

Allot Protects Regional Elections from DDoS Attack

About CTTI Catalunya

The Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) or Telecommunications and Information Technology Center of the Generalitat de Catalunya (Government of Catalonia) is a public entity established to integrate all of Catalonia's computing and telecommunication services under a single structure. CTTI is responsible for leading the direction, planning, management and control of all the computing systems and the telecommunication services of Generalitat de Catalunya.

Challenge

As the organization managing IT operations for the Catalunya elections during September 2015, CTTI knew it needed to deploy a security solution that could protect the infrastructure from "hacktivists" looking to disturb the region's political process. CTTI were looking for a proven solution that would be able to protect the infrastructure in real-time and prevent potential high-volume attacks at the network edges.



Vertical | Enterprise
Industry | Government
Region | EMEA
Solution | DDoS Protection

Challenge

- Proactive real-time protection against hacktivists during an election
- Prevent high-volume attacks at the network edges

Solution

The government of Catalonia, a long-time customer of Allot, leveraged Allot Service Gateways to obtain valuable network insights and to deliver superior QoS to various public administration agencies since 2009. Activating Allot DDoS Secure "as a service" to detect and block DDoS attacks within seconds before they threaten or interrupt network services, was a cost-efficient, rapid rollout solution for their security concerns.

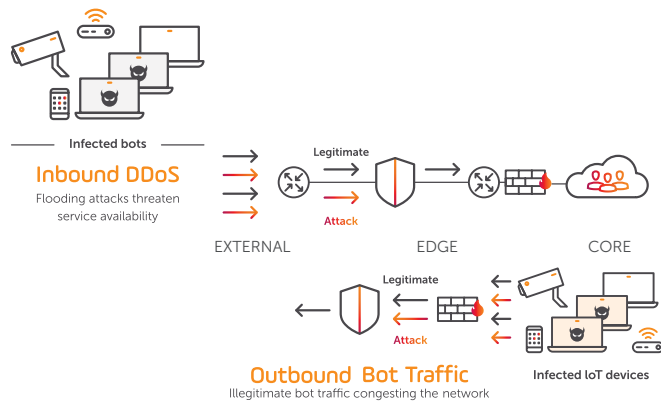
Benefits

- Real-time protection against high-volume attacks at network edge
- Uninterrupted network operations throughout the elections
- Flexible, just-in-time network protection against potential cyber-attacks

Solution

CTTI, an Allot customer since 2009, has leveraged Allot Service Gateway to obtain valuable network insights that enabled them to deliver superior quality-of-service (QoS) to various public administration agencies.

To prepare for recent elections, CTTI added Allot DDoS Secure as the first line of network defense. The network behavior anomaly detection (NBAD) sensor was already embedded in the Allot Service Gateway and was easily activated in conjunction with a cloud-based controller. The solution enabled CTTI's network to analyze and mitigate DDoS flooding attacks within seconds, before they have the potential to threaten or interrupt network services.



Allot DDoS Secure inspected 100 percent of the network traffic and surgically mitigated threats to ensure that the Catalanian elections could operate smoothly and without network disruptions.

The automated and highly scalable security solution was robust enough to stop even the largest-scale DDoS attacks, and successfully thwarted various SSDP-based DDoS attacks on the CTTI network.

CTTI benefitted from the DDoS protection provided by Allot DDoS Secure during the elections. The service was an important part of CTTI network security, mitigating SDDP-based attacks to ensure QoS on the network, and QoE for the voters.



I am very satisfied with the protection provided against DDoS attacks by Allot DDoS Secure throughout the critical operations that took place during the recent elections”

Lluís Guillén Cabrera,
TIC Services Director

Benefits

Allot DDoS Secure was a successful solution for the elections of the Catalanian government providing:

- Flexible, just in time protection against high volume attacks on the network edge
- Uninterrupted network operations throughout the elections
- Detection and mitigation of multiple SSDP-based DDoS attacks in real-time

Resources

[About DDoS Secure](#)

[About Service Aware DDoS Mitigation](#)

[Frost & Sullivan DDoS Mitigation Whitepaper](#)

Learn more about
Allot's Solutions »