CASE STUDY

TIER-2 SERVICE PROVIDER CHOOSES CORERO TO DELIVER DDoS PROTECTION AS A SERVICE

>summary

SCALE

Distributed edge with a combination of 100Gbps and 10Gbps transit and peering circuits, providing over 1Tbps of redundant capacity

SOLUTION

Corero SmartWall® Edge Threat Defense with NTD1100 protection devices

DEPLOYMENT MODEL

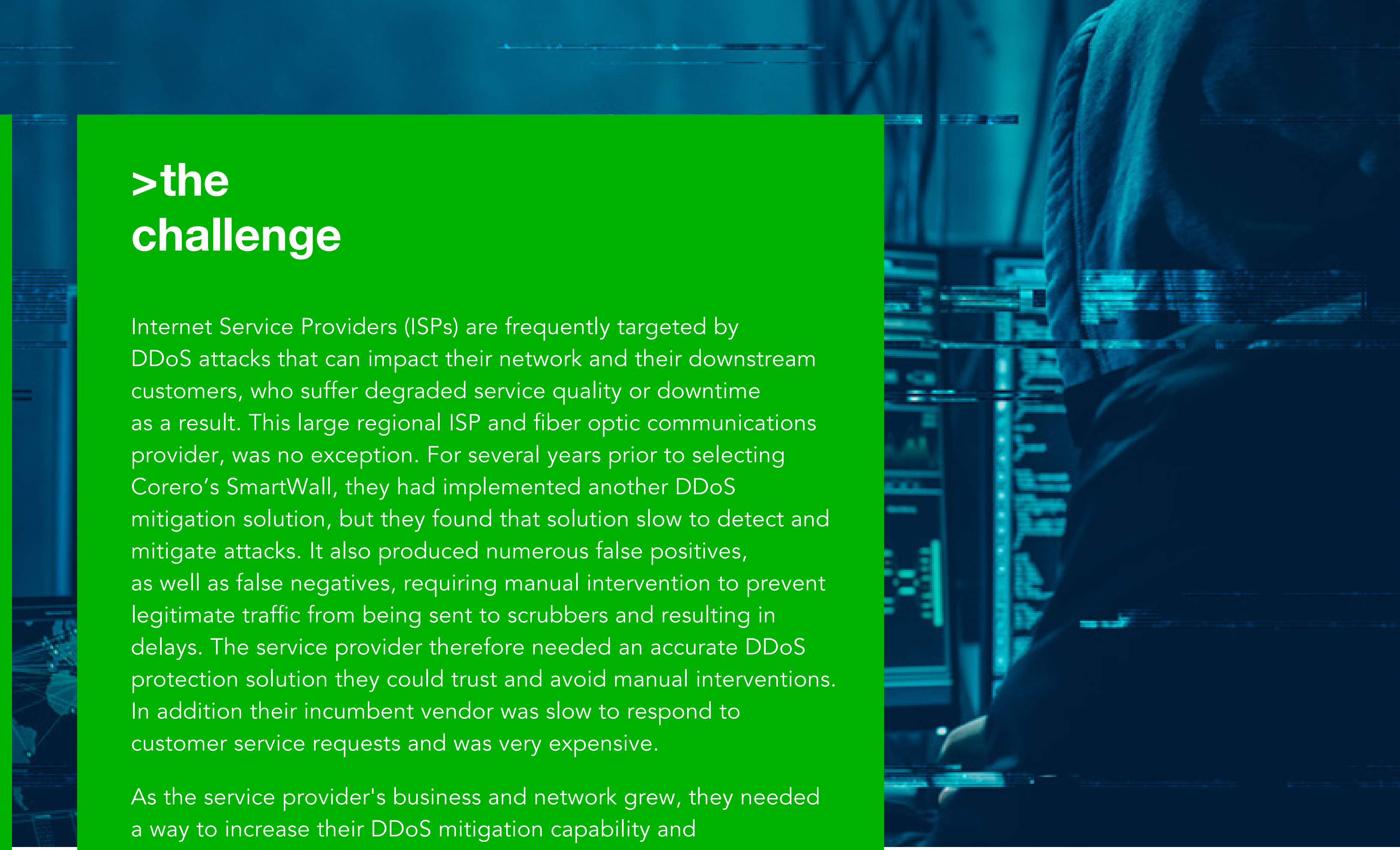
Edge Detection with automatic redirection to scrubbing device

COMMERCIAL MODEL

Subscription-based service for tenant customers

This US based, regional Tier-2 service provider delivers fiber-optic data, internet, data center, cloud unified communications, and managed services to enterprise and carrier customers throughout the Northeast and mid-Atlantic region.

Its 25,000-route-mile network connects nearly 13,000 lit locations, with access to an additional 125,000 locations.



>the challenge

Internet Service Providers (ISPs) are frequently targeted by DDoS attacks that can impact their network and their downstream customers, who suffer degraded service quality or downtime as a result. This large regional ISP and fiber optic communications provider, was no exception. For several years prior to selecting Corero's SmartWall, they had implemented another DDoS mitigation solution, but they found that solution slow to detect and mitigate attacks. It also produced numerous false positives, as well as false negatives, requiring manual intervention to prevent legitimate traffic from being sent to scrubbers and resulting in delays. The service provider therefore needed an accurate DDoS protection solution they could trust and avoid manual interventions. In addition their incumbent vendor was slow to respond to customer service requests and was very expensive.

As the service provider's business and network grew, they needed a way to increase their DDoS mitigation capability and remove the need to backhaul attack traffic across their network. They wanted a solution that did not create latency issues, or false-positives for their customers, and which reduced the potential of completely missing attacks.

>why they chose Corero

"The Corero solution is head and shoulders above our prior solution," said the customer's Head of Network Engineering. After vetting several DDoS protection vendors, we selected Corero because of their unique approach to DDoS protection. *"Corero offers features that no one else has, and the Corero SmartWall mitigates attacks in seconds rather than minutes, compared to the previous mitigation solution."* he continued.

The Corero appliance samples traffic, detects any attacks, and sends over a Border Gateway Protocol (BGP) FlowSpec, which is faster than waiting for BGP to propagate a route change. *"Our redirect is much faster - seconds vs minutes - because we are doing an out-of-band 100gig redirect with one-arm, instead of waiting for the BGP to update,"* explained the customer. *"Using BGP FlowSpec rather than BGP routing updates is what makes this system so much faster than our previous installation. It requires no more transporting of redirected traffic; it all stays at the border, at our peering routers,"* he added. *"As a one-arm solution, the NTD1100 saved us half a million dollars on transport."*

"With Corero, we've been able to save time and money both in terms of initial set up costs and in the cost of our SOC analysts' time spent fire-fighting DDoS attacks on our network."

Corero system engineers worked with the service provider to understand their network set-up, delivering a solution that met their specific requirements.

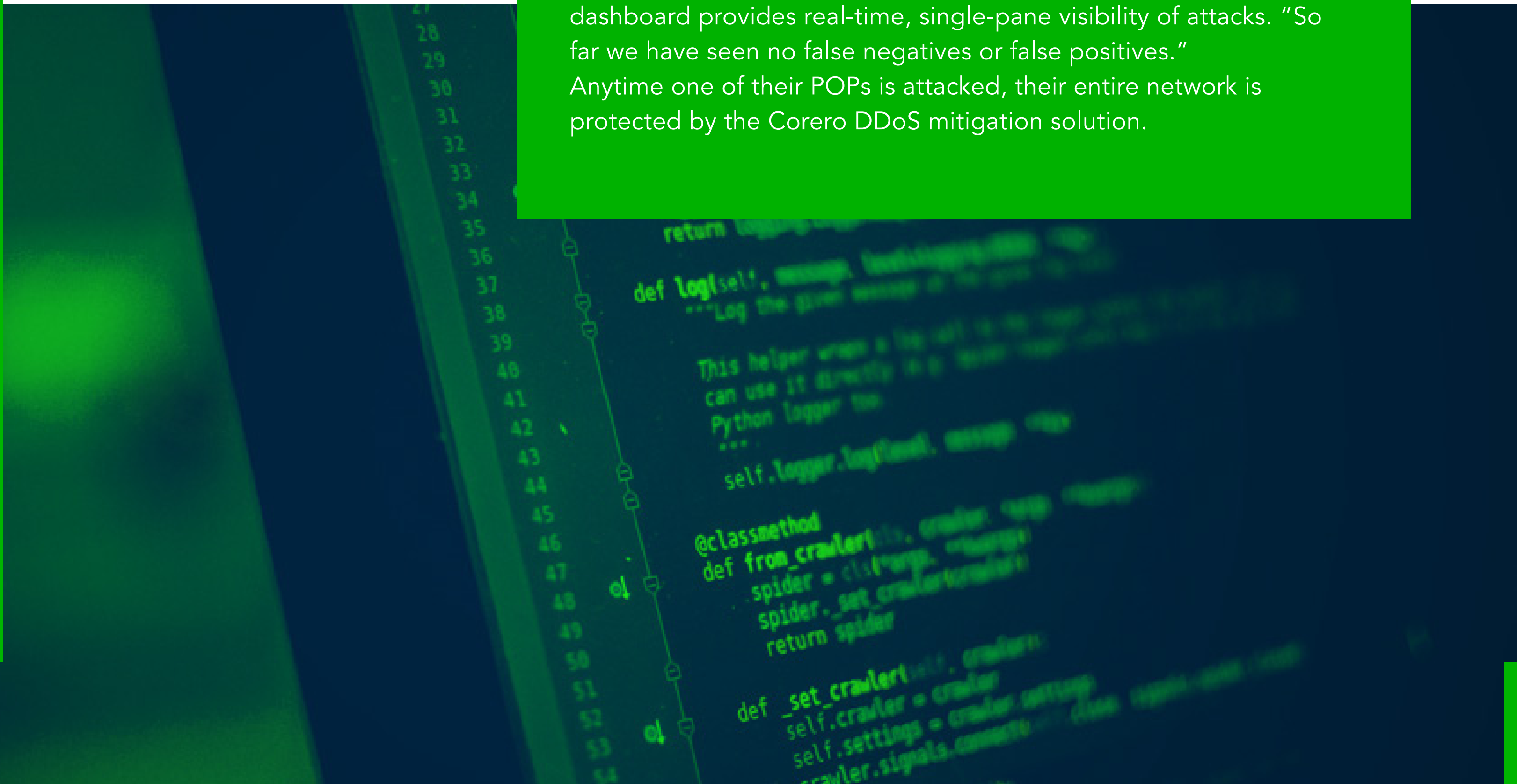
> *"Other DDoS vendors wanted us to BGP everything, or do in-line, but we can't do in-line because we are geographically diverse."*

Corero's true deep packet analysis is one of the biggest advantages. It inspects packets in real-time, as an attack is taking place, to determine which packets are valid and which are attack traffic. For the service provider, this capability to deeply analyze packets during attacks is invaluable because it ensures the system is running correctly, and instantly provides clear information about why a given packet was blocked. With Corero's automated packet filtering, their Security Operation Center (SOC) staff have the option to analyze traffic to make sure that it is valid, but at the same time, they have the reassurance that they don't need to spend time manually analyzing everything. Ultimately, this function saves them many valuable man-hours; time that can be spent on other priority tasks.

>the results

No impact from false positives or false negatives

Corero keeps their network clear of bad traffic, and the user dashboard provides real-time, single-pane visibility of attacks. "So far we have seen no false negatives or false positives." Anytime one of their POPs is attacked, their entire network is protected by the Corero DDoS mitigation solution.



Protection for the service provider's entire network

By using Corero's SmartWall to manage its core network, the service provider can offer additional DDoS protection as a service for those customers that need a higher level of protection. *"It is a big advantage that we can use the same platform to protect our own network and offer granular DDoS protection for our customers."*

Subscribers reap the benefits

Customers subscribing to the service provider's DDoS network protection service can now rest easy knowing that they have 24/7 defense in place to mitigate potential attacks that might otherwise cripple their critical network traffic.

The Corero SmartWall detects anomalies in network patterns in real-time, and alerts subscribers to unusally high levels of incoming connections from one or more sources. These customers pay a set monthly fee, regardless of the number of DDoS attack attempts, or the scale of the attacks.

Attack reporting is provided via a user-friendly portal, along with automated notifications, filters, and alerts. *"The multi-tenant portal is excellent, because it is very interactive and offers a lot of good data without being overcomplicated. It is very customizable so we can make things easier to view, and it gives customers the data they need so they can analyze what attacks were mitigated."* Recently, the Corero SmartWall mitigated a 34-gig attack on one of the service provider's customers; without protection, that attack would have knocked the 30G internet customer offline. Instead, service was able to continue uninterrupted.

The Corero SmartWall detects anomalies in network patterns in real-time.

> *"Our customers are definitely better off. We have 10 times the mitigation we had before, and so many more features at our fingertips. We haven't had a single complaint from any customer about downtime."*

Easy to Enroll Subscribers

The Service Provider has found that its customers are very eager to get DDoS protection, and Corero made it easy for them to promote its new service. *"The information packages Corero produce for our marketing and sales teams have helped us to resell the service. No other vendor offers that sort of additional support,"* said the customer.

Easy to Deploy and Energetically Efficient

The Corero system is designed to be plug and play and only took a couple of hours to set up. *"Even the tuning process was minor"* commented the customer, *"compared to our previous DDoS solution, Corero has been easy to implement. The appliances use very little energy and take up very little space."* He added that *"the energy efficiency of these boxes is better than anything I've ever seen on the market. Corero's 200 gig chassis uses less power than our previous 40 gig solution."*

Implementing Corero's SmartWall was straightforward and simple.

> Corero SmartWall highlights

- Operates in real-time, 24/7.
- Surgically and automatically removes DDoS attack traffic before it reaches critical systems, eliminating downtime, ensuring optimal performance and maximum availability.
- Delivers line-rate, always-on DDoS 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 incidents.
- Delivers 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 the DDoS packets without disrupting the delivery of legitimate network traffic.
- Corero's Smart-Rules leverage heuristic and closed-loop policy, so rules can be reconfigured and deployed on-the-fly, thereby responding rapidly to evolving, sophisticated DDoS attacks.
- Detects and mitigates attack traffic in under a second; not minutes or tens of minutes, as with traditional DDoS protection solutions.