RedgeGuardian

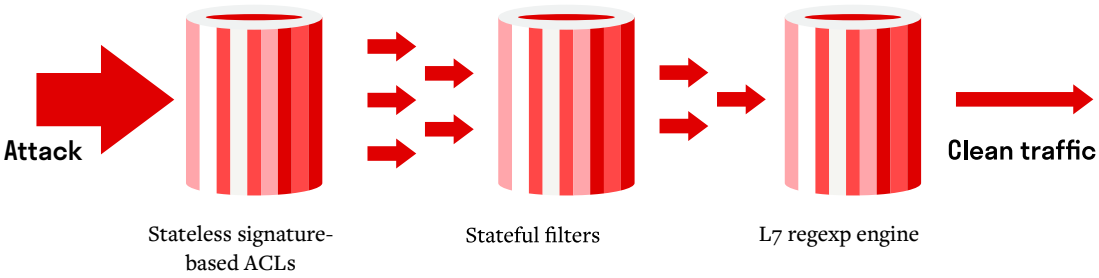
DDOS MITIGATION CLOUD

A BGP anycast global scrubbing service. Gain ultimate protection for servers, infrastructure, and digital content.

What is the Redge Guardian Cloud?

The Redge Guardian Cloud is an IP infrastructure protection service consisting of multiple scrubbing centers located in major internet exchange points (IXPs) worldwide. Each scrubbing center has at least 100G of connectivity and runs in-house-developed software capable of inspecting and filtering hundreds of millions of packets per second, thanks to its unique, scalable dataplane architecture.

The Redge Guardian Cloud is ready to handle fast-moving, terabit-scale attacks, including IoT-based threats. After detecting the attack with NetFlow/IPFIX/sFlow, the 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 the GRE tunnel.



The Redge Guardian Cloud traffic inspection pipeline comprises signature-based stateless filters, stateful filters and a high-performance L7 regex engine to fully protect the infrastructure against known and emerging threats.

Key benefits

- **State-of-the-art protection**
  The Redge Guardian Cloud offers protection from the widest range of known and zero-day attacks, including reflected NTP, SSDP, CLDAP and memcached floods, DNS attacks, TCP SYN or ACK floods, and many more. The system initiates mitigation within seconds and does not impact legitimate user traffic.

- **Ease of setup**
  Deploying Redge Guardian Cloud does not require any changes in network architecture. In the case of multiple internet uplinks, all of them are protected by a single service. The only necessary actions are GRE tunnel configuration and authorizing Redge Guardian to advertise parts of your IP address space. It is also possible to lease IP address range.

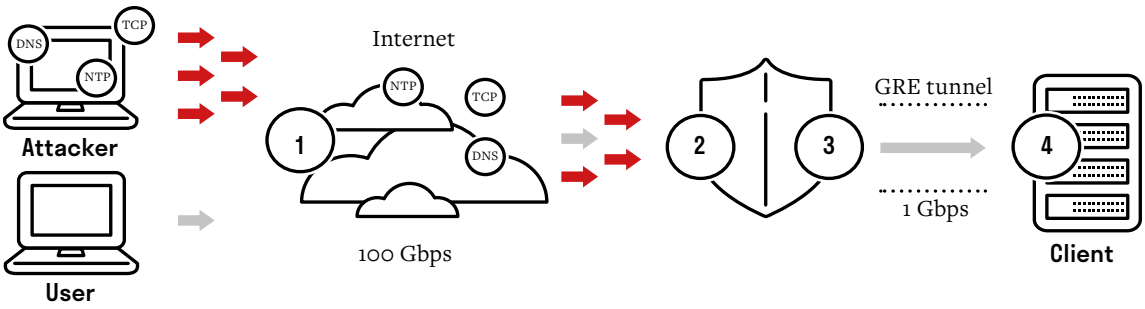
- **Software-driven flexibility**
  Customers may start BGP advertisements and apply different filtering policies with the Redge Guardian Cloud management portal.

- **Fully managed solution**
  Redge Guardian's customers are extensively supported by a dedicated Security Operations Team, which covers signature upgrades, fine-tuning and emergency response in the case of zero-day attacks.

Mitigated attacks

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

How Redge Guardian works



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

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

3. The filtered traffic is delivered to the client via direct peering at the IXP or via GRE tunnel.

4. The Redge Guardian platform does not interfere with outgoing traffic from the client network.

Anyone can be a target of a DDoS attack

Distributed Denial of Service (DDoS) attacks are on the rise, causing a huge threat to businesses and organizations that provide online services. Recent IoT vulnerabilities and the rise of new botnets have allowed attackers to enter the terabit-scale era, threatening even the largest businesses. No doubt, anyone can be a target.

You can mitigate these attacks in a cost-effective way

Redge Guardian allows multi-terabit scalability, providing you with comprehensive, premium protection from DDoS attacks.
It is your best insurance policy and is individually preconfigurable and tailored to your needs.

Features

Deployment / management	
Automated activation	Support for sFlow v5, NetFlow v5/v9/IPFIX Configurable activation thresholds
Manual / external activation	HTTP API call SYSLOG messages Management panel
Minimal protected subnet size	/24 (IPv4), /48 (IPv6)
Clean traffic delivery	
GRE tunnel	Optional key Fragmentation before or after encapsulation
Direct peering	Available in Warsaw (Equinix WA1), Prague (CE Colo) and London (Equinix LD8) n x 10G or n x 100G ports

They have trusted us:

R22 efigence dhosting.pl CloudFerro e-point NASK

Get in Touch

redgeguardian.com

info@redge.com