TeraGo Uses Radware's DDoS Attack Mitigation System to Power New Suite of Security Services

Business Need
TeraGo Networks owns and manages a national IP network, providing service to 46 major markets across Canada. The company required a market-leading DDoS detection and mitigation solution to protect its own infrastructure and to offer its customers a new suite of security services across its telco, data center and cloud hosting environments.

Why Radware's Solution
TeraGo Networks deployed Radware's Attack Mitigation System (AMS) to replace the company's existing RTBH-based security solution because it provides a more advanced, behavioral-based DDoS protection, higher levels of automation and for its simplicity of implementation.

Solution
Radware AMS is a real-time, behavioral-based cyber security solution that protects an organization's applications and networks against known and emerging threats, including DDoS, Internet pipe saturation, and SSL-based flood attacks.

Benefits
TeraGo's entire data center and cloud computing infrastructure is protected by AMS, reducing TeraGo's response times in the event of a cyber-attack and providing more value to customers while protecting their mission-critical systems. In addition, it has allowed TeraGo to offer its customers a suite of DDoS mitigation services, providing new business opportunities for TeraGo.

Overview

Headquartered in Ontario, Canada, TeraGo Networks owns and manages a national IP network, providing service to 46 markets across Canada. The company operates seven data centers, including two Tier 3 data centers in Mississauga, Ontario and Kelowna B.C. With its acquisition of RackForce Networks Inc., TeraGo now also offers a full line of cloud computing and storage devices. TeraGo is proud to help businesses save on costs and operate with greater efficiency by providing complimentary IT services that meet their telecom and data needs.

Challenges

As a provider of cloud computing and storage services, a cornerstone of TeraGo's business is ensuring that data is transported and stored with no risk of compromise or loss. Previously, TeraGo deployed remotely-

"With Radware's attack mitigation system, we can offer customers multiple DDoS mitigation options, allowing them to maintain business continuity while protecting their most vital asset – their data"

- Stewart Lyons, CEO at TeraGo

triggered black hole (RTBH) filtering to protect its IT infrastructure against attacks. Unfortunately, legitimate traffic could be blocked and TeraGo customers experienced slower response times.

Moreover, a volumetric DDoS attack against either TeraGo or one of its own victims could have a trickledown effect whereby multiple TeraGo customers could be impacted, resulting in dissatisfied customers and increased customer attrition.

Lastly, RTBH filtering could not be commoditized, preventing TeraGo from launching a suite of DDoS mitigation services that hit at the heart of what customers were requesting – a service to protect their business from an attack, allowing them to stay operational and available during a cyber assault.

The Solution

TeraGo selected Radware's AMS for its simplicity of implementation and the solution's ability to detect and clean traffic seamlessly, as well as providing new business opportunities for TeraGo.

Radware AMS is a behavioral-based real-time signature technology that detects and mitigates emerging network attacks in real time, such as zero-minute attacks, DoS/DDoS attacks, and application misuse attacks—all without the need for human intervention and without blocking legitimate user traffic.

Benefits

Since its implementation, AMS has averted a number of DDoS attacks that leveraged multiple source machines and dynamic IP addresses. AMS's built-in device fingerprinting constructed dynamic attack signatures to successfully protect the networks of TeraGo and its customers. Radware now protects TeraGo's IT infrastructure and customers without the need for human intervention, thereby reducing response times and providing more value to its customers.

Radware's AMS is now resold to TeraGo's customers as well, allowing them to protect their own IT infrastructure as well. The TeraGo services both detect and mitigate the attack when it arises. Throughout an attack, customers who purchase the service will retain connectivity, while the mitigation systems filter traffic, allowing clean traffic to pass and illegitimate traffic to be quarantined.

CRP-TeraGo-CS-01-2016/08 - US

radware