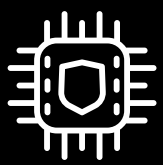
RedgeGuardian

DDOS MITIGATION PLATFORM

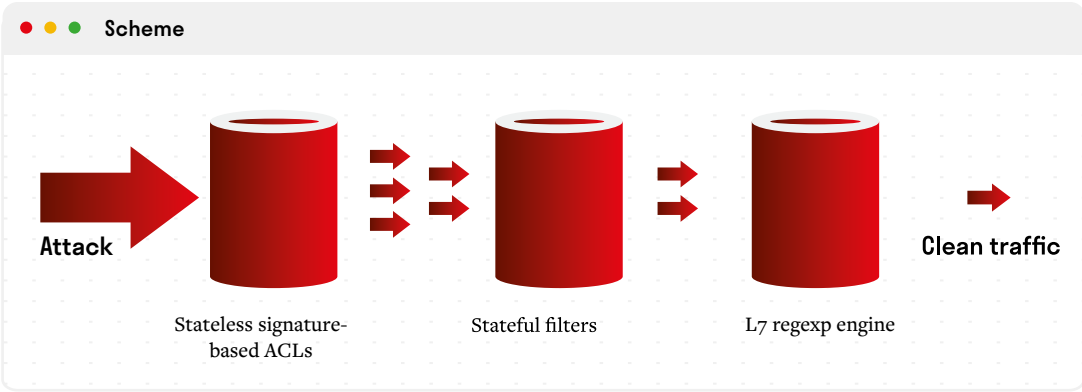


Protect your infrastructure with a software-defined, fully managed and carrier-grade solution.

What is Redge Guardian?

Redge Guardian is a carrier-grade, software-defined DDoS mitigation platform, ready to handle fast-moving, terabit scale attacks, including IoT-based threats. Redge Guardian provides the first layer of network security and allows inspecting and filtering of 100M+ pps on a single node thanks to its unique data plane architecture. To date, such a performance level was only achievable on FPGA and ASIC-based platforms.

Redge Guardian allows defining of the traffic inspection pipeline comprising signature-based stateless filters, stateful filters, and a high-performance L7 regex module in order to fully protect the infrastructure against known and emerging threats. Such an approach yields the highest mitigation accuracy with the shortest activation time and does not affect legitimate user traffic.



Key benefits

State-of-the-art protection

Redge Guardian 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 starts mitigation within milliseconds and does not impact legitimate user traffic.

Software-driven flexibility

Redge Guardian does not require custom hardware platforms - 100G+ performance can be achieved on a commodity x86 server. The deployment scenarios include inline, out-of-path or scrubbing center. Multitenancy support gives carriers an opportunity to monetize DDoS protection.

Fully managed solution

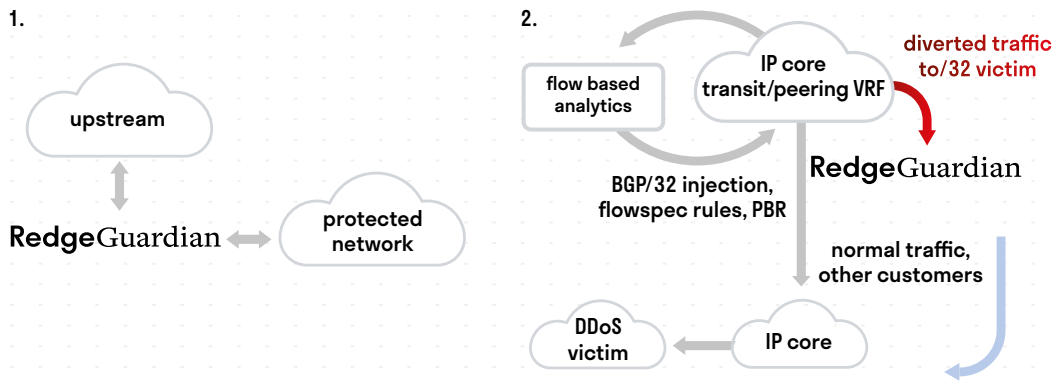
On-premises deployments are extensively supported by a dedicated Security Operations Team, which covers management, signature upgrades, fine-tuning and emergency response in case of zero-day attacks.

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)

Deployment scenarios

Scheme



In-line

In this scenario, Redge Guardian scrubber acts as a filtering bridge between pair of ports.

Off-path

Upon attack detection, /32 more specific routes are injected into transit/peering VRF, causing traffic redirection to scrubber. Clean traffic is injected into IP core.

Features

ACLs and Filters

Matchers

VLAN id, PCP, DEI	fragment type
protocol	TCP flags and URG pointer
source, destination address	ICMP code, type, id, sequence
source IP tag/mark	packet length
source, destination port or range	TTL/HLIM, ToS, DF
	payload pattern (up to 84B)

Actions

drop	pass with state, regex db and proto checks
pass	
ratelimit	

Hashing criteria

src/dst IP	DNS ID
src IP tag	first 8/16B of payload
src/dst port	HTTP path (up to 64B)
DNS FQDN	

Algorithms / actions

various algorithms, for example:

- ✓ tcp flow inspection
- ✓ fragment filter
- ✓ pass first, drop first
- ✓ pass second (with or without delay) per flow policing

Deployment / management

Clean traffic delivery

VLAN id, PCP override
source, destination MAC override or swap
GRE/IPIP/UDP tunnel
fragmentation before or after encapsulation
fragmentation PMTUD support
fragmentation with clear-df
balance over multiple exits

Performence

up to 100 Gbps and 100 Mpps on a single node

Latency

< 60 microseconds

Multitenancy

Yes, up to 8k tenants on a single instance

Management

TAP bypass (punt) to Linux stack

ingress packet sampling to Linux stack

ingress packet sampling to external sFlow collector

per customer counters (ready to integrate with time series databases and Grafana)

Licensing and support options

Part no.	Description
REDGE GUARDIAN-DP10	License for 10 GbE port. Basic support included for 1 year
REDGE GUARDIAN-DP25	License for 25 GbE port. Basic support included for 1 year
REDGE GUARDIAN-DP100	License for 100 GbE port. Basic support included for 1 year
REDGE GUARDIAN-SUB-Basic	Bugfixes, e-mail tech support, 8h x 5d, 120 min. response time
REDGE GUARDIAN-SUB-Essential	Updates & upgrades, e-mail & phone tech support, 10h x 5d, 30 min. response time
REDGE GUARDIAN-SUB-Enterprise	Updates & upgrades, e-mail, Slack & phone tech support, 24h x 7d, 10 min. response time

Why choose us

Distributed Denial of Service (DDoS) attacks are on the rise, causing a huge threat to businesses and organizations that provide online services.

There are websites being operated by criminal groups on which users can rent botnets, consisting of millions of infected devices. With just a few clicks, anyone can carry out an attack and devastate any unprotected network infrastructure. Recent IoT vulnerabilities and the rise of new types of DDoS botnet networks have allowed attackers to enter the terabit-scale era, threatening even the largest carriers and data centers.

DDoS attacks lead websites and data centers to go down or malfunction causing companies huge financial and reputational damage.

What industries do DDoS attackers target?

- ✓ ISPs/Telcos
- ✓ Media and Entertainment
- ✓ E-commerce
- ✓ Public entities
- ✓ Financial services
- ✓ Education

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.

Redge Guardian is the best insurance policy, individually preconfigurable and tailored to the client's needs.

They have trusted us:

NASK CloudFerro R22 dhosting.pl e-point efigence

Get in Touch

redgeguardian.com

info@redge.com