

Inline network protection

NuajBridge 2.5G

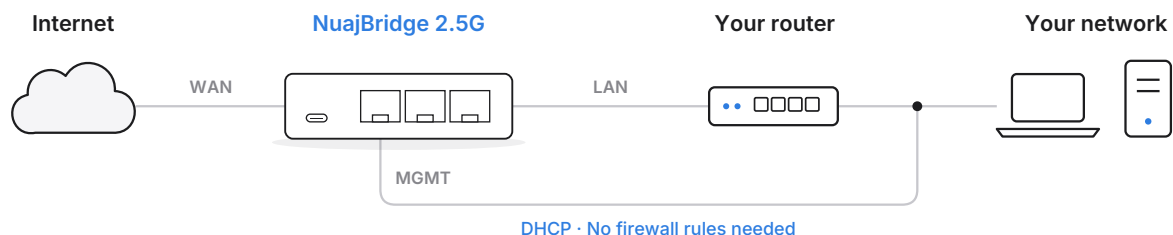
Inline protection for your 2.5 Gb/s internet link.

NuajBridge sits between your internet connection and your router and filters attacks out of your internet traffic, in both directions. It installs like a cable and is managed from the cloud.

4.3Gb/s Internet traffic, both ways at once 91% of the link, with every protection on.¹	97% Of a botnet DDoS attack stopped 0.71 Gb/s from 65,536 addresses at one of yours, while your traffic kept flowing.²
99.8% Of your traffic delivered during an attack The lowest result across six different attacks, each run with everyday traffic flowing.²	0 Packets lost or altered Out of 671 million carried both ways under sustained load, each one checked against what was sent.³

Installation

Fits in front of your router.



Transparent inline bridge

Your internet connection to the WAN port, your router to the LAN port. No change to your addressing, no proxy, no extra hop.

Both directions

Every packet in and out is inspected. Attacks it catches are dropped before they reach your network.

Out-of-band management

Plugged into your network behind the router, apart from the traffic it protects. It takes an address by DHCP and only connects out: no firewall rule to open.

Protection

Protection in layers.

DDoS attacks, large and small

Per-source rate limiting stops loud attackers. An address under attack is held to its own normal rate, and an adaptive rate limit caps the rest; replies to your own connections are let through.

Reflection and amplification attacks

Replies from DNS, NTP, memcached and similar services pass only when a device on your network asked for them.

Zero-day attacks

It learns your normal traffic and writes an attack signature that blocks only what sets the attack apart.

Port scans and brute-force attacks

It watches the ports your services listen on and blocks sources that keep failing to connect.

Threat intelligence

Curated threat feeds, your own blocklist and geo-blocking, for IPv4 and IPv6: up to 19.97 million entries.

Cloud-managed

DDoS reports, alerts and every setting, for one box or a fleet. An update is kept only once the box is back up and forwarding.

Stronger together.

When one NuajBridge catches an attacker, every network in the NuajProtect community blocks it, often before it reaches yours. You choose who you share with and how many separate devices must report an attacker first.

Visibility: see every threat, and why it was stopped

Every attack, reported

After each DDoS attack: what came, from which countries and networks, what was blocked and learned. By email, text or a daily digest.

Compromised devices

An alert when a device on your network keeps trying to reach listed addresses, a sign of infection; that traffic is blocked.

Why, for any address

Live traffic, an activity log, and a lookup that says why any address was blocked or let through.

Performance

Line rate from 256-byte packets, both ways.

Every protection on, and not a packet lost: the share of the link carried at each packet size.¹

Packet size	One direction		Both directions at once	
64 bytes		66%		58% ¹
128 bytes		92%		80%
256 to 1,518 bytes		100%		100%
Full-size packets: 4.93 Gb/s both ways				
Internet mix		100%		91%
IMIX: 2.33 Gb/s one way, 4.30 both				

¹ A production NuajBridge 2.5G and separate test equipment, October 12 to 16, 2026, every protection on; traffic from the internet came as replies to connections made from inside. Highest rate with no packet lost; link shares include each frame's preamble and gap. 64 bytes both ways: estimated from the measured both-ways share at 80 to 128 bytes, as the test equipment cannot send it. Internet mix: the simple IMIX (64, 594 and 1518 bytes at 7:4:1).

³ Each forwarded packet checked against what was sent: 5 minutes of 256-byte packets and 10 minutes of full-size packets at 99.9% of the link, both ways.

Under attack

Tested against real attacks, with your traffic flowing.

Six common attacks, one at a time, with 0.72 Gb/s of everyday traffic flowing each way.² A DDoS attack from 65,536 sources at one of your addresses is held to that address's normal rate, so your traffic still gets through.

Attack	Attack size	Stopped	Your traffic delivered
Botnet DDoS, small packets	0.71 Gb/s	97%	99.93%
DoS from a single source	0.71 Gb/s	100%	100%
DNS reflection	1.70 Gb/s	100%	100%
NTP reflection	1.64 Gb/s	100%	100%
Botnet DDoS, mixed sizes	1.65 Gb/s	96%	99.8%
Botnet DDoS, full-size packets	1.70 Gb/s	99%	100%

Back to normal at once. When the attacks ended, 100% of your traffic was delivered, with nothing to clear or restart.

Attack signatures

Learns what a new attack looks like.

A DDoS attack from 65,536 sources can keep each source under its limit. NuajBridge finds what the attack has that your traffic does not, such as a source port or a packet size, and blocks only that.⁴

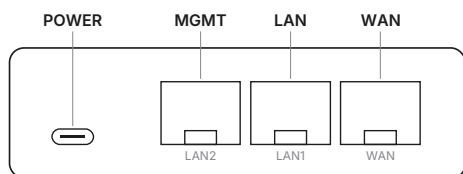
Attack	Attack size	Blocking from	Stopped by the end	Your traffic delivered
Botnet DDoS, full-size packets	1.70 Gb/s	34 s	100%	100%
Botnet DDoS, mixed sizes	1.65 Gb/s	3 s	99%	99.7%
Memcached reflection	1.68 Gb/s	2 s	97%	100%
Botnet DDoS, one packet size	1.61 Gb/s	35 s	100%	99.91%

² Everyday traffic: the internet mix at 0.25 million packets a second each way. Attacks from public address ranges, sized to fill most of the rest of the link, with a default protection profile.

⁴ Everyday traffic as in note 2, plus visitor-like traffic from 65,536 addresses. Blocking from: the first second in which nearly all of the attack was dropped. Stopped by the end: the share dropped over the closing part of the attack.

Hardware

Tech specs



Network ports

Two 2.5 Gigabit Ethernet, RJ45
WAN to your internet
connection, LAN to your router

Management port

One 1 Gigabit Ethernet, RJ45
For cloud management

Power

USB-C Power Delivery
5, 9, 12 or 20 V

USB

One USB 3.0 port
One USB 2.0 port

Cooling

Fanless

Operating temperature

0 to 70 °C ambient
32 to 158 °F

DDoS reports

Every attack, reported.

After every attack, a report: what came, what was blocked, what it learned, and your traffic through it all. Beside: a 45-minute bench attack on October 15, 2026, five kinds of DDoS attack in turn, with everyday traffic flowing.⁵

⁵ The report as sent, from its own data, on October 15, 2026; source addresses masked.
Figures are measurements, not guarantees.

Limits

What it can't do.

Stop attacks bigger than your link

They fill your internet link before they reach the box.
Those need your internet provider.

Block reflection with asymmetric routing

Reflection blocking needs to see requests going out. If
outbound traffic takes another path, turn it off.

NuajProtect

RESOLVED

FLOOD ABSORBED · NO ACTION NEEDED

Flood absorbed on NB-001007

Oct 15, 2026, 2:31 PM EDT

DURATION

45m

BLOCKED

1.04B

PEAK

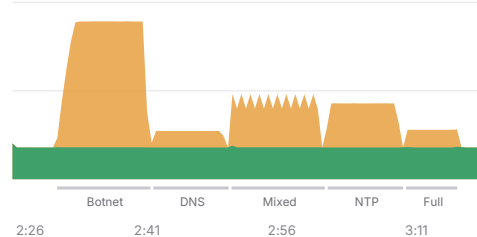
995K pkt/s

SOURCES

1,853 · 193 nets

Your traffic through the attack

Packets a second, five minutes either side



Reaching your network Blocked

Your traffic never stopped: at least 250K packets
a second got through, every second.

Where it came from

1,853 sources, 193 networks. Top three, masked.

•••••.13.0/24

United States

66.7M blocked

•••••.14.0/24

United States

64.3M blocked

•••••.6.0/24

United States

61.9M blocked

What it learned

- UDP to port 52000, 576-byte packets
- UDP from port 123, to port 52000

Single out DDoS traffic that looks like yours

Held to the rate limit: your connections carry on, but
new visitors to a public server may be dropped too.