DDoS Mitigation

A range of services for safeguarding your internet connectivity and services

www.post.lu

POST LUXEMBOURG

Better safe than sorry

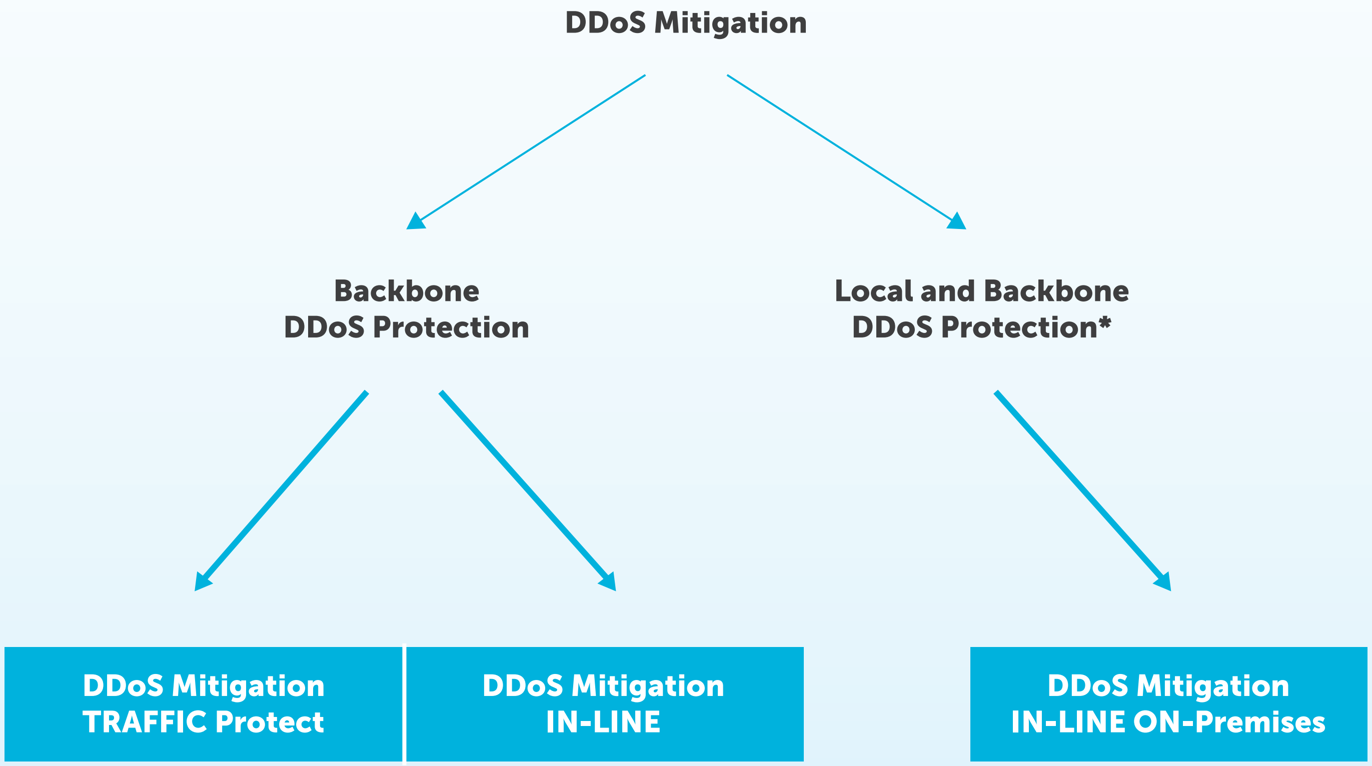
The risk of volume and application DDoS attacks is high and there may be multiple attempts. These attacks try to render an IT server, service or infrastructure unavailable by overcharging the server's bandwidth or by monopolising its resources until they are used up. Either type of attack results in your clients and users being unable to access your internet services.

At a time when businesses rely on their network to manage their business operations, these attacks represent a threat that must be taken seriously, especially in view of the possible repercussions and since no business sector is spared.

The only security service that can protect you against DDoS attacks is a DDoS Mitigation service. It should be an essential element of your IT security policy; one that supplements and safeguards your conventional security systems, which do not protect against DDoS attacks, such as firewalls, load balancers and DNS.

Our DDoS Mitigation range

Our DDoS Mitigation range meets the many different protection needs of our clients' internet services. It protects your infrastructure and internet services against volume and application attacks by mitigating your traffic, i.e. denying access to non-legitimate internet traffic and filtering your legitimate traffic via our DDoS systems..



DDoS Mitigation

Backbone DDoS Protection

Local and Backbone DDoS Protection*

DDoS Mitigation TRAFFIC Protect

DDoS Mitigation IN-LINE

DDoS Mitigation IN-LINE ON-Premises

These services are available on POST Telecom's DIA and IP-Transit business internet products and private cloud services.

*/ Eligible with POST Telecom's DDoS Mitigation IN-LINE equipment.

DDoS Mitigation TRAFFIC Protect

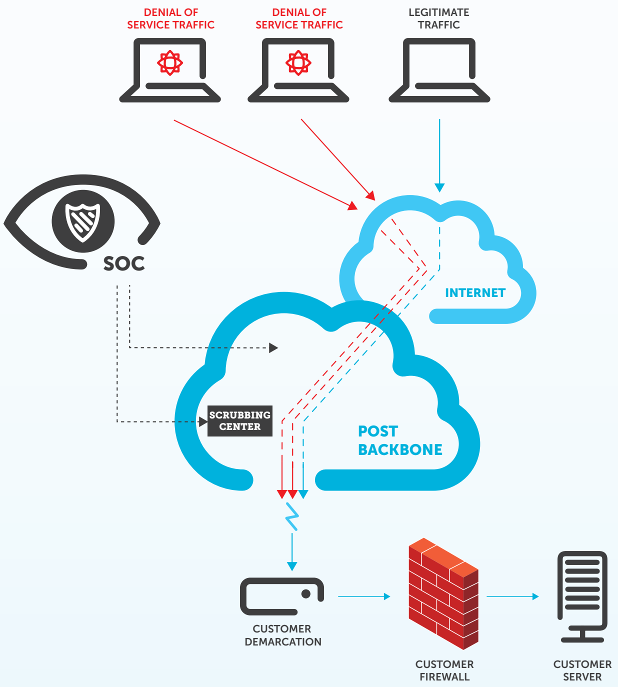
Our DDoS Mitigation TRAFFIC Protect service offers targeted protection against DDoS volume attacks such as:

- Bandwidth Exhaustion, i.e. saturation of your internet connectivity
- State-Exhaustion, i.e. saturation of the components of your internet-related IT infrastructure, such as load balancers, firewalls, etc.

It is managed 24/7 by our SOC (Security Operations Centre), which is dedicated to ensuring the security of our DDoS Mitigation network and services. Whenever the SOC detects an attacks, it triggers mitigation in reactive mode.

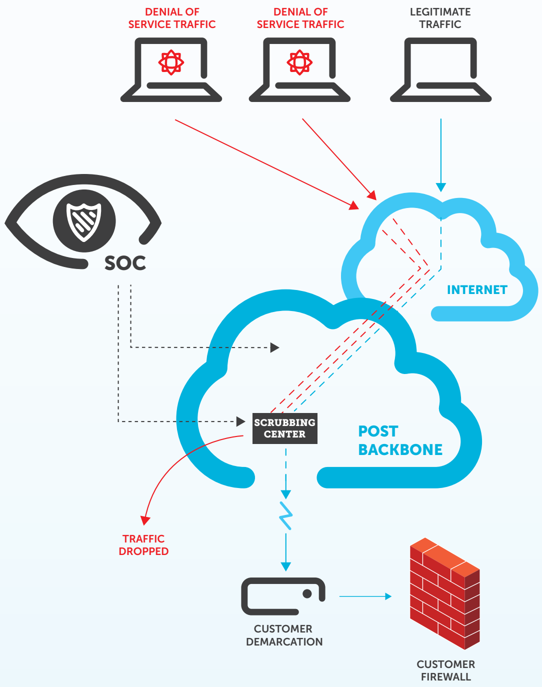
How does it work?

You network faces a DDoS attack



Detection of the attack by POST Telecom's DDoS solution and SOC

DDoS Mitigation TRAFFIC Protect by POST



Routing of traffic, denial of non-legitimate traffic

1.Real-time and high-speed analysis of the internet packets that are intended for you

2. 24/7 supervision and detection of traffic anomalies

3. 24/7 proactive triggering of mitigation by our SOC, according to rules that are defined based on your needs and expectations

4. Mitigation of the DDoS attack: traffic is routed to the central Scrubbing Centre which denies non-legitimate IP packets and sends legitimate IP packets to your services

5. Client is notified of the attack and coordinated with in order to optimise mitigation

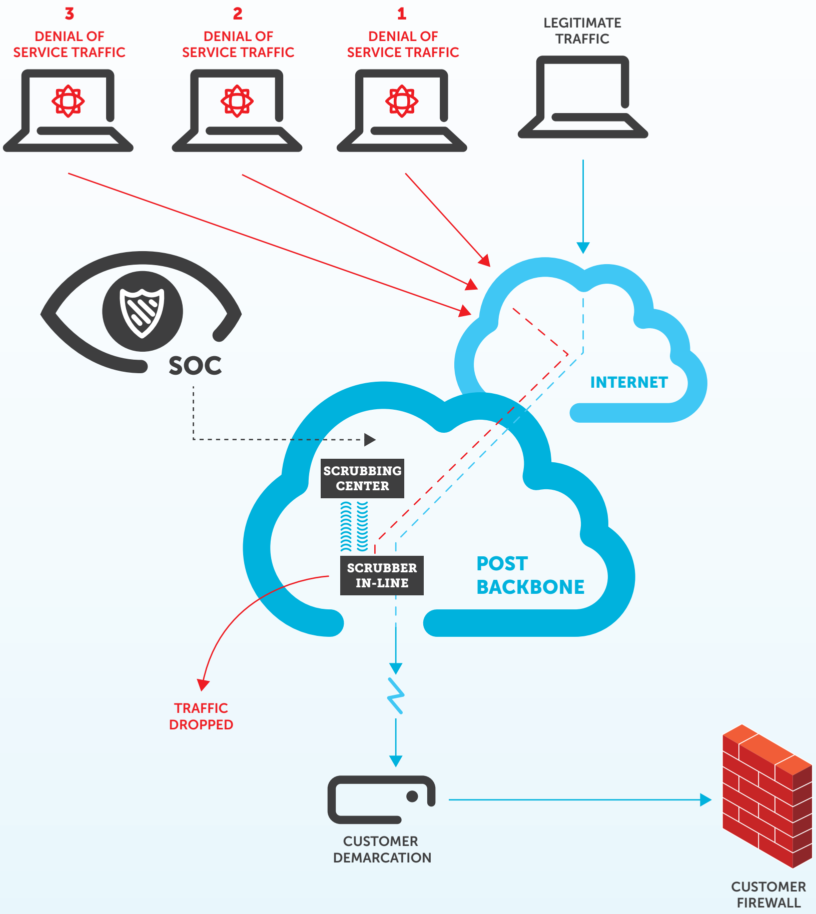
DDoS Mitigation IN-LINE

Our DDoS Mitigation IN-LINE covers your ongoing and real-time protection requirements to combat application and volume attacks. In this way it provides extensive protection against complex and multi-vector DDoS attacks.

How does it work?

Once the DDoS Mitigation IN-LINE is active, the client's internet traffic always passes through an IN-LINE Scrubbing centre, which applies continuous protective measures to internet traffic, in real time. An IN-LINE service is an ALWAYS ON service.

Your network faces a DDoS attack Continuous mitigation



1. Real-time analysis of all your internet traffic's IP packets that fall within the scope of the DDoS service

2. Detection of traffic anomalies and DDoS attacks within seconds

3. Automatic and real-time mitigation of your internet traffic

4. Client is notified of the attack and coordinated with in order to optimise mitigation.

DDoS Mitigation IN-LINE ON-Premises

This service addresses local DDoS-specific and highly-specialised needs and protection requirements against application attacks that target outgoing traffic (e.g. trying to saturate the client's IT infrastructure by downloading data).

POST Telecom integrates its DDoS Backbone Protection option into the DDoS Mitigation IN-LINE ON-Premises in order to offer enhanced protection against volume attacks that exceed internet access capacity thus guaranteeing access to the client's internet services.

For an analysis of your specific needs and requirements, contact us by email at **corporate.telecom@post.lu**

SUMMARY

		DDoS Mitigation TRAFFIC Protect	DDoS Mitigation IN-LINE	DDoS Mitigation IN-LINE ON-Premises
	Type/Aim of Protection	Protection of the client's internet access and IT infrastructure	Protection of the client's internet access, IT infrastructure and internet services	Dedicated local DDoS protection, limited to internet access capacity Option: Backbone DDoS Protection
	Type of DDoS attacks	**Volume**	**Volume and application**	**Volume and application**
Protection	**Application Layer**			
	Outgoing traffic			✔
	Incoming traffic	✔	✔	✔
	Network Layer			
	State Exhaustion	✔	✔	✔
	Bandwidth Exhaustion	✔	✔	✔
	24/7 Traffic monitoring	Included	Included	Included
	Mitigation	Proactive when SOC detects attacks	Continuous, in real time	Continuous, in real time
Protection Application	Manual	✔		
	Automatic		✔	✔
	Activation Prerequisite(s)	No equipment required		IN-LINE equipment

Advantages of the DDoS Mitigation range

- **Your secure 24/7 internet access** remains available, even during an attack: leverage our security expertise in order to protect your network, thus allowing your IT teams to focus on their core business
- **Continuity of your internet services is guaranteed** for your legitimate clients and users: attacks are detected and filtered before they reach your infrastructure
- **Single point of contact** for managing your internet access and DDoS security
- **Affordable insurance** against the threat of DDoS attacks
- **Financial and reputational protection:** safeguard against the financial repercussions that could be caused by an interruption of your internet services or the loss of client confidence
- **Flexible** configuration and setup of your DDoS protection, based on the scale and scope of your internet services that you need to protect
- **Controlled budget:** no need for additional equipment and/or human resources
- **24/7 assistance** from our SOC's security and cybersecurity experts in case of an attack
- **Localised solution** that is 100% Luxembourg-operated
- **Solution that complies** with restrictive local data management policies

For more information, contact your account manager
or go to **http://www.post.lu/en/business**