DSL Provider Establishes First Line of Defense Against Evolving DDoS Attacks

About the DSL Provider

This customer is a leading service provider in Canada. The company offers Internet connectivity and VoIP services to Canadian residential consumers and business customers. It is one of Canada's most experienced digital phone service (VoIP) providers and it delivers leading-edge Internet and network services, award winning voice services, and cloud-based phone systems (Hosted PBX).

Challenge

This service provider has been an Allot customer for almost a decade, having deployed Allot security solutions for inbound volumetric DDoS protection.

They originally approached Allot following a relatively large DDoS attack on their network. They could foresee the potential risk of scaled up attacks and decided to use DDoS mitigation to ensure that its network and its customers are protected from attacks and to prevent any collateral damage to its users.

At the same time, it was important that the implementation of robust security did not adversely affect network performance or the user experience. The challenge was to offer our customer value-added security features that would protect its network from DDoS attacks while assuring network services availability and consistent application QoE. Our customer needed a solution that was easy to integrate with its existing offering; one that could quickly identify inbound attacks, automatically mitigate those attacks, and provide protection with precision.

As time progressed, the solution needed to be seamlessly scalable and flexible, responsive to changing circumstances and new threats.

Vertical | Service Provider

Industry | Fixed

Region | North America

Solution | DDoS Protection

Challenge

o Rising frequency and volume of DDoS attacks on the network

o QoE at risk of being impacted by future attacks

o Need to integrate with existing solution

Solution

The service provider was already using Allot Service Gateways to monitor their network and generate valuable insights from their network data. Now they were able to benefit even more from our DDoS Secure product, which enables protection and mitigation of attacks in real-time. They wanted a "future-proof" solution, which made our scalability a vital factor in their decision. Being able to monitor everything from a unified portal sealed the deal for this long-time customer.
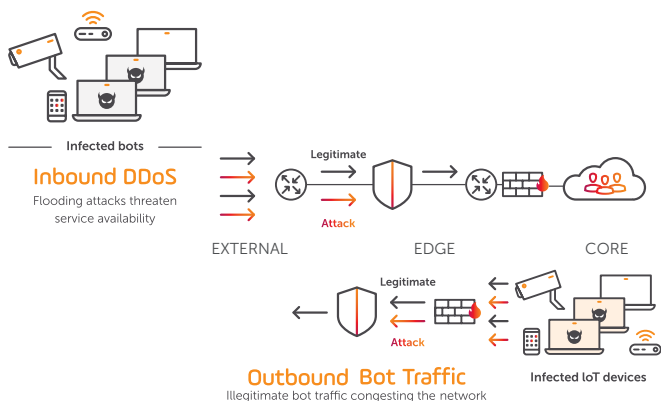
Benefits

o Gain full visibility of DDoS attacks and valuable threat intelligence

o Assure service availability and maintain high QoE

o Seamless scalability to address future need and delay infrastructure investment

Solution

Initially, the customer deployed Allot high performance DDoS detection sensors on its own servers, and the Allot Service Gateway Omega (SG-Omega) platform that it implemented for service deployment, delivery, and management. The SG-Omega was subsequently upgraded to the next-generation Allot Service Gateway Sigma E platform, on which our customer was able to activate the Allot DDoS Secure license.

DDoS Secure provides high-speed real-time detection, reporting and mitigation of DDoS attacks from the Internet. It reinforces service continuity by ensuring that services are uninterrupted and there is no collateral damage to non-targeted users (aka, innocent bystanders). Users are completely unaware of a DDoS attack on the network because there is no degradation to the quality of their service delivery.

As our customer anticipated, the challenge from DDoS attacks has become increasingly sophisticated and varied over the years. Allot was able to seamlessly scale the solution with its latest DPI-based platform, Allot Service Gateway Tera, to expand DDoS protection across the customer's national network. With Allot, the customer has the capability to deliver traffic management to ensure QoE, application control for QoS, and DDoS protection. Allot's solution is strategically deployed at a network level to

Inbound DDoS
Flooding attacks threaten service availability

EXTERNAL   EDGE   CORE

Outbound Bot Traffic
Illegitimate bot traffic congesting the network

Infected IoT devices

provide robust security for the network. Allot DDoS Secure is activated within the Allot Service Gateway multiservice platform already deployed in the network. From its inline vantage point, Allot inspects 100% of the network traffic and provides the industry's fastest and precise mitigation; Time to Mitigate < 60 seconds.

This service provider was the first Allot customer to deploy Allot DDoS Secure in North America. With Allot, it has been able to successfully mitigate attacks with increasing volumes year after year. Today, Allot helps this customer to mitigate a varied range of attacks including TCP (SYN) floods, UDP and HTTP floods, and NTP amplification.

> The Allot solution protects our network from DDOS attacks so that services are resiliently delivered, and our customers maintain their quality of experience"

Director of Network Engineering,
CSP, Canada

Benefits

Allot was chosen by this service provider for its ability to combine QoS with DDoS protection at a competitive price point with a solution that maintains subscriber quality of experience through an attack. By deploying Allot DDoS Secure within the Allot Service Gateway, the customer has been able to:

o   Protect subscribers from the largest volumetric DDoS attacks

o   Mitigate and avoid risk to the network and services

o   Address the changing nature of security challenges

o   The operator can confidently provide reliable access and protection for all users, and a consistently high QoE across its networks.

Resources

About DDoS Secure

About Service Aware DDoS Mitigation

Frost & Sullivan DDoS Mitigation Whitepaper

Learn more about Allot's Solutions »

allot   See. Control. Secure.

www.allot.com