RedgeGuardian

A novel approach to DDoS mitigation

Today DDoS attacks are one of the most important threats to IT infrastructure, causing major downtimes, customers dissatisfaction, image and financial losses.

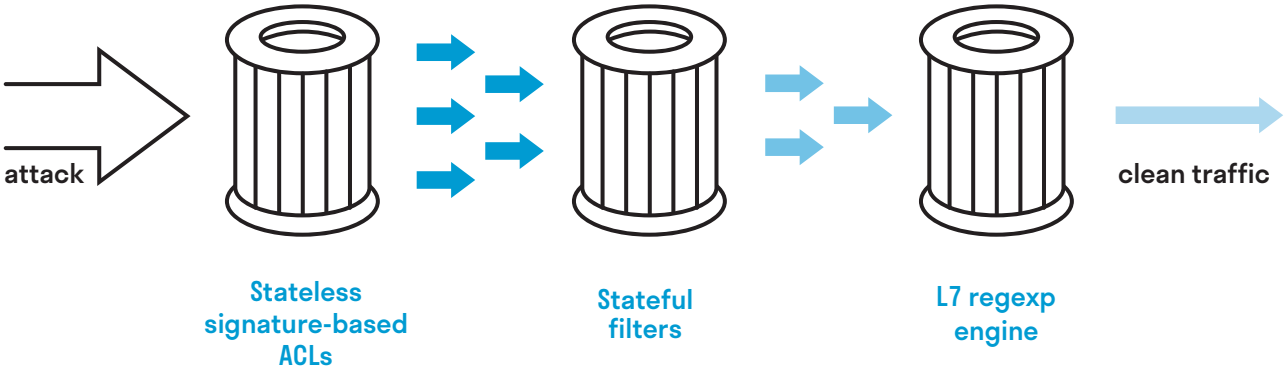
The are many reasons behind the DDoS attacks. Initially, they were motivated politically or ideologically, but in recent years, more and more ad-hoc attacks have been observed. This new cyber threat is known as „crime-as-a-service", or CaaS. There are websites operated by criminal groups on which users can rent botnets, consisting of millions of infected devices, in exchange for a small fee. With just few clicks, anyone can carry out an attack and devastate the victim's network infrastructure.

Recent IoT vulnerabilities and rise of new type of botnets, like Mirai, allowed attackers to enter terabit-scale era, threatening even the largest businesses.

What is Redge Guardian cloud?

Redge Guardian cloud is an infrastructure protection service, consisting of multiple scrubbing centers located in major internet exchange points (IXPs) all over the world. Each scrubbing center has at least 100G connectivity and runs an in-house developed software, capable to inspect and filter hundreds of millions packets per second, thanks to its unique, scalable dataplane architecture.

Redge Guardian cloud is ready to handle fast moving, terabit scale attacks, including IoT-based threats. After detecting the attack with NetFlow/sFlow, protected IP address space is announced from all scrubbing centers with BGP anycast. Incoming traffic is redirected to scrubbing centers, filtered and passed to the destination using GRE tunnel.



Redge Guardian cloud traffic inspection pipeline comprises of signature-based stateless filters, stateful filters and high performance L7 regexp module in order to fully protect the infrastructure against known and emerging threats.

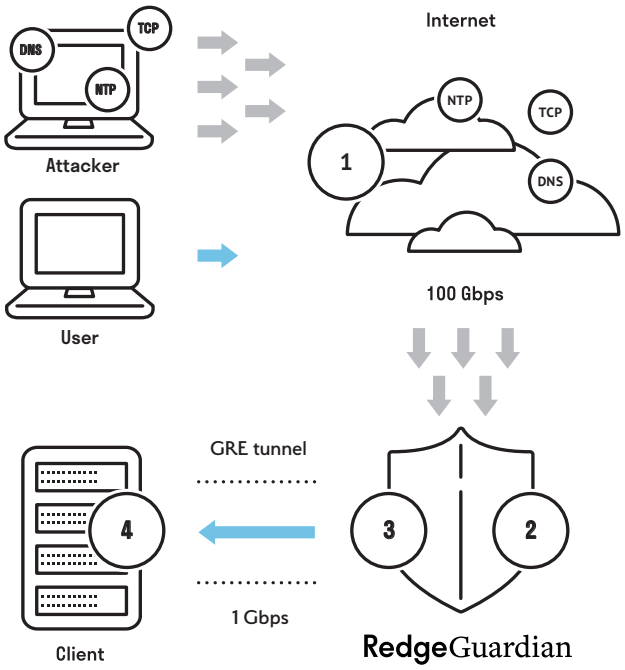
How Redge Guardian works

1. Service activation announces your route in BGP and redirects traffic to the nearest Redge Guardian scrubbing center.

2. In the scrubbing center the attack is filtered according to predicted rules configured for the client.

3. The delivered traffic is transferred to the client via direct peering in IX or GRE tunnel.

4. Redge Guardian platform does not interfere with out going traffic from client network.



Benefits

State-of-the-art protection

Redge Guardian cloud protects from the widest range of known and zero-day attacks, including reflected NTP/SSDP/memcached floods, DNS attacks, TCP floods and more. Redge Guardian cloud starts mitigation within **seconds** and does not impact legitimate user traffic.

Ease of setup

Setup of Redge Guardian service does not require the change of operator or network structure modification. In case of multiple Internet uplinks, all of them are protected by a single service. The only necessary actions are GRE tunnel configuration and allowing your IP address space to be announced by redGuardian. It is also possible to rent required amount of IP address space.

Software-driven flexibility

Redge Guardian cloud provides a management portal, allowing customization of filtering policies, access to statistics and events views.

Fully managed solution

Redge Guardian cloud customers are extensively supported by own Security Operations Team, which covers signature upgrades, fine tuning and emergency response in case of zero-day attacks.

Features

Detection / activation

Automated activation	• support for sFlow v5, NetFlow v5/v9/IPFIX • configurable activation thresholds
Manual / external activation	• SNMP traps • SYSLOG messages • management panel

Clean traffic delivery

GRE tunnel	Yes, with optional key Fragmentation before or after encapsulation
Direct peering	Available in Warsaw (Equinix WA1) and London (Equinix LD8) n x 10G or n x 100G ports

Mitigated attacks

- Chargen reflected response flood
- DNS reflected response flood
- Echo reflected response flood
- IKE PAYLOAD-MALFORMED response flood IPMI/
- RMCP reflected response flood
- LDAP query flood
- LDAP reflected response flood
- memcached reflected reponse flood
- MSSQL reflected response flood
- NetBIOS reflected response flood
- NTP reflected response flood
- QOTD reflected response flood
- RIP reflected response flood
- RPC Portmap reflected response flood Sentinel
- reflected response flood
- SNMP reflected response flood
- SSDP reflected response flood
- Steam query flood
- Steam reflected response flood
- TFTP reflected response flood
- UDP fragment flood
- UDP invalid packets
- TCP SYN/ACK/RST/ACK flood
- TCP fragment flood
- TCP invalid packets
- ICMP PING flood
- ICMP obsolete/legacy packets
- ICMP invalid packets (bad quote)
- ICMP fragment flood
- GRE invalid packets (destination address validation)
- IP invalid packets (checksum, fragment offset, packet length, spoofed source)