of its customers, as a value-added service. It sits in front of all the other services they offer, which is a big differentiator in the Australian hosting provider marketplace. "Other hosting providers are smaller so they rely on upstream transit providers rather than provide DDoS protection like we do," said Thorne. "We are able to guarantee our customers consistent service availability because we have our own on-premise DDoS mitigation platform; that's been a competitive differentiator," he added.

Corero SmartWall At a Glance

- Provides 80 Gigabits of protection across the VentraIP Australia network, including VentraIP Australia's own customer control panels
- Surgically removes DDoS attack traffic automatically, before it reaches critical systems, ensuring optimal performance and maximum availability
- Delivers line-rate, in-line, denial of service protection from 20Gbps to 100Gbps, per rack unit, in a solution that scales to Terabits per second of performance
- Prevents the impact of attacks ranging from simple volumetric floods, to sophisticated state exhaustion attacks, at layers 3 to 7
- Delivers comprehensive visibility for attack analysis and forensics

Results for VentraIP Australia:

- Black-holing of traffic is avoided
- No longer rely on another company to filter DDoS traffic
- Maximum levels of service availability are maintained for hosted customers, even in the face of a DDoS event
- DDoS attacks are automatically mitigated locally at each of their multiple locations across Australia
- Reduced staff numbers and time required for handling DDoS attacks
- Improved customer satisfaction
- Improved brand reputation
- Service offering is differentiated from competitors

corero

As the DDoS threat landscape continues to evolve, enterprise, hosting and service provider customers around the world rely on Corero for industry-leading defense systems to provide 24/7, automatic attack mitigation services, with threat visibility, sophisticated reporting and analytics. For over a decade, Corero has been providing state-of-the-art, highly-effective, automatic DDoS protection solutions.

For more information, visit www.corero.com