DDP
S

DeiC - DDoS Protection Service

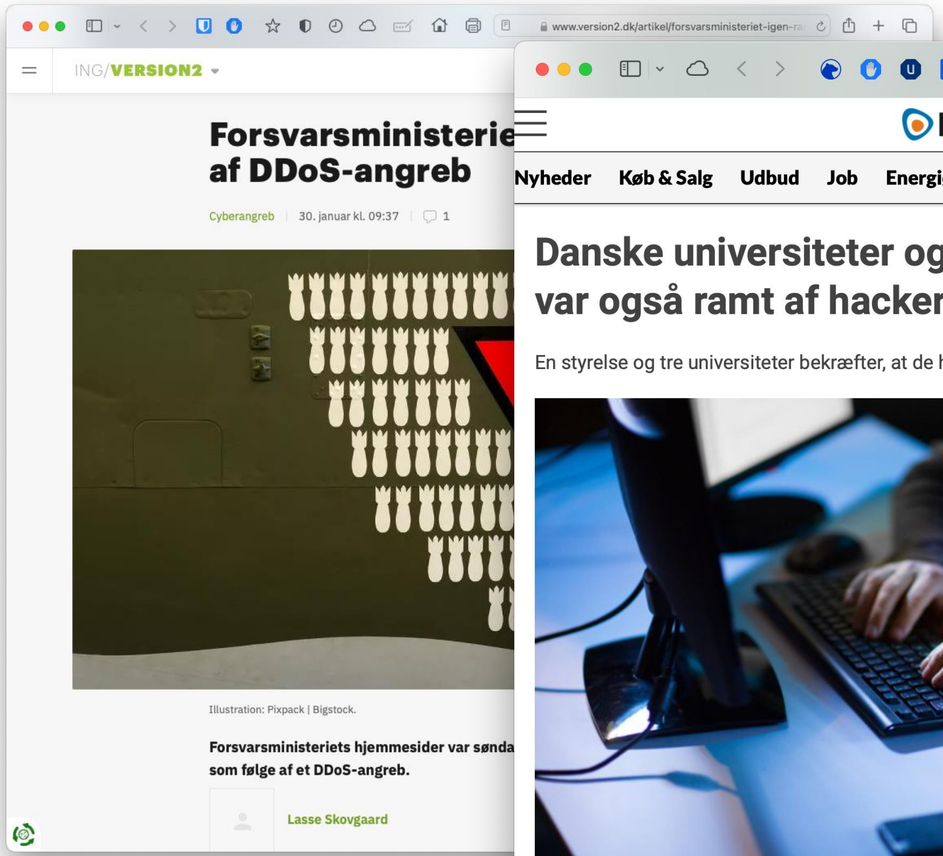
> Om DeiC

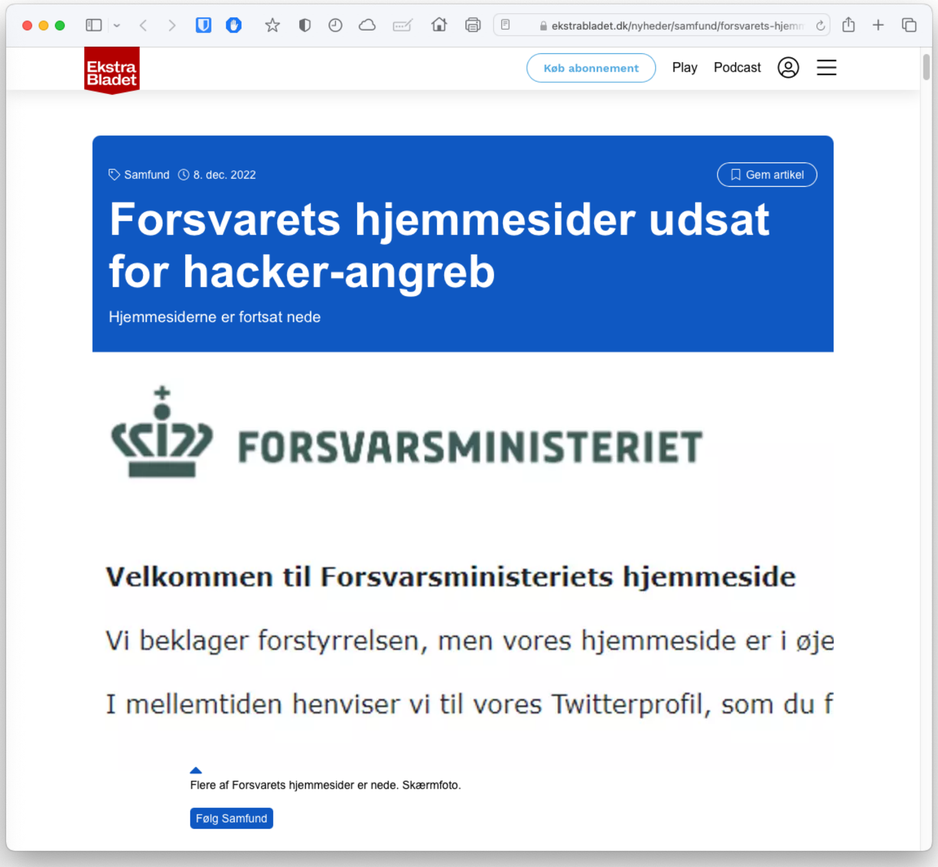
- DeiC coordinates the Danish digital infrastructure as an umbrella for the eight Danish universities to ensure delivery of computing, storage and network infrastructure to Danish research, teaching and innovation
- See https://www.deic.dk

Beskyttelse mod truslen fra cyberaktivister

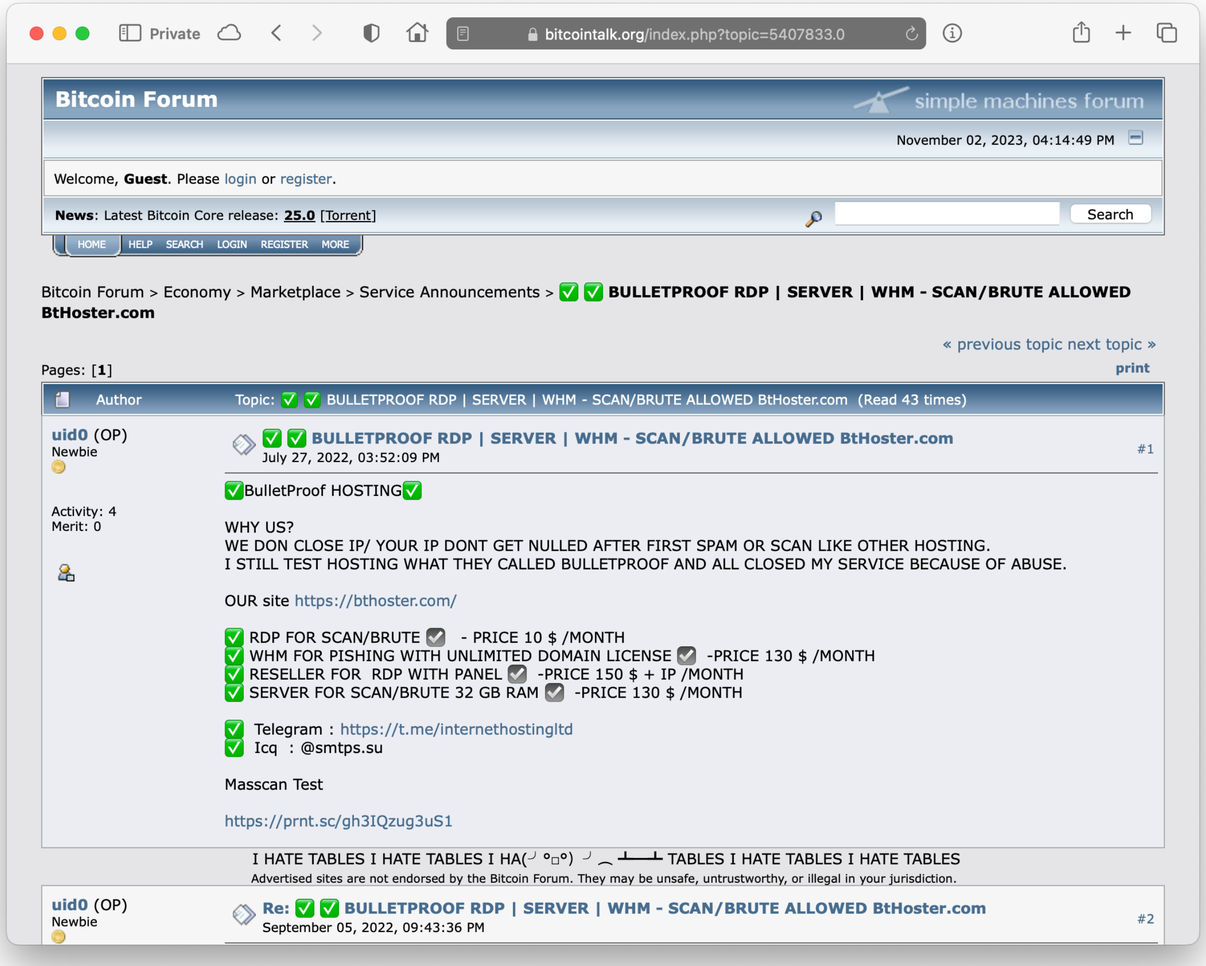
Danske universiteter kom i vinteren 2023 i cyberaktivisternes søgelys uden nogen synlig grund. Truslen fra cyberaktivister er kommet for at blive, men hvad kan man gøre for at undgå at blive et offer for aktivisternes forsøg på at gøre skade og få opmærksomhed? Med udgangspunkt i de konkrete og mere vellykkede angreb på danske ministeriers hjemmesider i første halvår 2023 gennemgås hvordan ***DeiCs DDoS Protection service****, kan mindste effekten af et DDoS-angreb og hvordan institutioner på forskningsnettet kommer på.*

> Hvordan undgår man det her





> Skyldes måske firmaer som disse



> Resultatet er oftest dette

[redacted] @[redacted] ah, finally, we know why we have to waste our time on DDoS this time around: "Дания отправит на Украину пакет военной помощи в размере 524 млн долларов, а мы передадим DDoS-привет порталам русофобской Дании!🇩🇰"

something like DK is supporting Ukraine with a military package of $ 524 mil. , so we are sending greetings to the rusofob DK ...

but they report (so far) only attention to www.vejdirektoratet.dk and www.fm.dk, not mention of cert.dk

[redacted] @[redacted] perhaps they're using an old attack list, because you're definitely still under attack

[redacted] ser ud til jeg er under angreb på [redacted]navneservere

der er lige nu 7638 unike servere der har spurgt mig om TXT records på cisco.com

.. jeg har talt sammen i ca. 6 minutter ..

nu er det 9958 unike servere

det er helt sindsygt

10237

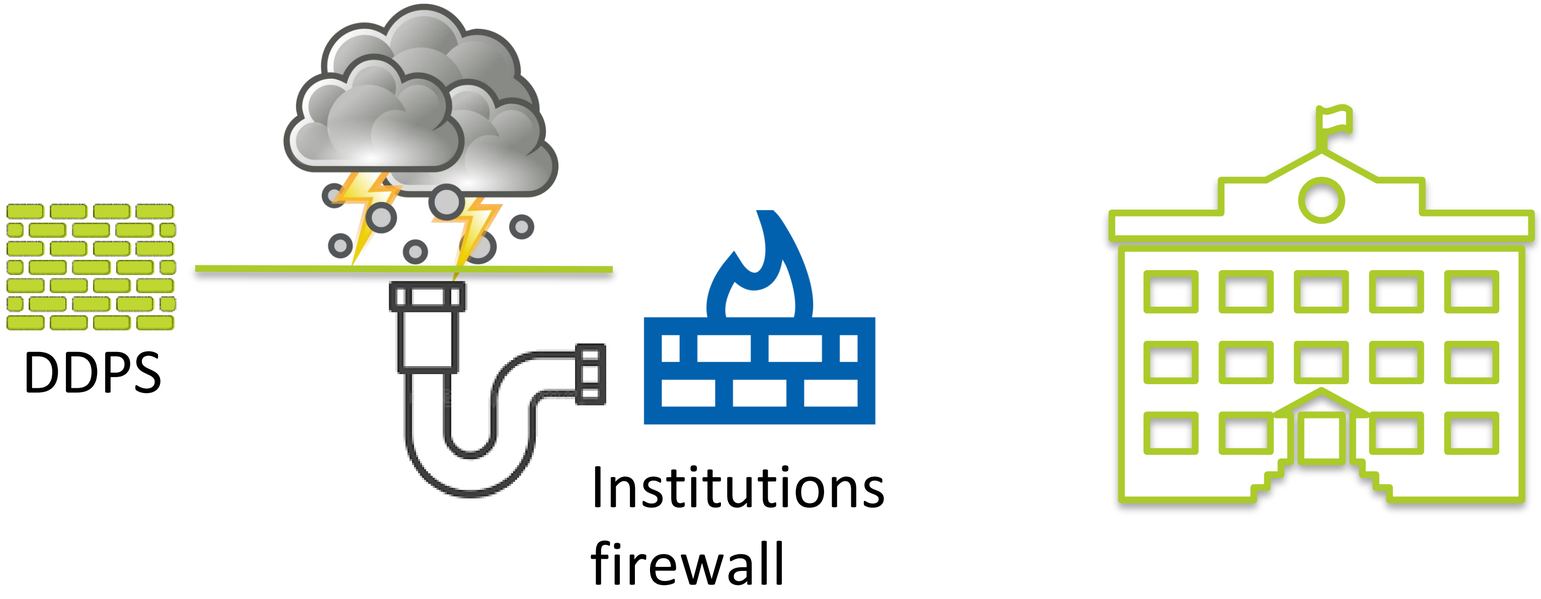
[redacted] 14626 ..

> Resten af præsentationen

- Hvad er DDPS
  - hvad skal det løse
  - hvem er det lavet til
  - hvad er det ikke designet til
  - hvordan bruges det
- Status
- Spørgsmål og kommentarer

> Hvad skal det løse - Distribueret Denial of Service

- > Tidsbegrænset
- > Volumetrisk
- > Kan rettes mod alt og **kan** kamufleres som legitim trafik
- > Et volumetrisk angreb kan kun løses *upstream*



> Hvad skal det løse - Imødegåelse af DDoS

- **Planlægning**: Et *roadmap* for hvad der skal ske ved et DDoS angreb, notifikations- og eskalations procedurer
- **Reducer angrebsfladerne** for eksponerede systemer og planlæg skalering
  - Anvendelse af en **cloud** (dvs. gøre det til andres problem) f.eks. AWS eller Cloudflare
- Simpel og **robust arkitektur** (reverse proxy, statiske web-sites, flere uplinks etc)
- **Netværksovervågning** der trigger ved anormaliteter

- Vigtigste forsvars-parametre:
  - **Kapacitet** (planlagt)
  - **Reaktionstid** (automatisk)

> Hvem og hvad er DDPS lavet til

- DeiC self service DDoS mitigation for alle med en forskningsnettilslutning
- Tidsbegrænset ad-hoc beskyttelse mod volumetriske angreb mod infrastruktur og systemer bag DeiCs core routere
- Baseret på BGP flowspec, men med en central database og logning

- API og Web UI
  - midlertidige regler med en start og slut tid
  - API regler løselig baseret på BGP flowspec syntax
  - Web UI: mere restriktiv regelbeskrivelse, anvendelse af skabeloner

> Hvad er DDPS når vi får NORDUnet med på det

- Mulighed for at black hole route (dele af) en institutions adresser forskellige steder hos NORDUnet
  - Blokkering af adgang til en institutions net / services uden for non-nordic peers
  - Blokkering af adgang til en institutions net / services uden for GEANT

- Trafik til en institutions net / services fra Forskningsnet vil være uberørt

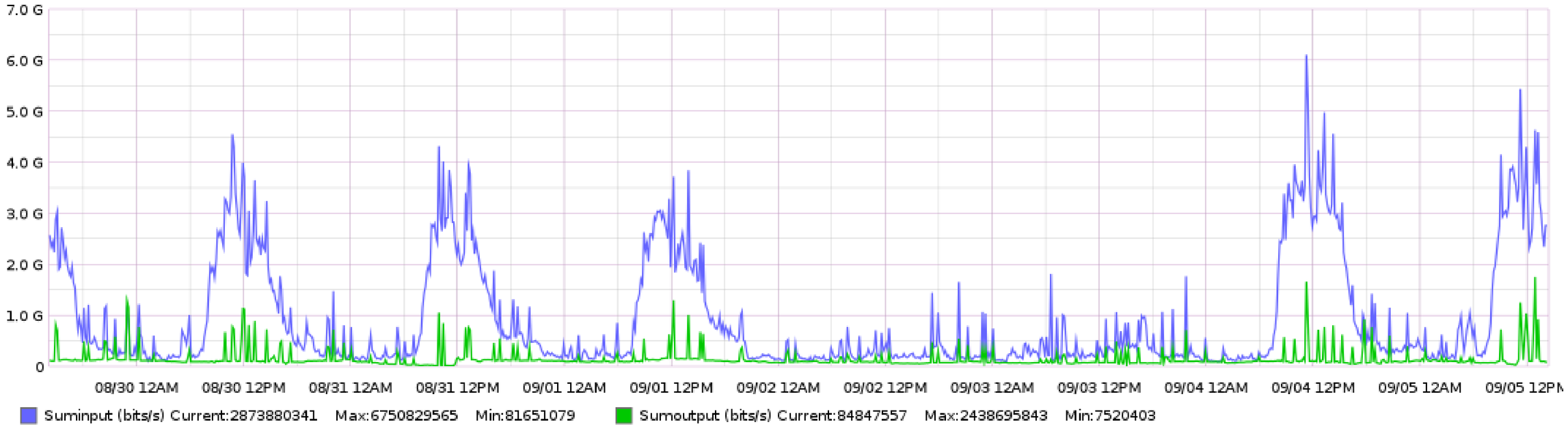
> NORDUnet BGP black hole route communities

```
2603:664 Do not advertise to Commodity (transit)
2603:665 Do not advertise to Commodity and non-Nordic Peerings.
2603:666 Do not advertise to Commodity and Peerings.
2603:667 Do not advertise to non-NORDUnet-member R&E.
2603:668 Only advertise to GEANT R&E sessions and nothing else
```

> Hvad er DDPS ikke

> en permanent fremskudt firewall

> en detection engine



> Hvem har lavet det

> Source, dokumentation og et vagrant image er på github.com/deic-dk/DDPS

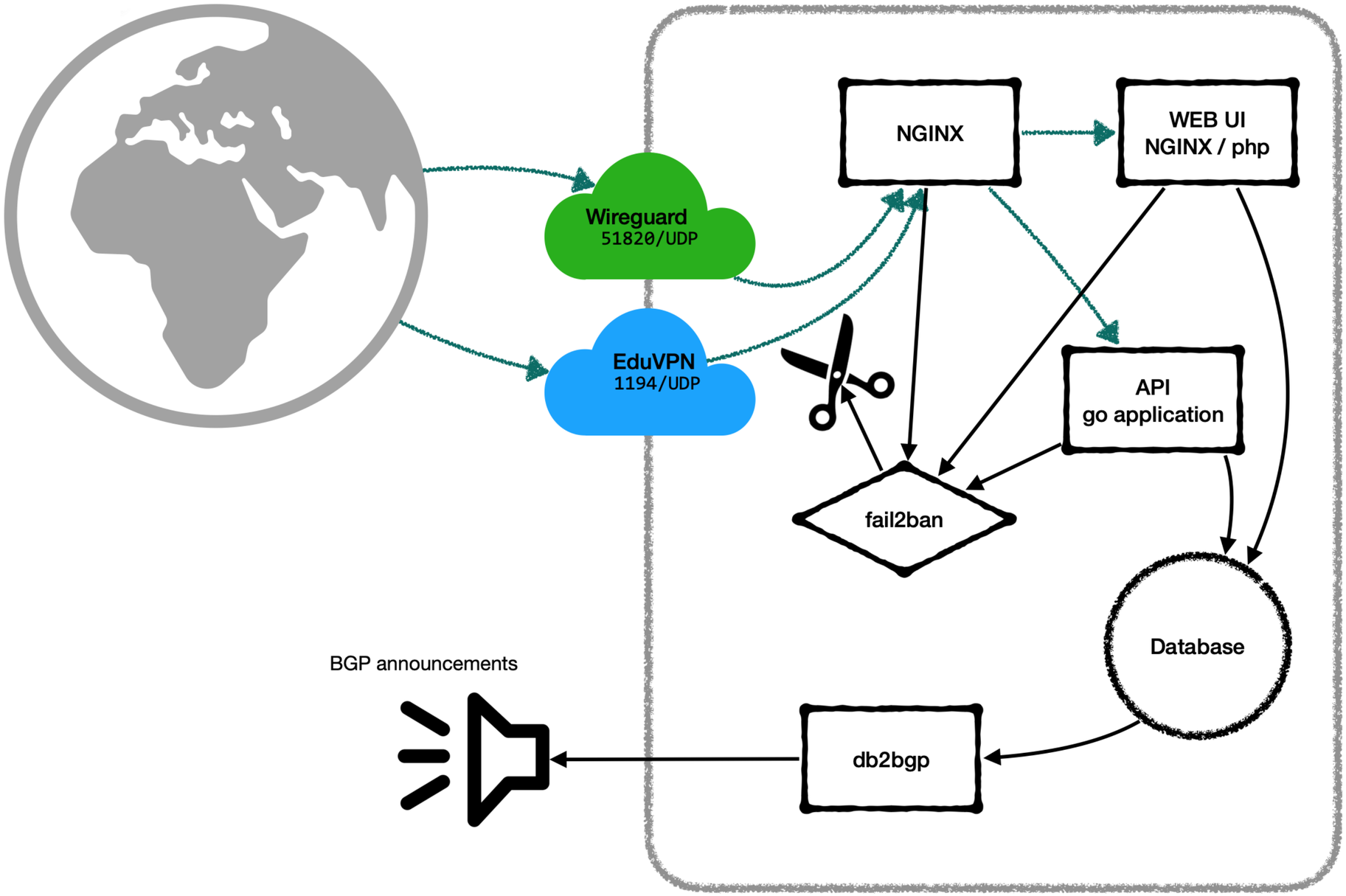
> Hvem og hvad vil have glæde af det?

- Udstyr bag forskningsnet core rutere incl. netværksudstyr bag uplink til DIX og NorduNET.
  - Enforces i LGB, ORE og PR1 (DIX router)

- Tilbydes alle på forskningsnet, men adgang kræver
  - WAYF login
  - En forskningsnettilslutning

> Pris

> Del af det at have en forskningsnet tilslutning


Wireguard
51820/UDP
EduVPN
1194/UDP
NGINX
WEB UI
NGINX / php
API
go application
fail2ban
Database
db2bgp
BGP announcements

Inde i DDPS - hvem kan hvad

- En *global administrator* der kan
  - Oprette, slette og ændre alle organisationer, brugere og netværk
- En *organisations administrator* der kan
  - Oprette og slette organisationens brugere og netværk, tildele rettigheder, lave regler osv.
- En *organisations netværksadministrator / API bruger* der kan
  - Oprette og slette regler for tildelte netværk
- En *organisations monitor* bruger der kan
  - Se aktive og udløbne regler

> Hvordan får man adgang til DDPS

> Skriv til ddps-info@deic.dk og bed om adgang
> Følg vejledningen i svaret

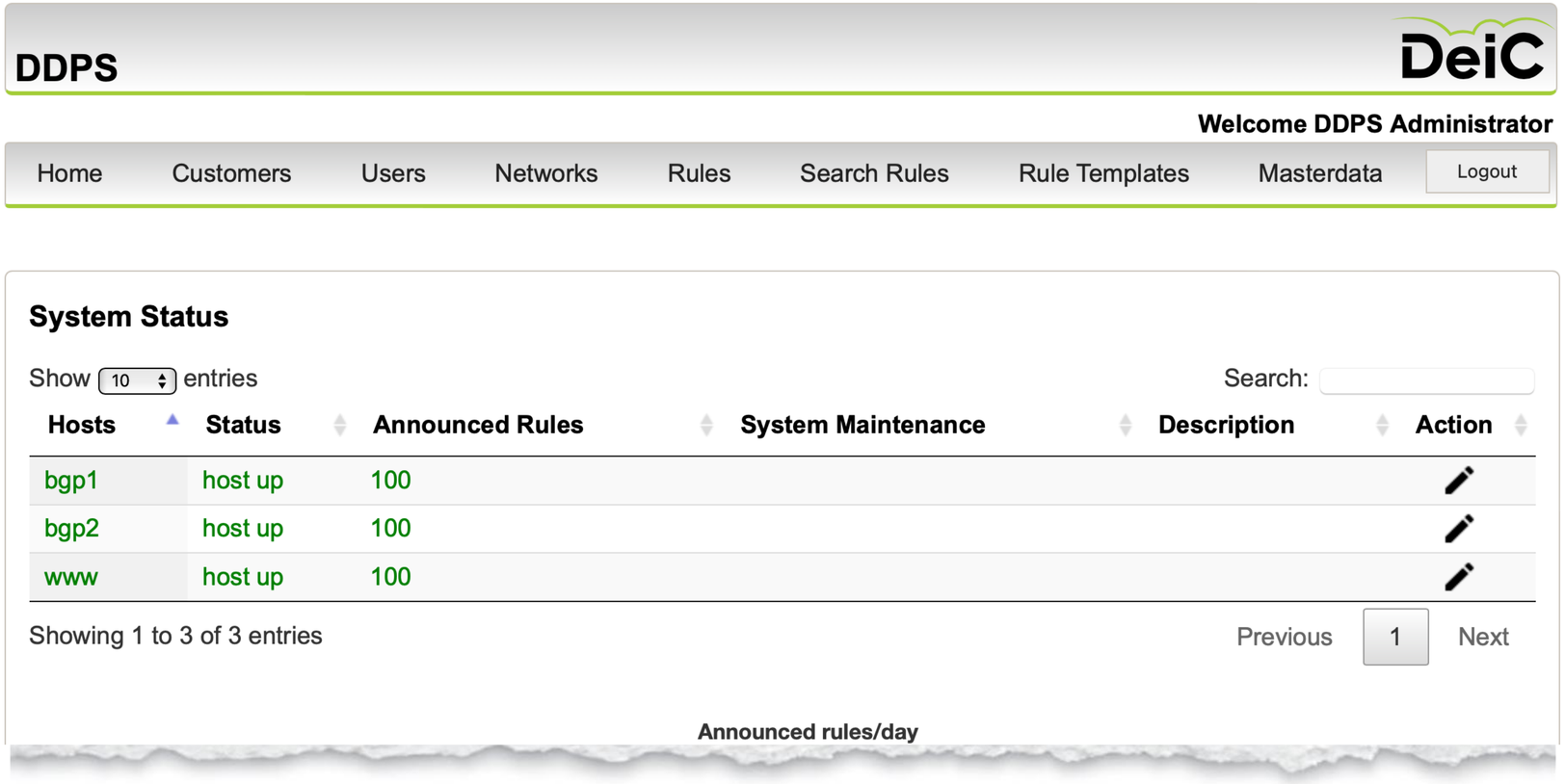
> Kræver enten WAYF og OpenVPN
> eller Wireguard

> PC: software installation kræver administrative rettigheder

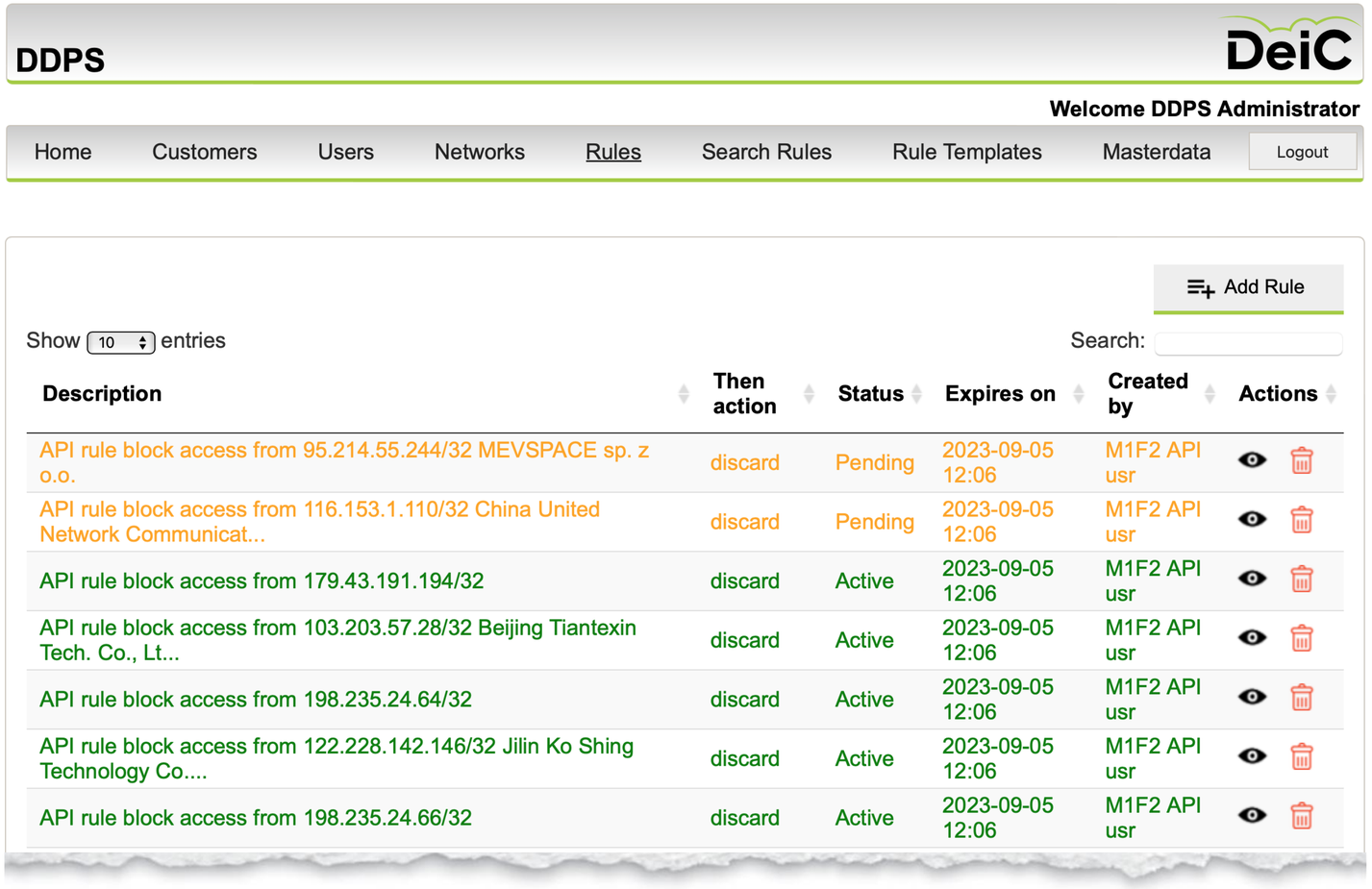
> Systemet kan kun tilgås via VPN (fra hele verden)

> Opsætning og adgang osv. kan laves via f.eks. Zoom eller on-site

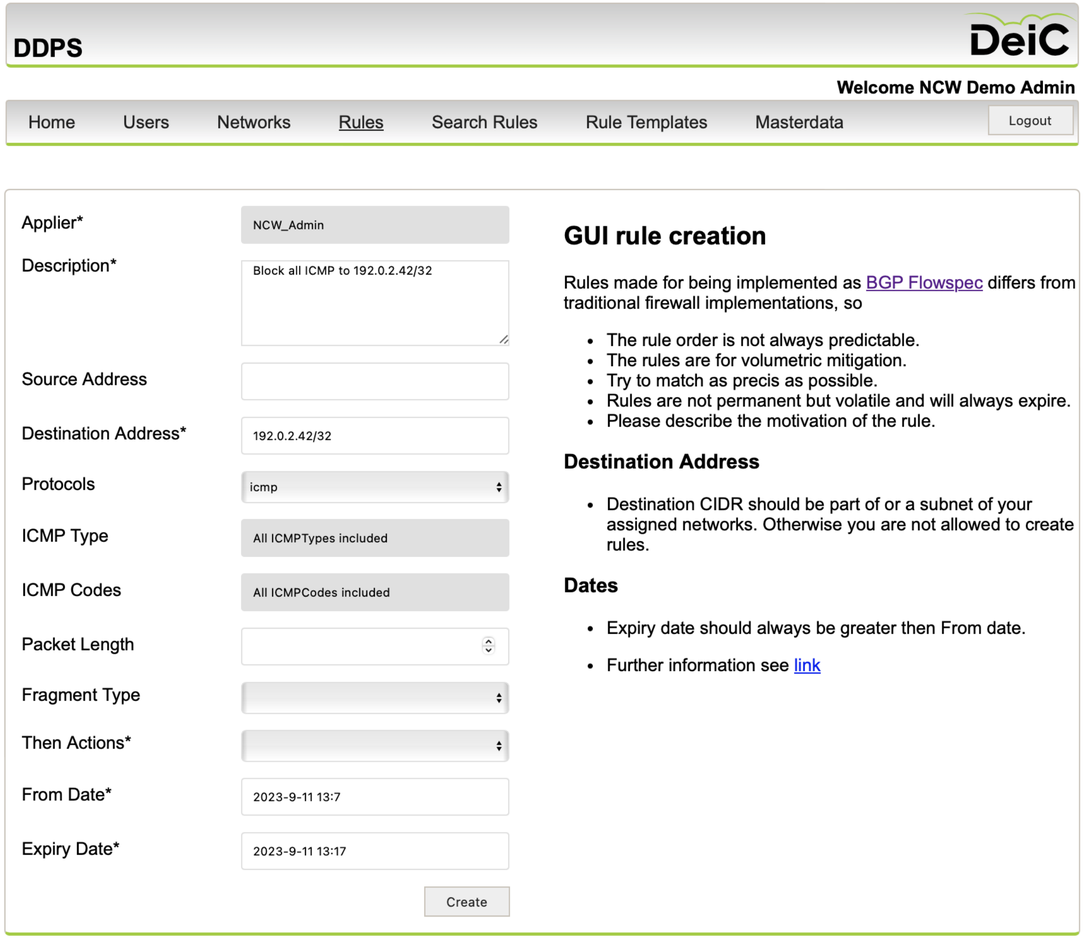
> Hvordan ser det ud?



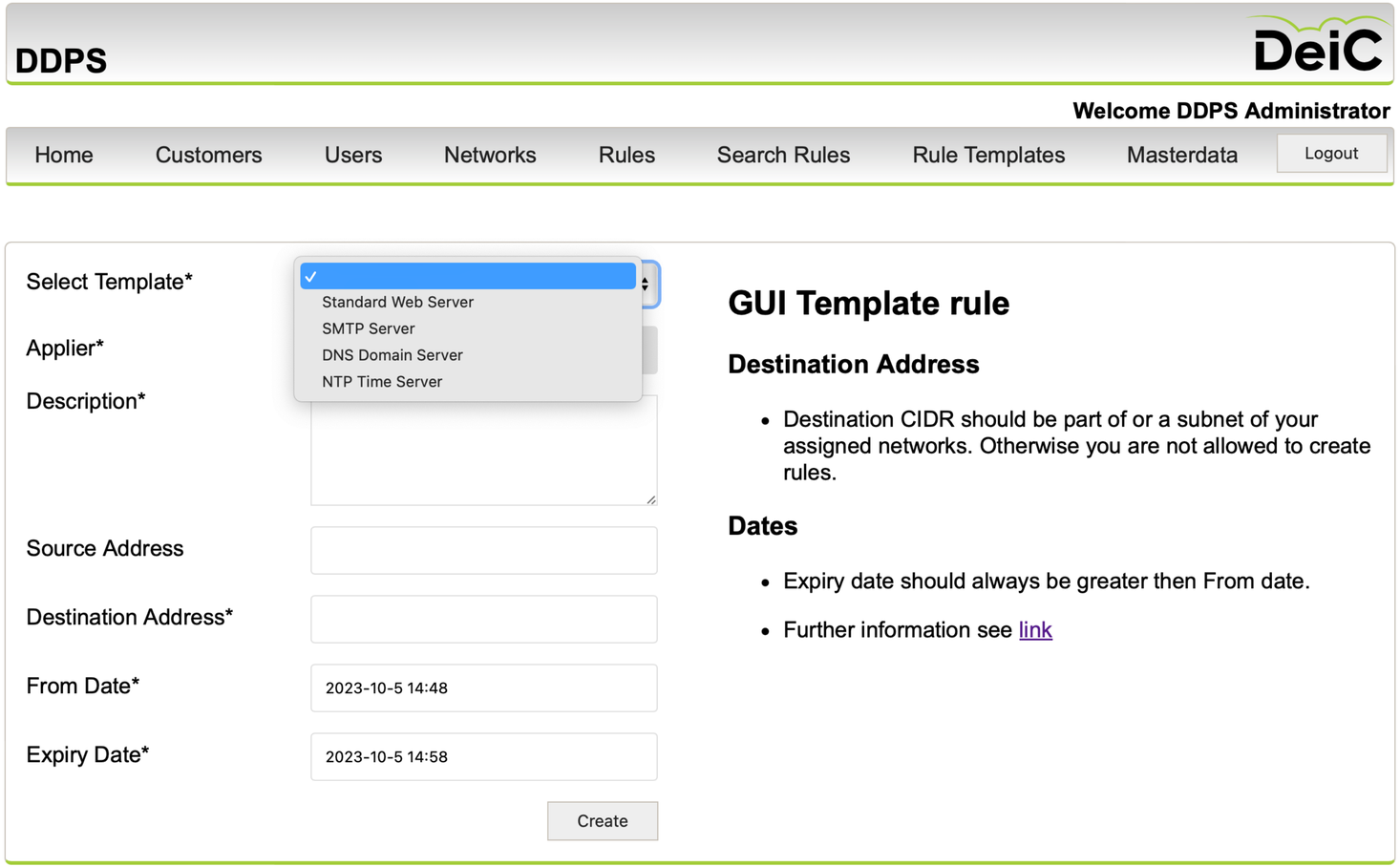
> Hvordan vises regler



Hvordan laves nye regler



> Nye regler baseret på skabeloner



> Regler via API'et

> Hver linie indeholder et OR udtryk, mindst ét skal være opfyldt

> Alle linier skal have et opfyldt match for at reglen trigger

```
{
  "durationminutes" : "10",
  "destinationport": "<=79 >=81&<=442 >=444",
  "sourceport": "",
  "icmptype": "",
  "icmpcode": "",
  "packetlength": "",
  "dscp": "",
  "description": "web server rules",
  "destinationprefix": "10.0.0.10/32",
  "sourceprefix": "0.0.0.0/0",
  "thenaction": "discard",
  "fragmentencoding": "dont-fragment is-fragment first-fragment last-fragment",
  "ipprotocol": "<=5 >=7 <=16 >=18",
  "tcpflags": ""
}
```

OR OR …

AND
AND
AND
….

> Integration med DDoS detektion

- Integration med **Suricata**, se https://medium.com/@mshulkhan/detection-attack-using-suricata-1-5ea7b2f62551 eller https://github.com/arvindpj007/Suricata-Detect-DoS-Attack
  - Læs output fra `/var/log/suricata/fast.log` (`IP proto, src,dst, sport,dport`) eller `eve.log` (json) meget mere info

- Integration med **FastNetMon** Community edition, se f.eks. https://github.com/deic-dk/DDPS/blob/master/src/example_client/using_the_api_with_fastnetmon.md
  - Læs output med notify_script_path og blokker baseret på tcpdump i tekst format

- Læs et sample og find grænseværdierne for de parametre der vises, erstat source med 0.0.0.0/0 hvis der er forskellige source adresser

> Store mængder legitim trafik

> Ved simple angreb, slå adresse informationen op med https://github.com/NikolaiT/IP-Address-API

```
curl 'https://api.incolumitas.com/?q=217.114.43.228'
```

```
  "asn": {
    "asn": 199785,
    "route": “217.114.43.0/24",
```

```
curl 'https://api.incolumitas.com/?q=AS199785'
```

```
  "prefixes": [
    "45.132.1.0/24",
    “87.251.76.0/24” ...
```

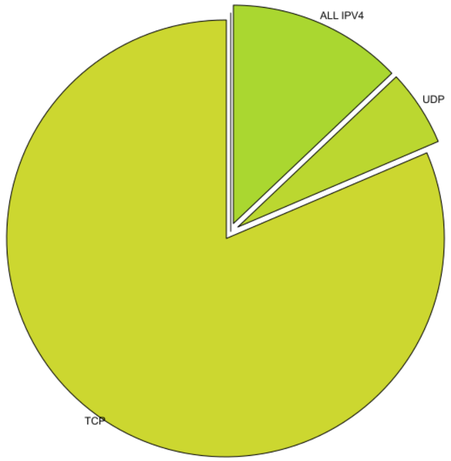
> Store mængder uønsket trafik

- Kør et script mod API'en der laver
  - Block UDP fragments
  - Block NTP amplification
  - Block DNS amplification
  - Discard TCP and UDP chargen
  - Discard TCP and UDP QOTD (Quote of the Day)
  - Discard IP protocol 47, GRE
  - ratelimit SSDP
  - ratelimit SNMP
  - Discard memcached amplification
- Bemærk at det med sikkerhed vil påvirke overvågning og nogle services

> I den nære fremtid …

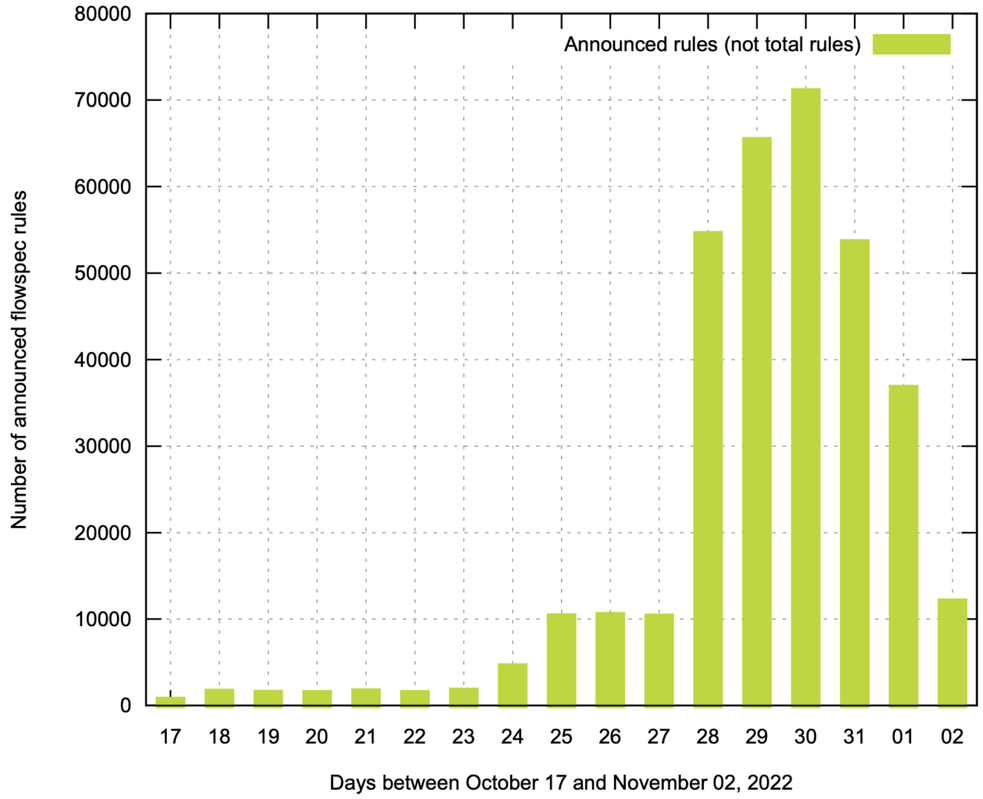
- Vi håber på at Netdrift og NORDUnet snart har fået BGP communities på plads, så man kan
  - Stoppe annoncering af ens net / adresser hos NORDUnet / Upstream / Peers
  - Adgang blokkeret fra net uden for NORDUnet / Forskningsnet / GÉANT
  - Ikke perfekt men bedre end intet
  - kan implementeres uden man ved hvad man bliver angrebet med

> Stress test



1.1 Announced flowspec rules

The graph below shows the number of *announced* flowspec rules per day. Only announcements are recorded, not withdrawal. Notice that while flowspec rules may span multible days, the chart only shows new announcements made on each specific day(s).



Nuværende status

- Systemet er stadig i *early roll-out*
  - Vi har 3 institutioner der anvender systemet og 2 der i gang med det
- Problemer vi ikke lige havde forudset
  - Det er ikke alle institutioner der tillader deres netværksteknikere at administrere deres egne maskiner; det giver VPN udfordringer
  - Det er ikke alle der anvender WAYF
  - Det er let at destruere vores eget udstyr når man tester

> Hvad så?

- **IPv6 enforcement** (rfc8956 - Dissemination of Flow Specification Rules for IPv6)
  - RFC8956 (Proposed Standard) gik EOL i 2021
  - Ingen idé om hvordan det håndteres i Juniper og Cisco
  - Nogen omskrivning nødvendig af DDPS
- **Blokkering på længere afstand** (f.eks. i GEANTs udstyr, 1500 km “fra os”)
  - Definer BGP communities baseret på afstand
  - Blokker kun i Forskningsnet uplink (BGP community)
  - Samarbejde med NorduNET og GÉANT
  - Nogen omskrivning nødvendig

> Spørgsmål?

> Kontakt: ddps-info@deic.dk