# DeDDoS

Soluție hardware inovativă anti-DDoS, bazată pe inteligență artificială (IA)

CONSORȚIUL

UNIVERSITATEA BUCUREȘTI
Contractor/ Coordonator

ACADEMIA TEHNICĂ MILITARĂ „FERDINAND I"
Partener 1

NEXTGEN SOFTWARE
Partener 2

# Proiect

- Coordonator: Paul Irofti
- Proiect: PN-IV-P6-6.3-SOL-2024-2-0197
- Consorțiu:
    1. UB (coordonator)
    2. ATM
    3. Nextgen Software SRL.

- Echipa: 36 membrii
- Finanțator: UEFISCDI
- Buget: 5.341.847 lei (~ 1.068.370 euro)
- Perioadă: 3 iulie 2024 - 2 iulie 2026

# Echipa: Universitatea din București

- Paul Irofti -- Principal Investigator
- Radu Ionescu -- Senior Researcher
- Andrei Pătrașcu -- Senior Researcher
- Cristian Rusu -- Senior Researcher
- Andrei Hîji -- Assistant Researcher
- Silviu Gheorghe -- Master Student
- Ionel Ștefăniță Secioreanu -- Master Student
- Petrișor Tănasă -- Master Student
- Nicolae Cleju -- Senior Researcher(July 2024 - July 2025)
- Alexandru Apostu -- PhD Student (November 2024 -July 2025)

# Echipa: Academia Tehnică Militară

- Ion Bica -- Principal Investigator
- Mihai Togan -- Senior Researcher
- Constantin Grumazescu -- Researcher
- Ioana Preda -- Researcher
- Ștefan-Ciprian Arseni -- Assistant Researcher
- Constantin-Dan Avram -- Assistant Researcher
- Iulian Țiță -- Assistant Researcher
- George-Codrin Hariga -- Assistant Researcher
- Adina Pluțu-- Master Student
- Ioana Cișmaș -- Master Student
- Luca Coratu -- Master Student
- Alexandra-Ioana Buzățoiu -- Master Student
- Alexandra-Victoria Ciuvat -- Master Student
- Florina Conchințoiu -- L1 Technician

# Echipa: Nextgen Software SRL

- Vlad Gladin -- Senior Researcher
- Daniel Tache -- Researcher
- Emilian-Cristian Bonciu -- L2 Technology Engineer
- Mădălina-Andreea Diaconu -- L2 Technology Engineer
- Cristian Ștefan Ene -- L2 Technology Engineer
- Mihai Tănase -- L2 Technology Engineer
- Adrian Sandu -- L2 Technician
- Mirabela Andreea Budulan -- Researcher
- Bogdan Legănaru -- Principal Investigator (August 2024 - March 2025)
- Viorel Tiganescu -- L2 Technology Engineer
- Alin Ungureanu -- Researcher

# Privire de ansamblu

- tipuri de atacuri
- colectarea și structurarea datelor pentru algoritmii AI
- generarea de trafic cu AI
- detecție și mitigare

Bazat pe articolul de revistă:

A. Apostu, S.F Gheorghe, A. Hîji, N. Cleju, A. Pătraşcu, C. Rusu, R.T. Ionescu, and P. Irofti, *“Detecting and Mitigating DDoS Attacks with AI: A Survey,”* pp. 1--62, 2025.

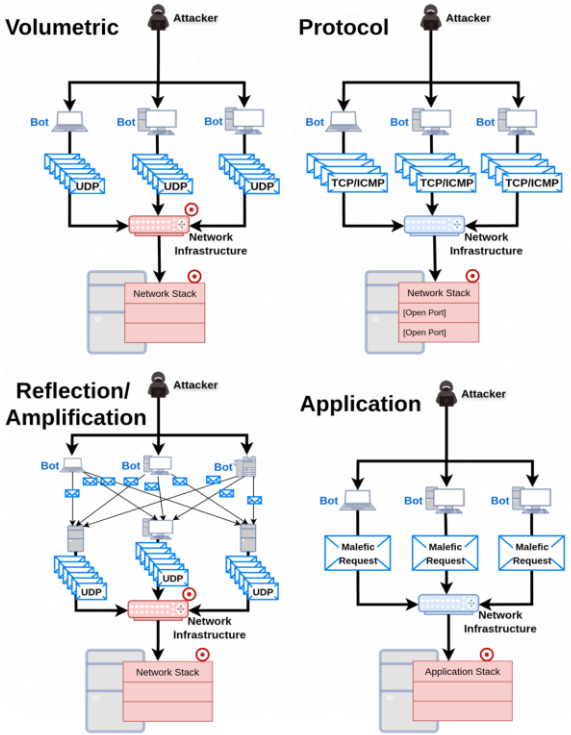
# Atacuri DDoS

**Taxonomie:**

- volumetric
- reflection/amplification volumetric
- protocol level
- application level

**Victime:**

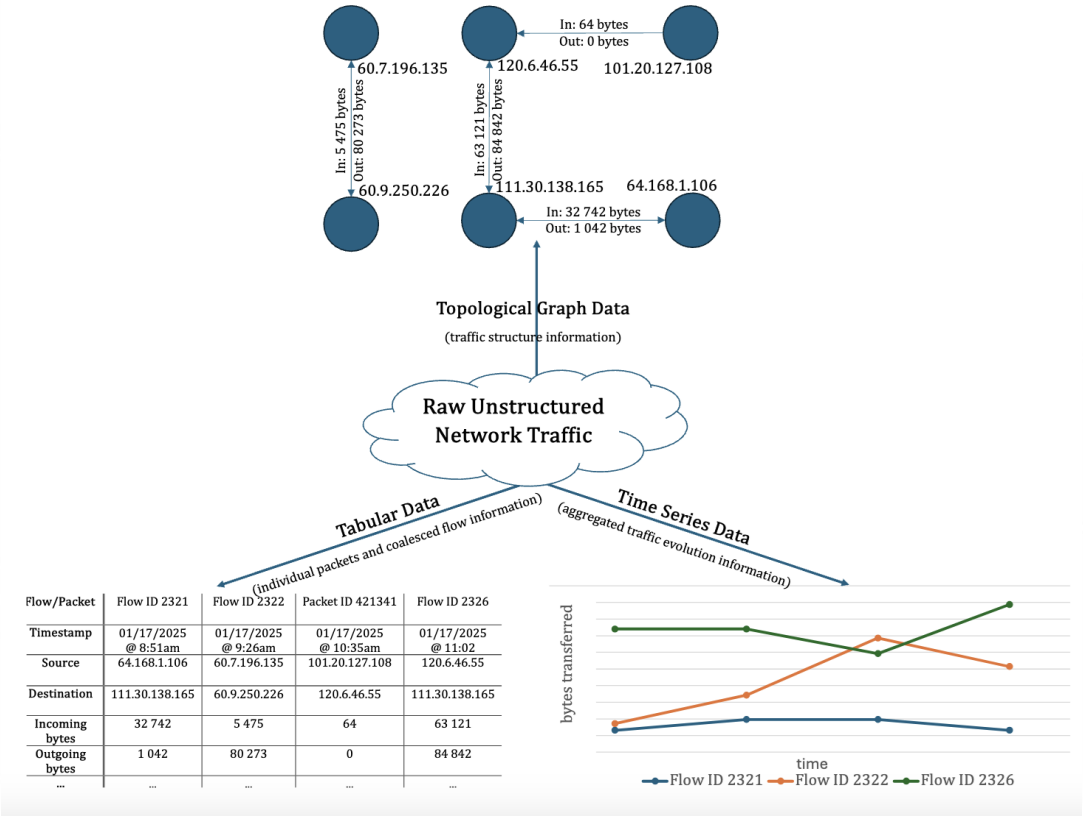
- rețele de calculatoare
- utilizatori casnici



# Structura datelor

Organizarea datelor:

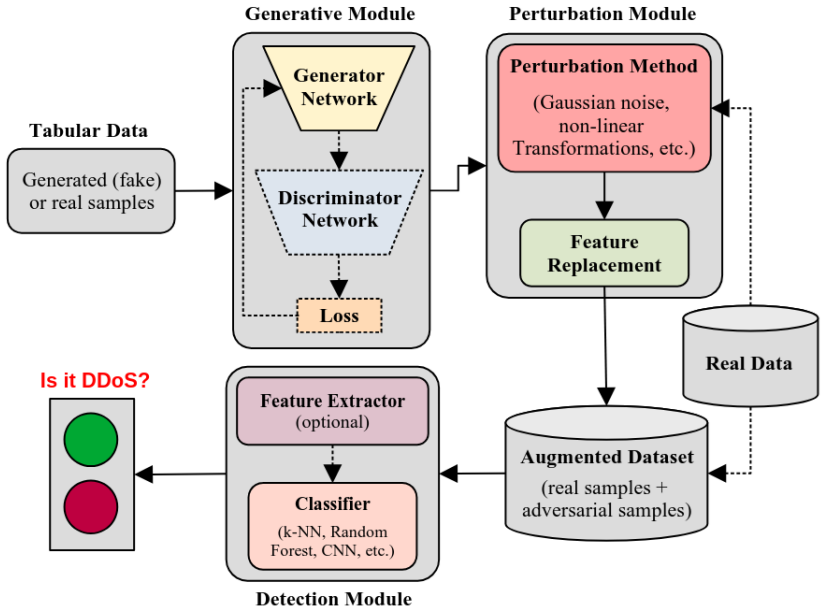
- serii de timp
- date tabulare
- topologie de grafuri




| Flow/Packet | Flow ID 2321 | Flow ID 2322 | Packet ID 421341 | Flow ID 2326 |
|---|---|---|---|---|
| Timestamp | 01/17/2025 @ 8:51am | 01/17/2025 @ 9:26am | 01/17/2025 @ 10:35am | 01/17/2025 @ 11:02 |
| Source | 64.168.1.106 | 60.7.196.135 | 101.20.127.108 | 120.6.46.55 |
| Destination | 111.30.138.165 | 60.9.250.226 | 120.6.46.55 | 111.30.138.165 |
| Incoming bytes | 32 742 | 5 475 | 64 | 63 121 |
| Outgoing bytes | 1 042 | 80 273 | 0 | 84 842 |
| ... | ... | ... | ... | ... |

# AI pentru antrenare, detecție și mitigare

- antrenare adversarială pentru detecție
- exemple și atacuri adversariale
- mitigare cu reguli generate de AI

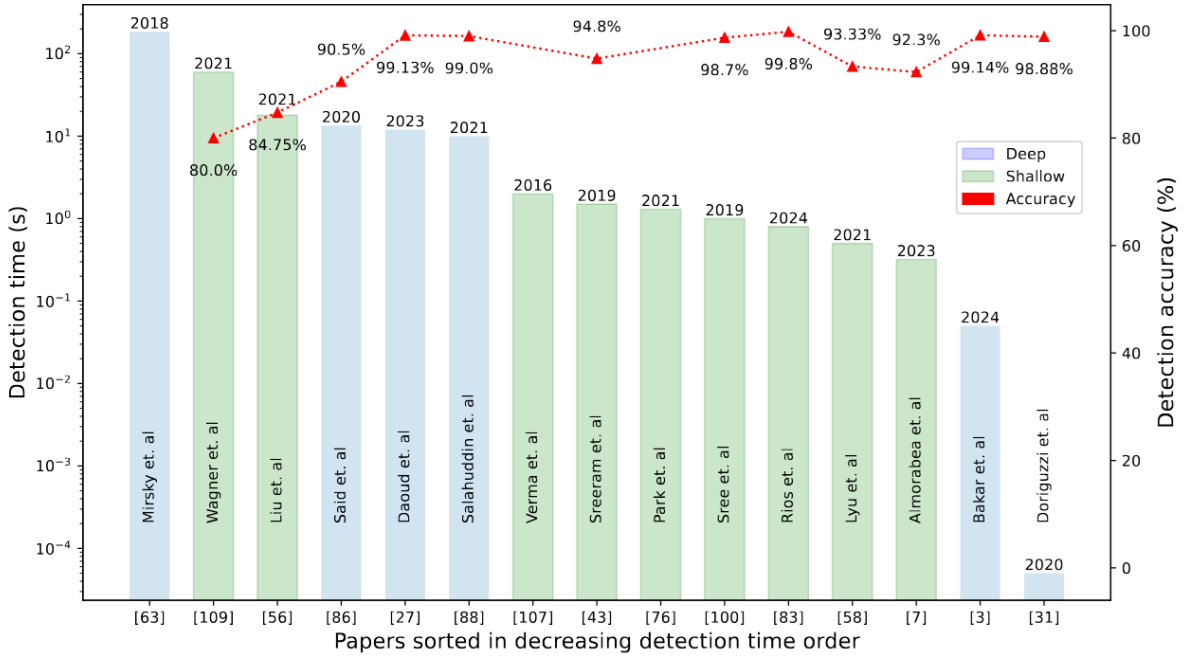


# Durata până la oprirea unui atac

Etape

- atac
- captură trafic
- procesare AI
- alertare
- blocare

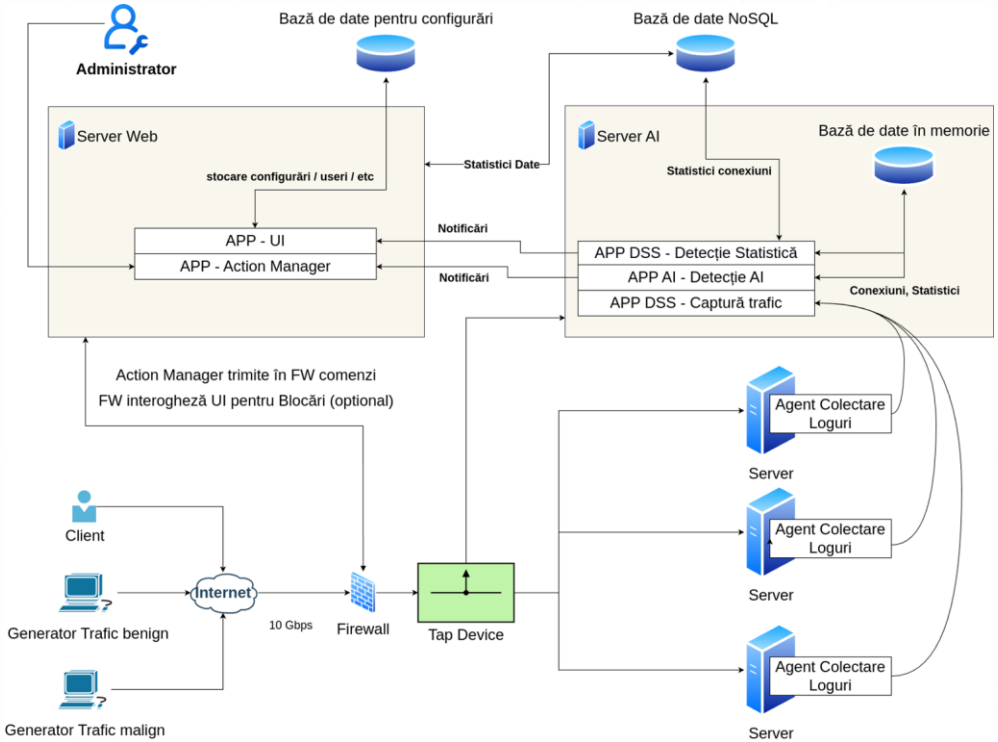
DeDDoS ~30-40s



# Arhitectura DeDDoS

# Arhitectură

- server AI + DB
- firewall
- hardware tap
- agenți L7
- ATLAS polygon
  10G DDoS traffic



# Componenta Hardware

**Server AI** Supermicro 5126GS-TNRT2

- **GPU** 2 x NVIDIA H200 141GB
- **CPU** 2 x AMD EPYC 9655 C96 T192
- **Conectivitate:** Supermicro AOC-STG-I4S Intel XL710-BM1 chipset 4-ports SFP+; Supermicro AOC-STGF-I2S Intel XC710 Chipset – 2-port SFP+
- **HDD** 8x7.68TB NVMe Gen 4
- **RAM** 1536.GB DDR5 RDIMM

**Trafic** TAP 10Gbps DataCOM TS-1404

- 2x 1G/10G LC Taps
- 2x 1G/10G Monitor Ports
- 1x 1G port de management; 1x port consolă

**Server Web** Supermicro 2025HS-TNRT

- **CPU** 2 x AMD EPYC9655 C96 T192
- **Conectivitate** Supermicro AOC-STG-I4S Intel XL710-BM1 chipset 4-ports SFP+; Supermicro AOC-STGF-I2S Intel XC710
- **HDD** HDD: 12x 7.68TB NVMe Gen 4
- **RAM** 1536.GB DDR5 RDIMM

**Firewall** Fortigate 201g

- FG-201G-BDL-950 (60)
- FortiGate-201G Hardware FortiCare Premium
- FortiGuard Unified Threat Protection (UTP)
- cu switch Mikrotik CRS309-1G-8S+; 8x 1/10G SFP+

# Componenta Software

**Server AI**

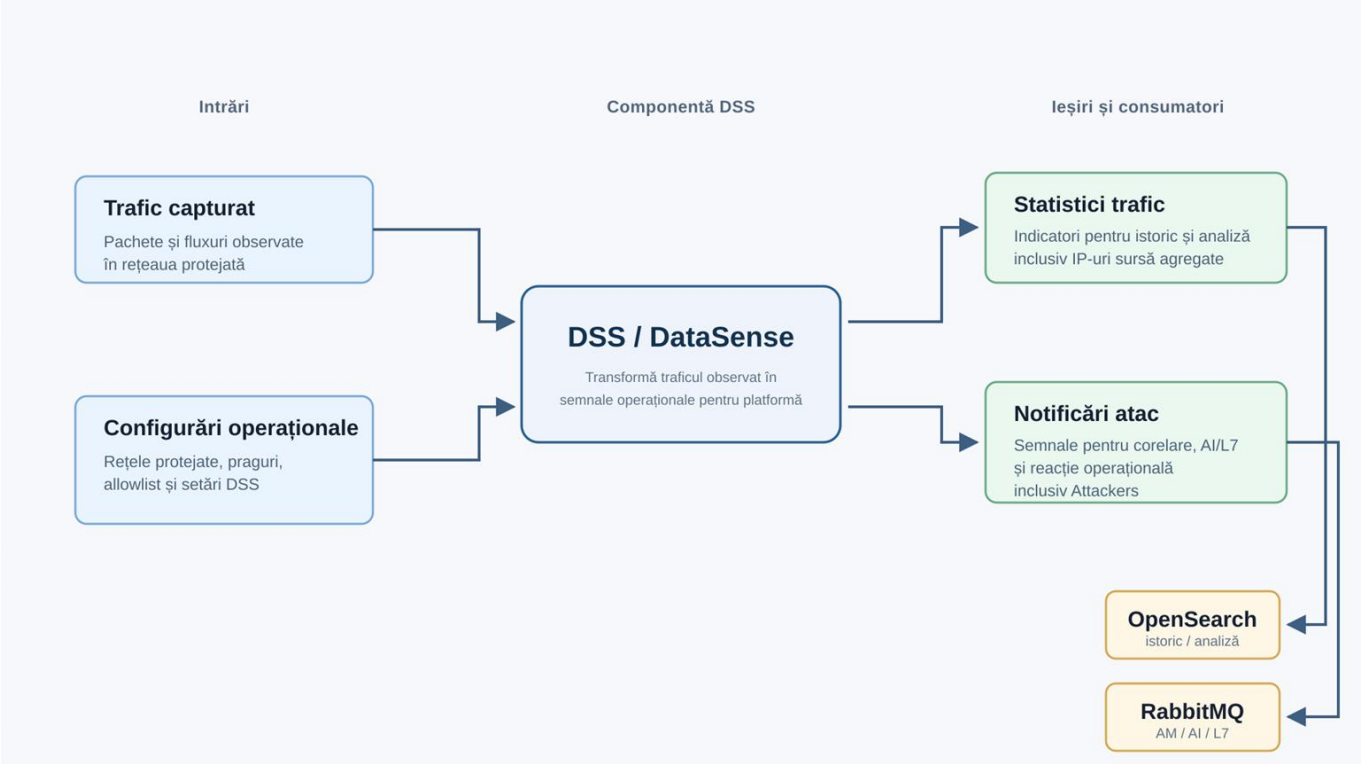
- Captură: Data Sense
- Stocare: baza de date în memorie
- Detecție: reguli statice
- Detecție: alogritmi AI

**Server Web și DB**

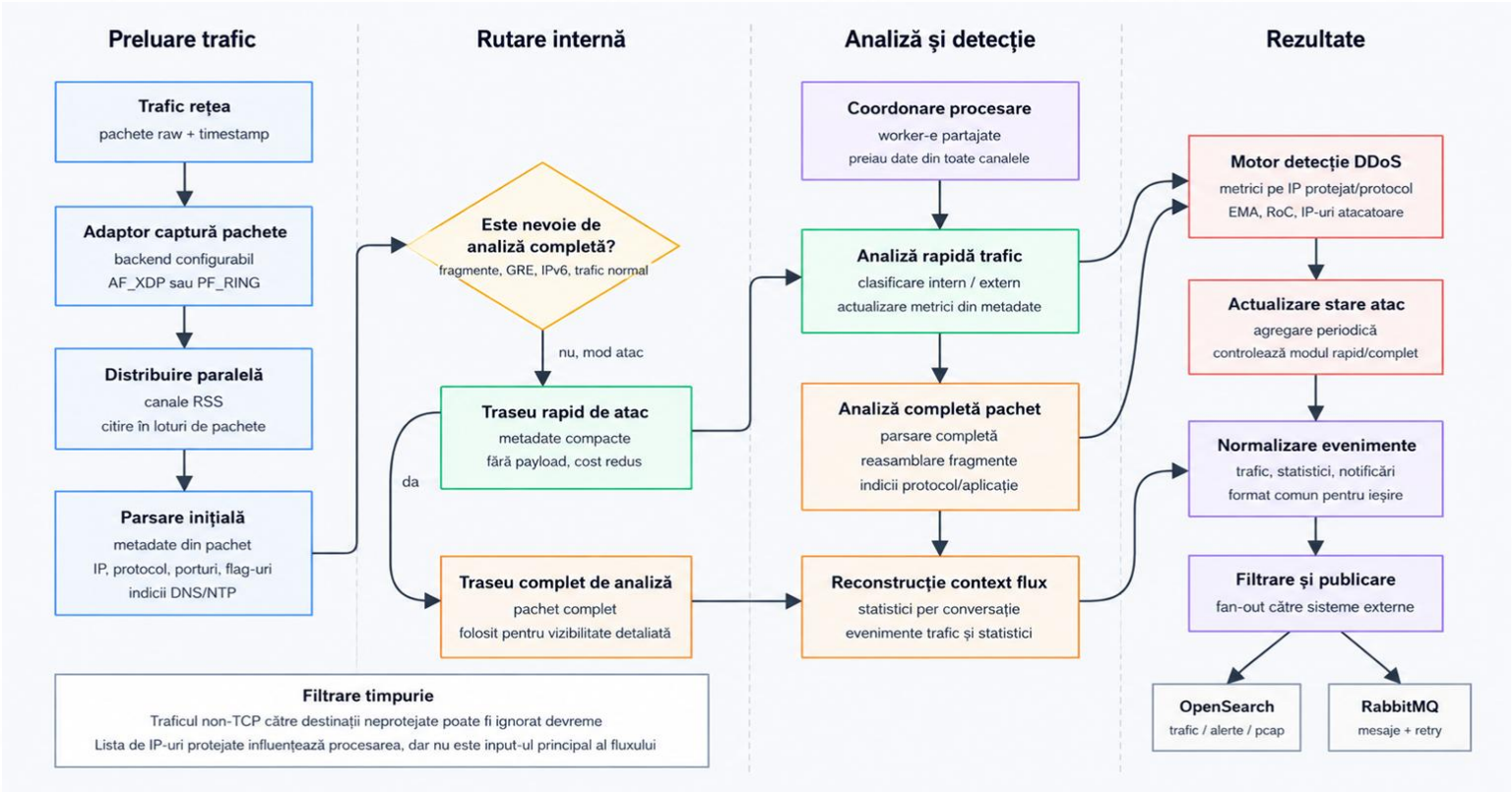
- Stocare: baza de date pe disk
- Interfață: platforma web
- Interfață: vizualizare notificări
- Interfață: vizualizare atacuri
- Interfață: administrare
- Mitigare: Action Manager

# Captură trafic

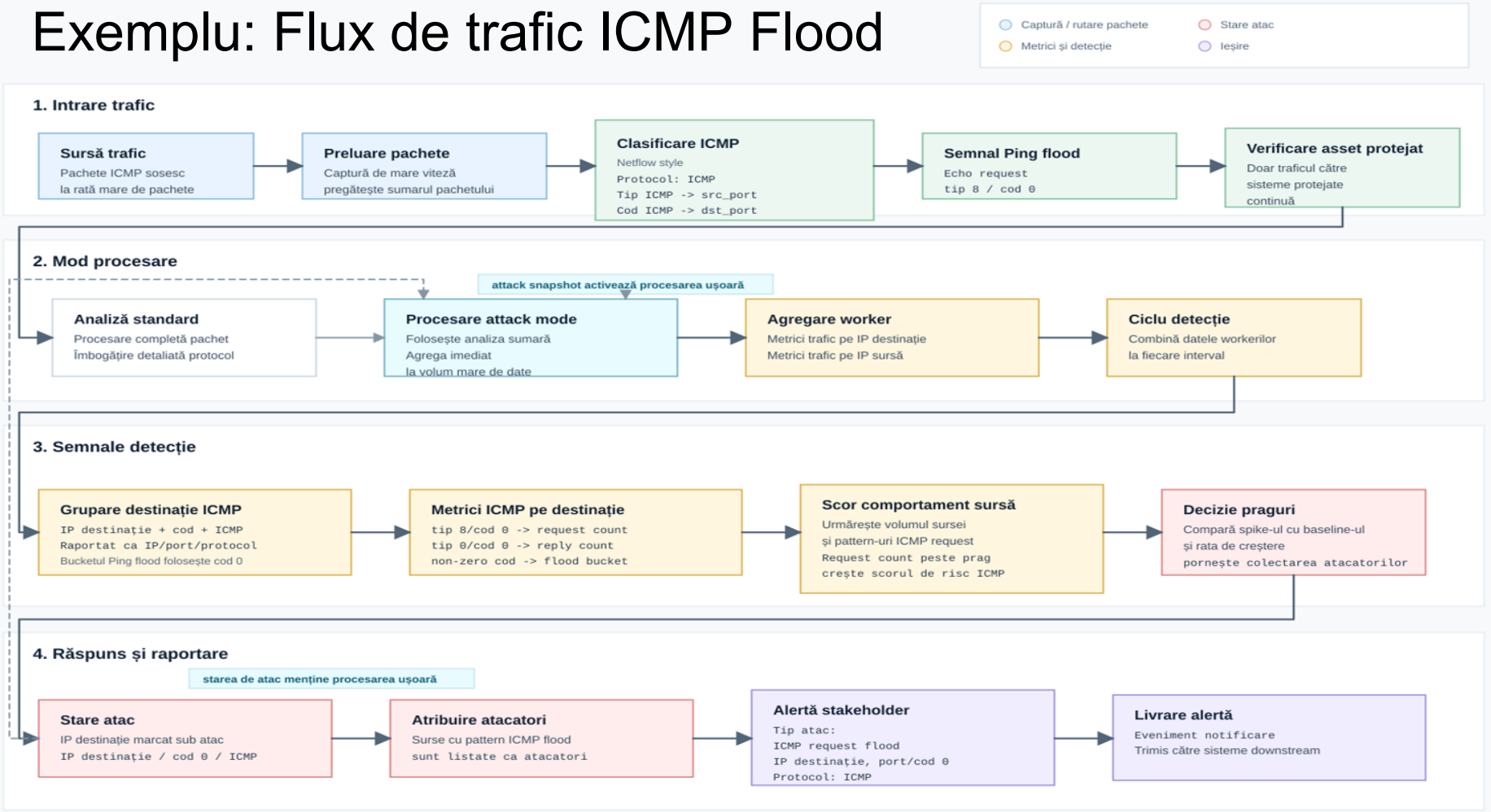
# Arhitectura DSS - High Level



# Arhitectura DSS - flux intern



# Exemplu: Flux de trafic ICMP Flood

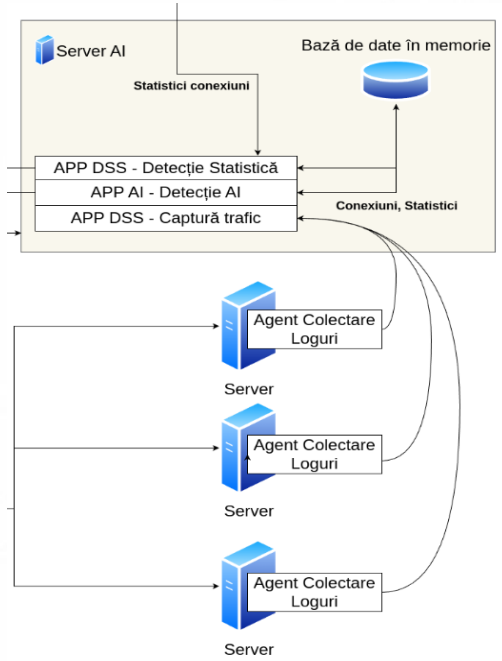


# APP DSS - Captura trafic

- Fluxul începe când traficul din reteaua protejata este observat în punctul de captura.
- Transforma traficul brut în indicatori operationali despre fluxuri, surse, destinatii si servicii vizate.
- Trimite indicatorii suspecți către componentele de detecție și reacție pentru analiza ulterioară.
- Operatorii obțin vizibilitate rapidă asupra traficului real, fără investigare manuala continua.
- Rezultatul principal: baza comuna de observare pentru detecție, corelare flow-uri și mitigare.

# Agenți pentru colectare informații la nivel de aplicație

- Cel mai adesea traficul TCP/IP este criptat.
- Informațiile specifice despre protocol sunt greu de obținut din traficul de IP.
- Informațiile pot fi colectate la nivel de aplicație din loguri iar apoi uniformizate pentru a fi analizate de sisteme specifice.



# Colectarea informațiilor privind activitatea serverelor de web

- serverele de web scriu informații despre activitate în jurnale (de obicei access.log și error.log)
- jurnalele corespunzătoare diverselor servere / versiuni sunt eterogene.
- **fluentd** uniformizeaza datele și le scrie în opensearch (pentru a fi folosite la învățare) și în rabbitmq (pentru a fi folosite la analiză).


```
{
  "remote_addr": "10.102.28.3",
  "logtime": "19/May/2026:13:07:47 +0000",
  "timestamp": "1779196067.283",
  "method": "GET",
  "path": "/sample-page",
  "http_version": "1.1",
  "code": "404",
  "size": "312",
  "referrer": "-",
  "agent": "Go-http-client/1.1",
  "last": "-",
  "type": "access",
  "host_address": "10.110.0.2",
  "host_port": "80"
}
```

# Colectarea informațiilor privind starea generală a sistemului

- Datele privind starea serverelor sunt culese din prometheus (program de monitorizare)
- **fluentd** uniformizeaza datele și le scrie în opensearch (pentru a fi folosite la învățare) și în rabbitmq (pentru a fi folosite la analiză).


```
{
  "machine": "10.110.0.2",
  "timestamp": 1779197495,
  "metrics": {
    "node_intr_total":
      [{"labels": {}, "value": 24938701578}],
    "node_load1":
      [{"labels": {}, "value": 0.99}],
    "node_load5":
      [{"labels": {}, "value": 1.05}],
    "node_load15":
      [{"labels": {}, "value": 0.94}],
    "node_memory_MemAvailable_bytes":
      [{"labels": {}, "value": 6236581888}]
  }
}
```

# Stocarea în baza de date

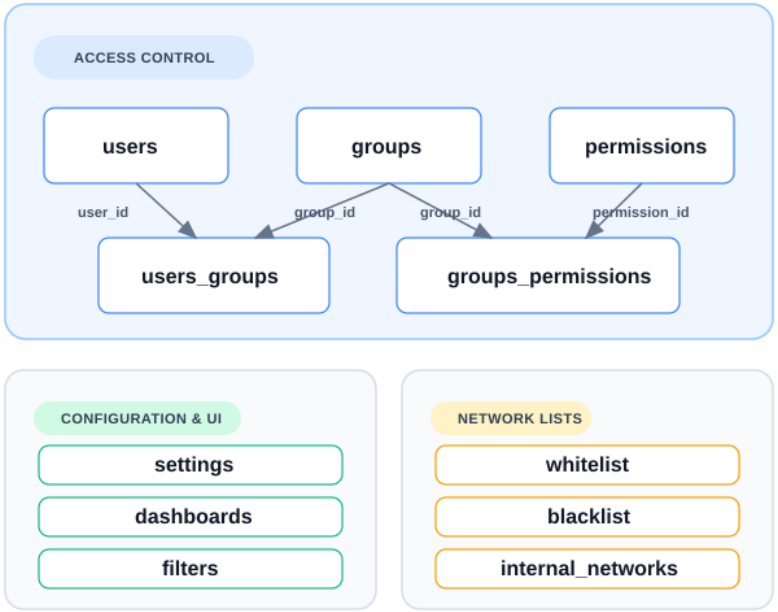
# MariaDB: baza de date pentru configurarea soluției

Pastreaza configurarile care controlează comportamentul operațional al soluției.

Setările fiecărei aplicații sunt gestionate centralizat din Aplicația Web și puse la dispoziția celorlalte aplicații prin API.

Blocklist-ul este punctul de legatura dintre deciziile aplicației Action Manager și lista expusă către firewall.

Valoarea principala: control centralizat asupra regulilor care stabilesc ce se monitorizează, ce se exclude și ce se blochează.



# OpenSearch: stocare operațională

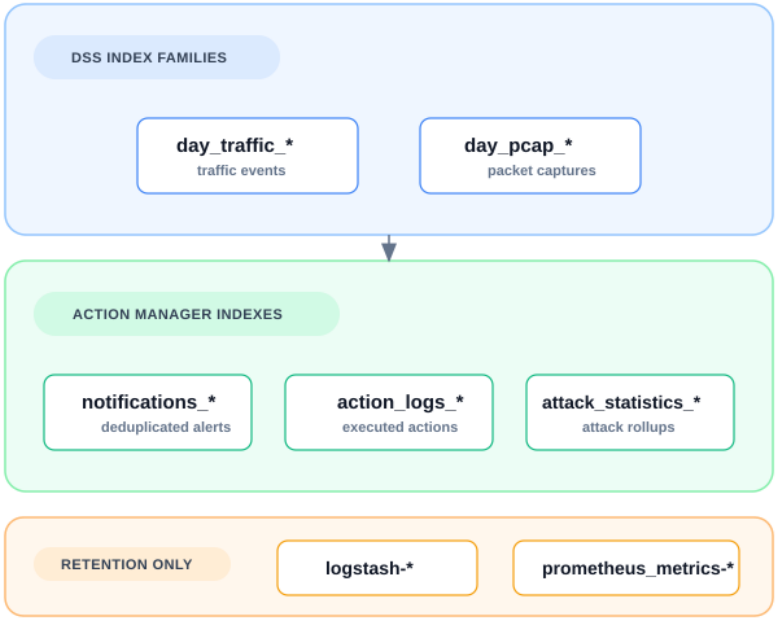
Pastreaza istoricul operațional folosit pentru analiza, reantrenarea modelelor AI și sustinerea generării alertelor.

DSS scrie în OpenSearch datele de trafic și capturile relevante, oferind istoricul operațional necesar pentru analiză, detecție și corelarea evenimentelor de securitate.

Modelele AI folosesc istoricul pentru a compara comportamentul curent cu datele observate anterior.

Action Manager persista notificările, atacurile și  jurnalul acțiunilor pentru trasabilitate post incident.

Valoarea principala: oferă memorie operațională pentru detecție, corelare, audit și îmbunătățirea continua a alertelor.



# Detecție

# Componentă de detecție DDoS cu reguli statice (DSS)

Evaluează traficul observat pentru a recunoaște tipare cunoscute de atac DDoS.

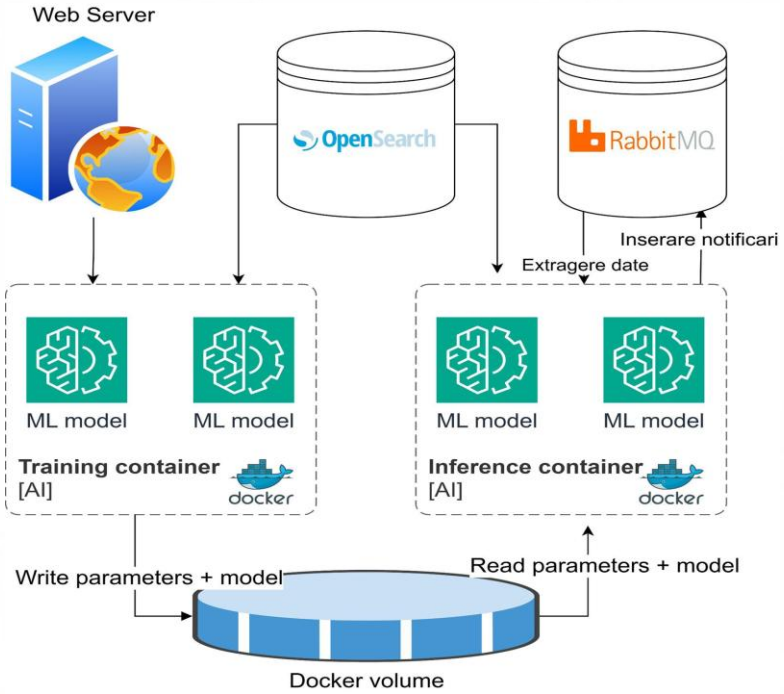
Notifica un incident când traficul către aceeași victimă depășește pragurile configurate, optimizate și se menține peste nivelul normal al ferestrei de monitorizare.

Grupează semnalele după victimă și tip de atac, pentru a evita notificari redundante pentru același incident.

Sursele exceptate explicit sau varfurile scurte de trafic trebuie tratate ca excepții operaționale, nu ca atacuri confirmate.

Rezultatul principal: notificari predictibile, explicabile și utile pentru corelare în Action Manager.

# Arhitectură DDoS bazată pe AI



# Arhitectură DDoS bazată pe AI

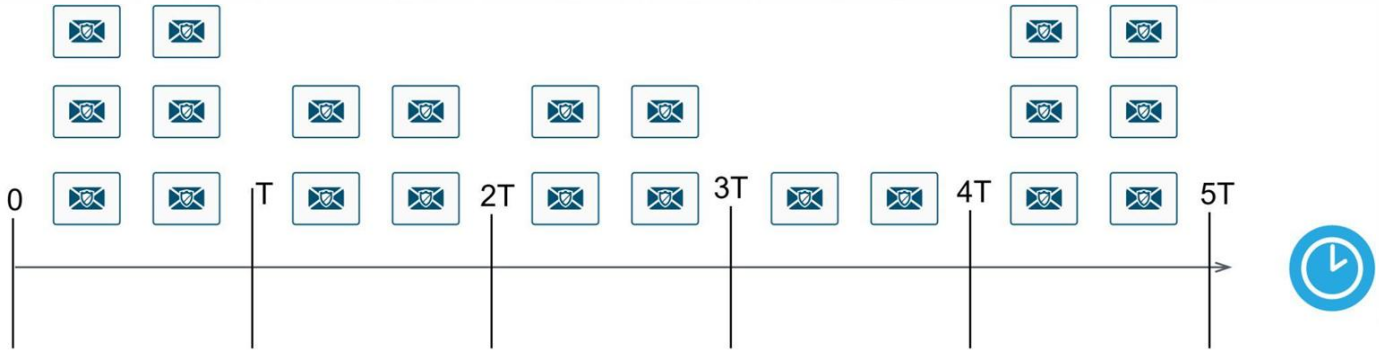
- Containerele de antrenare/inferență extrag datele din OpenSearch folosind query-uri specifice
- Fiecare container de inferență consumă mesaje dintr-o coadă RMQ dedicată
- După ce containerul de antrenare finalizează procesul de antrenare, va scrie într-un volum atât modelul antrenat + parametrii utilizați
- Containerul de inferență verifică dacă fișierele din respectivul volum au fost updatate, iar când acest lucru se întâmplă noul model este încărcat, iar noii parametrii sunt folosiți

# Detecție AI: volumetric și protocol

- Izolarea modelelor de detecție prin containere dedicate
- Există  câte 2 containere (Antrenare + Inferență) pentru fiecare dintre următoarele atacuri:
  - TCP SYN Flood
  - TCP RST Flood
  - TCP ACK Flood
  - ICMP Flood
  - UDP Flood
  - DNS Query Flood/Amplification
  - NTP Amplification
- În acest fel, după ce are loc prima antrenare, inferența nu va mai fi întreruptă
- Fiecare container procesează doar datele corespunzătoare tipului de atac pe care trebuie să îl detecteze

# Detecție AI: Preprocesarea datelor

- Agregarea flow-urilor în cadrul unor ferestre de timp de lungime configurabila
  - La antrenare sunt extrase din OpenSearch cu query-uri specifice (denumite Aggregations)
  - La inferență aceste agregări sunt construite manual cu ajutorul flow-urilor din RMQ
    - Ordinea flow-urilor ce sosesc din RMQ nu e neaparat cea corespunzătoare timpului de start al acestora
    - Permiterea unei perioade de întârziere



# Detecție AI: Preprocesarea datelor

- Agregarea va presupune
  - Sumarea următoarelor caracteristici ale flow-urilor din fiecare fereastră:
    - Numărul total de pachete pentru ambele direcții (Fwd / Bwd)
    - Lungimea totală a pachetelor (pentru ambele direcții)
    - Numărul de flag-uri SYN
    - Numărul de flaguri RST
    - Numărul de flaguri ACK
  - Medierea următoarelor caracteristici:
    - Media lungimii pachetelor din cadrul flow-urilor (pentru ambele direcții)
  - Alte caracteristici utile pentru detecția atacurilor DDoS:
    - Numărul de IP-uri sursă ce apar în cadrul ferestrei de timp
    - Entropia IP-urilor sursă

# Detecția atacurilor DDoS la nivelul ferestrelor de timp

- Rezultatele agregărilor sunt folosite de 2 modele distincte (pentru fiecare tip de atac)
- Primul model va avea o perspectiva globală (va fi antrenat cu valorile corespunzătoare tuturor agregărilor din perioada de antrenare)
  - Va detecta anomaliile globale
  - Isolation Forest/LSTM Autoencoder
- Cel de-al doilea va detecta spike-urile din seriile de timp rezultate în urma agregărilor (pentru anumite caracteristici) pentru ultimele X ferestre de timp
  - Robust Z-Score

# Detecția IP-urilor ilegitime din cadrul unei ferestre de timp

- Folosirea unor agregări realizate la nivelul ferestrelor de timp + IP-urilor sursă
  - Antrenarea unor modele de detecție de anomalii cu aceste agregări (construite cu datele din OpenSearch)
  - Evaluare agregărilor construite cu datele din RMQ și sortarea scorurilor de anomalie
- Calcularea contribuției fiecărui IP sursă din fereastră la anumite caracteristici și sortarea (în ordine descrescătoare)
- Aplicarea unor praguri (atât pentru scorul de anomalie, cât și pentru contribuția la caracteristica specifică)
- Intersecția celor 2 liste rezultate și trimiterea notificărilor în RMQ

# Detecție AI: Arhitectură și detecție Layer 7

- **L7 volume detector**
  - Datele istorice pentru comportamentul normal, numărul de conexiuni pentru fiecărui server web
  - Activitate peste așteptări conduce la identificarea IP-urile care fac cele mai multe cereri, alerte
- **L7 oversized header detector**
  - Serverele de web jurnalizează atacuri de tip continuation (prin intrări de tip ‘oversized header’)
  - Activitate peste așteptări, într-o perioadă fixă de timp, conduce la identificarea IP-urilor, alerte
- **L7 compute detector**
  - Se învață o corelație între cererile adresate și încărcarea produsă serverului web
  - Se învață comportamentul normal al serverului (încărcarea așteptată)
  - Activitate peste așteptări, sunt determinate IP-urile sursă care par să cauzeze cea mai mare încărcare și se ridică o alertă pentru acestea.

# Arhitectură și detecție a atacurilor slow din date de Layer 3

- Atacurile Slow L7 nu **pot fi detectate doar din jurnale**
  - cererile pot să nu fie finalizate niciodată, iar în jurnale nu apar intrări corespunzătoare
- **Soluție**: este necesară detecția la nivel de conexiune IP
- **Dificultate**: datele de nivel 3 sunt criptate la nivelul dispozitivului TAP
- Modelul învață raportului de conexiuni stabilite versus conexiuni închise într-o fereastra de timp de lungime suficientă, în condiții normale
- Activitate peste așteptări, dacă **procentul de conexiuni deschise este disproporționat de mare versus predicția modelului** atunci sunt determinate IP-urile sursă și sunt generate alerte

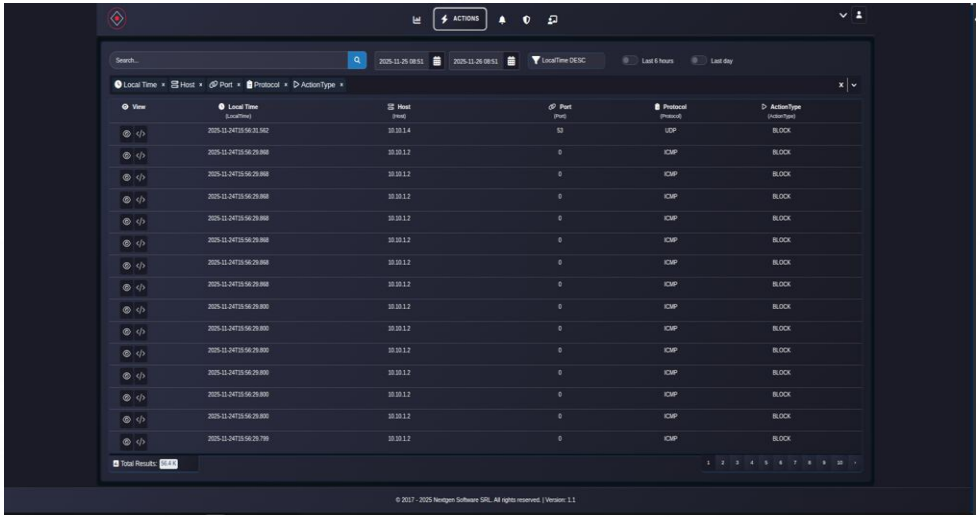
# Interfața cu utilizatorul

# Componenta de interfață cu utilizatorul

- Interfața susține atat monitorizarea în timp real, cat si investigarea post incident
- Operatorul urmărește dashboard-uri, filtrează evenimente și consulta detalii despre incidente
- Valoarea principala: reduce timpul de investigare și standardizează modul de operare

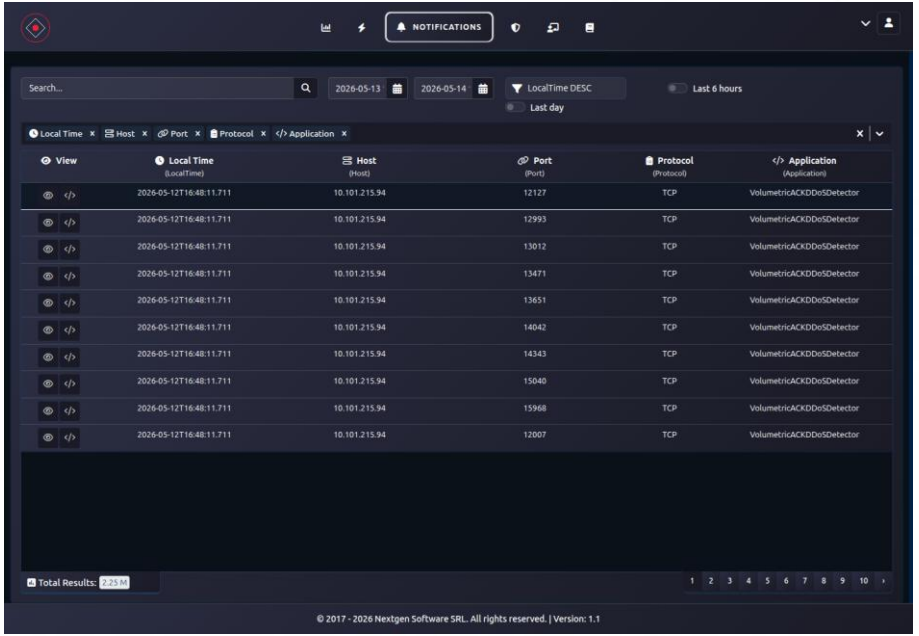
# ACTIONS: jurnalul acțiunilor Action Manager

- Prezinta actiunile executate de Action Manager ca raspuns la atacurile detectate
- Fiecare înregistrare arată cand a avut loc acțiunea, hostul afectat, protocolul, tipul acțiuni o referință către notificare care a generat acțiunea
- Filtrarea, detaliile și exportul acțiuni susțin analiza post incident și auditul acțiunilor efectuate
- Valoarea principala: trasabilitate între alertă, decizie și măsura aplicată în firewall



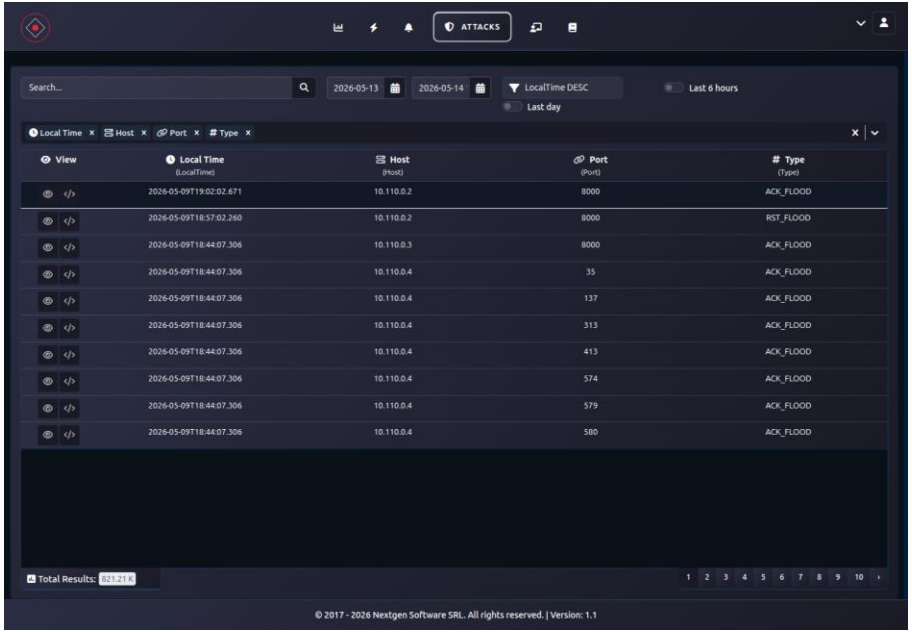
# Modulul de vizualizare a notificărilor (NOTIFICATIONS)

- Centralizează alertele raportate de componentele de detecție
- Operatorul vede cine a generat alertă, ce aplicație sau host este vizat și cand a aparut
- Valoarea principala: vizibilitate rapidă asupra riscurilor detectate în timp real



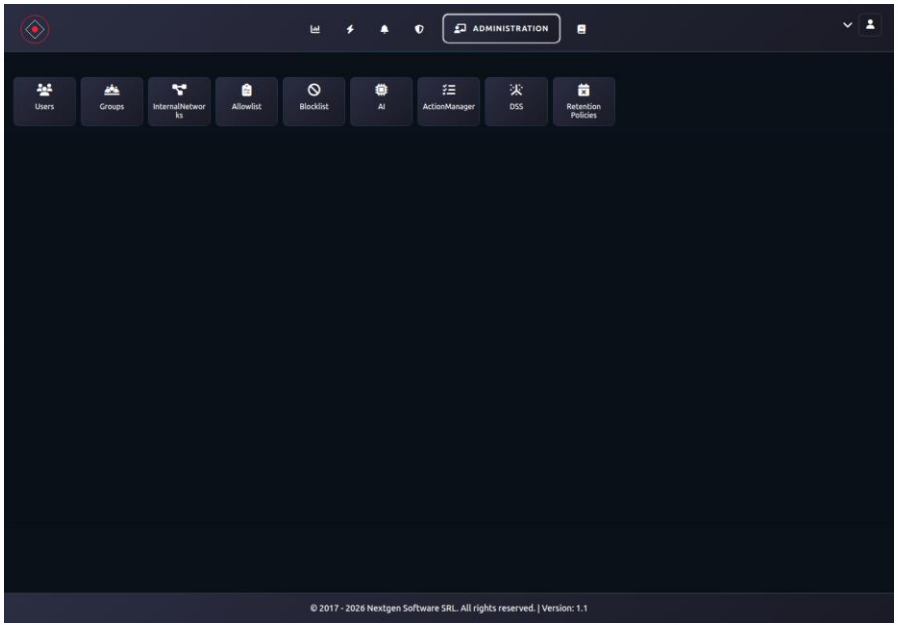
# Modulul de vizualizare a Atacurilor (ATTACKS)

- Prezinta atacurile DDoS validate si agregate de platforma
- Un atac este afișat după ce Action Manager validează notificarea, o deduplica și actualizează statistica de atac
- Operatorul poate urmări victimă, momentul apariției și tipul atacului
- Fluxul de lucru susține investigarea prin filtrare, sortare, vizualizare detalii și export
- Valoarea principala: prezentare de ansamblu asupra întregului flux al atacului, nu doar asupra alertelor individuale

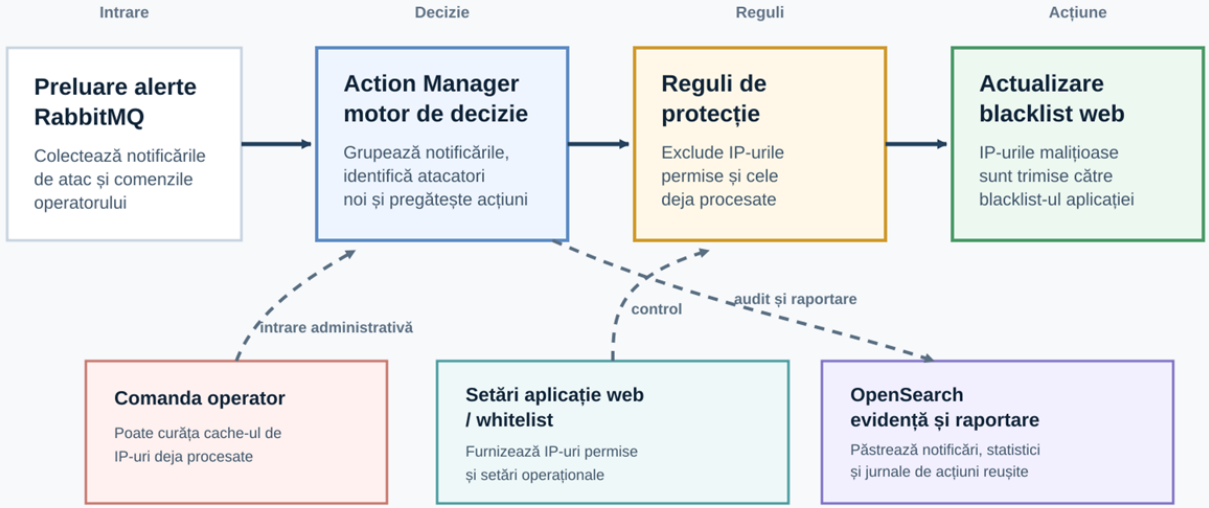


# Modulul de administrare a soluției (ADMINISTRATION)

- Este zona de configurare controlată a platformei
- Administratorii autorizați gestionează utilizatori, grupuri, rețele blocklist și allowlist
- Regula de business principala: ip-urile din allowlist nu sunt blocate
- Valoarea principala: guvernanta, control și adaptabilitate fără intervenții tehnice directe



# Action Manager: legătura dintre detecție și blocare



# Testare și validare: Poligonul ATLAS

# Componente pentru testare și simulare atacuri DDoS

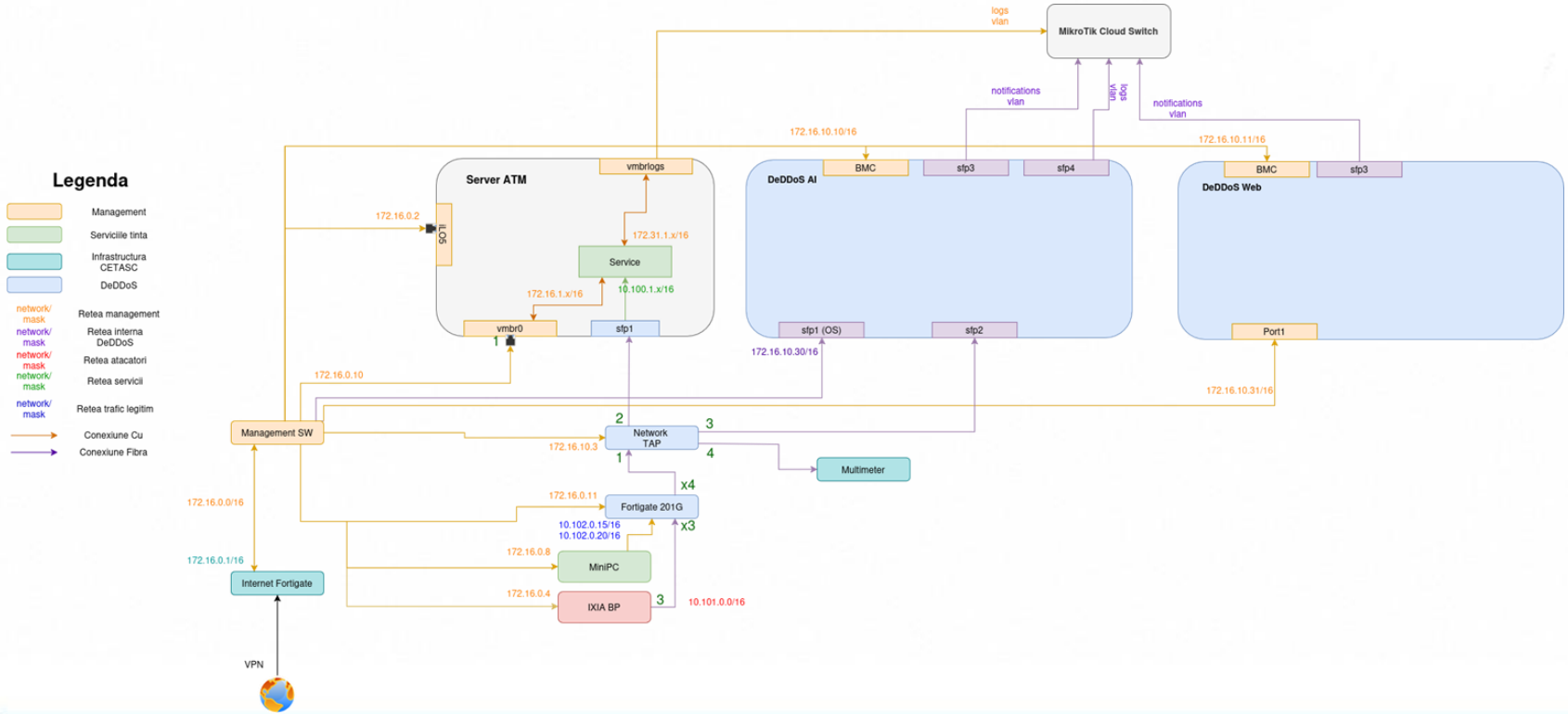
Testarea este realizata prin intermediul a doua echipamente:

- Mini PC - dispozitivul care se ocupă de generarea traficului legitim
- IXIA Perfect Storm One - dispozitivul care se ocupă de generarea traficului malițios

Echipamentele menționate sunt conectate la nivel fizic în echipamentul Fortigate 201G și stimulează rețeaua WAN (clienții serviciilor expuse).

În plus multimetrul este conectat la o interfata destinata analizoarelor de trafic a tap-ului cu scopul de a valida volumul de trafic generat.

# Componente pentru testare și simulare atacuri DDoS (2)

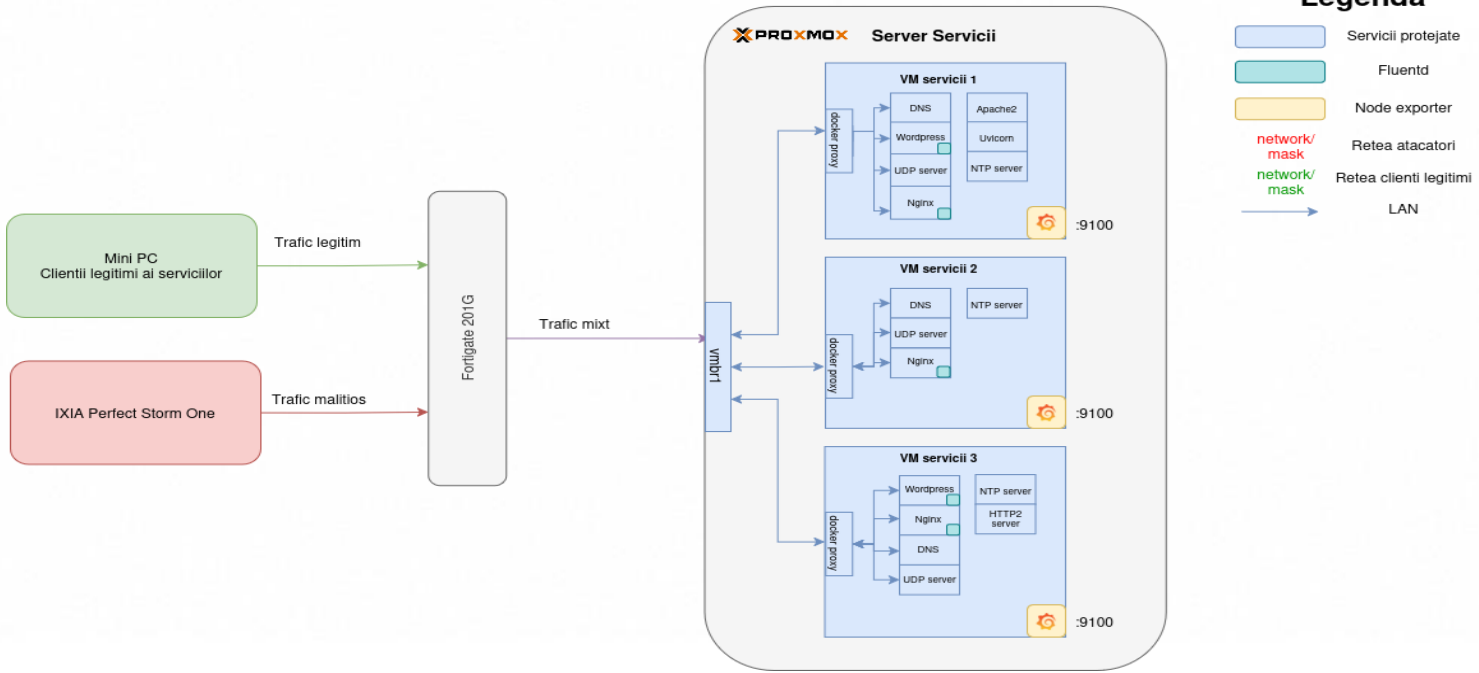


# Matricea de atacuri

| Tip | Atac | DSS | AI |
|---|---|---|---|
| **Volumetric: Flood** | ICMP Flood | ✓ | ✓ |
| | UDP Flood | ✓ | ✓ |
| | UDP Frag | ✓ | ✓ |
| | IPSec Flood | ✓ | X |
| | ICMP Frag | ✓ | ✓ |
| **Volumetric: Amplificare** | DNS Amplification | ✓ | ✓ |
| | NTP Amplification | ✓ | ✓ |
| | Smurf Attack | ✓ | ✓ |
| | Fraggle Attack | X | ✓ |

| | | | |
|---|---|---|---|
| **Protocol** | SYN Flood | ✓ | ✓ |
| | ACK Flood | ✓ | ✓ |
| | SYN ACK Flood | ✓ | X |
| | RST Flood | ✓ | ✓ |
| | Ping of Death | ✓ | X |
| | BGP | ✓ | X |
| **Aplicație** | DNS Query Flood | ✓ | ✓ |
| | R-U-Dead-Yet (RUDY) | X | ✓ |
| | Slowloris | X | ✓ |
| | HTTP Flood | X | ✓ |
| | HTTP/2 Continuation Flood | X | ✓ |

# Zoom L7 (pentru ATLAS)



# Generarea traficului legitim

Traficul legitim a fost generat folosind un mini PC ce contine următoarele teste:

- Transmitere cereri DNS legitime către serviciile țintă
- Transmitere cereri HTTP
- Transmitere mesaje ICMP Echo Request
- Transmitere cereri NTP
- Testarea aplicațiilor HTTP care conțin endpoint-uri solicitante
- Transmitere de mesaje HTTP versiunea 2
- Transmiterea de pachete UDP cu date aleatoare

Platforma care orchestreaza rularea acestor teste este *Forcad* și folosește *Celery* pentru a coordona workerii. Sunt utilizate 2 adrese IP: 10.102.0.15, 10.102.0.20

Am generat trafic legitim și folosind adrese IP sursă randomizate.

# Crawler log-uri HTTP

Python crawler care generează load pe un container de Wordpress, pentru a simula traficul unor utilizatori normali.

Logurile ajung în OpenSearch, de unde sunt consumate.

| Status Code | Action |
|---|---|
| 200 | Citește postare<br>Vizualizează pagina<br>Vizualizează categorie<br>Caută pe blog<br>Vizualizează feed-ul<br>Posteaza un comentariu |
| 400 | Accesează pagina de admin |
| 401 | Încearcă să publice o postare |
| 404 | Caută o categorie inexistenta |
| 405 | Folosește ruta greșită când încearcă să comenteze |

# Generarea traficului malițios

Traficul malițios a fost generat preponderent prin intermediul echipamentului IXIA Perfect Storm One în care au fost realizate teste pentru fiecare scenariu de atac.

În total au fost implementate un număr de 45 de teste:

- 18 cu viteze de 10G
- 20 cu viteze cu 1G
- 2 pentru Slow Loris și RUDY.
- 2 în care au fost variați diferiți parametri precum bandwidth, număr de conexiuni simultan, variația numărului de pachete în funcție de timp (eg. Oscilatoriu)
- 3 pentru generare de trafic legitim la viteze mari

# Generarea traficului malițios (2)

Fiecare tip de atac a fost implementat separat pentru rețeaua de 1G și pentru rețeaua de 10G întrucât este necesară definirea arhitecturii de rețea pe care o folosește testul.

De asemenea, am implementat teste care conțin mix de trafic din mai multe tipuri de atacuri.

Traficul malițios a fost generat dintr-o rețea separată care ulterior, după trecerea acestuia de firewall, era imbricat cu traficul legitim.

# Generarea traficului malițios (3)

| Name | Test Type | Interfaces | Created By | Last Run By | Pass/Fail | Bandwidth (Mbps) | Created | Last Changed |
|---|---|---|---|---|---|---|---|---|
| Solutii8_10G_Armageddon | | 1 | admin | admin | failed | 10000 | Sun Mar 29 2026 1... | Tue May 19 2026 2... |
| Solutii8_10G_DNSAmplification | | 1 | admin | admin | passed | 10000 | Mon Mar 31 2025 0... | Tue May 19 2026 2... |
| Solutii8_10G_DNSFlood | | 1 | admin | admin | passed | 10000 | Mon Mar 31 2025 0... | Mon Feb 16 2026 2... |
| Solutii8_10G_HTTPGetFlood_CS | | 1 | admin | admin | canceled | 10000 | Mon Mar 31 2025 0... | Mon Apr 06 2026 2... |
| Solutii8_10G_HTTPGetFlood_SS | | 1 | admin | | | 10000 | Mon Mar 31 2025 0... | Mon Mar 31 2025 0... |
| Solutii8_10G_HTTPPostFlood_CS | | 1 | admin | admin | canceled | 10000 | Mon Mar 31 2025 1... | Mon Mar 31 2025 1... |
| Solutii8_10G_HTTPPostFlood_SS | | 1 | admin | | | 10000 | Mon Mar 31 2025 0... | Mon Mar 31 2025 0... |
| Solutii8_10G_ICMPFlood | | 1 | admin | admin | passed | 11000 | Mon Mar 31 2025 0... | Mon May 18 2026 ... |
| Solutii8_10G_ICMPFragmentation | | 1 | admin | admin | passed | 10000 | Wed Feb 18 2026 ... | Fri Mar 27 2026 01... |
| Solutii8_10G_ICMPReplyFlood | | 1 | admin | admin | passed | 10000 | Mon Mar 31 2025 0... | Thu May 07 2026 2... |
| Solutii8_10G_NTPAmplification | | 1 | admin | admin | canceled | 10000 | Wed May 06 2026 ... | Wed May 06 2026 ... |
| Solutii8_10G_StressTest | | 1 | admin | admin | canceled | 10000 | Sun Jul 20 2025 18... | Sun Mar 15 2026 2... |
| Solutii8_10G_StressTestICMP | | 1 | admin | admin | passed | 10000 | Sun Jul 27 2025 17... | Sun Jul 27 2025 17... |
| Solutii8_10G_TCPACKFlood | | 1 | admin | admin | canceled | 10000 | Thu Apr 23 2026 2... | Tue May 19 2026 0... |
| Solutii8_10G_TCPRSTFlood | | 1 | admin | admin | passed | 10000 | Mon Mar 31 2025 0... | Mon May 18 2026 ... |
| Solutii8_10G_TCPSYNACKFlood | | 1 | admin | admin | canceled | 10000 | Thu Apr 23 2026 2... | Fri Apr 24 2026 05:... |
| Solutii8_10G_TCPSYNFlood | | 1 | admin | admin | passed | 10000 | Mon Mar 31 2025 0... | Sun Apr 26 2026 2... |
| Solutii8_10G_UDPFlood | | 1 | admin | admin | passed | 10000 | Mon Mar 31 2025 0... | Sun May 17 2026 2... |

# Generarea traficului malițios (3)

| Name | Test Type | Interfaces | Created By | Last Run By | Pass/Fail | Bandwidth (Mbps) | Created | Last Changed |
|---|---|---|---|---|---|---|---|---|
| Solutii8_1G_Armageddon | | 1 | admin | admin | canceled | 1000 | Sun Sep 07 2025 03:... | Thu Mar 26 2026 00:... |
| Solutii8_1G_DNSAmplification | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 01:... | Tue Dec 16 2025 17:... |
| Solutii8_1G_DNSFlood | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 02:... | Sun May 17 2026 22:... |
| Solutii8_1G_HTTPGetFlood_CS | | 1 | admin | admin | canceled | 2000 | Mon Mar 31 2025 02:... | Thu Sep 25 2025 20:... |
| Solutii8_1G_HTTPGetFlood_SS | | 1 | admin | admin | canceled | 1000 | Mon Mar 31 2025 02:... | Wed May 06 2026 03... |
| Solutii8_1G_HTTPPostFlood_CS | | 1 | admin | admin | failed | 1000 | Mon Mar 31 2025 16:... | Mon Mar 31 2025 16:... |
| Solutii8_1G_HTTPPostFlood_SS | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 02:... | Mon Mar 31 2025 02:... |
| Solutii8_1G_ICMPFlood | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 00:... | Sat Jan 24 2026 04:3... |
| Solutii8_1G_ICMPFlood_Mixed | | 1 | admin | admin | canceled | 1095 | Mon Mar 31 2025 20:... | Thu Apr 03 2025 16:... |
| Solutii8_1G_ICMPFragmentation | | 1 | admin | admin | passed | 10000 | Thu Jun 05 2025 22:... | Wed Apr 08 2026 23:... |
| Solutii8_1G_ICMPReplyFlood | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 00:... | Tue Nov 11 2025 22:... |
| Solutii8_1G_NTPAmplification | | 1 | admin | admin | passed | 1000 | Sat Jun 07 2025 03:5... | Tue May 19 2026 01:... |
| Solutii8_1G_TCPRSTFlood | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 02:... | Thu Jul 31 2025 18:0... |
| Solutii8_1G_TCPSYNFlood | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 00:... | Mon Dec 08 2025 21:... |
| Solutii8_1G_TCPSYNFlood_Mixed | | 1 | admin | admin | canceled | 995 | Tue Apr 01 2025 22:... | Sun Apr 06 2025 23:... |
| Solutii8_1G_TCPSYNFlood_Ramp | | 1 | admin | admin | canceled | 1000 | Mon May 19 2025 03... | Mon May 19 2025 04... |
| Solutii8_1G_TCPSYNFlood_Sine | | 1 | admin | admin | canceled | 1000 | Mon May 19 2025 03... | Mon May 19 2025 04... |
| Solutii8_1G_TCPSYNFlood_SS | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 01:... | Mon Mar 31 2025 17:... |
| Solutii8_1G_UDPFlood | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 01:... | Mon May 11 2026 22... |
| Solutii8_1G_UDPFragmentation | | 1 | admin | admin | passed | 1000 | Mon Mar 31 2025 01:... | Sun Nov 09 2025 21:... |

# Concluzii

# Limitări și dificultăți

- dificultatea definirii conceptului de **trafic normal**
- capacitatea modelelor AI de a **generaliza** la tipuri de atacuri noi
- **separarea** corectă între trafic cu volum ridicat și un atac DDoS deliberat
- **identificarea** atacatorilor în cazul multor atacatori care mimează utilizarea normală
- **dificultatea** de interpreta traficului criptat asociat serverelor de WEB, capturat de TAP
- **eterogenitatea** formatului jurnalelor de layer 7, funcție de software-ul folosit și configurarea acestuia
- **sensibilitatea modelelor**, controlul numărului de False Positives generat
- calitatea detecției depinde semnificativ de **hiper-parametrii modelului**

# Limitări și dificultăți: continuare

- **stabilitatea și robustețea soluției** pentru funcționarea corectă continuă inclusiv în timpul unui atac DDoS
- **dificultatea detectării** de atacuri DDoS **generate/potențate de către AI**
- **dificultatea generării traficului legitim** din surse multiple simultan și din range-ul atacatorilor
- **simularea atacurilor** cu **distribuție uniforma a adreselor IP sursa** pentru a imita comportamentul rețelelor **botnet**
- restricții impuse la nivelul echipamentelor firewall privind dimensiunea maximă a listelor de blocare a adreselor IP
- limitările soluțiilor actuale în tratarea mecanismelor de captură a traficului pe platforme de procesare cu peste 150 de core-uri

# Direcții viitoare

- metode/modele **adaptive**, **robuste** la parametrii modelelor
- **detecție** cu date compuse din trafic L3, jurnale L7, și statistici încărcare sistem
- **mitigarea complexă** cu AI: măsuri proactive, reguli complexe și adaptive de apărare
- **analiza jurnalelor** și detectarea anomaliilor folosind modele de limbaj
- metode cu **factor uman în proces,** care solicită instrucțiuni sau alte informații de la operatori, dacă este nevoie
- simulare atacuri în care **adresele IP sursa variază pe masura ce atacul avansează**
- **unificarea rețelei de atacatori cu cea de utilizatori legitimi** și folosirea de **adrese IP publice**
- Explainable AI (**XAI**): rezultate interpretabile

# DEMO

# Întrebări?