



DDDP S

DeiC - DDoS Protection Service

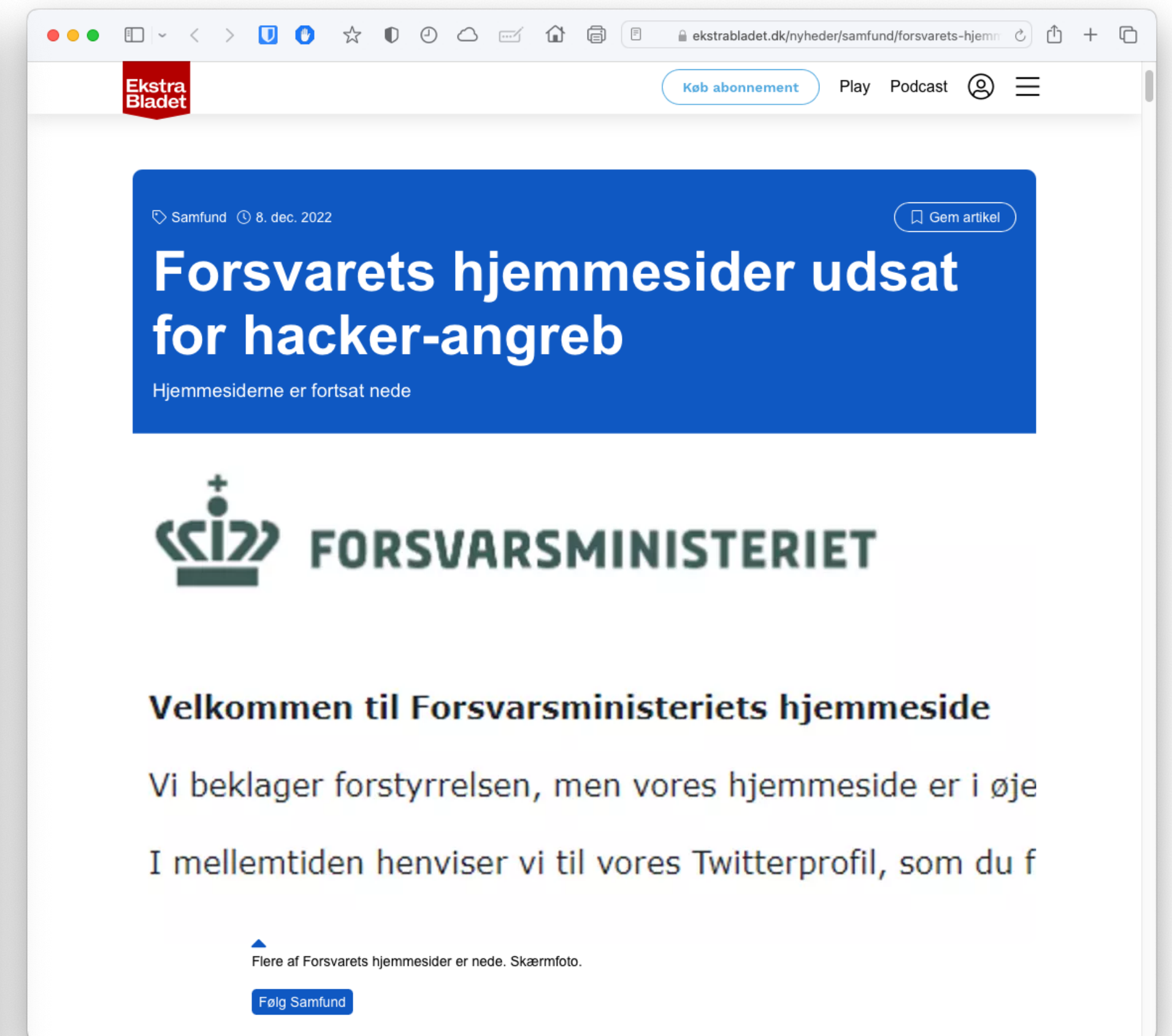
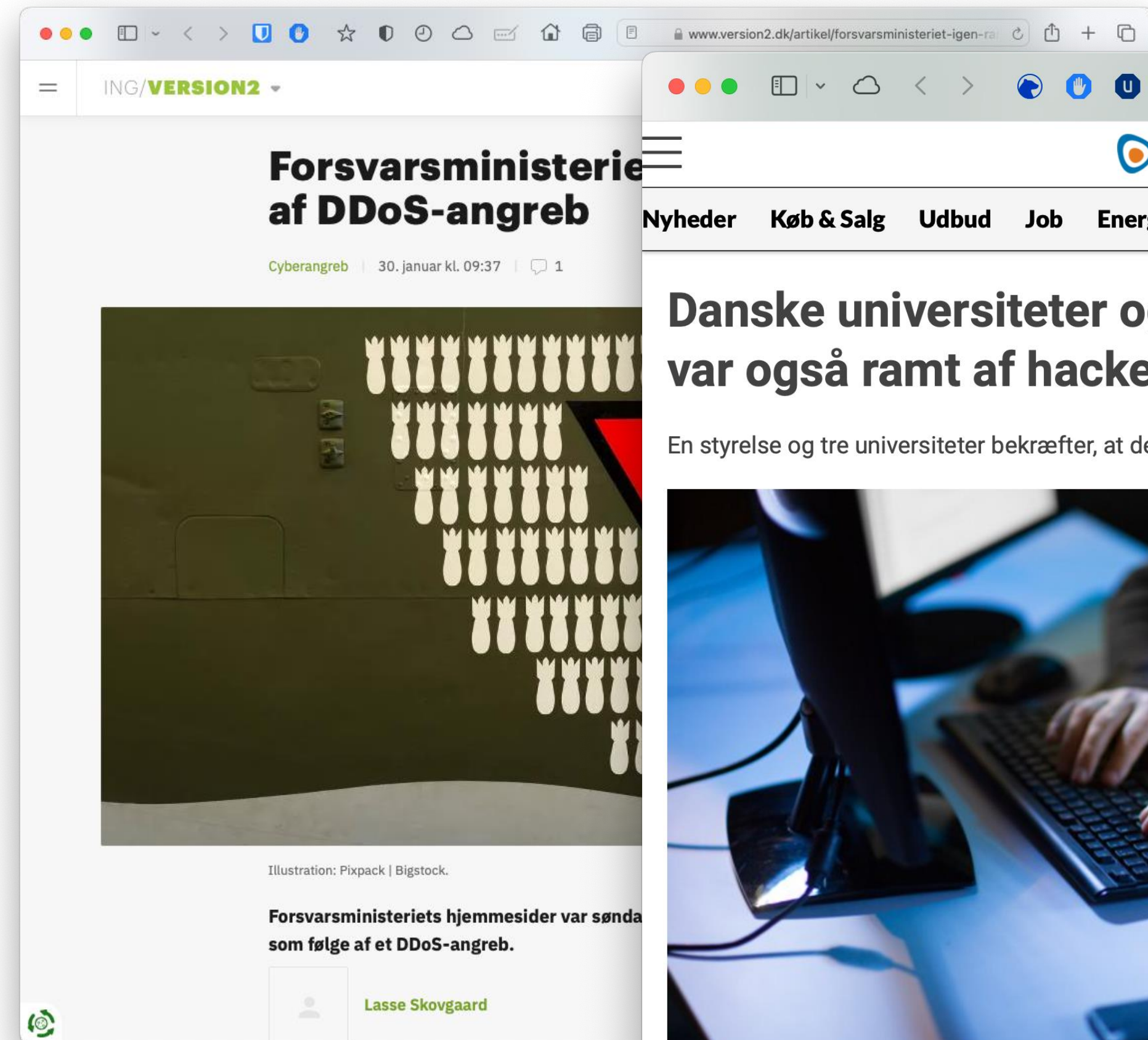
> Om DeiC

- > 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

The screenshot shows a forum post on BitcoinTalk.org. The browser address bar indicates the URL is bitcointalk.org/index.php?topic=5407833.0. The forum header includes the Bitcoin Forum logo and a search bar. The post title is "BULLETPROOF RDP | SERVER | WHM - SCAN/BRUTE ALLOWED BtHoster.com" with two green checkmarks. The author is "uid0 (OP) Newbie" with 4 activity and 0 merit. The post content includes:

- ✓ BulletProof HOSTING ✓
- WHY US?
WE DON CLOSE IP/ YOUR IP DONT GET NULLED AFTER FIRST SPAM OR SCAN LIKE OTHER HOSTING.
I STILL TEST HOSTING WHAT THEY CALLED BULLETPROOF AND ALL CLOSED MY SERVICE BECAUSE OF ABUSE.
- OUR site <https://bthoster.com/>
- ✓ RDP FOR SCAN/BRUTE ✓ - PRICE 10 \$ /MONTH
- ✓ WHM FOR PISHING WITH UNLIMITED DOMAIN LICENSE ✓ -PRICE 130 \$ /MONTH
- ✓ RESELLER FOR RDP WITH PANEL ✓ -PRICE 150 \$ + IP /MONTH
- ✓ SERVER FOR SCAN/BRUTE 32 GB RAM ✓ -PRICE 130 \$ /MONTH
- ✓ Telegram : <https://t.me/internethostingltd>
- ✓ Icq : @smtps.su
- Masscan Test
- <https://prnt.sc/gh3IQzug3uS1>

At the bottom of the post, there is a warning: "I HATE TABLES I HATE TABLES I HA(°_°) TABLES I HATE TABLES I HATE TABLES. Advertised sites are not endorsed by the Bitcoin Forum. They may be unsafe, untrustworthy, or illegal in your jurisdiction."

A reply by "uid0 (OP) Newbie" is visible at the bottom, titled "Re: BULLETPROOF RDP | SERVER | WHM - SCAN/BRUTE ALLOWED BtHoster.com" dated September 05, 2022.

> Resultatet er oftest dette

@ 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

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

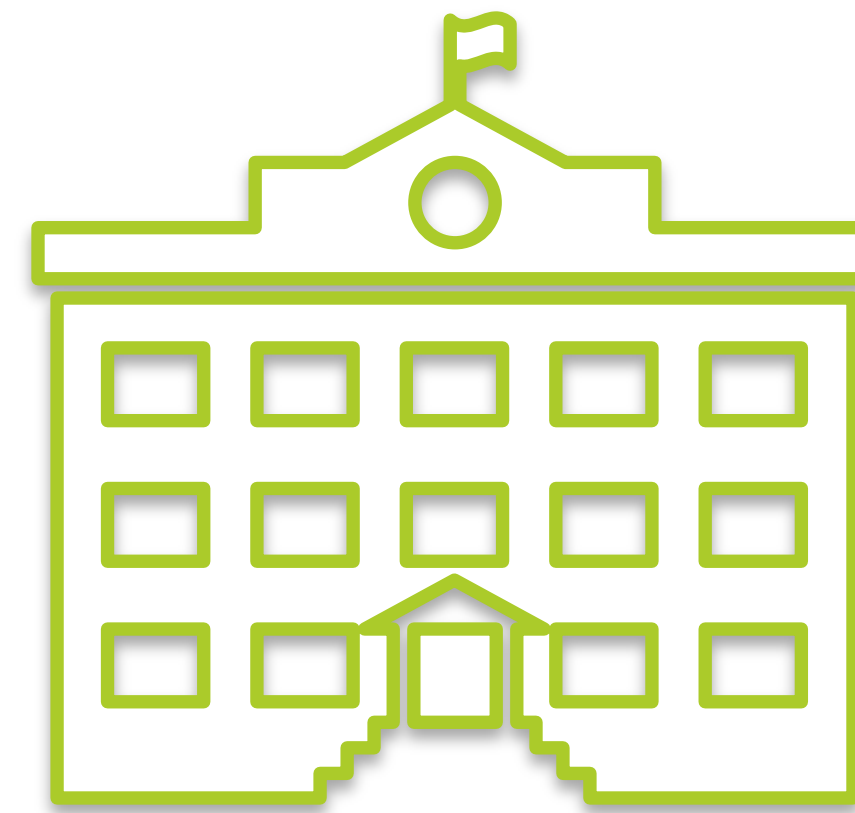
ser ud til jeg er under angreb på navneservere
der er lige nu 7638 unike servere der har spurgt mig om TXT records på cisco.com
.. jeg har talt sammen i ca. 6 minutter ..
nu er det 9958 unike servere
det er helt sindsygt
10237
14626 ..

> **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.

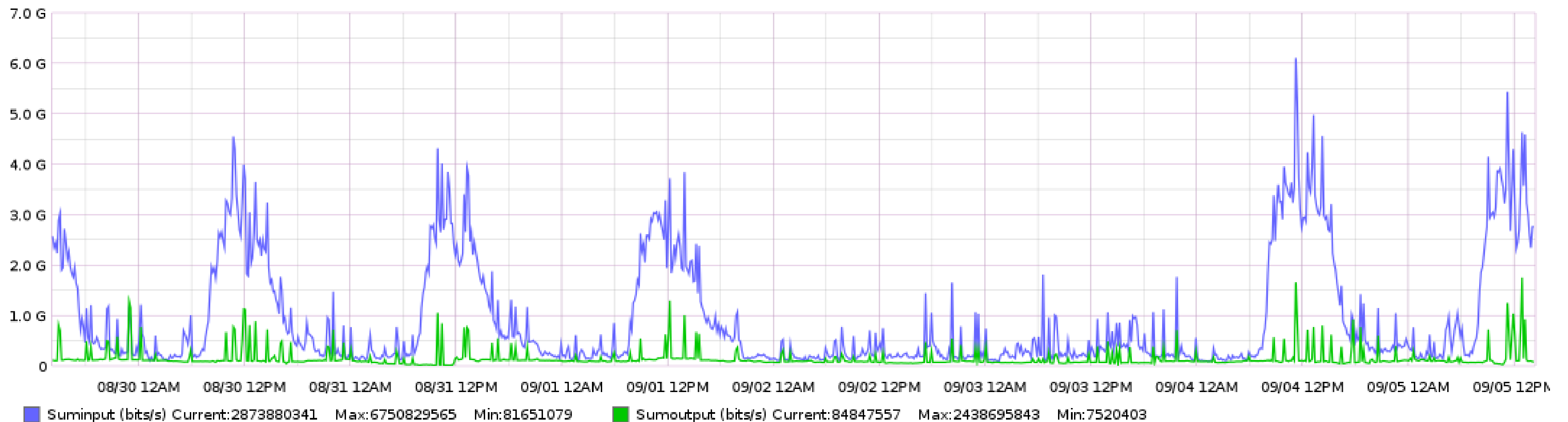
2603:666 Do not advertise to Commodity and Peerings.

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

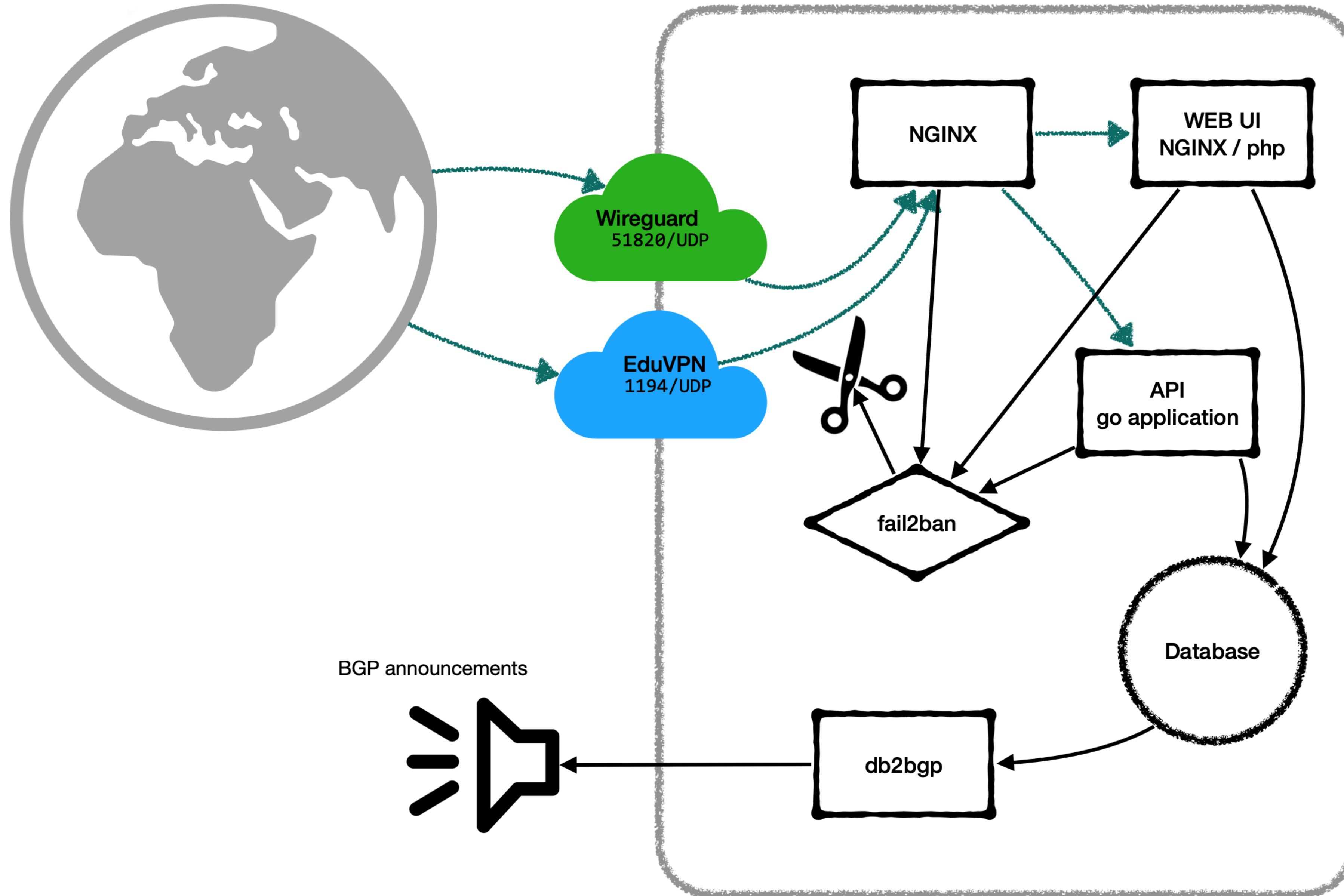
- > Source, dokumentation og et vagrant image er på github.com/deic-dk/DDPS

> 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



> **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?




DDPS 

Welcome DDPS Administrator

Home Customers Users Networks Rules Search Rules Rule Templates Masterdata Logout

System Status

Show entries Search:


Hosts	Status	Announced Rules	System Maintenance	Description	Action
bgp1	host up	100			
bgp2	host up	100			
www	host up	100			

Showing 1 to 3 of 3 entries Previous Next

Announced rules/day



> Hvordan vises regler

DDPS


Welcome DDPS Administrator

Home
Customers
Users
Networks
Rules
Search Rules
Rule Templates
Masterdata
Logout


+ Add Rule

Show 10 entries Search:

Description	Then action	Status	Expires on	Created by	Actions
API rule block access from 95.214.55.244/32 MEVSPACE sp. z o.o.	discard	Pending	2023-09-05 12:06	M1F2 API usr	👁 🗑
API rule block access from 116.153.1.110/32 China United Network Communicat...	discard	Pending	2023-09-05 12:06	M1F2 API usr	👁 🗑
API rule block access from 179.43.191.194/32	discard	Active	2023-09-05 12:06	M1F2 API usr	👁 🗑
API rule block access from 103.203.57.28/32 Beijing Tiantexin Tech. Co., Lt...	discard	Active	2023-09-05 12:06	M1F2 API usr	👁 🗑
API rule block access from 198.235.24.64/32	discard	Active	2023-09-05 12:06	M1F2 API usr	👁 🗑
API rule block access from 122.228.142.146/32 Jilin Ko Shing Technology Co....	discard	Active	2023-09-05 12:06	M1F2 API usr	👁 🗑
API rule block access from 198.235.24.66/32	discard	Active	2023-09-05 12:06	M1F2 API usr	👁 🗑



> Hvordan laves nye regler

DDPS


Welcome NCW Demo Admin

Home
Users
Networks
Rules
Search Rules
Rule Templates
Masterdata
Logout

Applier* NCW_Admin

Description* Block all ICMP to 192.0.2.42/32

Source Address

Destination Address* 192.0.2.42/32

Protocols icmp

ICMP Type All ICMPTypes included

ICMP Codes All ICMPCodes included

Packet Length

Fragment Type

Then Actions*

From Date* 2023-9-11 13:7

Expiry Date* 2023-9-11 13:17

Create

GUI rule creation

Rules made for being implemented as [BGP Flowspec](#) differs from traditional firewall implementations, so

- The rule order is not always predictable.
- The rules are for volumetric mitigation.
- Try to match as precis as possible.
- Rules are not permanent but volatile and will always expire.
- Please describe the motivation of the rule.

Destination Address


- Destination CIDR should be part of or a subnet of your assigned networks. Otherwise you are not allowed to create rules.

Dates

- Expiry date should always be greater then From date.
- Further information see [link](#)



> Nye regler baseret på skabeloner

DDPS


Welcome DDPS Administrator

Home
Customers
Users
Networks
Rules
Search Rules
Rule Templates
Masterdata
Logout

Select Template* Standard Web Server

SMTP Server

DNS Domain Server

NTP Time Server

GUI Template rule

Destination Address

- Destination CIDR should be part of or a subnet of your assigned networks. Otherwise you are not allowed to create rules.

Dates

- Expiry date should always be greater then From date.
- Further information see [link](#)

Applier*

Description*

Source Address

Destination Address*

From Date*

Expiry Date*

> 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

```
1 {
2   "durationminutes" : "10",
3   "destinationport": "<=79 >=81<=442 >=444",
4   "sourceport": "",
5   "icmptype": "",
6   "icmpcode": "",
7   "packetlength": "",
8   "dscp": "",
9   "description": "web server rules",
10  "destinationprefix": "10.0.0.10/32",
11  "sourceprefix": "0.0.0.0/0",
12  "thenaction": "discard",
13  "fragmentencoding": "dont-fragment is-fragment first-fragment last-fragment",
14  "ipprotocol": "<=5 >=7 <=16 >=18",
15  "tcpflags": ""
16 }
```

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

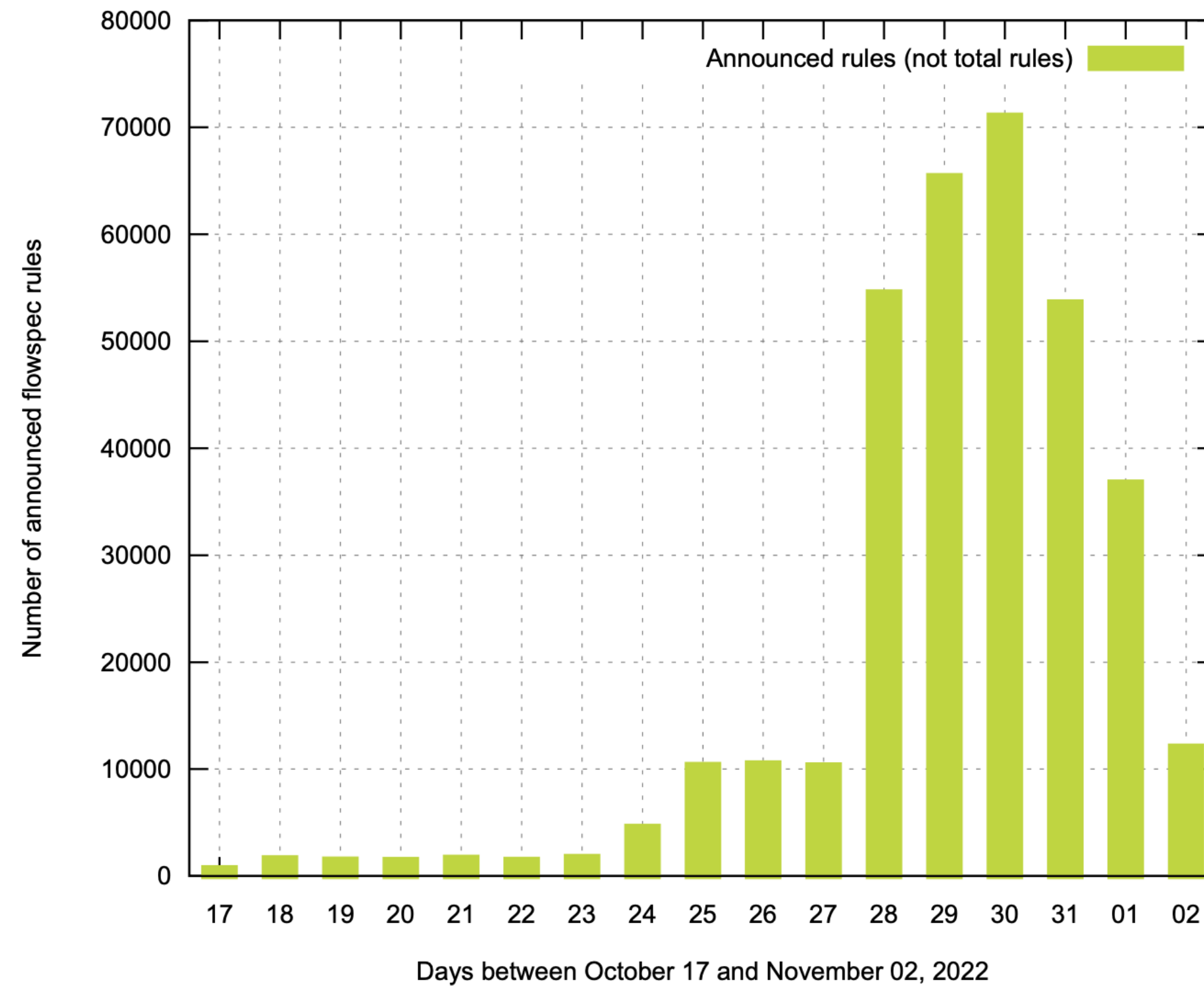
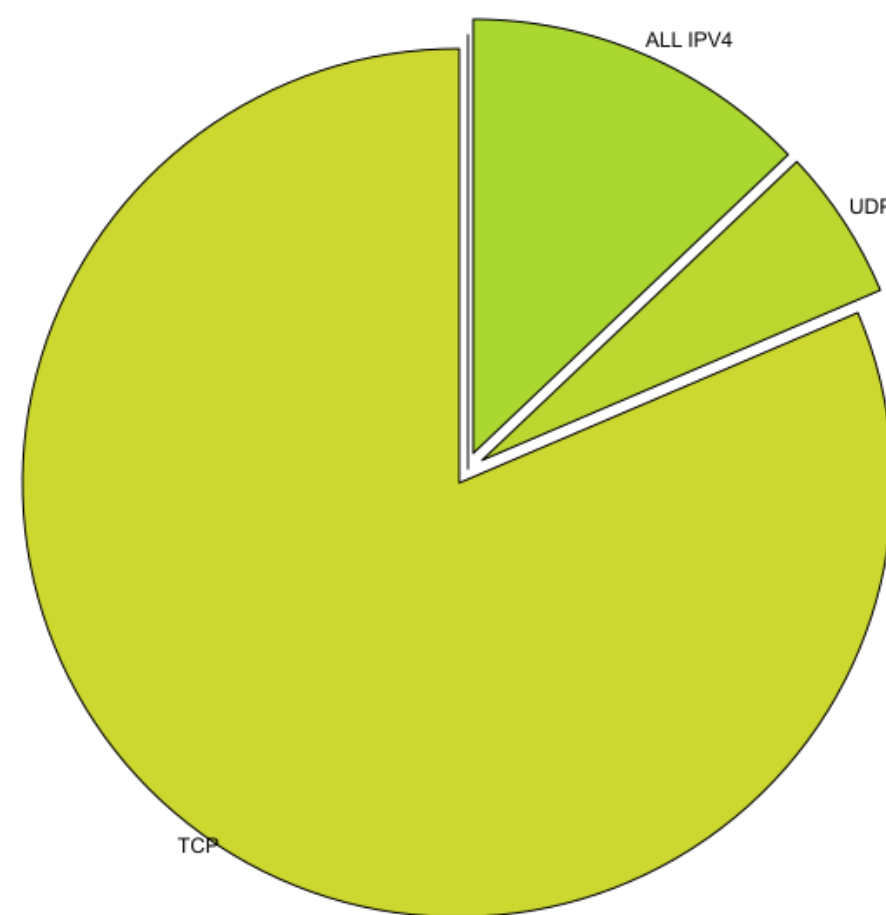
> I den nære fremtid ...

- > 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 multiple 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