Arelion

Customer FAQ

Network security

Network security

Frequently Asked Questions

—

When we talk about “network security”, what do we mean?

For those familiar with the telecoms industry, “network security” is a frequently used term. But it can mean many different things. When we talk about network security at Arelion, we refer to the overall security of your connectivity ecosystem. This generally includes your Internet connection, your Local Area Network (LAN) and any Wide Area Network (WAN) services or infrastructure.

What is a DDoS attack?

A Distributed Denial of Service (DDOS) attack is a common type of cyberattack where the objective of the attacker is to overwhelm targeted resources with sheer volumes of illegitimate traffic. This could be as simple as overwhelming the Internet connection to your web servers use, or more complex attacks where these servers are bombarded with complex requests that overload CPU or memory resources. Critically, attack traffic is sent from a distributed network of attacking machines to make blocking difficult and also to generate large scale attacks. This is often done using a botnet.

What is a Botnet?

A botnet is a network of machines infected by a virus that allows hackers to draw upon multiple (and distributed) resources to instigate an attack. Botnets are generally global in scale and provide attackers with the capability to launch large attacks. In the past these botnets tended to exploit servers, but nowadays domestic computers and Internet of Things (IoT) devices form a major part of these networks. IoT devices in particular have become increasingly common in this context because their security is often weak or non-existent, leaving them open to manipulation.

What is “carpet bombing”?

DDoS “carpet bombing” is an attack on a range of IP addresses, often at a lower intensity for each individual IP address/block, but with a significant overall impact when combined. This approach is intended to create collective damage by helping attack traffic slip below thresholds for automatic detection and mitigation.

How large are attacks today and how long do they persist?

Huge attacks happen from time-to-time, but it is important to remember that the vast majority are quite small – below 10Gb/s and with a duration of less than 20 minutes. This is of course cold comfort for someone with a critical link and only a few hundred Mb/s of capacity.

What is blackholing?

Blackholing is where traffic is 'null routed' to a non-existent network address block by a network element - effectively removing it from the network altogether. RTBH allows customers or end users to request that their service provider discards traffic directed to one of their IP addresses/blocks. This is not a perfect solution because traffic is discarded indiscriminately – whether it is malicious or not.

Safeguards should be implemented by your service provider to prevent the blackholing of IP addresses you do not own. RPKI is important in this context and Arelion is proud to be one of the main advocates of IP address security on the Internet.

What is RTBH?

Remote Trigger Black Holing (RTBH) is a method of initiating blackholing remotely in a different network or network device which isn't directly connected.

What is multihoming?

Quite simply, multihoming is where an organization has multiple upstream IP connectivity suppliers. This creates challenges when mitigating DDoS attacks because attack traffic often comes from many directions, of which only some may be covered by your DDoS mitigation services. Because of our extensive network and direct connectivity to global Internet routes – via customers and peers, Arelion can successfully intercept and cushion the effects of malicious traffic by scrubbing it in our network.

What is scrubbing?

Scrubbing is the process of removing DDoS traffic that targets your connection whilst continuing to send legitimate traffic during an attack. In this respect it differs from blackholing in that it doesn't block traffic indiscriminately and normal connectivity is maintained. With a good scrubbing, setup attacks should be barely noticed at all.

When do cyberattacks typically occur?

An organization's defenses should of course be in place 24/7/365, but our data shows that most attacks occur at weekends and to a lesser extent on Fridays and Mondays. It is thought that this is because cybercriminals try catch organizations when manpower is limited and defenses are low.

What do we mean with intelligent mitigation?

Intelligent or automatic mitigation uses complex algorithms to distinguish legitimate high bandwidth usage from a DDoS attack. Once an attack scenario is determined, mitigation and other defenses are initiated automatically.

What market trends in network security can we expect in the coming years?

Predictions are always difficult to make, but here are a few trends we expect to see:

- *Botnets will continue to grow in importance:* Botnets are the fuel that allows DDoS attacks to function, especially as reflector attacks become more and more easy to filter out using tools such as Flowspec. The expansion of botnets into everyday IoT devices is a real threat than needs to be countered effectively.

- *The threat of DDoS attacks will be used as much, if not more so, as the attacks themselves.* While for some (activists, for example) the attack itself is the endgame, serious attacks (excluding those by state actors) are mostly used by criminals to extort money. This could either be a 'ransom demand' during an attack itself, or the threat of a DDoS attack if payment isn't made.

- *The barriers of entry for those wishing to implement DDoS attacks will continue to decline.* The combination of websites that offer DDoS for hire (or free) via diverse botnets is effectively DDoS as a Service. Anyone who has an Internet connection, and a very small amount of technical knowledge can already launch a small attack. With more resources and research, more damage can be done and the botnets that fuel these attacks will continue to expand. It is important to remember that it is not the hackers who pay for the bandwidth, but rather those targeted (and infected).

- *DDoS attacks will be increasingly used as a weapon in cyber warfare between nation states and cyber defense will become critically important:* As we have seen in the ongoing war in Ukraine, DDoS attacks have become an important component of hybrid warfare. Notably, however, are the different reactions to it. In some cases, the response has been to evacuate digital infrastructure to the cloud, where the formidable defenses of hyperscaler infrastructure are considered a safe harbor. In other cases, the response has been to shore up sufficient in-country network capacity to deal with it. Either way, cyber warfare is unfortunately here to stay.