

Inline network protection · Preliminary

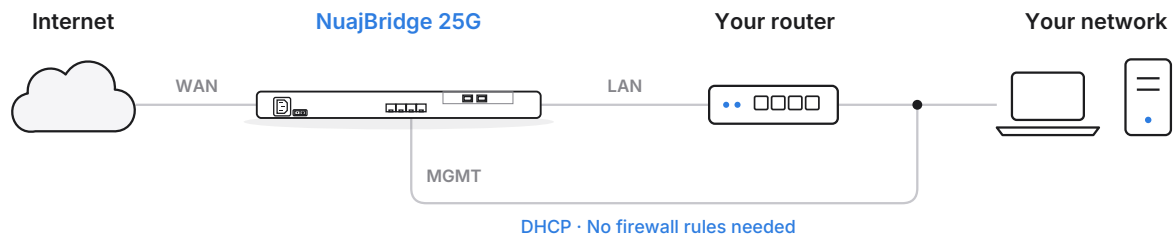
NuajBridge 25G

Inline protection for your 25 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.

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.

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

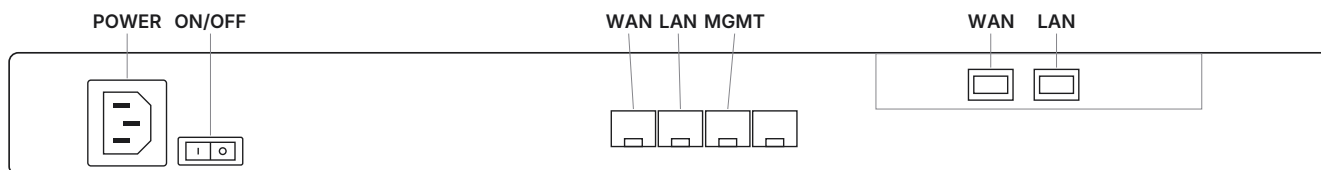
An alert when a device on your network keeps trying to reach listed addresses, a sign of infection; that traffic is blocked.

Why, for any address

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

Hardware

Tech specs



Network ports

Two 25 Gigabit Ethernet, SFP28
WAN to your internet connection, LAN to your router; 10 Gb/s with SFP+ modules

Copper network ports

Two 2.5 Gigabit Ethernet, RJ45
A WAN and LAN pair, used when the SFP28 pair is not cabled

Management port

One 2.5 Gigabit Ethernet, RJ45
For cloud management

Power

AC, IEC C14 inlet
With a power switch

Form factor

1U rack unit

USB

Four USB 3.0 ports

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.

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.

Block reflection with asymmetric routing

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