360° Security Transformation: Building Resilience with Open-Source Tools

A case study of layered defense protecting 50,000+ users at University of Dhaka, at zero licensing cost.

Md Mahedi Hasan

Senior Cybersecurity Analyst

ICT Cell, University of Dhaka

Agenda

Perimeter Security
OPNsense NG Firewall · Suricata IDS/IPS

Network Segmentation
DMZ · Management · Data zones

Secure Remote Access
OpenVPN · WireGuard · MFA · RBAC

Web Application Defense
CrowdSec · Nginx bouncer · Community intel

Security Visualization
Grafana · Prometheus · Dashboards

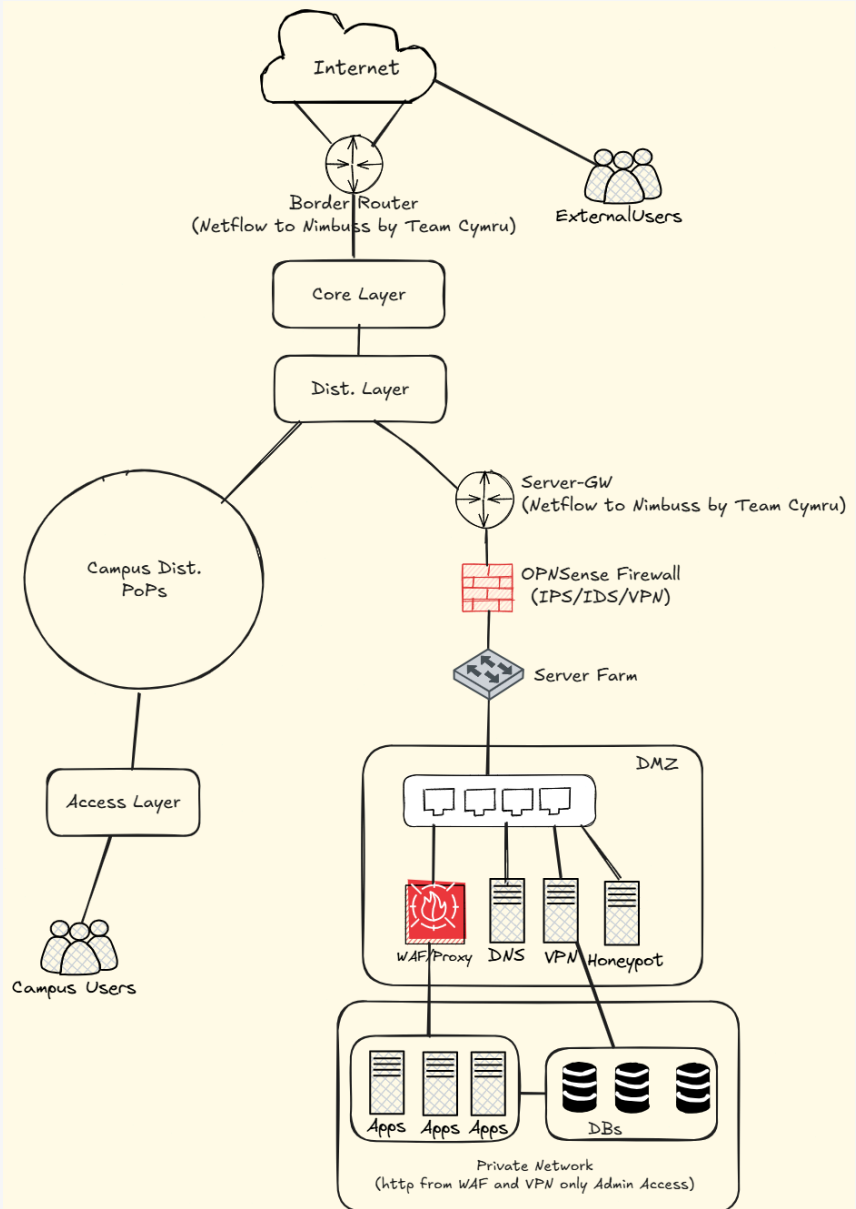
Security Monitoring
Wazuh SIEM · FIM · CVE scanning

DNS Security
DNSSEC · .bd TLD signing · Chain of trust

Outcome & User Experience
Real-world results · 50K-user experience

Cost Analysis
Open-source stack · $0 vs $20k/mo alternatives

Network Architecture & Traffic Flow



Outbound — Internal User → Internet

Access Layer VLANs → NAT + DNS RPZ → Core Layer → Border (RPKI · Netflow to Nimbus) → Internet

Routing Security: RPKI ROV blocks hijacked prefixes

DNS Protection: RPZ drops queries to malware C2 and phishing domains before exit

Inbound — External User → Campus Services

Border — RPKI · uRPF · Nimbus → Core → Server-GW → OPNsense IPS / VPN → DMZ — WAF + CrowdSec → Apps → DB (VPN only)

DDoS Absorbed: 50% drop in origin CPU — edge blocks flood before servers

Web Attacks Blocked: Millions of IPs auto-blocked at WAF — zero manual action

Zero DB Exposure: DB zone unreachable from internet at any layer

OPNsense Firewall: Control, Inspect, and Contain

Minimize Attack Surface

Only HTTPS and VPN face the internet. Everything else is denied at the edge.

Inspect Before Trust

Suricata runs inline — malicious traffic is blocked before it reaches any service.

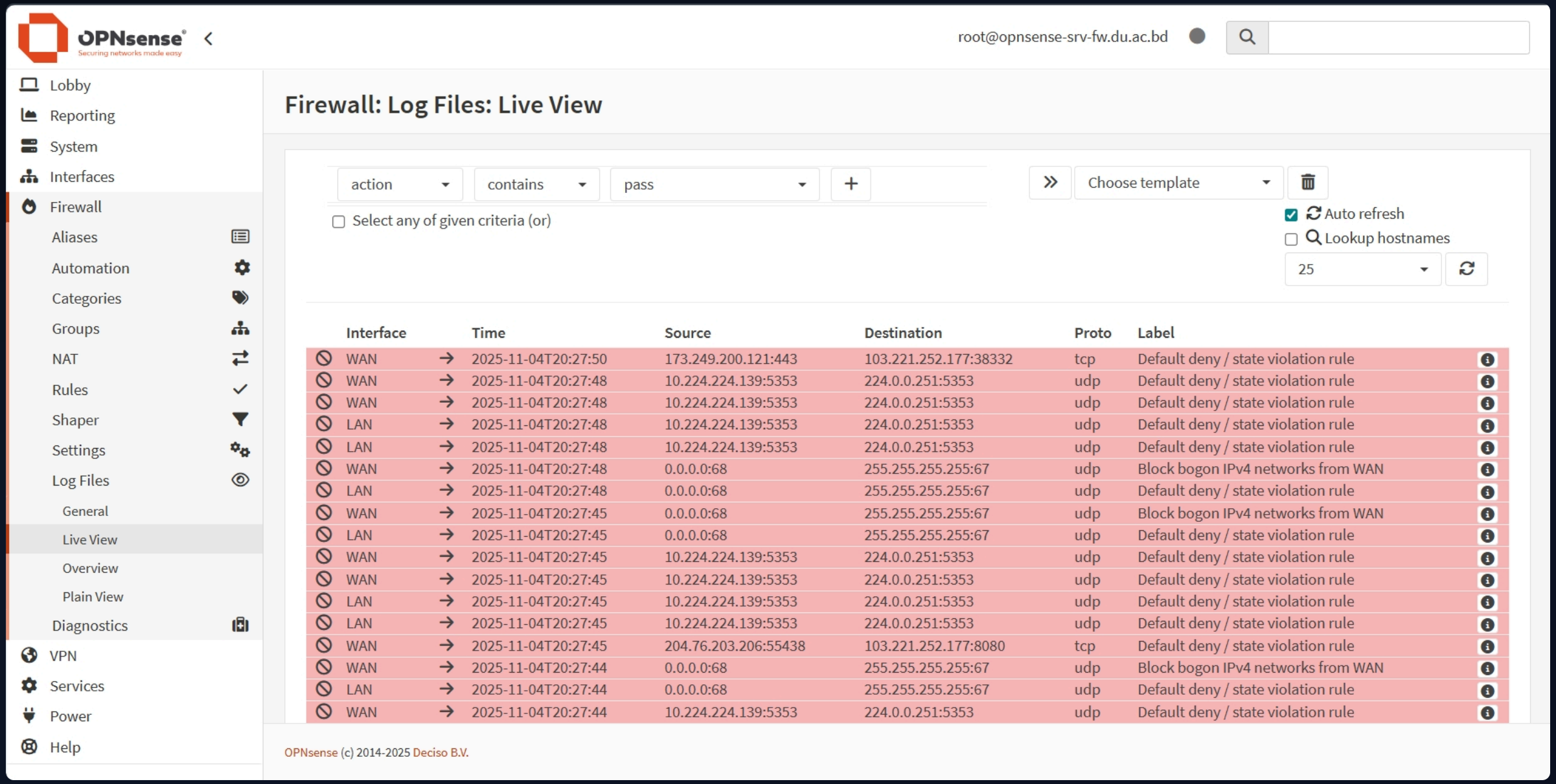
Enforce Segmented Paths

NAT, ACLs, and VLAN policy keep traffic on approved routes. No free lateral movement.

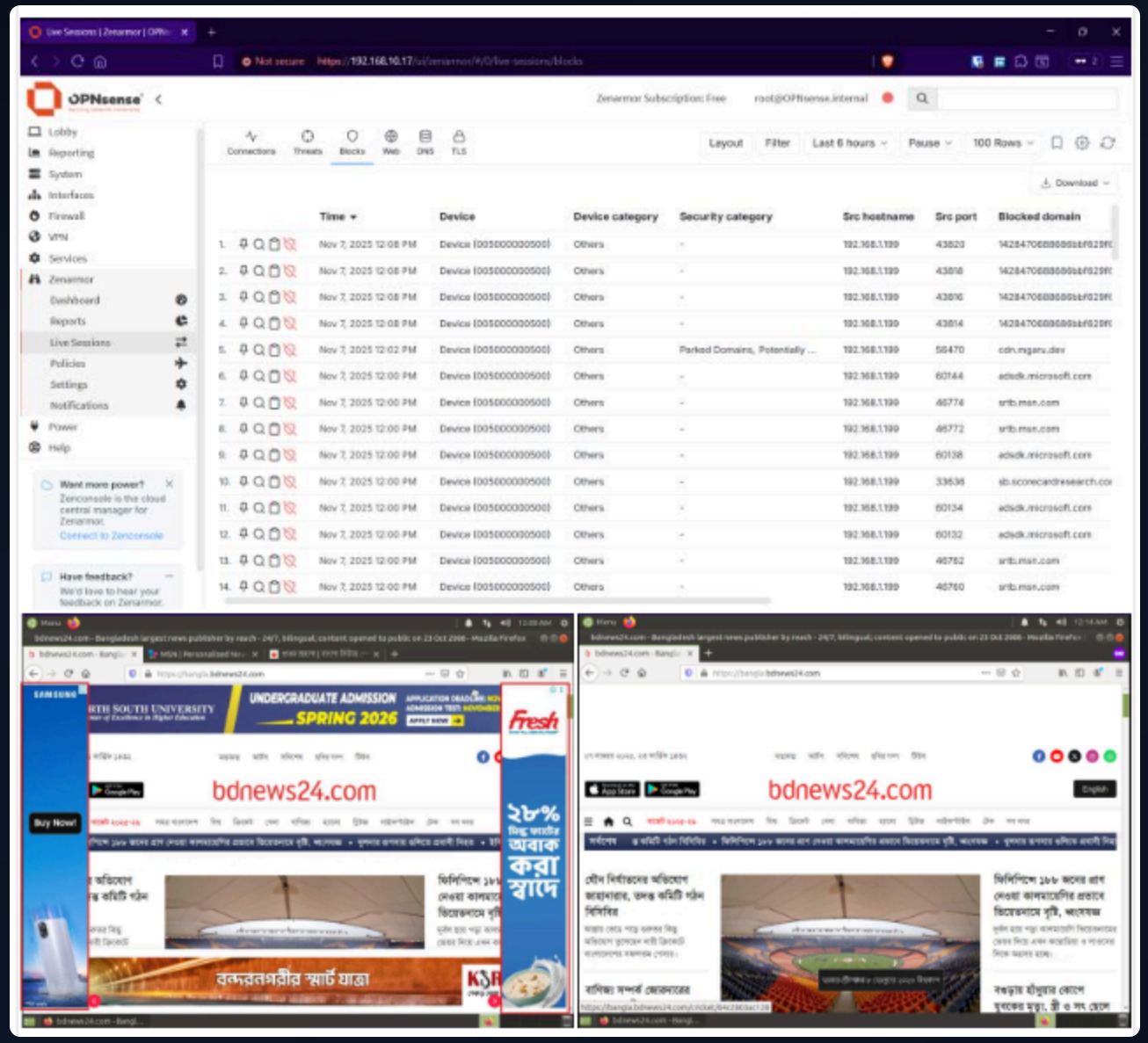
Protect Availability

HA, QoS, and rate controls keep services up during traffic spikes and abuse events.

OPNsense Dashboard— Live Traffic View



🛡️ Blocking Trackers and Ads with OPNsense + Zenarmor



Network Segmentation: From WAN to Services

WAN
Only a tiny public attack surface

↓

OPNsense
NAT, ACLs, IDS/IPS, GeoIP, rate limits

↓

DMZ
Reverse proxy and CrowdSec-protected web services

Management
VPN-only access for admins and operators

Data Zone
No direct internet route, strict east-west policy

Exposure Reduced
Only required ports are published; all other paths die at the perimeter.

Lateral Movement Limited
DMZ, management, and data each keep a separate trust boundary.

Forensics Ready
Firewall and NAT decisions are logged for correlation in Wazuh.

Secure Remote Access — VPN

Remote User
Staff or admin starts a trusted session

Strong Auth
TOTP plus certificate-based access

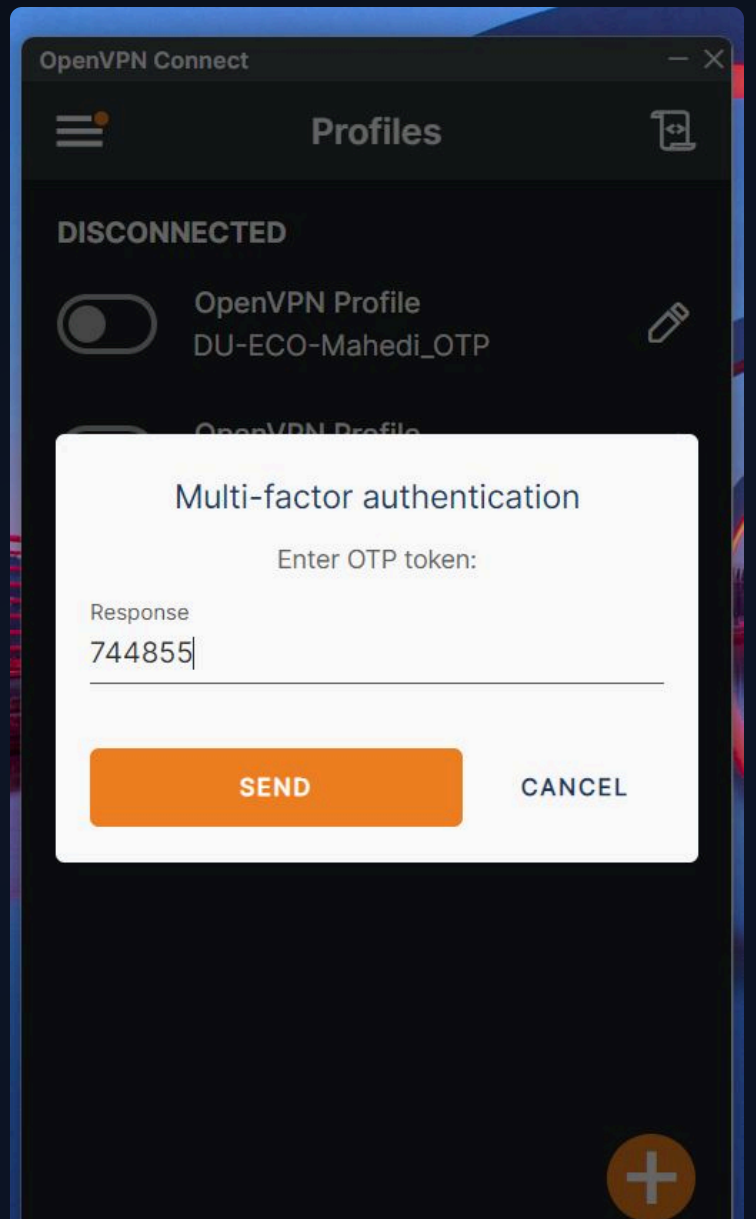
VPN Gateway
OPNsense terminates and logs all sessions

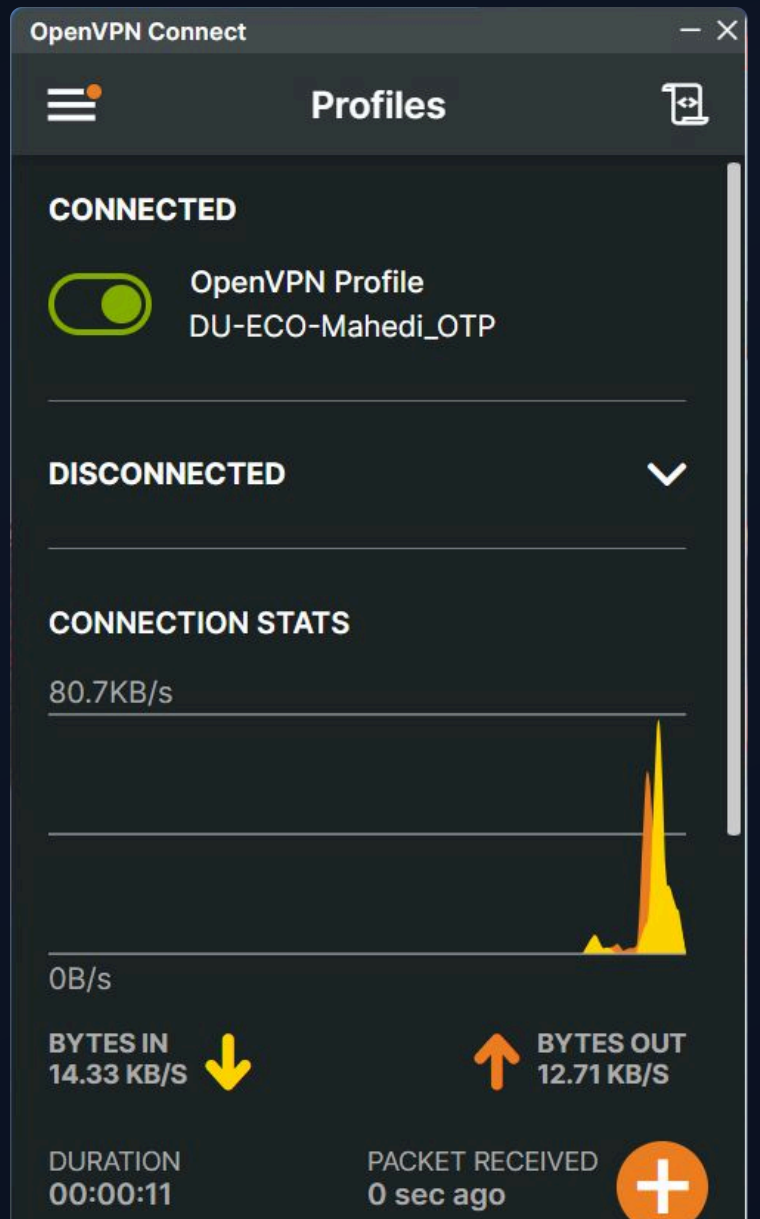
RBAC Policy
Least-privilege access to management-only zones

Operational Goal
Remove direct admin exposure from the internet. One gate, one checkpoint, logged end to end.

Security Outcome
All traffic routes through the tunnel — no split tunneling — so we can inspect everything going in and out.

OpenVPN Configuration





CrowdSec: Fast Blocking with Community Intel

Detect Real Attack Behavior

Scenarios catch brute force, scans, and abuse — no static signature lists to maintain.

Deploy Without Disruption

Nginx bouncer integration is lightweight — added quickly with no architecture changes.

Block in Seconds

Flagged sources are blocked at the Nginx layer immediately. No manual step.

Visible Impact

Block counts and attack trends are in the dashboard — clear evidence of what it stops.

CrowdSec Architecture with Nginx

Web Traffic
HTTP/S requests hit Nginx

→

Log Parser
Agent parses access and error logs

→

Scenario Match
SQLi, XSS, brute force, scans

→

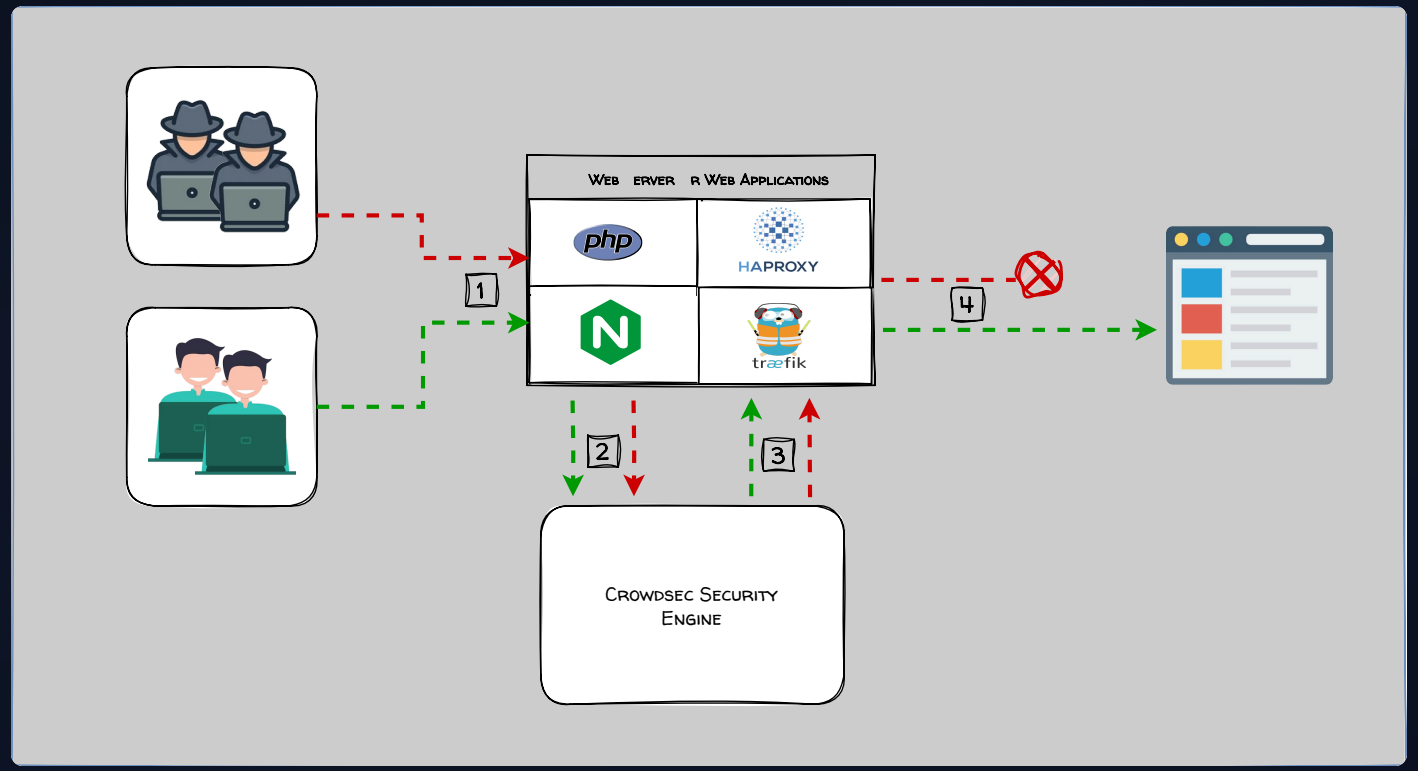
Local API
Decision engine with no cloud dependency

→

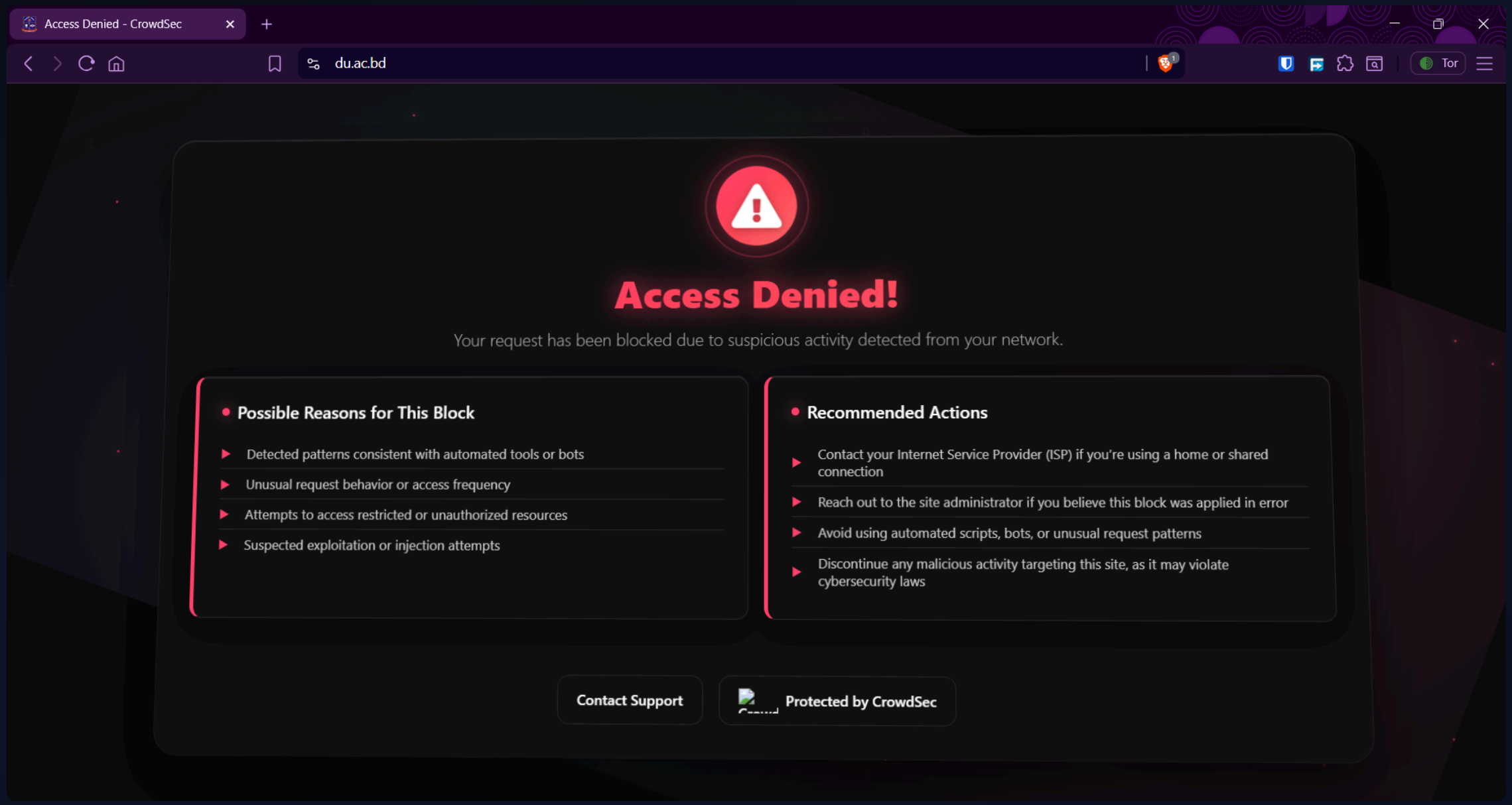
Nginx Bouncer
Block at proxy layer with low latency

→

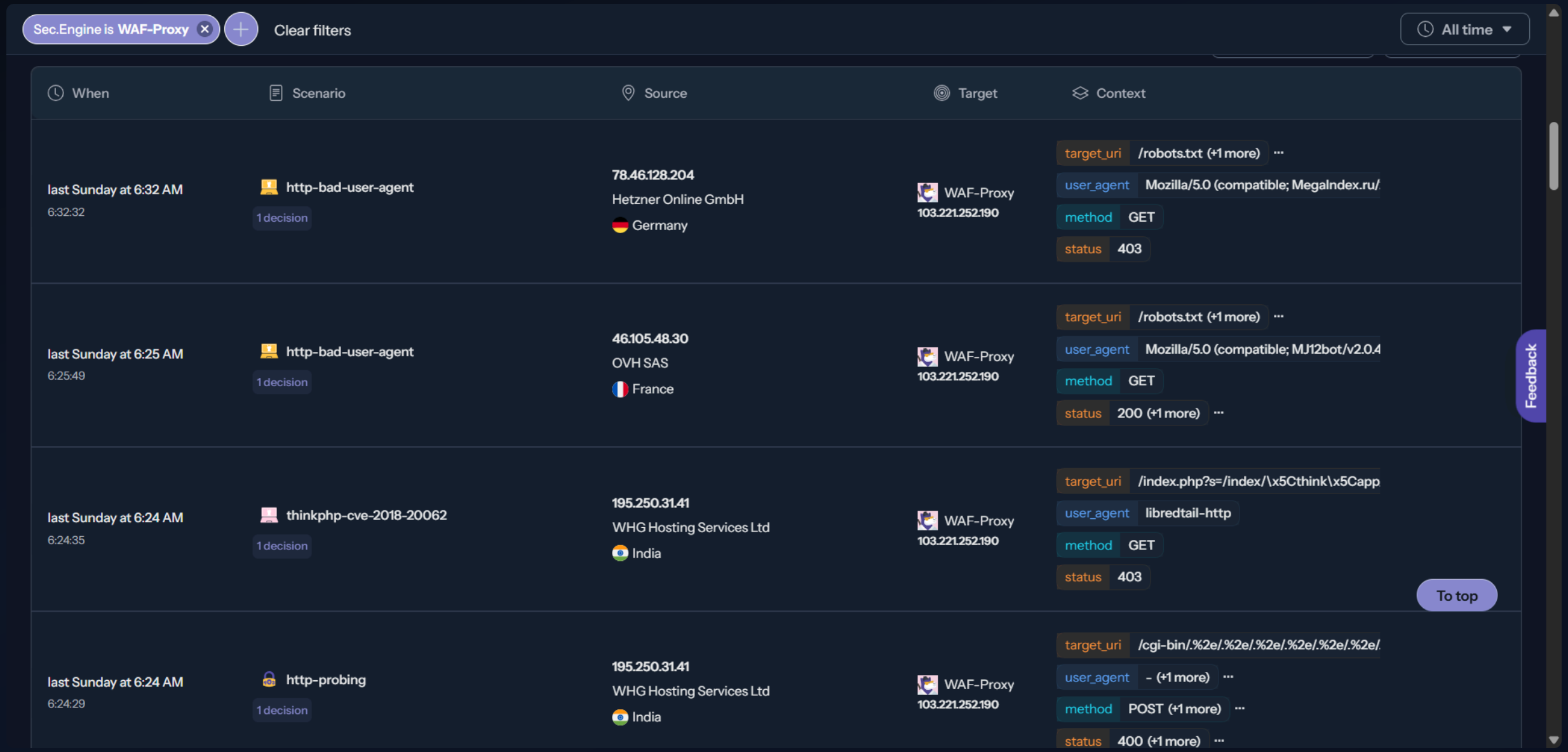
Origin Server
Only clean traffic reaches the app



🚫 Blocked Bad Network with CrowdSec



CrowdSec Security Dashboard



Grafana Monitoring — CrowdSec Metrics

DDoS Web Traffic Blocked by CrowdSec

Wazuh SIEM — Unified Security Monitoring

Collect

Ingest firewall, WAF, VPN, endpoint, and server telemetry into one searchable timeline.

Correlate

Link network events to host activity so each incident can be traced from entry point to response.

Verify

FIM, rootkit checks, and CVE scans tell us when something changed on a host — and whether our containment actually held.

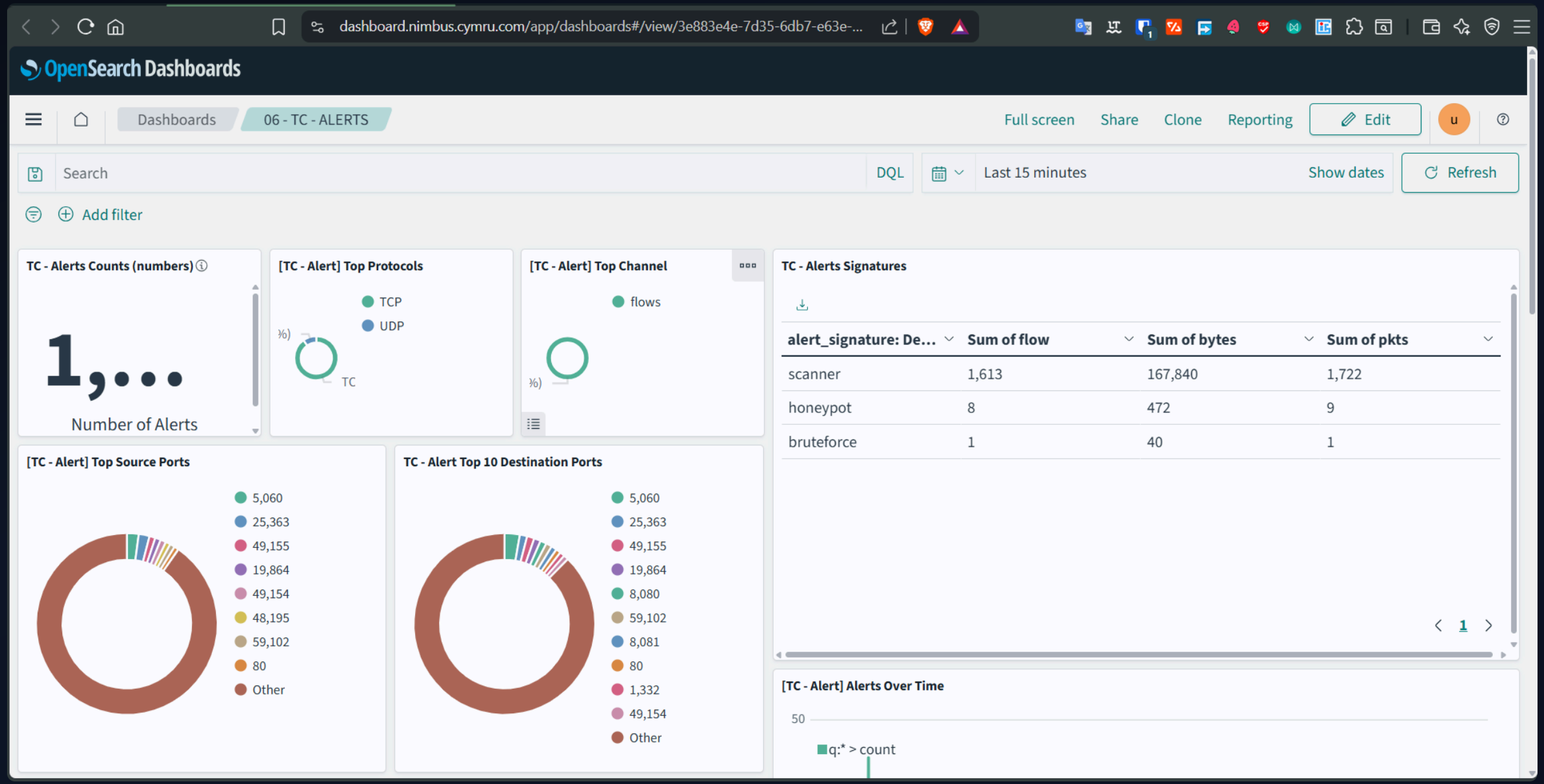
Escalate

We tune rules to cut the noise. Only alerts that genuinely need a human response reach the team.

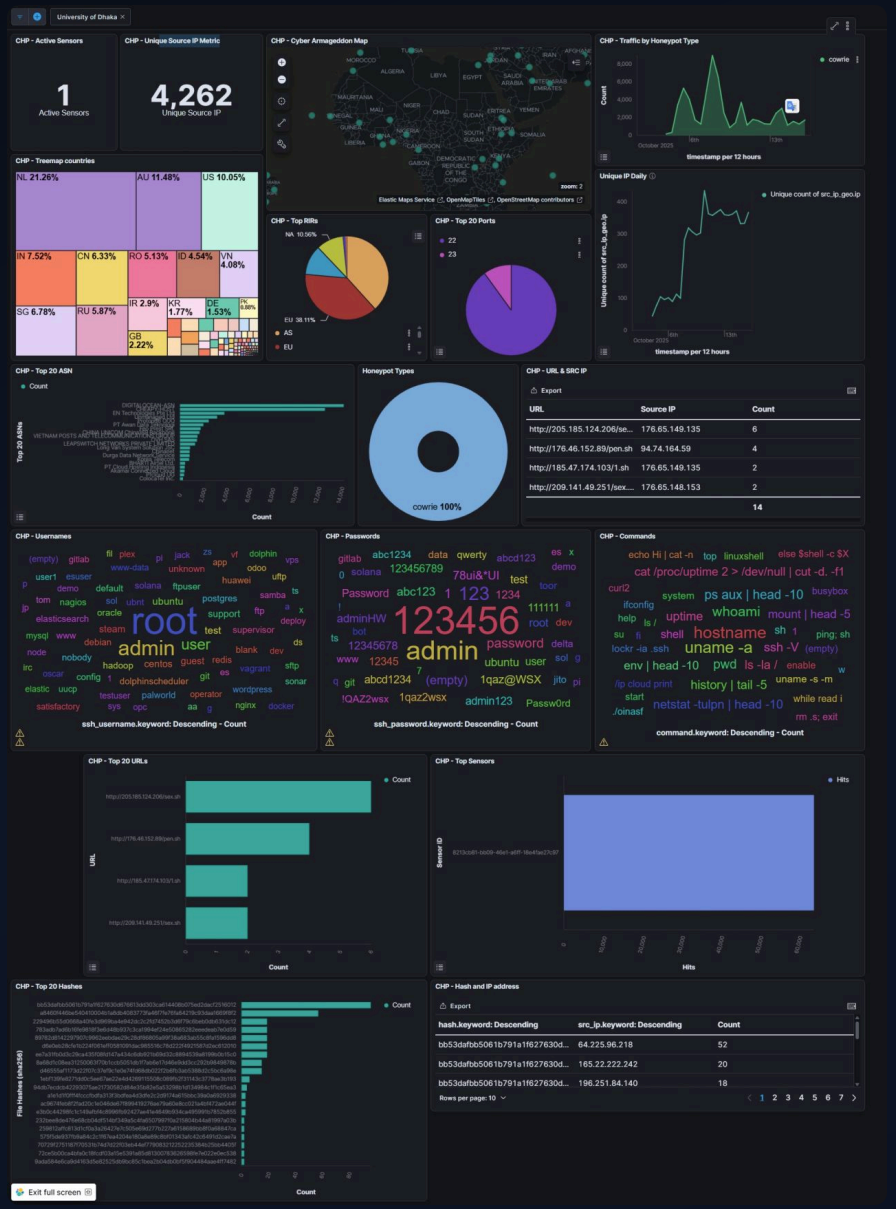
Integrations

Integrates Suricata IDS/IPS, CrowdSec block decisions, VirusTotal enrichment, and OPNsense plus VPN telemetry.

Nimbus Security Dashboard by Team Cymru



APNIC Honeynet Dashboard



Honeypot Sensor Security Analysis Report

Sensor ID: 8213cb81-bb09-46e1-a6ff-18e4fae27c97

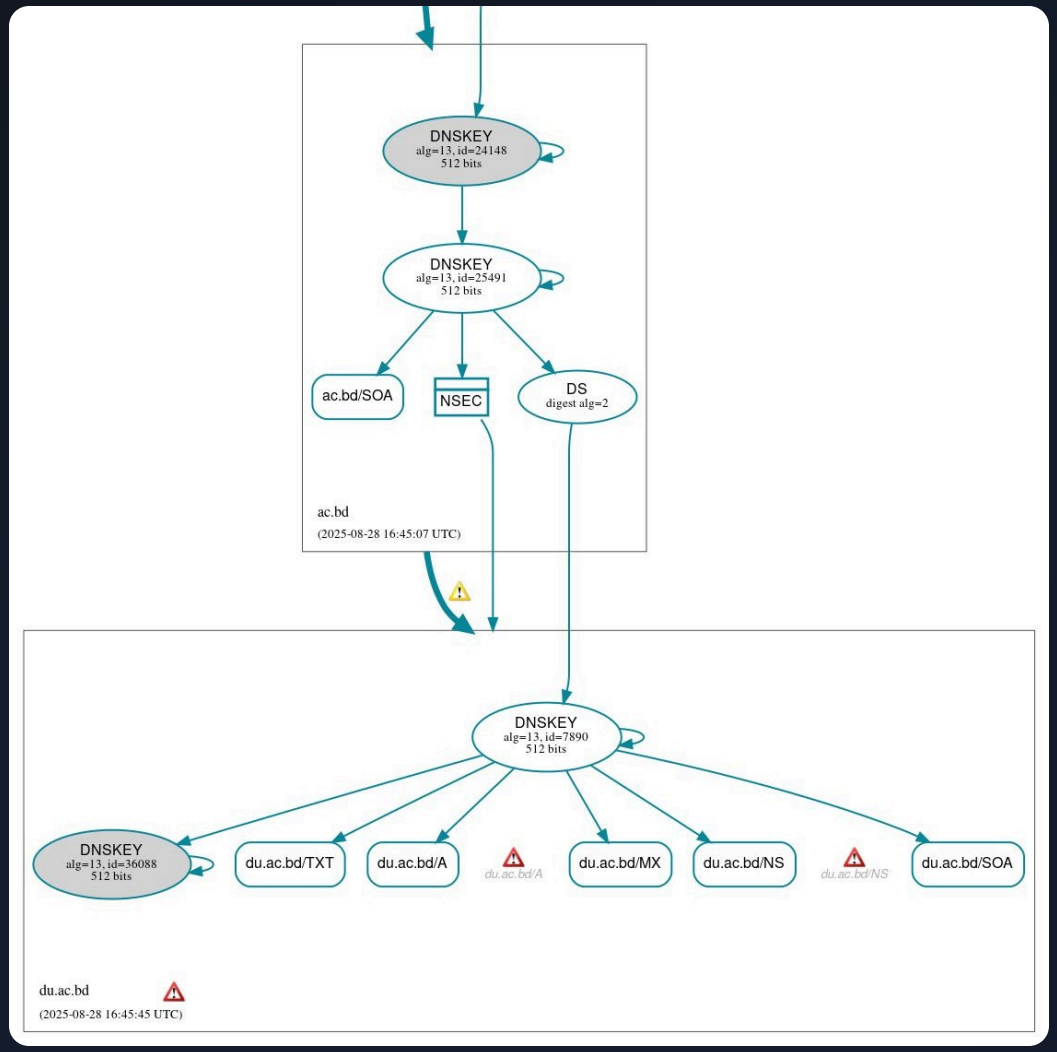
Active Period: October 3, 2025 - October 15, 2025 (12 days)

Executive Summary

- **CRITICAL:** 63,070 malicious connection attempts detected in just 12 days
- **THREAT LEVEL:** High-intensity automated brute force attacks from 4,170 unique IP addresses
- **MALWARE ACTIVITY:** 14 malware download attempts identified targeting IoT/server infrastructure
- **GEOGRAPHIC DIVERSITY:** Attacks originating from 993 autonomous systems across 50+ countries
- **PRIMARY VECTORS:** SSH (90%) and Telnet (10%) protocols targeted

TOTAL ATTACK EVENTS	UNIQUE IP ADDRESSES	UNIQUE USERNAMES
63,070	4,170	786
UNIQUE PASSWORDS	**UNIQUE COMMANDS**	**AUTONOMOUS SYSTEMS**
7,525	158	993
MALWARE URLS	**DAILY ATTACK RATE**	
4	5,256	

🔑 DNS Security & DNSSEC at du.ac.bd



What Was Done

- **du.ac.bd** — one of the first .bd domains with DNSSEC enabled
- Part of the team that first signed the **.bd TLD**
- Raised DNS security standards across **Bangladesh academia**

Why DNSSEC Matters

- **Integrity** — cryptographically signed DNS answers prevent tampering
- **Anti-Spoofing** — stops DNS cache poisoning attacks
- **Chain of Trust** — Root → TLD → Domain validation
- **User Protection** — reduces DNS hijacking and phishing risk

Outcome & User Experience

50% Server Resource Freed

Edge blocking cut CPU and memory load to origin servers by up to 50%.

Minimal False Positives

Real users pass through. Scanners and bots don't.

Better User Experience

Servers stopped struggling. Response times improved — users noticed.

Full-Stack Resilience

Each layer backs the one before it. One gap doesn't expose everything.

Secure Developer Access

VPN-only access to management zones. No direct internet exposure, full audit trail.

Production-Proven Stack

Live on a 50,000-users Operational network.

Cost Analysis — Zero to Minimal

Zero-Cost Stack

- **NG Firewall:** OPNsense (open-source)
- **Virtualization:** Proxmox VE + PBS (open-source)
- **WAF:** CrowdSec (open-source)
- **SIEM:** Wazuh community edition
- **Monitoring:** Grafana + Prometheus + Loki (OSS)
- **VPN:** OpenVPN + WireGuard (open-source)
- **DNSSEC:** BIND9 (open-source)

+ Optional Paid Add-ons

- **CrowdSec Enterprise:** ~$29/month (optional)
- **Grafana Cloud Pro:** ~$19/month (optional)
- **VirusTotal API:** Free tier sufficient for our scale

- Total monthly cost: **$0 – $48 / month**
- vs. **$5,000–$20,000/month** for commercial equivalents

Key Takeaways

Defense-in-Depth

Firewall, IPS, VPN, WAF, SIEM, DNS. Breach one layer; the rest still hold.

Open-Source Is Enterprise-Ready

Zero licence cost. Commercial equivalents run $15–20k per month.

SIEM Is Not Optional

Threats that bypassed individual tools surfaced in the SIEM.

Automate from Day One

Millions of IPs blocked automatically. No analyst needed for routine blocks.

Segment Aggressively

No database was ever internet-reachable. Lateral movement had nowhere to go.

Share and Participate

What you learn in production, others need in their planning. Present at NOGs.

Thank You

Questions & Discussion

"Open source isn't a budget compromise — it's a deliberate choice. Come ask me why."

Let's stay in touch:

mahedi@du.ac.bd | cse.mahedi@gmail.com

https://mahedi.net | linkedin.com/in/mahedicse