netshop
Data Center Services

AEGIS
Shield Against DDoS

Early Access

TECHNICAL OVERVIEW

Aegis DDoS Protection

Coverage, performance and MT4/MT5 suitability today, and what is coming next.

---

3 sites
London: LD4, LD6, LD7

24/7
automatic detection and mitigation

Per IP
protection, onboarded from your IP list

HOW IT WORKS

On-demand scrubbing, with blackholing as the safety net

1 · Detect

Flow telemetry from each datacenter's border, analysed 24/7 per IP address

2 · Decide

Known attack type? Within capacity? Platform healthy?

3 · Divert

Only the attacked /32 is re-routed by BGP, inside our network

4 · Scrub

Stateless, line-rate filtering on dedicated scrubbing nodes

5 · Return

Clean traffic is delivered to your server

Peacetime: your traffic never passes through Aegis. No extra hop, no added latency.

Fallback: anything Aegis cannot clean is blackholed upstream (RTBH), the industry-standard response.

Attack coverage: today and next

Attack vector	Early Access today	Pipeline
UDP reflection / amplification: DNS, NTP, SSDP, Memcached, CLDAP, SNMP, Chargen, STUN	Scrubbed	Next: 12 more reflector protocols (currently in validation)
Spoofed, bogon-source and malformed TCP traffic	Dropped	—
Random-port UDP floods	Per-IP rate cap	—
IP fragment floods	Per-IP rate limit	—
TCP SYN floods	Blackhole fallback	Next: scrubbed (currently under testing)
TCP floods to ports you don’t use	Blackhole fallback	Next: dropped per IP, based on your declared services (currently under development consideration)
ICMP floods	Blackhole fallback	Next: scrubbed (currently under testing)
TCP ACK floods to your service ports	Blackhole fallback	By design: no stateless ACK rule
HTTP/HTTPS and slow-connection attacks (L7)	Not covered	Not in current scope

1 · PROTECTION COVERAGE

Filter engine: 50 rules, six families

Source validation

Enforcing

Spoofed, bogon and port-0 traffic dropped on sight.

Reflection attacks

Enforcing

13 reflector protocols blocked, SSDP also by payload.

Per-IP rate caps

Enforcing

UDP and fragment floods capped per address.

TCP protocol sanity

Enforcing

Invalid TCP flags, malformed SYNs and reflected SYN-ACKs.

ICMP hygiene

Enforcing

Odd ICMP types dropped; ping floods capped per address.

TCP flood defence

In validation

SYN limits, SYN challenge and per-IP service guard.

27 rules enforce today, 5 are staged in would-drop mode and 18 count for telemetry and validation. No rule may drop until it has proven itself in count-only mode on live traffic.

1 · PROTECTION COVERAGE

Scope of protection

Which layers are covered?

L3/L4

Volumetric network-layer attacks: UDP reflection, UDP floods and fragment floods are scrubbed. Application-layer (L7) traffic is not inspected.

Which IPs are protected?

Per IP

Protection is enabled per /32. Every address on your onboarding list is covered; any address not listed falls back to blackholing.

Custom ports, incl. MT4/MT5?

Yes

Aegis matches attack signatures, not your service ports, and forwards everything else. MT4/MT5 TCP ports pass untouched; UDP services and thresholds can be tuned per IP.

Always on, or on detection?

Auto-triggered

Detection runs 24/7. Only the attacked IP is diverted through Aegis, and it returns to the normal path when the attack ends.

2 · PERFORMANCE AND MITIGATION

Capacity, speed and latency

Mitigation capacity

8 Gbps per site

Up to 8 Gbps scrubbed per site today, shared by that site's protected IPs; larger attacks fall back to blackholing. Scaling to 200 Gbps as new upstream capacity comes online.

Added latency?

None in peacetime

Outside an attack, traffic never passes through Aegis. During mitigation it takes one extra hop through a stateless filter inside our London network.

Time to mitigate

Improving

Detection and diversion are fully automatic. An edge platform upgrade, with hardware on order, shortens time to mitigate; measured figures will be published once it is live.

Packet-rate ceiling

Scaling

The main attack vectors are dropped at line rate on dedicated nodes. A new scrubbing platform built for 200G interface, and a higher-throughput packet engine, are in the pipeline.

When can traffic be interrupted?

While an attack is scrubbed, legitimate TCP traffic keeps flowing. Only an attack that cannot be scrubbed causes the IP to be blackholed until it ends.

SCRUBBED

You stay online, sessions continue

UDP reflection and amplification, UDP floods, fragment floods

BLACKHOLE FALLBACK TODAY

The IP is unreachable until the attack ends

TCP and ICMP floods, attacks above capacity, platform unhealthy

Moving out of fallback next: SYN and ICMP floods (rules in testing), and TCP floods to ports outside the services you declare.

3 · MT4/MT5 COMPATIBILITY

Built not to disturb trading sessions

Suitable for MT4/MT5?

Yes, with caveats

No extra hop in peacetime, a stateless filter during attacks and no TCP rate limits by default. Caveat today: TCP floods fall back to blackholing.

Existing sessions kept?

Yes

Aegis keeps no connection state and deliberately has no ACK-flood rule, so established sessions are not reset or dropped while traffic is scrubbed.

Per-port rules?

By our engineers

Set by our network team today and run in count-only mode before they drop. A per-IP list of your declared TCP services is coming, first viewable, then editable.

Legit clients blocked?

Low risk

Rules match attack signatures, not client behaviour, and limits are per IP. Running UDP services such as VoIP or DNS? We give them a custom UDP and threshold profile.

4 · MONITORING AND REPORTING

Visibility into every attack

Monitoring dashboard

24×7 NOC Team

Our NOC tracks live mitigations and capacity 24/7. A customer view of your protected IPs, declared services and attacks is in the pipeline.

Attack reports and history

Yes

A PDF report per attack (type, outcome, traffic), with 30 days of attack history.

Notifications

On blackhole

You are emailed when an address is blackholed and again when it is released. Scrubbed attacks need no action from you and are covered in the attack report.

API and monitoring export

Not Available Yet

No customer API, webhooks or Zabbix/Grafana export today. Tell us if your team needs one.

5 · SLA AND SUPPORT

Automated around the clock

Fully automated, 24/7?

Yes

Detection, decision, diversion and fallback run without human action, with continuous health checks and automatic fallback if the platform degrades.

Attack exceeds capacity?

Blackhole fallback

The attacked IP is blackholed upstream to protect the rest of the network, while other protected IPs stay scrubbed.

Support during attacks

On-call

Attacks, platform issues and capacity events page our on-call engineers automatically.

Mitigation SLA

Early Access

Best effort during Early Access, with no time-to-mitigate guarantee. SLA terms come with general availability.

PIPELINE

Where Aegis is heading

Now

Early Access

- 8 Gbps scrubbing capability
- UDP reflection and amplification scrubbing
- 27 enforcing filter rules, incl. per-IP rate caps
- Automatic detection, diversion and RTBH fallback
- Attack reports; email on blackhole and release
- Available in London: LD4, LD7

Next

In progress

- Capacity scaled to 200 Gbps
- Edge upgrade: detection moves ahead of the datacenter
- SYN and ICMP flood scrubbing
- Per-IP TCP filtering from your declared services
- Customer view of your IPs and services
- Availability in all major London sites (LD4, LD7, LD6)

Later

Planned

- Higher-throughput packet engine
- Self-service editing of your declared services
- Extend availability in Netherlands, Singapore and beyond

SUMMARY

Where Aegis fits today

Strong fit

- UDP volumetric attacks, up to 8 Gbps per site
- No added latency in peacetime
- Sessions kept while scrubbing
- Per-attack reports, 30-day history

Current limits

- TCP and ICMP floods: blackhole fallback
- No Layer 7 protection
- Protection per listed IP
- No customer API or monitoring export

Closing the gaps

- 200 Gbps scrubbing capacity
- SYN and ICMP flood scrubbing
- Per-IP TCP filtering
- Customer view of your IPs and services

To onboard: send your IP list and the services you run sales@netshop-isp.com.cy