corero

CASE STUDY

A2 Hosting Finds an Effective DDoS Protection Solution

A2, a Web hosting company, overcame the problem of DDoS attacks on its network by implementing Corero's SmartWall® Threat Defense System.

A2 Hosting is a high-performance Web hosting company located in Ann Arbor, Michigan. The company's mission is to provide customers with ultra-reliable services and continuous, U.S.-based support from its Guru Crew team. Since 2003, A2 Hosting has offered innovative, affordable, and developer-friendly hosting for small and medium-sized businesses and Web professionals worldwide.

Customers seeking fast hosting options can host Web sites of any size on A2 Hosting's Turbo server platform, which features page load speeds up to 20 times faster compared with competing hosts. The company's solutions include shared hosting, reseller hosting, virtual private server (VPS) hosting, and dedicated server hosting.

CORERO SMARTWALL AT A GLANCE

- Surgically and automatically removes DDoS attack traffic, before it reaches critical systems, ensuring optimal performance and maximum availability
- Delivers line-rate, always-on distributed denial of service attack protection, in a solution that scales to tens of Terabits per second of protected throughput
- Prevents impact from even the most sophisticated DDoS attacks ranging from volumetric floods, to state exhaustion attacks, at layers 3 to 7
- Delivers comprehensive visibility for analysis and forensics, before, during and after attacks

The DDoS Problem

Like many hosting companies, A2 Hosting has been targeted by Distributed Denial of Service (DDoS) attacks, sometimes on a daily basis, and over the past several years has found that those attacks have become increasingly sophisticated and difficult to mitigate. If not mitigated, DDoS attacks can cause downtime or service disruption, not only for the hosting provider but also its customers. Even an indirect hit on a customer site could cause collateral damage to a hosting provider's other customers who co-reside or are reliant on the infrastructure transporting the attack.

Most DDoS attacks are relatively small and short in duration, but they can still have a big impact on the availability of applications and services. For that reason, organizations increasingly need always-on DDoS protection to ensure their business continuity. For A2 Hosting, most DDoS attacks are small in volume and short in duration, some of which are not very noticeable to human security analysts. However, the company has experienced several attacks that registered over 100 Gbps.

Previous Vendors Failed to Solve the Problem

Over several years, A2 Hosting deployed a series of low-cost DDoS protection offerings from various security vendors, but none of those were easy-to-install, easy-to-use, or effective. Even the automated systems that were supposed to flip the bad traffic to a cloud scrubbing service frequently failed, often requiring manual intervention. Furthermore, those solution providers failed to provide good customer support. That combination of poor functionality and poor customer support sometimes resulted in extended downtime for the company's customers. Bryan Muthig, founder and CEO of A2 Hosting, states,

> "When you have a severe DDoS attack, every second counts, yet our previous vendors did not respond quickly when we really needed them to get our services back online."

THE CORERO SOLUTION

To effectively address the ongoing DDoS problem, A2 Hosting consulted with other Web hosting providers to see what they were using for DDoS mitigation. The company narrowed down its options to two vendors: Corero, and one of Corero's large competitors. After discussions with other industry veterans, and getting a better understanding of each vendor system, it became clear that Corero was the right solution.

A2 Hosting deployed Corero's SmartWall DDoS Protection platform in early 2020. Among the key attributes of the solution that appealed to A2 Hosting were its high performance, reliability, ease-of-use, and ease-of-deployment.

> "The implementation process was quick and uneventful," said Muthig.

Deep Packet Inspection

One of the key features of Corero's SmartWall TDS is its automated, multi-stage detection and mitigation pipeline that ensures the highest possible protection against DDoS. The solution can handle large network-based DDoS attacks or floods and reflective amplified spoof attacks, as well as attacks that are generally too small to be detected by traditional out-of-band systems.

This protection is built around the mantra of "do no harm" to ensure that legitimate traffic is not impacted by false positives. The SmartWall delivers comprehensive DDoS protection and visibility by inspecting every inbound packet header and payload data, and surgically removing the DDoS packets without disrupting the delivery of legitimate network traffic. Corero's Smart Rules leverage heuristic and closed-loop policy, allowing them to be reconfigured and deployed on-the-fly, thereby enabling organizations to respond rapidly to evolving, sophisticated DDoS attacks. This process of detection and mitigation typically occurs in under a second, rather than minutes, or tens of minutes, as with traditional DDoS protection solutions.

Always-On Protection

Because the SmartWall appliance works in real-time and is always operating, it identifies any attacks and protects the networks against these before any damage is done. The Corero solution has been consistent in stopping all DDoS attacks well before they can have an impact on A2's network or the applications and services running on it.

The Deployment Model

A2 Hosting deployed SmartWall appliances in all of its data centers, located in Arizona, Michigan, Amsterdam, and Singapore. The Web hosting company is using these appliances in conjunction with a cloud scrubbing service from Corero, which is delivered with their partner Neustar. The cloud service adds more than 11 terabits of cloud-based protection to the defenses, across 14 global datacenters. The cloud scrubbing, when activated, returns cleaned traffic to A2 Hosting's locations via the on-premises SmartWall appliances for final inspection, before legitimate traffic is allowed onto the network.

The Corero Cloud Hybrid protection ensures that, regardless of where an organization is located, attacks in danger of saturating incoming links can be quickly redirected to one or more of the dedicated multi-terabit scrubbing centers around the globe. This seamlessly returns clean traffic to maintain the highest-quality service, regardless of the DDoS attack size.

> The Corero Threat Defense Cloud service "gives us a great insurance policy for large attacks," says Muthig.

VALUE-ADDED OFFERING

A2 Hosting offers DDoS protection for free to all of its customers, as a value-added service. "In this day and age, attacks are inevitable and our interests are aligned in keeping our customers online and happy," Muthig says. "We don't need to charge extra for that."

Saves Time for A2 and their Customers

One of the most important benefits of SmartWall is that it allows A2 Hosting to focus on its core business. The platform has significantly decreased the number of incidents the company has to handle. "We've gone from being constantly distracted by DDoS attacks, to only occasionally having to intervene," Muthig says. "Prior to the Corero solution, our technical people were constantly dealing with DDoS; they were focused too much on fixing outages," he says. Now they are free to focus on project work and pursue more productive, innovative tasks. This benefit extends to A2 Hosting's customers as well, because it enables them to focus on their core business instead of worrying about DDoS attacks.

Improves Brand Reputation

Improved standing among customers is another big benefit of the deployment. In the past, when major outages occurred, some customers would take to social media to blast the hosting provider with bad reviews. Since the company rolled out the Corero solution, Muthig has observed a marked improvement in A2's reputation, and a huge reduction in the customer churn that sometimes followed the network outages that had been caused by DDoS attacks.

> Muthig says, "It's difficult to quantify the financial gains made possible by the new DDoS protection measures, but the consensus is we wouldn't want to go back to the way it was, prior to implementing the Corero solution."

BENEFITS FOR A2

- No need to blackhole or null route traffic
- No blocking of legitimate customer traffic
- Maximum levels of service availability are maintained for customers, even in the face of a DDoS event
- DDoS attacks are automatically mitigated
- Saved time for engineers so they can focus on the core business
- Improved brand reputation and customer reviews
- Reduced customer attrition
- Increased acquisition of new, larger customers

With the Corero SmartWall Cloud Hybrid solution in place, A2 Hosting is now able to effectively identify and stop DDoS attacks of all sizes, quickly, automatically, and effectively. Its entire network infrastructure is protected by Corero. And, the setup is still new, so results will only improve as A2 technicians tweak the settings to work best for the company's environment. "We feel comfortable that we have a strong set of tools in place for our network to be able to handle DDoS more effectively than ever," Muthig says.

> "The maturity and quality of the product, and the level of support we're getting, is far superior to what we've had in the past. Right out of the box it worked better than the previous solutions we tried."

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