Arelion

Frequently Asked Questions

DDoS Mitigation

DDoS Mitigation

Frequently Asked Questions

—

10 quick questions for our IP & Security Product Manager at Arelion

What is a DDoS attack? Give us some insights about it

DDoS means Distributed Denial of Service. There are many different types of attacks, but essentially, they are attempts by an attacker to disrupt or take down a service.

This is done by flooding a host or network with large volumes of traffic, either in terms of bits or packets per second, so that the network or server is overwhelmed and unable to operate effectively. It is distributed because it uses many machines, typically home PCs infected by viruses, to instigate the attack.

In the last few years, we have seen an increase in this activity. Although on average, the attacks may be a bit smaller than we have seen in the past, they are a lot more frequent and increasingly complex.

Use of “amplification attacks” and “carpet bombing”, for example, makes these DDoS attacks a lot harder to detect, and to mitigate, at least in a non-automated and systematic way.

Another notable trend we have seen is the increase of extortion activity where the cybercriminal runs smaller attacks, not enough to take a service offline, but noticeable, perhaps for a short period. They then threaten to repeat this, on a larger and longer scale, unless a ransom is paid.
A DDoS mitigation service or system is there to continuously monitor, detect, and filter out malicious activity, leaving the service operational for the legitimate users.

How does the Arelion DDoS service work?

All the edge routers in AS1299 send traffic data in the form of NetFlow, BGP and SNMP to our DDoS system. Using detailed profiling and continuously updated threat intelligence, this data is analyzed for attack traffic. This is all run by our dedicated in-house SecOps team and backed by our industry leading DDoS vendor. If the system detects malicious traffic destined to one of our DDoS customers, it will initiate a redirect within our network to the nearest scrubbing center. Arelion has 5 of these locations globally. Using a variety of methods, we ensure that the traffic is routed to the scrubbing center nearest to the source of the attack, rather than the target. This ensures the lowest possible increment in Round Trip Delay (RTD).

Also, as this redirect is internal to our network, we can redirect only the traffic we absolutely need to – right down to a single host /32. This means that we leave as much customer traffic flowing as normal as we possibly can, minimizing the attack impact still further.

Once the traffic reaches the scrubbing center, it passes through our Threat Management System which drops the malicious traffic and allows the good/legitimate traffic through. This ‘clean’ traffic is sent into a clean VRF or other tunnel and handed to the customer’s nearest port.

Once the attack is over, any redirections are withdrawn, and peacetime routing is restored.

What about the onboarding process? Is that complicated?

The onboarding process should not be complicated, but it really depends on the customer. Arelion offers quite a lot of flexibility to our customers which could add complexity. However, for most of our customers we recommend simply applying default settings, so all we need is some admin information (i.e., contacts for alerts and reports etc.) and details of the IP prefixes they wish to protect.

Customers may not want all of their IP's protected, and some may run very sensitive DNS, web or email servers. These can be configured into the system separately allowing for customization of thresholds. Our solution engineers work with customers to optimize the set-up.

Multi-homed DDoS service - what is it and how does it work?

Multi-homed DDoS is Arelion's solution for customers who buy IP access from more than one provider. Typically, in this scenario the customer would buy DDoS protection from each provider, but this service allows customers to buy a complete DDoS service solution from just us, covering the whole system end to end.

- Multi-homing service works very much like our base service, but with a couple of key additions:
    - We need to be able to 'see' the traffic that doesn't flow through our network. For this, we need the customer to send Netflow (or SFlow) data from the relevant edge routers to our system.
    - We need to be able to steer traffic to our network when we see an attack, so that we can push it to our scrubbers. To do this, we initiate a friendly BGP hijack, by announcing a more specific prefix to our peers and customers. Once the attack is over, we release this BGP announcement and traffic returns to the normal path.
- Multi-homing service is a fully automated feature.
- Based on these two key things, the service may not suit everyone. Some customers may even struggle with providing Netflow data (e.g., due to security policy or not having capable devices). Our more specific announcement should win the BGP routing decision, so ideally in normal operation the customer announces /23 or larger prefixes to the outside world. The prefixes to be protected by us must be covered by an RPKI ROA that has AS1299 as originating ASN and a max length of 24. Our systems will not initiate a BGP announcement that would not be considered valid by RPKI validation.

The multi-homed DDoS service allows for Arelion, as the provider, to have full knowledge of the customer traffic and data. Once we set up the service, do we need to have any legal papers signed regarding GDPR?

AS1299 is a very large IP Transit backbone, with large number of connected ASN's globally and edge traffic > 70Tbs, so we obviously have access to a lot of data.

We use this data for the purpose of supplying the services, running and maintaining the network. So, this does mean collecting flow data and using that within our analysis tools to determine the network demands for planning and forecasting.

For DDoS we use this kind of data to detect and identify suspicious traffic. We only apply these more detailed detection mechanisms to customers who purchase our DDoS services.

With multi-homing, there's a slight difference as we need to collect some data that is not available from our AS1299 routers, but from customer routers themselves. We ask customers to send us not only Netflow/sFlow data from the routers on their other boundaries, but also SNMP data.
This enables us to better identify the external interfaces and only look at the interfaces that are relevant to the service we provide.

Arelion ONLY uses data for the purpose of providing the DDoS Service and we do not retain this data any longer than needed.

Is it possible to have "Premium IP Transit service" that by definition includes DDoS?

We currently do not offer such a service. In principle it is possible and it's something we may consider in the future. If and when we do, it's likely to be part of our Enterprise Product portfolio.

What is Arelion's maximum DDoS traffic capacity available?

We need to explain a bit more about the mechanisms we have available to mitigate DDoS attacks

- Highly-capable edge routers – meaning they support detailed filtering and Flowspec when needed
- Filtering pre-TMS. We have dedicated routers fronting our TMSs. Here our SecOps team manages filters on an ongoing basis
- TMS. These are the vendor scrubbing devices and form our last line of defense. They are modular and each can easily be upgraded to 400Gb/s each before a new chassis is needed

For these reasons, finite TMS scrubbing capacity is less relevant for us, as AS1299 essentially forms a global scrubbing centre. We have successfully mitigated a peak attack of >990Gbps. This capacity is currently being upgraded to ensure that it is future-proofed for our customers.

Is there any alternative to the billing method Arelion offers now, i.e., based on clean traffic, based on ports, including DDoS "burst"?

Currently – our only charging model is based on actual mitigation minutes. This, we believe, is pretty unique in the market. As mentioned, there might be some 'all inclusive' options coming in the future, but we are not planning on introducing a charging based on either clean or 'dirty' traffic.

Is it possible to have a DDoS quick deployment option marketed, i.e. that CSC/NOC can implement within minutes on a "Sunday night" when the client is under attack?

We are working on being able to launch an 'Express DDoS' which would be exactly as described – an existing IP customer can tell us they are under attack and to which prefix(es), so we can instruct our routers to divert traffic to those prefixes to the TMSs. This would be a quick way to get traffic scrubbed. It is not a replacement for the full DDoS service and can run for up to 24 hours. Client would be responsible for telling us to stop the mitigation.

Few quickfire questions from new clients/early adopters of DDoS:

Is there a learning phase?

Yes – this is typically done during Delivery – and can be relatively short. It's there to set some baselines in the system.

What if I realize I made a mistake on the IP addresses?

Simply notify Customer Service Center and we can get these amended/removed. The capability to update through the portal is road-mapped and is a priority for Arelion.

Am I limited in the number of IP addresses?

No, we do not have a limitation. You can have a number of prefixes – down to /32 host IP. We also protect IPv6 addresses, which have their own configured managed objects.

How do I make changes on my Mobile Operator configuration?

Currently by updating the configuration template and sending back to CSC.