

## VOO Extends Infrastructure Capacity with Granular Congestion Management and DDoS Protection

### About VOO

VOO is the leading provider of broadband cable services in southern Belgium. VOO delivers digital TV, telephony, and high speed Internet service at 50, 100 or 150 Mbps, as well as mobile services primarily to residential customers in Wallonia and Brussels. The company has been one of the fastest growing service providers in Europe, currently serving around half a million subscribers.

### Challenge

VOO's growth trajectory and ability to attract new customers and keep them depends on the operator's ability to deliver non-stop access with consistently good quality of service. As a shared media, cable connectivity is highly vulnerable to congestion. VOO's fast expansion was challenged by frequent and unpredictable episodes of congestion mainly on upstream channels which have limited capacity and could not accommodate the bandwidth demand. While preliminary investigation led VOO to suspect P2P traffic as the main cause of the recurring congestion, the operator was lacking the network visibility to validate this assumption. In addition, some congestion episodes were so extreme they completely disabled service delivery impacting tens of thousands of customers. VOO assumed their network was suffering cyber attacks, but had no visibility to confirm it. While frequent network capacity expansion alleviated the congestion temporarily, this was not a sustainable strategy for VOO as the costs involved were very high and the relief was short-lived. Instead, they needed a more comprehensive solution that could pinpoint the cause of the congestion and where it was coming from, and also allow them to control it cost-effectively and in compliance with net neutrality guidelines.

### Solution

The first order of business was to deploy Allot Service Gateway Tera at a critical access-aggregation junction in the network, giving VOO full visibility of network traffic per CMTS channel or bonding group. The granular **traffic visibility** provided by Allot showed VOO that 10% of CMTS upstream bonding groups were congested and confirmed that the culprit was P2P traffic which consumed 80-90% of the upstream bandwidth. VOO used Allot's innovative **CMTS congestion management** solution to monitor traffic per CMTS channel or bonding group; to detect congestion per CMTS element according to predefined thresholds, and to enforce subscriber QoS policy in real-time with the same granularity. By managing the bandwidth utilization of P2P applications, VOO was able to reduce congested bonding groups from 10% to 1% almost immediately, which freed up bandwidth for other services and assured the customer experience.

VOO also activated Allot's **DDoS protection** service which is fully integrated in Allot Service Gateway and found that the unpredictable service disruptions were indeed caused by massive Distributed Denial of Service attacks, in particular NTP and DNS amplification attacks, and UDP fragmented floods.

*“By keeping DDoS traffic off the network and managing CMTS congestion precisely where it occurs, we have been able to delay infrastructure expansion by 2 years and to save millions.”*

**Tamara Leemans**  
VOO CTO

### Challenge

Discover the source of persistent network congestion and reduce it without frequent investment in additional infrastructure.

### Solution

Deploy Allot Service Gateway Tera with fully integrated CMTS congestion management and DDoS protection provided by Allot ServiceProtector.

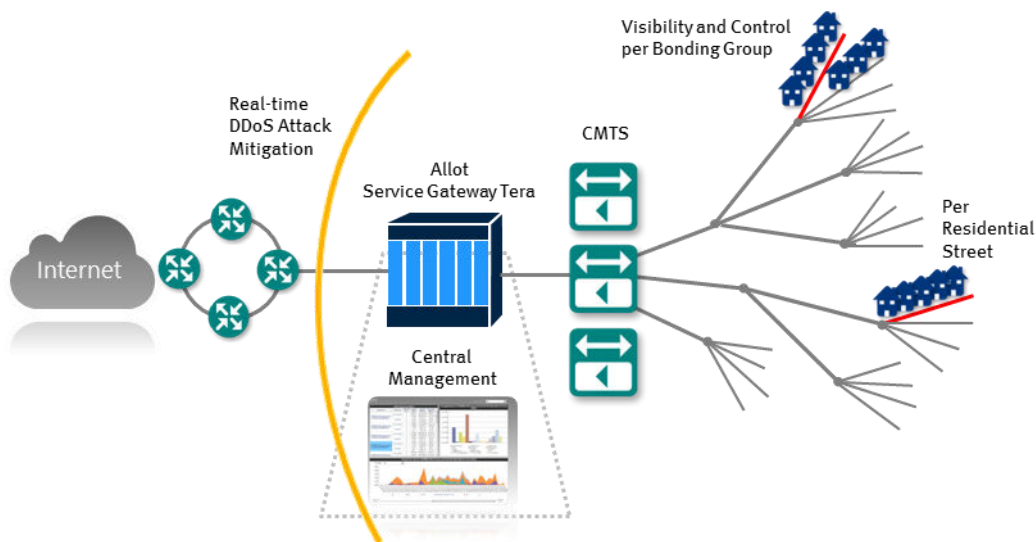
### Benefits

- Delay infrastructure investment and reduce costs
- Assure service availability
- Maintain consistent quality of service
- Enhance customer satisfaction

Once the Allot ServiceProtector sensor was activated, VOO saw that their network often sustained 20-40 cyber attacks per day, with volumes reaching 60 Gbps per attack and completely saturating network resources. Using Allot ServiceProtector, to surgically mitigate the attacks, VOO has freed up Gigabits of bandwidth. Most importantly, they have eliminated service outages. Today, real-time alerts notify VOO when a threat is detected and when it has been mitigated. Detailed attack-mitigation logs, event analytics, and trend/distribution reports support VOO's network planning, threat management and operational decisions, while Allot's unified management console monitors network and user activity and manages threat protection across the operator's entire network. As a result, VOO is now recognized as the best performing network for delivering Netflix video content.

## Deployment

Allot Service Gateway Tera is strategically deployed between CMTS aggregation and the core networks. From a central vantage point, VOO manages CMTS congestion management policy as well as the DDoS Protection service provided by Allot ServiceProtector, which is embedded in every Allot Service Gateway. As a result, VOO is able to see and manage all traffic on the network at a very granular level. Instead of controlling CMTS policy based on IP subnets, which can affect an entire residential neighborhood, VOO can enforce QoS policy on a discrete saturated node(s) that affects only one street in the neighborhood.



## Benefits

By deploying Allot Service Gateway with fully integrated CMTS Congestion Management and DDoS Protection services, VOO is able to:

- Free up available bandwidth on the upstream and postpone investment in infrastructure expansion by 2 years!
- Neutralize DDoS flooding attacks automatically, before they affect network performance
- Maintain consistently good quality of experience across the entire network
- Comply with net neutrality by managing congestion precisely where and when it occurs
- Extend infrastructure lifetime with more accurate investment schedules
- Reduce the complexity and time spent on CMTS congestion management

## Conclusion

Cable network operators like VOO cannot afford to compromise network performance and service availability due to congestion that is unpredictable and difficult to control. Allot integrated network visibility, CMTS congestion management, and DDoS protection solutions have enabled VOO to reduce capex by extending the lifetime of their existing cable infrastructure and to retain customer loyalty by delivering consistently good Quality of Experience to customers.