ACORUS
NETWORKS

Keep your business on

ACORUS NETWORKS

- We are a French Cybersecurity company created in 2014
- More than 100% of revenue growth year over year since our creation
- As an Internet Service Provider (AS32580) we provide more than 1,5 Tbps of network capacity and more than 2 Tbps of distributed mitigation worldwide in Paris, Luxembourg, Amsterdam, London, New-York and soon in Singapore
- We protect small as well as large Enterprise's Internet connections against DDoS attacks at the Network and Application levels
- Our Cloud protection service protects one of the biggest e-commerce websites in France - Cdiscount
- The world's leading Internet of Things (IoT) connectivity service, Sigfox, uses our large scale and protected Transit infrastructure
- We guarantee the protection of the well-known French online investigative and opinion journal - Mediapart

In a world becoming more open and connected, Internet attacks are increasingly frequent and within the reach of all. The stakes for the future are for everyone to be capable of protecting its online business, image or data exchange effectively against the increase of DDoS attacks (Distributed Denial of Service).

In 2016, almost 75% of all global brands, organizations and companies worldwide were victims of a DDoS attack. And, once a business is attacked, there is an 82% chance that it will be attacked again, while 45% have already been attacked six or more times, according to Infosecurity Magazine.

As no industry is free from the risks, Acorus Networks provides a large scale Cloud infrastructure protection service to its customers like government, defense, media, e-commerce, retail, transport, healthcare, gaming etc. Acorus Networks guarantees high availability of their systems by protecting them against ever-sophisticated DDoS attacks.

OUR VISION

We believe that today attacks can come from everywhere and from everybody.

Indeed, new trends like the Internet of Things (IoT) or Software Defined Networking for Enterprise like SD-WAN will continue to grow the attacks surface. The increasing worldwide use of insecurely connected devices (smartphones, cameras, TV…) reinforce the power of attackers who can exponentially augment the bandwidth of DDoS attacks. Every year the average size of attacks had been getting larger until it reached more than 1,25 Gbps in 2017.

Today more than ever, the connected world counts on innovation to defend itself against this kind of attacks and to keep the businesses on the track.

Let us recall MIRAI attack in 2016 : by infecting thousands of connected cameras, attackers could launch a powerful DDoS attack which caused a multi-million dollar loss for the companies. Regarding healthcare, hospitals are exchanging more and more data on the Internet to monitor the health status of several hundreds patients. One can only imagine the damage it would cause if this flow of critical information was disrupted by a DDoS attack. Likewise, the media post hot news online. Obviously, subscribers cannot admit any unavailability on a newspaper website, otherwise they would unsubscribe. For e-commerce, sales can represent millions of transactions per day and one hour without the Internet might cost million dollar loss.

Therefore we have many good reasons for getting an innovative solution to prevent these disadvantageous situations from happening.

Keep Visibility and Control against DDoS Attacks

ACORUS NETWORKS SOLUTIONS

Acorus Transit Protect

IP Transit service from 100Mbps to 100Gbps of Internet bandwidth, protected by access lists configured by the customer, via a portal of commands or API to filter IP prefixes, protocols and ports.

Acorus Cloud Protect

Solution based on a robust reverse proxy architecture, hosted and managed by Acorus Networks, to protect http/https websites effectively against multi-vector attacks.

Acorus Infra Protect

Intelligent mitigation solution for network and application traffic, managed by Acorus Networks in its own secure large scale infrastructure, to protect in real time automatically your Internet access against DDoS attacks.

Acorus User Portal

A customized portal allows you to visualize your legitimate traffic in real time, be alerted by Acorus Networks' detection service regarding abnormal traffic peaks and apply actions automatically to counter confirmed DDoS attacks.

OUR MISSION

Every day Acorus Networks helps customers to build the best architecture that can respond quickly to DDoS attacks. Every new brick we create and add to our detection and mitigation intelligent system is driven by the desire to help our customers to counter these type of attacks as effectively as possible. This allows them to remain competitive, accessible and confident in the increasingly connected world, today and tomorrow.

Moreover, by having complete and clear visibility on their legitimate traffic in real time, our customers can automatically launch a definitive response in order to block the attacks directly from their customized portal and integrated API and keep their businesses afloat.

OUR CUSTOMERS

In 2016, more than 58% of global DDoS attacks' victims were IT services and Cloud companies, followed by financial services, 28%; the media and entertainment, 6%; ISP and telecom, 4%; and education, 1%.

Acorus Networks provides large scale Network and Cloud protection against advanced and volumetric DDoS attacks without being intrusive to your current internet access. No equipment is needed to be installed on the customer's premises as Acorus Networks' traffic detection and scrubbing service is provided ahead of the customer's connection.

Our team of DDoS security experts ensure automated mitigation of detected volumetric and multi-vector DDoS attacks and guarantee only legitimate traffic bandwidth is passed to the end user.

Customers like e-commerce, the media, IoT infrastructure provider, web hosting, entertainment or gaming companies trust our solutions:

Cdiscount

sigfox

MEDIAPART

Scoop.it!

webedia.
ENGAGING AUDIENCES WITH PASSION

ymagis

TECHNICAL SPECIFICATIONS

- Large scale and resilient multiple 100G backbone infrastructure connecting several Acorus Networks scrubbing datacenters
- Intelligent mitigation solution against DoS/DDoS L3-L7 attacks : tcp, udp, icmp, dns, igmp, syn, http, https, spoofng, zero day, bot management, javascript challenges, WAF and others
- Direct BGP or GRE tunnel routing connection support
- Analytics L3-L4, L7, bots
- Unified customer portal :
  - visualize your legitimate traffic in real time
  - receive alerts
  - control mitigation on demand via integrated API
  - customize your reports
- Simple smart pricing :
  - Monthly Subscription Fee including Mitigation Hours
  - Options : extra scale of VIPs, prefixes, AS, Analytics
- 24/7 L3 support, five 9s
- SOC option for prevention

ACORUS NETWORKS

Corporate Headquarters
Tour Egée, 9-11 Allée de l'Arche
92400 Courbevoie - France

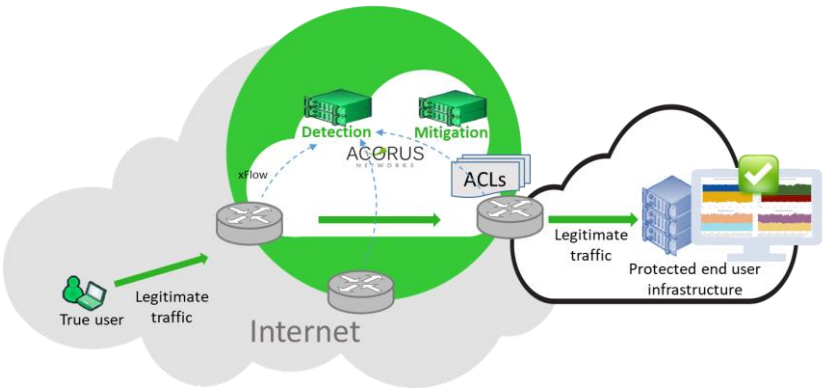
Office in France
215 Avenue Georges Clemenceau
92000 Nanterre - France

Contact us :
+44 7713 275 701
+33 1 8413 8186
info@acorus.net

www.acorus-neworks.com

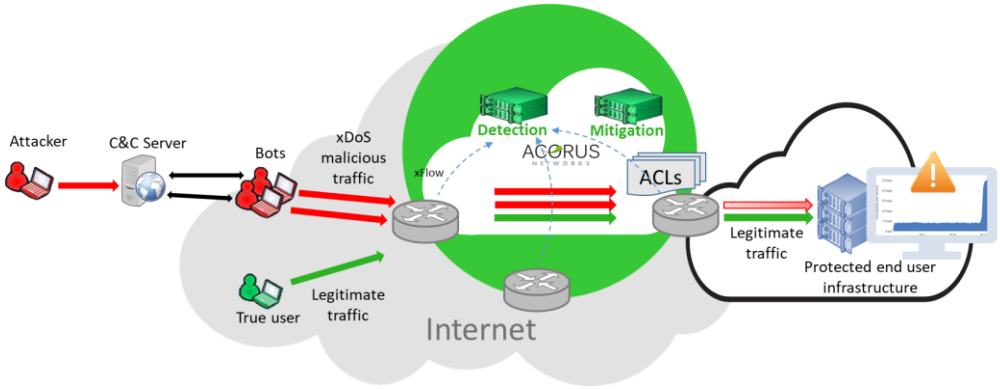
REAL TIME VISIBILITY

Customers can manage their legitimate traffic in real time, thanks to a customized portal offering accurate graphs and security statistics on their Internet sources, destinations, protocols, AS paths, bots which might risk the security of the data.



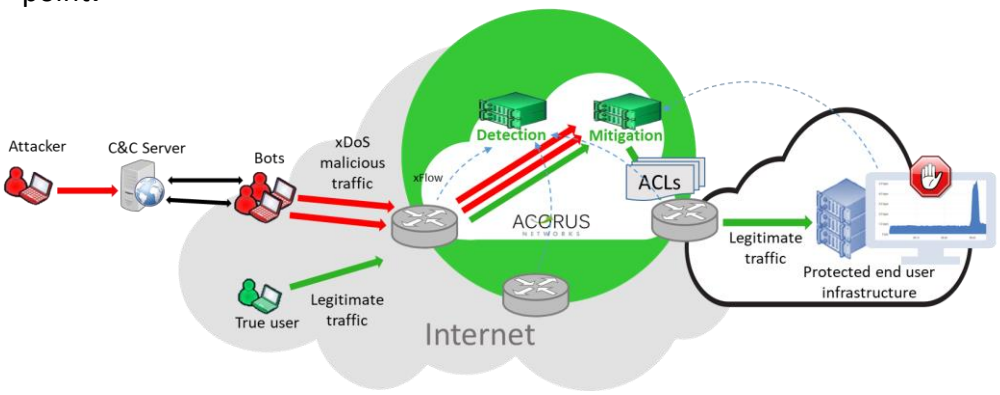
LIVE DETECTION & ALERT

In case of abnormal peaks of traffic, Acorus Networks experts' team alerts customer of the possible risk of DDoS attack. The detection system avoids a false positive and gives the customer a choice to analyze the peak rate deeper or launch a mitigation command through the portal.



MITIGATION ON DEMAND

A simple and unified Graphic User Interface affords the customers to order a mitigation on demand in Acorus Networks large scale Cloud infrastructure and return only legitimate traffic back to their access point.



It is simply a matter of time before cyber-criminals flood your network or website to damage your legitimate traffic causing business interruption. So keep your business on, thanks to Acorus Networks DDoS protection.