DjiNN

Agentic DDoS OPS

AI-Powered Operations Layer for GenieATM

Siarhei Matashuk | CCIE #27340 | Genie Networks

European Peering Days · Bologna · March 2026

This is not a product pitch.

This is an engineering discussion about an approach we believe in.

Some of what I'll show is working. Some is R&D.

I'll clearly separate facts from plans.

Double CCIE · 20+ years in ISP operations · Genie Networks

No marketing. Just engineering pain — and what we're doing about it.

The Pain We All Know

Cognitive Overload

Dozens of screens, manual threshold tuning, tribal knowledge in Slack threads

Set-and-Forget Thresholds

Detection drifts from reality. Missed attacks or alert fatigue. No continuous tuning

Expertise Walks Out the Door

Senior engineer leaves — half the institutional knowledge goes with them

Minutes Matter

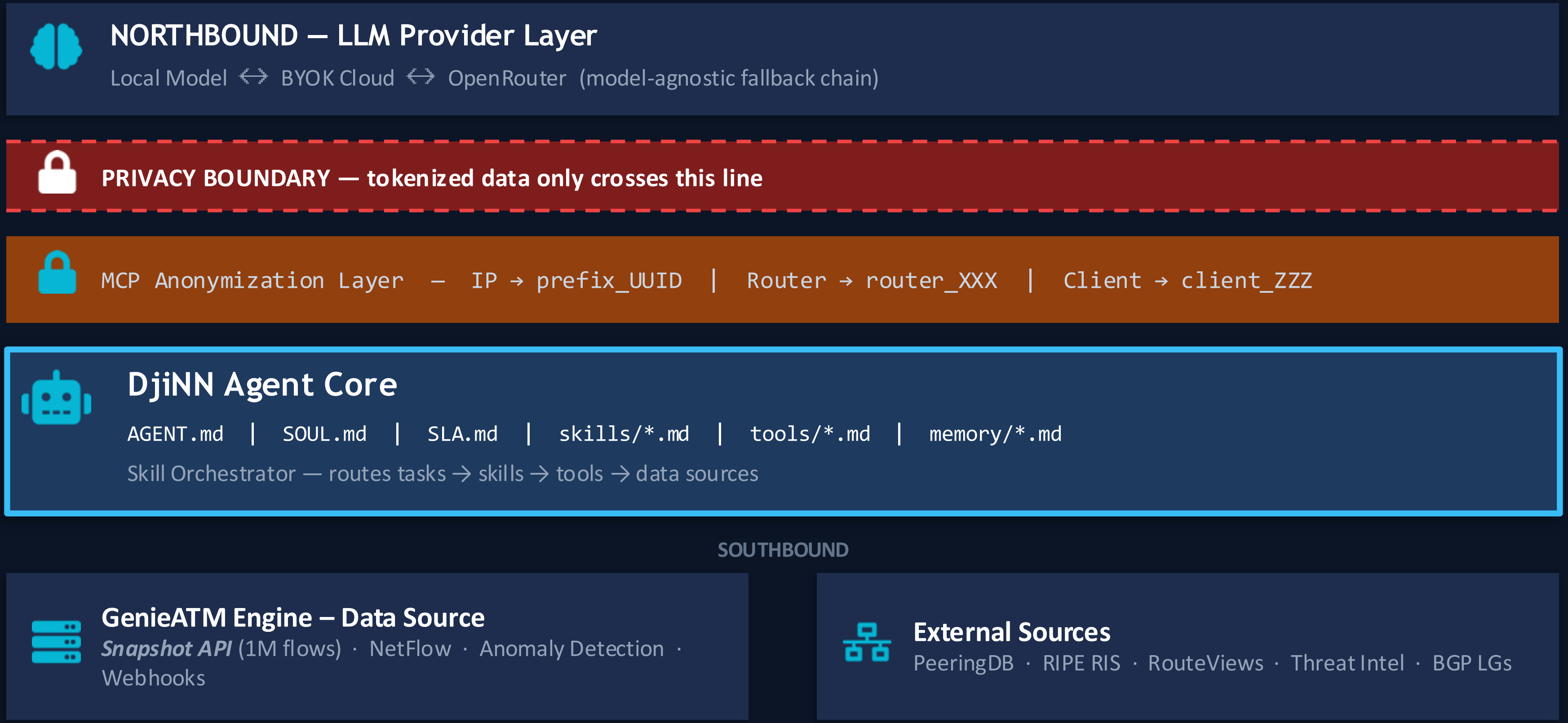
DDoS context assembly from 5+ sources before mitigation can even begin

Sound familiar?

What if your detection engine could talk to you?

An AI agent that sits on top of GenieATM via API,
operates as a team of specialized virtual NOC/SOC roles,
and gets smarter with every incident.

Architecture — North/South + Privacy Boundary



NORTHBOUND — LLM Provider Layer

Local Model ↔ BYOK Cloud ↔ OpenRouter (model-agnostic fallback chain)

PRIVACY BOUNDARY — tokenized data only crosses this line

`MCP Anonymization Layer — IP → prefix_UUID | Router → router_XXX | Client → client_ZZZ`

DjiNN Agent Core

`AGENT.md | SOUL.md | SLA.md | skills/*.md | tools/*.md | memory/*.md`

Skill Orchestrator — routes tasks → skills → tools → data sources

SOUTHBOUND

GenieATM Engine – Data Source

Snapshot API (1M flows) · NetFlow · Anomaly Detection · Webhooks

External Sources

PeeringDB · RIPE RIS · RouteViews · Threat Intel · BGP LGs

Anatomy of a Skill

A skill is a .md file. Not code. A job description for a virtual team member.

```
# Platform SRE

## Role
Platform reliability engineer for GenieATM.

## Schedule
Run every 15 minutes via cron.

## Checks
1. CPU > 80% sustained 5 min → alert
2. Memory > 85% → alert
3. Core processes running → verify
4. Snapshot freshness > 2 min → alert

## Boundaries
Never delete raw data without approval
2 failed self-heals → escalate
```

~30 lines of text

A NOC engineer reads, understands, and modifies in 5 minutes

No SDK, no code

New skill = writing a job description, then git push

Git-versioned

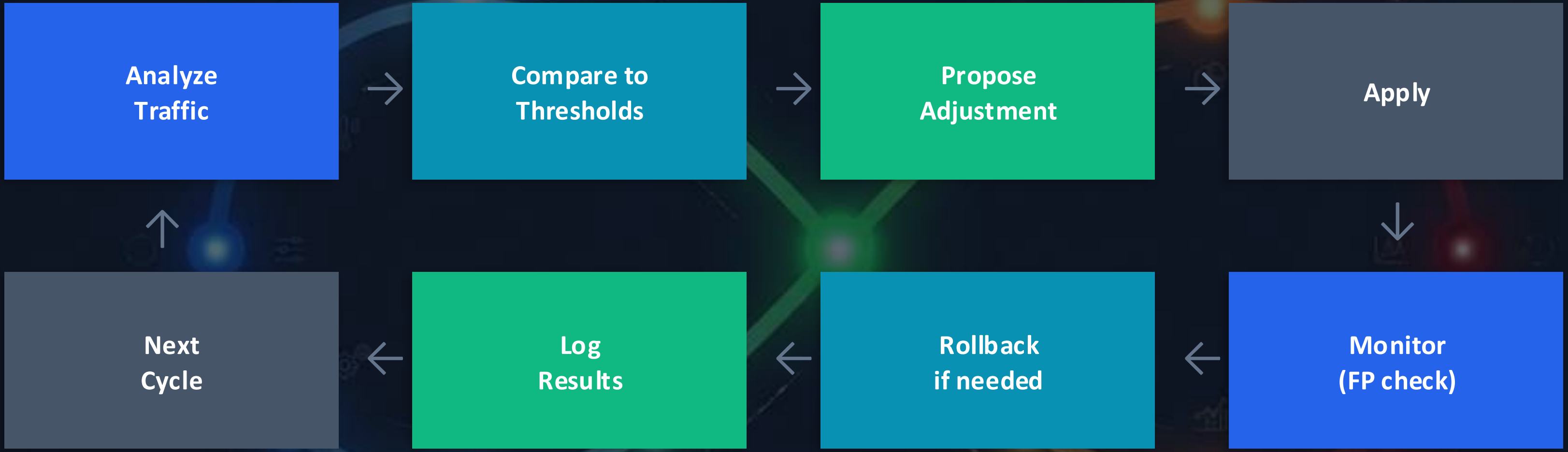
Every change is a commit with full audit trail

Declarative

Skill says WHAT. Agent figures out HOW via tools layer

Baseline Analyst — Threshold Tuning Loop

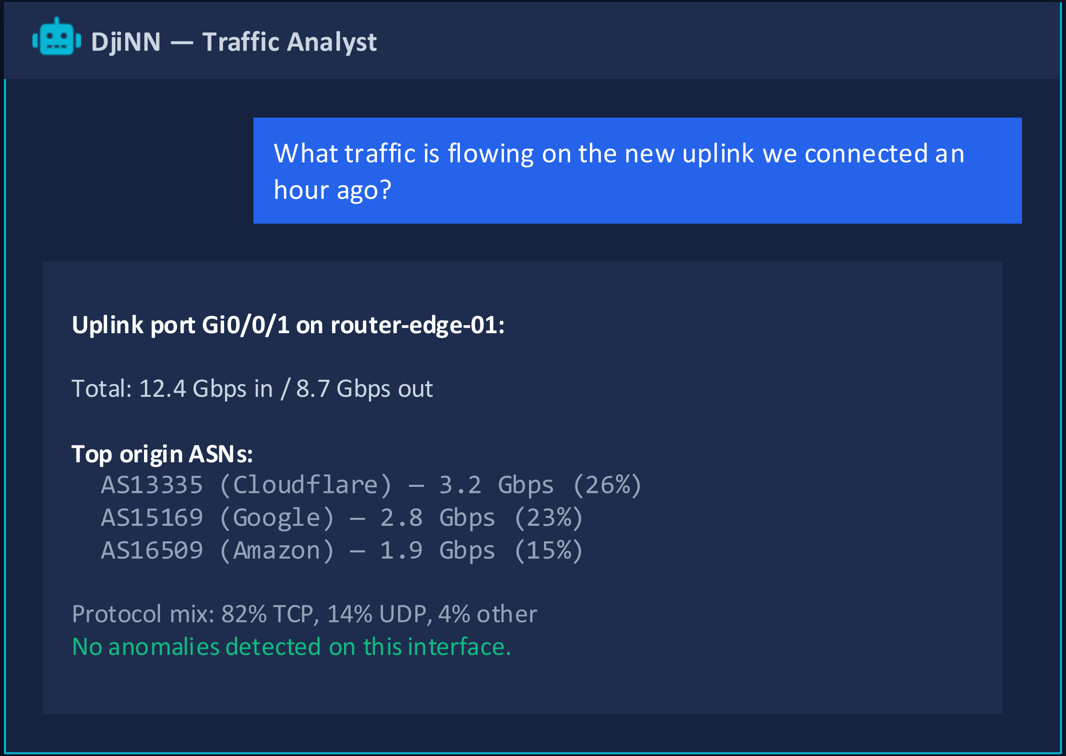
Threshold tuning is the #1 ongoing maintenance burden for DDoS detection.



Runs on schedule during peacetime. Embedded operational playbook — a senior engineer's checklist.

Set-and-forget → missed attacks or alert fatigue. This skill keeps detection calibrated continuously.

Traffic Analyst — Conversational Network State



DjiNN — Traffic Analyst

What traffic is flowing on the new uplink we connected an hour ago?

Uplink port Gi0/0/1 on router-edge-01:

Total: 12.4 Gbps in / 8.7 Gbps out

Top origin ASNs:

```
  AS13335 (Cloudflare) — 3.2 Gbps (26%)
  AS15169 (Google) — 2.8 Gbps (23%)
  AS16509 (Amazon) — 1.9 Gbps (15%)
```

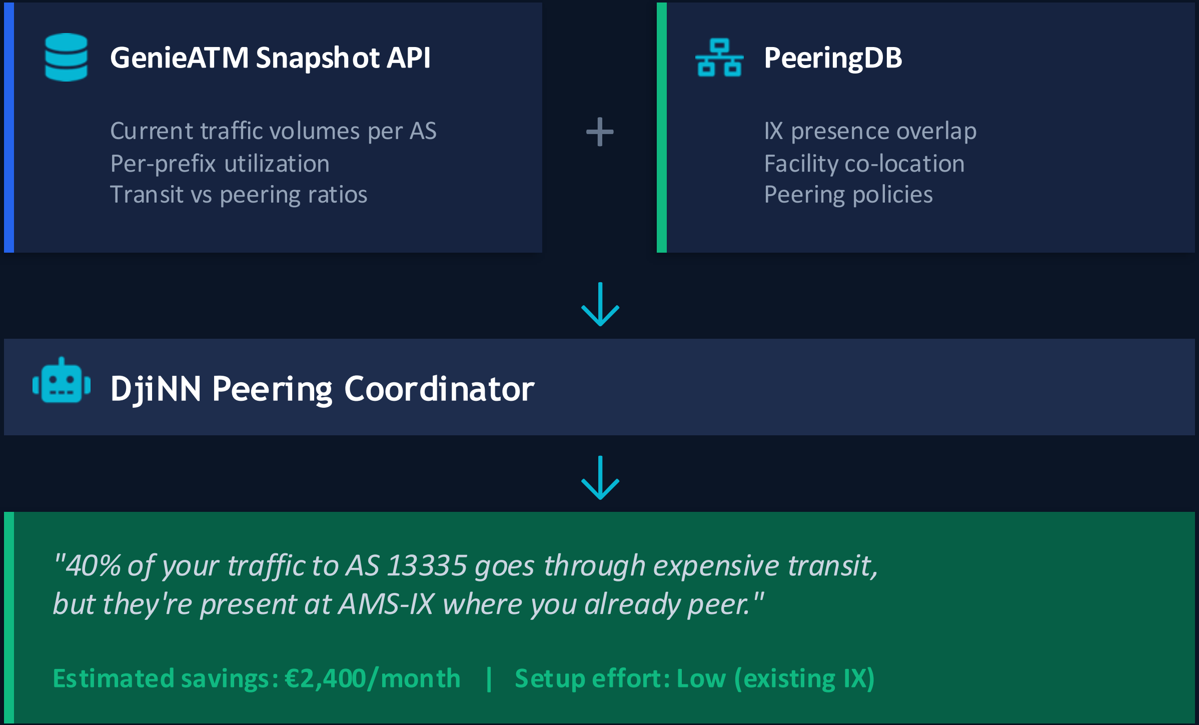
Protocol mix: 82% TCP, 14% UDP, 4% other

No anomalies detected on this interface.

Powered by Snapshot API

- 1M latest enriched raw flows in hot in-memory cache
- Millisecond query response time
- Multi-dimensional breakdowns: origin-AS, protocol, geo, top talkers
- Both live snapshot and historical disk data
- Any team member gets answers — no query syntax needed

Peering Coordinator — Proactive Cost Optimization



GenieATM Snapshot API

Current traffic volumes per AS
Per-prefix utilization
Transit vs peering ratios

+

PeeringDB

IX presence overlap
Facility co-location
Peering policies

DjiNN Peering Coordinator

"40% of your traffic to AS 13335 goes through expensive transit, but they're present at AMS-IX where you already peer."

Estimated savings: €2,400/month | Setup effort: Low (existing IX)

Why this matters

- Peering decisions are high-value but analysis is tedious
- Cross-referencing traffic + PeeringDB manually takes hours
- Agent automates research, presents ROI estimates
- Monitors peering health and utilization trends over time

The Virtual NOC/SOC Team — 9 Skills

Baseline Analyst

Continuous threshold tuning with auto-rollback

MVP

Traffic Analyst

Natural-language queries to live network state

MVP

Peering Coordinator

Cost optimization via PeeringDB cross-reference

MVP

Incident Responder

Attack context assembly + mitigation options

Phase 2

Platform SRE

System health monitoring + self-healing

Phase 2

Reporting Analyst

On-demand dashboards from text descriptions

Phase 2

Forensics Analyst

Auto post-mortems + organizational memory

Phase 3

Capacity Planner

Trend analysis + proactive upgrade recs

Phase 3

Deployment Engineer

First-run setup + architecture guidance

Phase 3

Each skill is a .md file in git — add, modify, or remove without touching the core agent

The Hard Parts — Honest Assessment

What keeps us up at night (besides DDoS attacks)

Data Privacy

"Where does my data go?"

MCP anonymization layer tokenizes all sensitive data. Real values never leave the perimeter. Local model option = zero data exposure.

LLM Latency

"AI is too slow for real-time"

Rule-based fallback for time-critical scenarios. LLM handles enrichment and investigation — not the initial detection trigger.

Trust

"I don't trust AI with my network"

Maturity model: start with recommendations only. Human approves all destructive actions. Autonomy earned, not assumed.

We don't have all the answers yet. But we know what questions to ask.

Trust Maturity Model — Earned, Not Assumed

Level 0 **Alert Only**	Level 1 **Assisted**	Level 2 **Supervised**	Level 3 **Autonomous**
Detection + notification (status quo)	Detection + enriched context + recommendation	Auto-mitigation for known patterns, approval for new	Full autonomy with audit trail + rollback
Current state	**Human-in-the-loop**	**Human-on-the-loop**	**Autonomous**

We start here

Transition to next level only when operational trust is established through track record.

Let's Build This Together

I didn't come here to sell you anything.

I came because I believe this approach — agentic operations on top of proven detection — is where our industry is heading.

We're building an early access program for operators who want to shape this in practice.

Let's talk at our booth.

Scan for Early Access