DDOS PROTECTION

CoreGate DDoS Shield

Detect volumetric attacks in seconds. Automatic mitigation with RTBH and FlowSpec, coordinated with your upstreams, plus incident reports.



Monitored traffic	Detection	Mitigation	Alerts
10–800 Gbps	flow-based	RTBH · FlowSpec	email · webhook

01 How it works · Attack spotted, rule applied

Flow data from edge and core is analysed continuously. When a threshold for a target is crossed, a FlowSpec rule or RTBH is triggered automatically according to the attack type.

ATTACK
UDP flood → 203.0.113.10
Volumetric traffic

→

COREGATE DDoS SHIELD
threshold exceeded
Flow analysis and decision

→

UPSTREAM · EDGE
FlowSpec · RTBH
Filter or blackhole

02 Features

Flow-based detection
Threshold and anomaly detection on sFlow, NetFlow and IPFIX.

FlowSpec mitigation
Filter only the attack traffic and let legitimate traffic through.

Alerts and reporting
Email and webhook alerts, incident history and attack reports.

Integrated with BGP Edge
Rules apply directly through CoreGate BGP Edge Gateway.

Automatic RTBH
Blackhole the target at your upstream to protect the rest of the network.

Per-target thresholds
Different thresholds per customer, prefix or service.

Automatic rollback
Rules are withdrawn automatically when the attack ends.

Cluster, failover and OTA
Up to 16-node clusters, automatic failover and zero-downtime updates, all from the central management system.

03 Licensing

DDoS Shield has its own licence structure and is quoted individually for your network.

04 Deployment scenarios

ISP

Protecting subscribers

An attack on one subscriber is stopped before it fills the whole network.

HOSTING

Data centre and hosting

Respond to attacks on customer servers with per-service thresholds.

UPSTREAM

Upstream coordination

For large attacks, RTBH and FlowSpec rules are signalled to the transit provider.

05 Capacity grows, service keeps running

Cluster architecture
Scale horizontally and vertically. Add up to 16 nodes to grow capacity as you need it.

Automatic failover
If a node goes down, sessions and traffic move to the other nodes automatically.

OTA updates
Updates roll out node by node, with no maintenance window and no subscriber impact.

Security and vulnerability detection
The platform is scanned continuously, and detected vulnerabilities and threats are remediated automatically.

24/7 monitoring and support
Our NOC watches your platform around the clock, steps in before issues grow, and support is always open.

Centralised management
Every node, site and licence from one console, with configuration, monitoring and reporting together.

06 Frequently asked questions

How fast are attacks detected?
Flow data is analysed continuously; action is taken within seconds of a threshold being crossed.

What's the difference between RTBH and FlowSpec?
RTBH drops all traffic to the target IP; FlowSpec filters only traffic matching the attack signature.

What if my upstream doesn't support FlowSpec?
FlowSpec rules run on your own edge; for large attacks that fill the link, the target IP is signalled upstream with RTBH.

Which flow formats are supported?
sFlow, NetFlow v5/v9 and IPFIX.

Get a quote for DDoS Shield

Your subscriber count and peak traffic are all we need to send a licence and hardware recommendation.

sales@coregate.com.tr
+90 850 650 0 500
coregate.com.tr