Case Study

Global Tier-1 Internet Service Provider, India

genie NETWORKS

Business Need

The customer is one of the largest Tier-1 internet service providers in the world and a leading Managed DDoS Security Service Provider (MSSP) in India. A highly effective DDoS solution with seamless scalability was required to expand its DDoS architecture globally.

Solution

The customer chose to deploy Genie's Solution for many years to detect and protect its network against major DDoS floods. It also used the solution to offer clean pipe services to its end customers creating extra revenue streams.

Why Choose Genie

Genie Networks delivered a highly effective Out-of-the-Path DDoS solution with behavior-based detection and the option to integrate seamlessly with the customer's mitigation method. The solution offered a 3-tier architecture for xFlow collection, anomaly detection, reporting and MSSP Portal with seamless scalability and failover at each layer.

Overview

The customer is one of the largest global Tier 1 Internet Service Providers (ISPs) and one of the major clean pipe solution providers in India. Being a competitor in the DDoS market, the customer also aims to be a global top DDoS Managed Security Service Provider. Asides from providing internet bandwidth to a large database of consumers, it also offers a range of network services, hosting, cloud services, unified communications, mobility and IoT solutions.

Challenges

Being a service provider and considering the need for an Out-of-Path solution, xFlow is the major technology that can be used for DDoS detection and protection. The customer had many global PoPs to serve its global end customers and therefore needed a solution which can be scaled seamlessly across geographical locations globally. The solution needed to provide accurate and fast DDoS and anomaly detections with seamless failover at each Layer, irrespective of failure at any geographical locations.

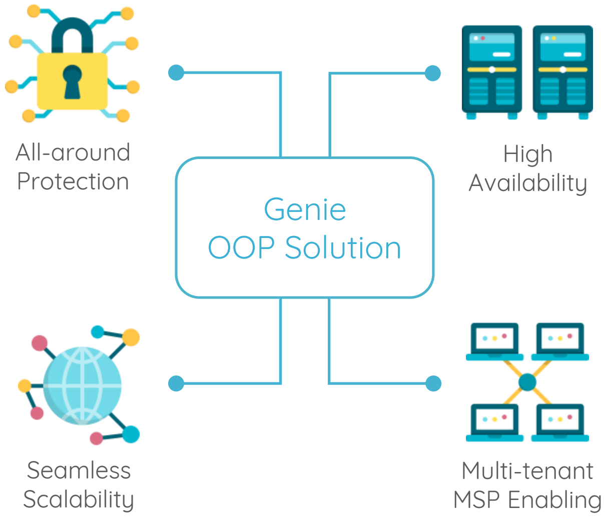

Figure 1: Out-of-Path Solution by Genie Networks

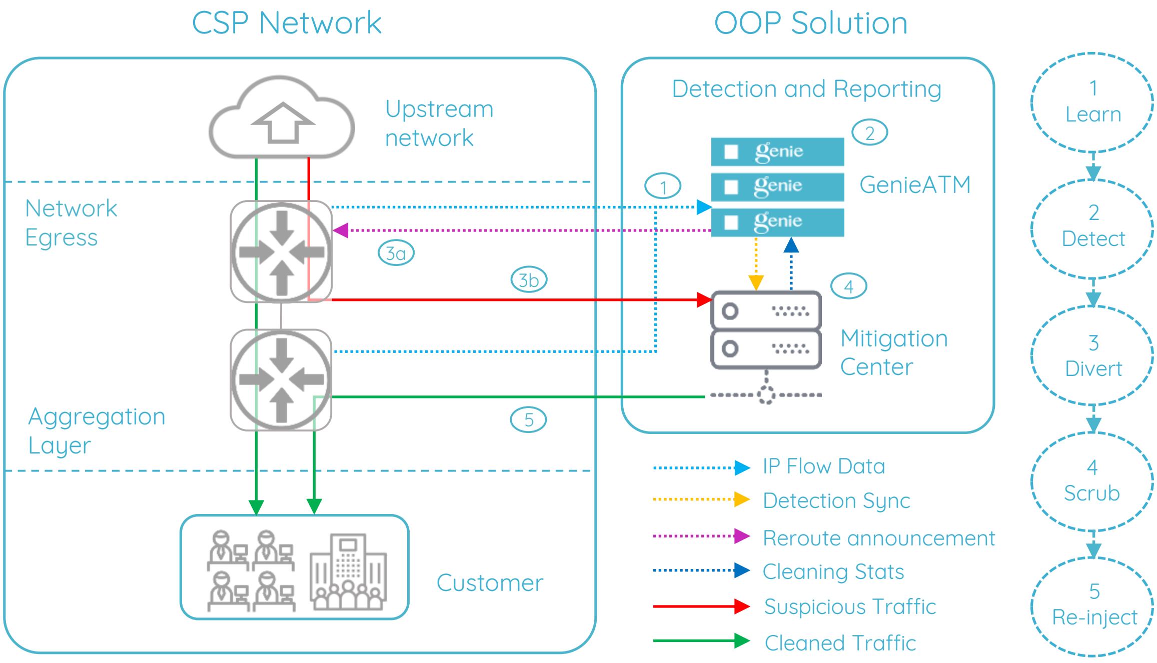

Figure 2: How Genie OOP Solution Works

The customer deployed an Out-of-Path solution by Genie Networks that collected xFlow information from CPE routers of ISP's end customers. GenieATM established BGP peering relationship with the routers that took corresponding actions against suspicious traffic with a mitigation mechanism chosen by the ISP during an anomaly event.

All routers were configured to send the xFlow information to GenieATM which could collect any type of xFlow regardless of the router maker. For example, it could be NetFlow, jFlow, cFlow, sFlow or even IPFIX in some customer setups. GenieATM analyzed the flow information received from these CPE routers and used either behavioral algorithms or customer-configured values to detect an attack. Out-of-Path deployment ensured that the solution was completely non-intrusive. Thus during the peace time i.e. when there were no attacks on the network, traffic continued to flow along its normal path as updated by the BGP routing tables from BGP peers.

When an attack was detected, GenieATM acted according to the mitigation mechanism configured, i.e. either a Flowspec integration with routers; Blackhole mechanism to dump entire traffic to a null route; or used a third-party mitigation unit to scrub the attack traffic and send the cleaned traffic to the customer.

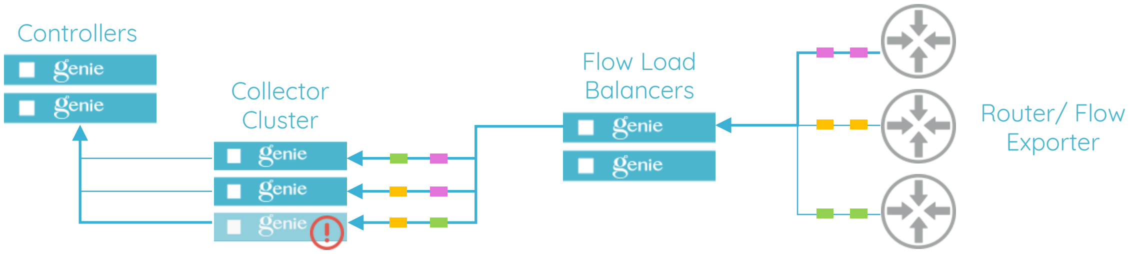

Figure 3: A 3-tier Architecture FLB Solution by Genie Networks

The setup was composed of a 3-tier architecture that included:

- Flow Load Balancers (FLB) setup to receive the flows from CPE routers and distribute these flows to backend Collectors as per their capacities and load
- Collectors to receive and process the xFlow information received from Flow Load Balancers
- Controllers to provide a unified user interface and aggregate the data received from Collectors and compile necessary reports

This 3-tier architecture offers seamless failover at each tier, i.e. FLB tier, Collector tier and Controller tier. Genie's FLB solution offered unique scalability where any number of Collectors could be deployed across any locations when more capacity was needed. Even if any Collector failed from the cluster, FLB detected this failure and continued sending the xFlow information to all other available Collectors as per their load and capacities. This setup also ensured that there was no need to change any configuration on the routers had any Collector failed. It was the FLB IP that received all flows from the routers and even had any collector failed, the routers would not be affected and would continue to send flows to FLB.

Also, FLB setup worked in Virtual Router Redundancy Protocol (VRRP). Thus a failure of any FLB unit seamlessly continued its function with the available unit in VRRP pair. The Controller units also functioned in VRRP and offered seamless failover.

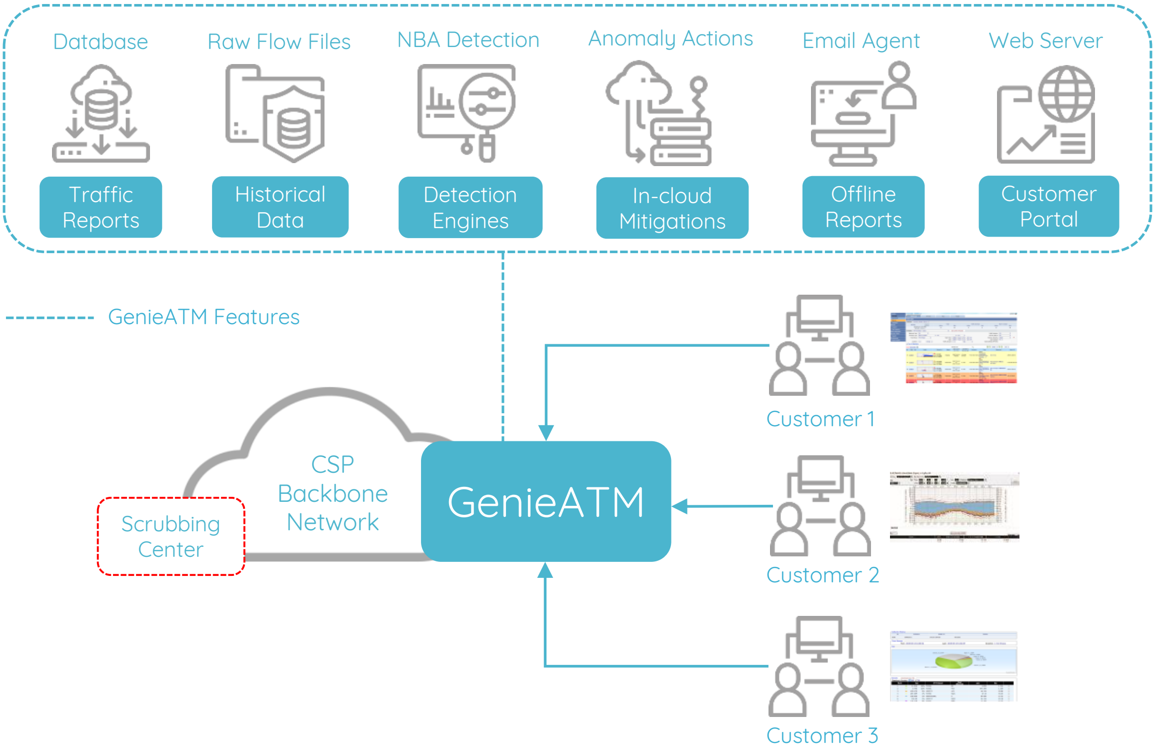

Figure 4: GenieATM as an MSSP Solution

Since the customer was an MSSP, it also offered an interface to its end customers who had subscribed to clean pipe services. Each subscriber could create its user account based on Role Based Access Control (RBAC) and had access to its own network reports and detection and mitigation status.

GenieATM maintained all information related to anomaly and data as per customer profiles to ensure each customer could only access its own managed service entities and not any profile of other customers. Only MSSP administrator could have access to all the profiles since it was required to manage all customers and conduct time-to-time monitoring and reporting to maintain their Service Level Agreements (SLAs).

The customer managed to stay out of DDoS trouble with the highly available and scalable solution provided by GenieATM. As a multi-tenant MSSP-enabling platform, Genie's solution also helped the customer earned additional profits by leveraging GenieATM's features as value-added managed services for its end customers.

About Genie Networks

Genie Networks is a leading provider of network traffic intelligence and security solutions that ensure complete visibility into data traffic trends and instant protection against cyber threats. Learn more at www.genie-networks.com.

© 2019 Genie Networks Limited. All rights reserved.