



SANOG

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

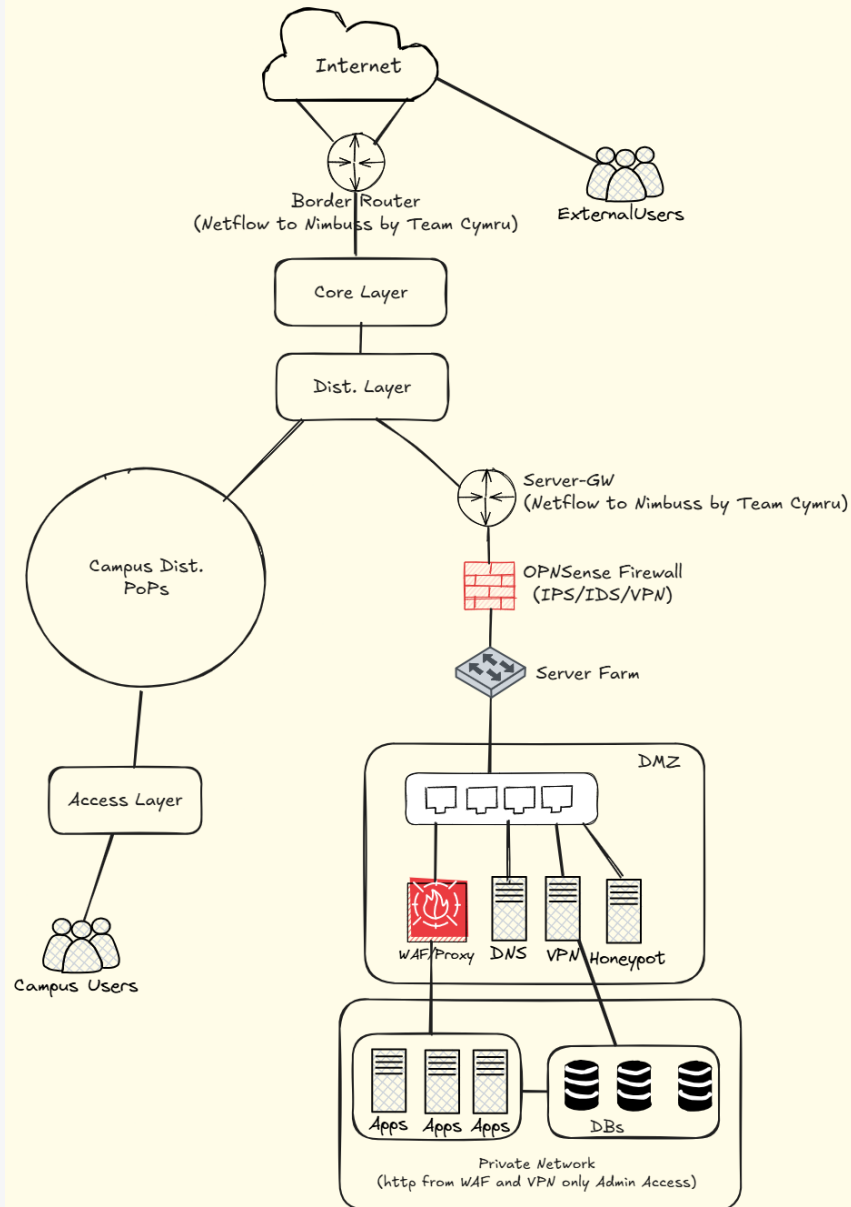
Real-world results · 50K-user experience



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

**OPNsense®**
Securing networks made easy

<

root@opnsense-srv-fw.du.ac.bd



Lobby

Reporting

System

Interfaces

Firewall

Aliases

Automation

Categories

Groups

NAT

Rules

Shaper

Settings

Log Files

General

Live View

Overview

Plain View

Diagnostics

VPN

Services

Power

Help





















Firewall: Log Files: Live View

action

contains

pass

+

>>

Choose template



☐ Select any of given criteria (or)

☒  Auto refresh

☐  Lookup hostnames

25



	Interface	Time	Source	Destination	Proto	Label	
	WAN	→ 2025-11-04T20:27:50	173.249.200.121:443	103.221.252.177:38332	tcp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:48	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:48	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	LAN	→ 2025-11-04T20:27:48	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	LAN	→ 2025-11-04T20:27:48	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:48	0.0.0.0:68	255.255.255.255:67	udp	Block bogon IPv4 networks from WAN	
	LAN	→ 2025-11-04T20:27:48	0.0.0.0:68	255.255.255.255:67	udp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:45	0.0.0.0:68	255.255.255.255:67	udp	Block bogon IPv4 networks from WAN	
	LAN	→ 2025-11-04T20:27:45	0.0.0.0:68	255.255.255.255:67	udp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:45	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:45	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	LAN	→ 2025-11-04T20:27:45	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	LAN	→ 2025-11-04T20:27:45	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:45	204.76.203.206:55438	103.221.252.177:8080	tcp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:44	0.0.0.0:68	255.255.255.255:67	udp	Block bogon IPv4 networks from WAN	
	LAN	→ 2025-11-04T20:27:44	0.0.0.0:68	255.255.255.255:67	udp	Default deny / state violation rule	
	WAN	→ 2025-11-04T20:27:44	10.224.224.139:5353	224.0.0.251:5353	udp	Default deny / state violation rule	

OPNsense (c) 2014-2025 Deciso B.V.

Blocking Trackers and Ads with OPNsense + Zenarmor

The image displays the OPNsense Zenarmor web interface. The top navigation bar includes 'Lobby', 'Reporting', 'System', 'Interfaces', 'Firewall', 'VPN', 'Services', 'Zenarmor', 'Dashboard', 'Reports', 'Live Sessions', 'Policies', 'Settings', 'Notifications', 'Power', and 'Help'. The main content area shows a table of blocked domains under the 'Blocked' tab.

	Time	Device	Device category	Security category	Src hostname	Src port	Blocked domain
1.	Nov 7, 2025 12:08 PM	Device [0056000000000]	Others	-	192.168.1.130	43020	14284706886868f828fc
2.	Nov 7, 2025 12:08 PM	Device [0056000000000]	Others	-	192.168.1.130	43018	14284706886868f828fc
3.	Nov 7, 2025 12:08 PM	Device [0056000000000]	Others	-	192.168.1.130	43016	14284706886868f828fc
4.	Nov 7, 2025 12:08 PM	Device [0056000000000]	Others	-	192.168.1.130	43014	14284706886868f828fc
5.	Nov 7, 2025 12:02 PM	Device [0056000000000]	Others	Parked Domains, Potentially ...	192.168.1.130	55470	cdn.mgarni.dev
6.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	60144	adsk.microsoft.com
7.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	46774	urlb.man.com
8.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	46772	urlb.man.com
9.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	60138	adsk.microsoft.com
10.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	33636	sb.scorecardresearch.co
11.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	60134	adsk.microsoft.com
12.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	60132	adsk.microsoft.com
13.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	46762	urlb.man.com
14.	Nov 7, 2025 12:00 PM	Device [0056000000000]	Others	-	192.168.1.130	46760	urlb.man.com

Below the table, two browser screenshots of bdnews24.com are shown. The left screenshot shows the website with various ads and banners. The right screenshot shows the same website with ads blocked, resulting in a cleaner layout.

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

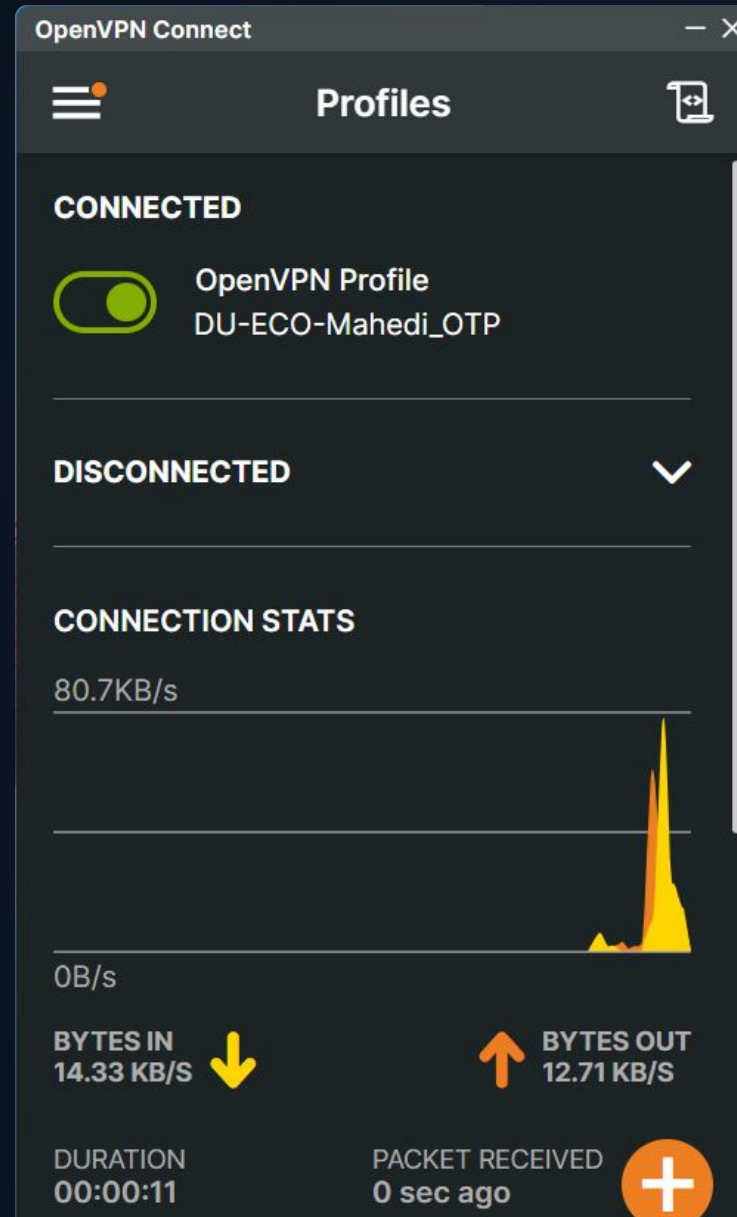
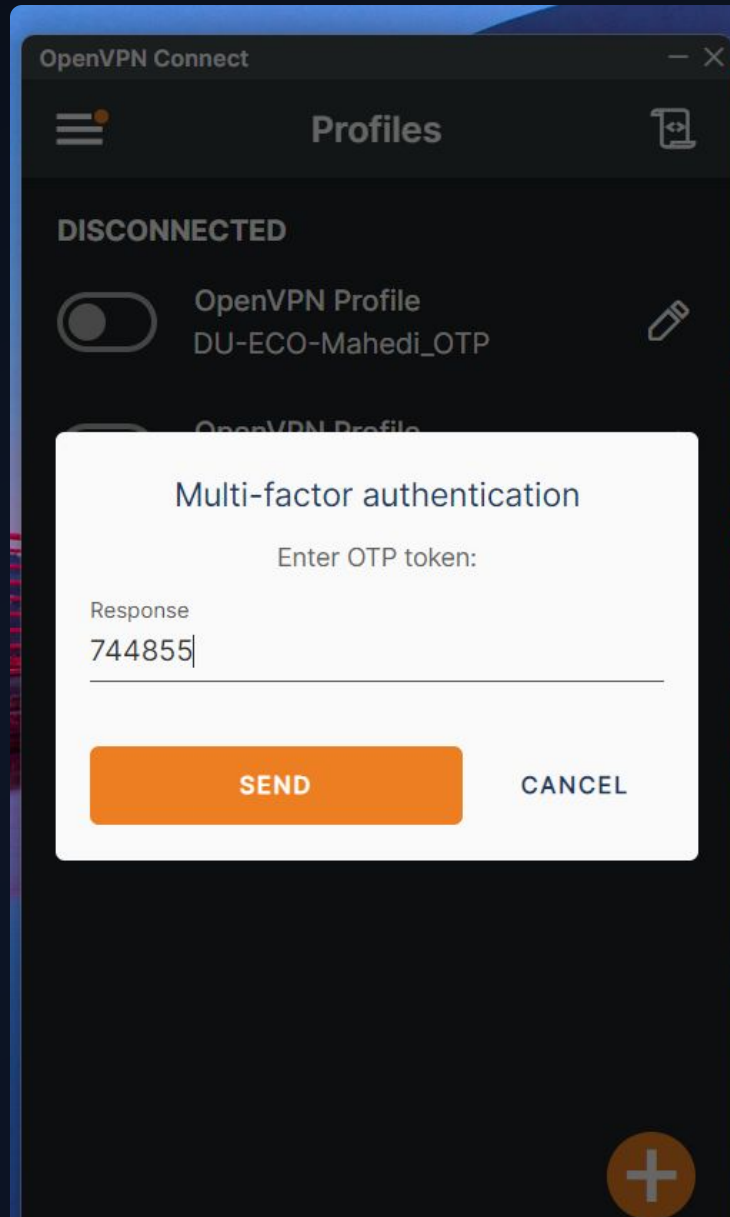
Remove direct admin exposure from the internet. One gate, one checkpoint, logged end to end.



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

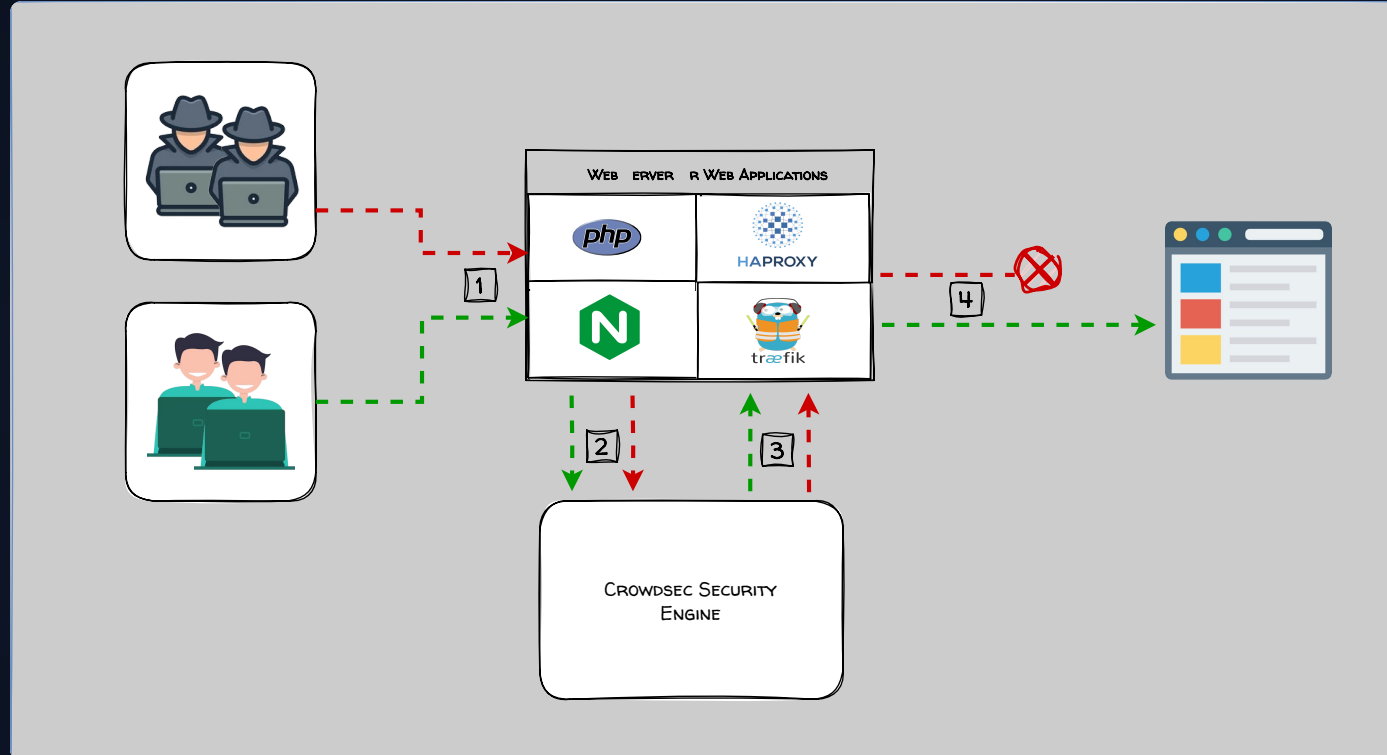
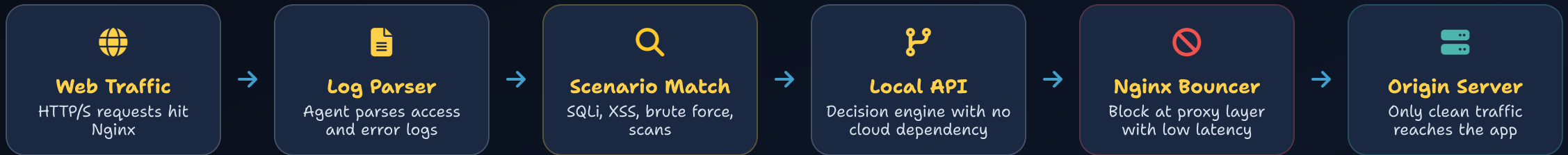
Flagged sources are blocked at the Nginx layer immediately. No manual step.

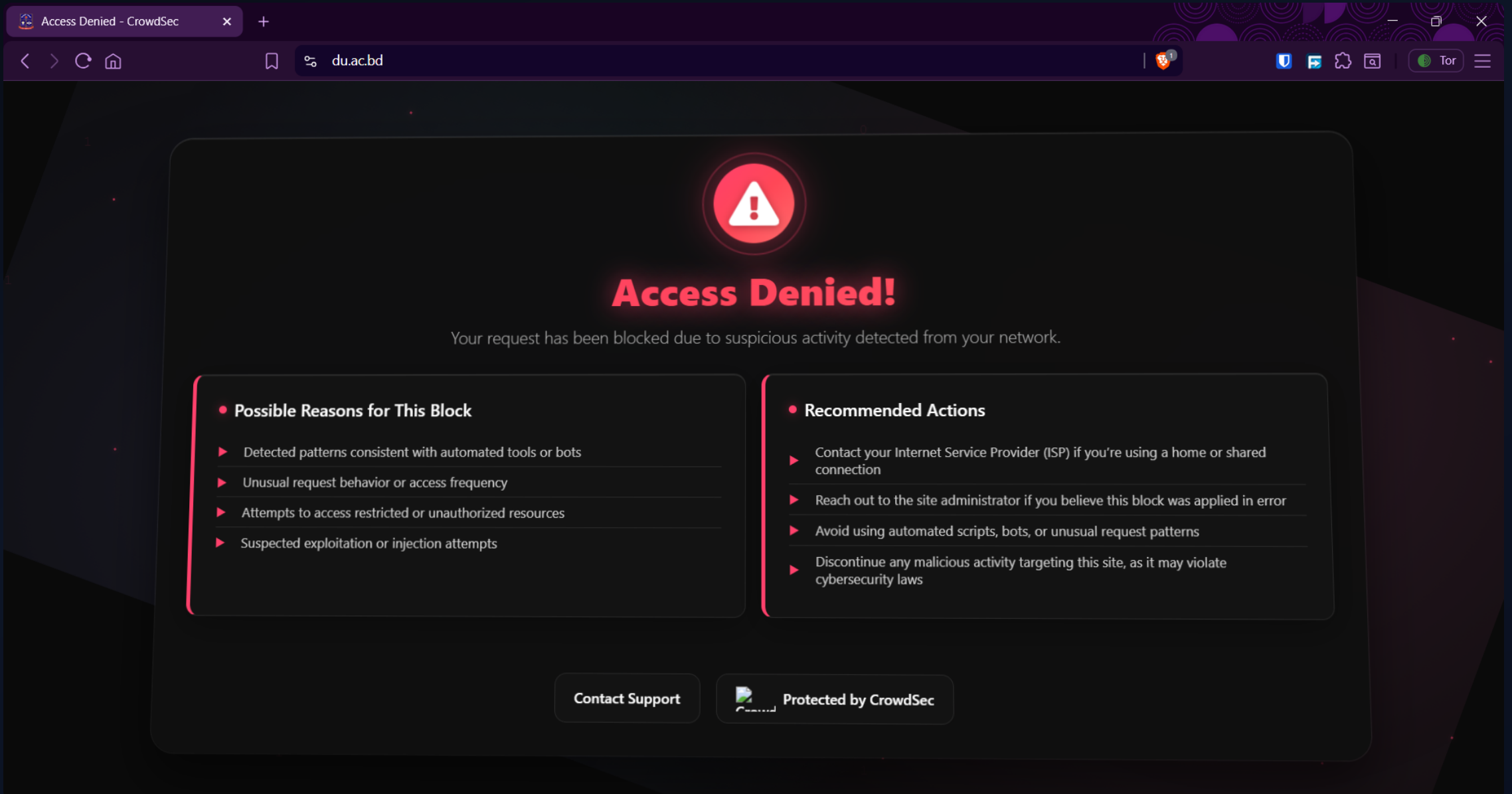


Visible Impact

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

CrowdSec Architecture with Nginx





CrowdSec Security Dashboard

Sec.Engine is WAF-Proxy x



Clear filters

All time v

When

Scenario

Source

Target

Context

last Sunday at 6:32 AM
6:32:32

http-bad-user-agent
1 decision

78.46.128.204
Hetzner Online GmbH
Germany

WAF-Proxy
103.221.252.190

target_uri /robots.txt (+1 more) ...
user_agent Mozilla/5.0 (compatible; MegaIndex.ru/
method GET
status 403

last Sunday at 6:25 AM
6:25:49

http-bad-user-agent
1 decision

46.105.48.30
OVH SAS
France

WAF-Proxy
103.221.252.190

target_uri /robots.txt (+1 more) ...
user_agent Mozilla/5.0 (compatible; MJ12bot/v2.0.4
method GET
status 200 (+1 more) ...

last Sunday at 6:24 AM
6:24:35

thinkphp-cve-2018-20062
1 decision

195.250.31.41
WHG Hosting Services Ltd
India

WAF-Proxy
103.221.252.190

target_uri /index.php?s=/index/\x5Cthink\x5Capp
user_agent libredtail-http
method GET
status 403

last Sunday at 6:24 AM
6:24:29

http-probing
1 decision

195.250.31.41
WHG Hosting Services Ltd
India

WAF-Proxy
103.221.252.190

target_uri /cgi-bin/%2e/%2e/%2e/%2e/%2e/%2e/
user_agent - (+1 more) ...
method POST (+1 more) ...
status 400 (+1 more) ...

To top

Feedback

Grafana Monitoring — CrowdSec Metrics



DDoS Web Traffic Blocked by CrowdSec



CrowdSec Security Report

November 17 - November 24, 2025

89.6M

ATTACKS PREVENTED

↑ 226899% from previous period

Top Attack Behaviors Blocked

HTTP Scan	16.0M
HTTP DoS	15.4M
HTTP Bruteforce	15.4M

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

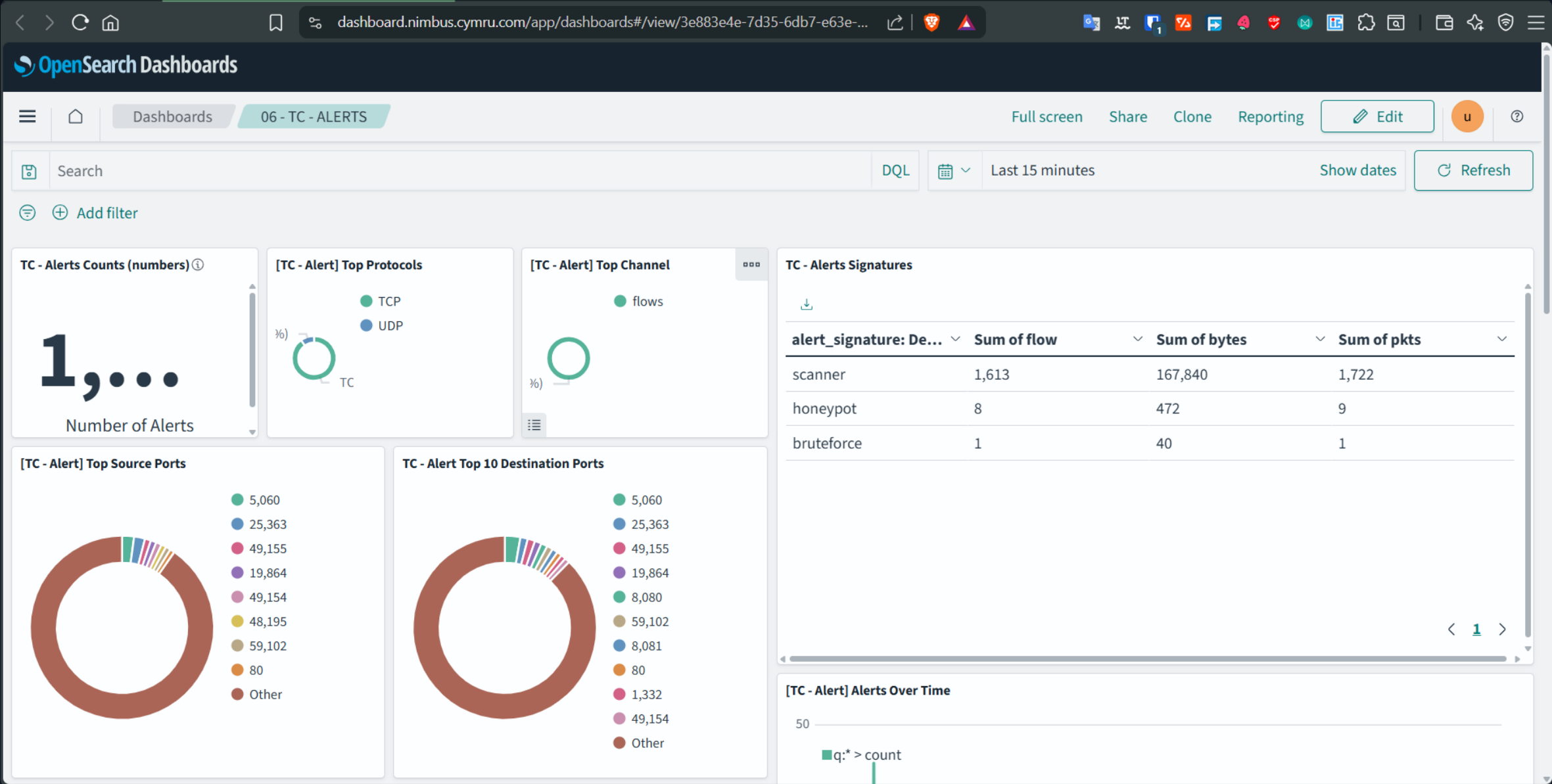
We tune rules to cut the noise. Only alerts that genuinely need a human response reach the team.



Integrations

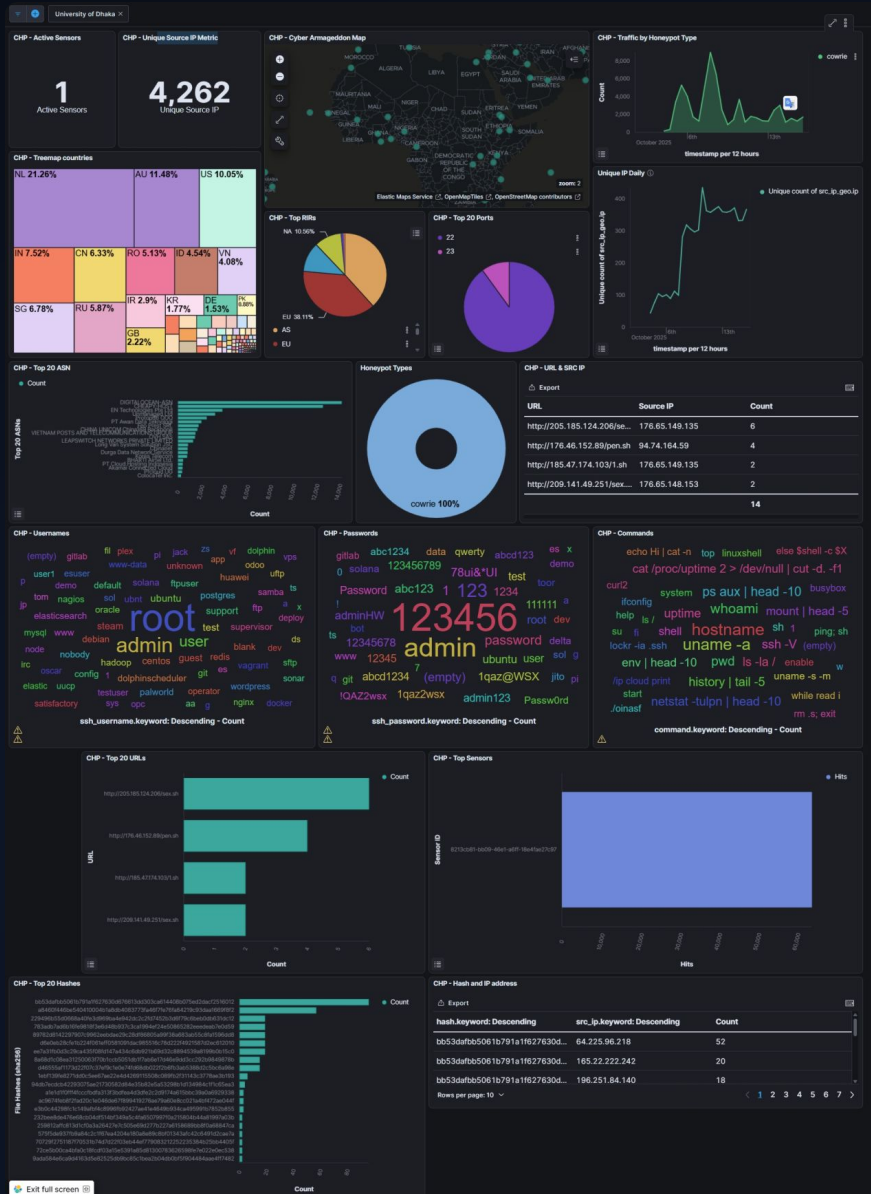
Integrates Suricata IDS/IPS, CrowdSec block decisions, VirusTotal enrichment, and OPNsense plus VPN telemetry.

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

63,070

UNIQUE IP ADDRESSES

4,170

UNIQUE USERNAMES

786

UNIQUE PASSWORDS

7,525

UNIQUE COMMANDS

158

AUTONOMOUS SYSTEMS

993

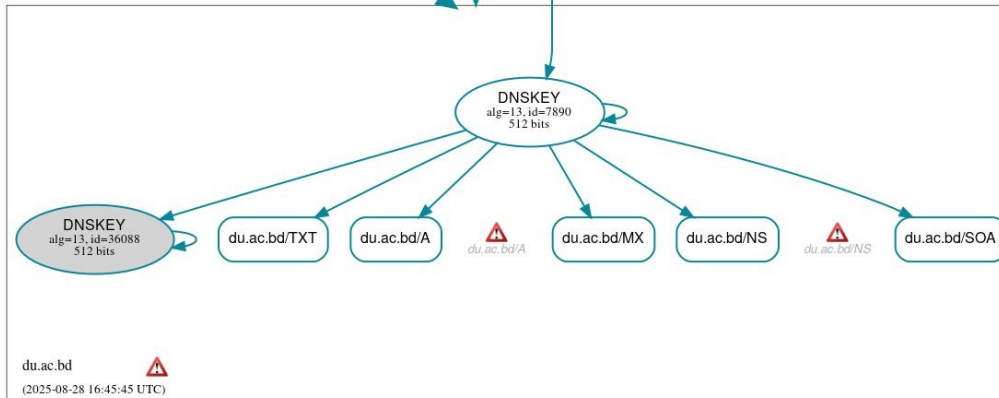
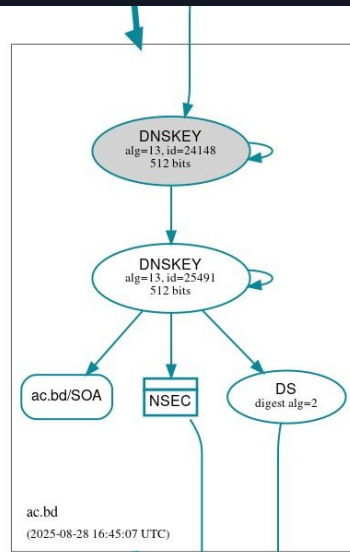
MALWARE URLS

4

DAILY ATTACK RATE

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> | [in linkedin.com/in/mahedicse](https://www.linkedin.com/in/mahedicse)

