Block On Demand skal være et *GUI* værktøj til manuelt at at lave BGP flow spec regler for egne net. Det bør ikke kaldes *Firewall On Demand*: det giver forkerte associationer: regler er ikke permanente og bør kun anvendes til beskyttelse mod DDoS angreb, **ellers overbelastes udbydernes kant-routere**.

SoD er tænkt som en central service for forskningsnet kunder og skal ses i sammenhæng med det sideløbende projekt der gå ud på automatisk at imødegå DDoS angreb ved hjælp af BGP flow spec.

Reglerne beskrives via en web-baseret GUI og laves af en forskningsnet kundes netværksadministrator. Reglerne bliver submittet via BGP flowspec og enforces via *access lister* i kantroutere på forskningsnet og de peering partnere der tillader flow spec baseret filtrering.

Regler vil som udgangspunkt altid være midlertidige - hvilket er en følge af den valgte teknologi. Systemet tillader regler inden for følgende grænser:

- regler er *midlertidige* og har et *start* og et *sluttidspunkt*
- regler registreres med et *kunde prefix* hvilket gør visualiseringen lettere
- regler beskriver *enten* indgående filtrering mod *egne net* eller udgående filtrering fra *egne net*
- filtrering er underlagt de 12 filtreringsmuligheder der findes i flow spec:
    - Type 1 - Destination Prefix
    - Type 2 - Source Prefix
    - Type 3 - IP Protocol
    - Type 4 – Source or Destination Port
    - Type 5 – Destination Port
    - Type 6 - Source Port
    - Type 7 – ICMP Type
    - Type 8 – ICMP Code
    - Type 9 - TCP flags
    - Type 10 - Packet length
    - Type 11 – DSCP
    - Type 12 - Fragment Encoding

Mht. type 1 og type 2 vil gælde, at *den ene parameter altid er egne net* og den anden parameter altid er et eksternt net. En mere detaljeret beskrivelse findes i RFC 5575 - Dissemination of Flow Specification Rules - IETF Tools .

SoD version 1.0 vil rent teknisk bestå af følgende komponenter:

- En database med alt indhold (intet i filsystemet)
- En Web baseret GUI
- scripts/programmer til
    - opdatering af databasen med *forskellige default objekter*,
    - log information fra *fastnetmon* (rettes senere til også at være flow spec data)
    - udtræk af *regler* der skal enforces via ExaBGP.

Der vil skulle laves en infrastruktur i forbindelse med projektet der skal omfatte følgende: - internt RCF1918 netværk mv. beskyttet af en pf firewall - Apache web-server evt. med en NGINX front-end som ekstra sikkerhed. - Postgress database idet den har indbygget IPv6 og IPv4 data typer.

1. Databasedesign

Databasedesignet findes her.

2. Web baseret GUI

Den web-baserede GUI vil bestå af følgende uafhængige komponenter:

- En *kundevendt policy editor* med mulighed for at

    1. oprette, ændre og slette regler
    2. oprette, ændre og slette *netværks*- og *service*-objekter
    3. se en oversigt af blokkering for egne net
    4. administration af netværksadministratorer med rettigheder i forhold til egne net (hvem må blokere adgang til bestemte net)

Det sidste punkt (4) kan evt. udskydes til senere. I oversigten (3) vil indgå både *manuelle regler* oprettet i GUI'en og *automatiske regler* lavet af fastnetmon.

2.1. Administratorer

Administratorer findes i to kategorier: - DBADMIN: må oprette *NETADMIN* administratorer og subnet for en kundes interne net samt lave regler for netværk - NETADMIN: må lave regler for bestemte netværk

Det er fristende at udvide modellen til at NETADMIN må oprette subnet for egne netværk, men det bliver hurtigt meget omstændigt og kan udelades.

2.2. Netværksobjekter

Der vil fra start være et *cidr* for hvert af en kundes netværk samt en række prædefinerede service og eksterne netværksobjekter, alle definerede i databasen.

Hver kunde kan kun se egne netværksobjekter.

Der vil derudover være følgende netværksobjekter:

- Any: dvs alle netværk undtagen egne
- Forskningsnet: *vores* netværk
- Net baseret på landekoder, f.eks. `DK` .

2.3. Serviceobjekter

Der vil fra start være en række prædefinerede serviceobjekter; f.eks. `SMTP` defineret som IP protokol 17 (TCP) og port 25.

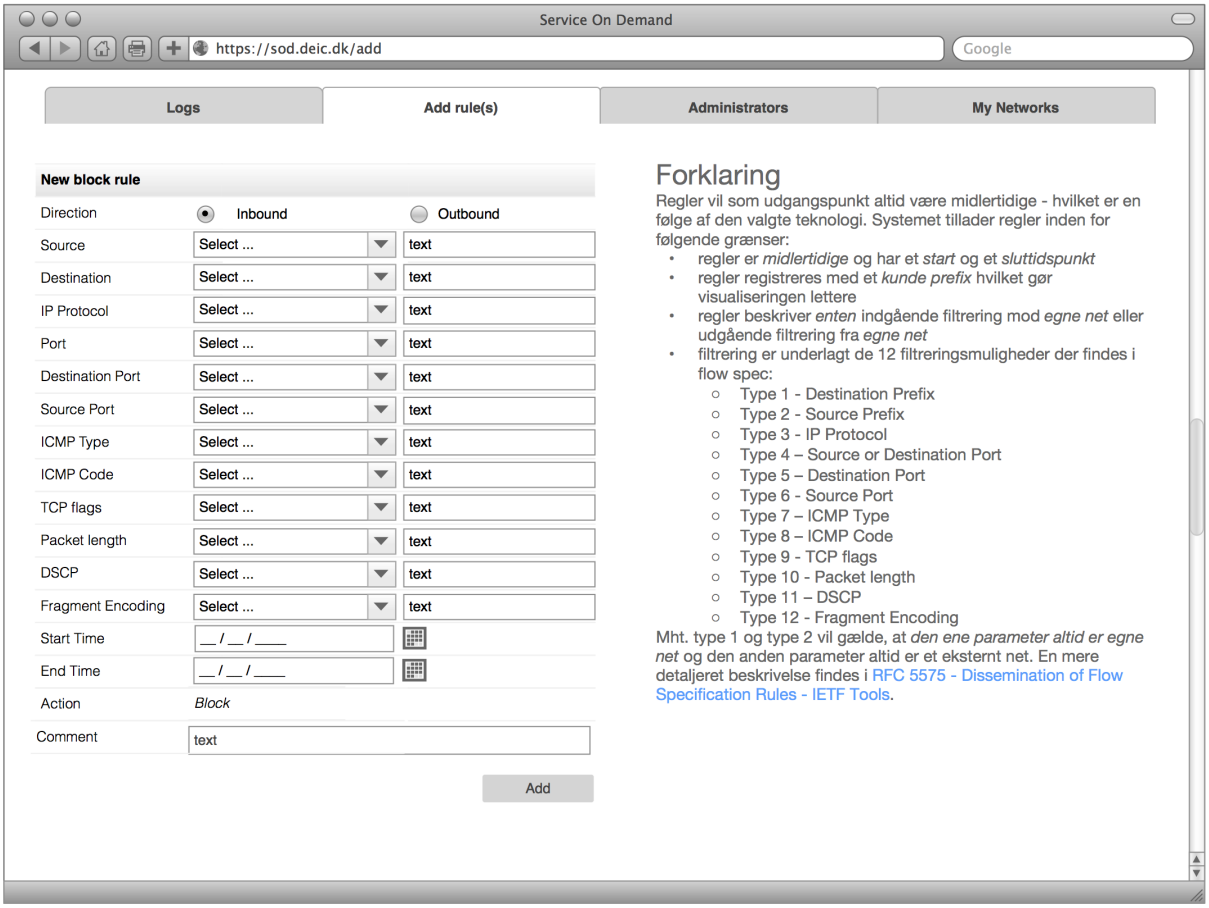
2.4. Blokkeringsregler

Blokkeringsregler oprettes af en administrator (enten en DBADMIN eller en NETADMIN) på baggrund af netværksobjekter (interne og eksterne netværk eller subnet), service objekter samt et tidsrum en blokkeringsregel skal være gyldig.

Oprettelse af blokkeringsregler vil følge denne skabelon:

1. tilføj regel: indgående `ELLER` udgående
2. Vælg Source og Destignation:
    1. F.eks. fra en *pull down* liste af brugerdefinerede netværksobjekter samt kundens netværk `ELLER` en specifik IP range `ELLER` en specifik IP adresse `ELLER` et globalt objekt.
3. vælg service: Any `ELLER` præ-defineret `ELLER` brugerdefineret
    1. vælg præ-defineret fra f.eks. pull-down
    2. brugerdefineret: angiv TCP og/eller UDP samt port range, `ELLER` ICMP type og code `ELLER` TCP flag `ELLER` pakkestørrelse `ELLER` IP protokol.
4. Angiv *start tid* og *slut tid*.

Det kunne f.eks. se sådan ud:



Alle ICMP typer bør være med fra start som prædefinerede objekter (1 hhv 58) skal der kunne angives en `TYPE` og en `CODE` se wikipedia.

Grænseværdierne for alle legale valg skal læses fra tabellerne i databsen.

2.5. Brugerdefinerede serviceobjekter

Når brugeren vælger noget der ikke er defineret i forvejen (et af brugerens interne net eller f.eks. en prædefineret service som `SMTP` skal oplysningerne gemmes som et nyt objekt der vil kunne genbruges.

Brugerdefinerede serviceobjekter skal indeholde følgende felter:

- Service objektnavn, f.eks. RDP
- IP protokol (255 numre, se wikipedias artikel om IP numre). Det vil nok kun være en delmængde der er aktuel, brugeren skal vælge den fra en liste. ICMP bør ikke være her: det skal være prædefineret. Det samme for f.eks. GRE, og en lang række af de andre.
- For UDP og TCP (6 og 17) skal der kunne anføres en (liste af) portnumre
- En pakkestørrelse
- TCP flag: se Wikipedia om Transmission Control Protocol - med en kortere beskrivelse her
- En kort beskrivelse.

Dvs. der skal først vælges *IP protkol* og for TCP og UDP skal der kunne vælges portnumre (en liste?) og for alle en pakkestørrelse. Et legalt brugervalg er f.eks. ICMP type 5 code 0 (*Redirect Datagram for the Network*) med en bestemt pakkestørrelse.

Objektet skal gemmes under kundens informationer.

Brugerdefinerede netværksobjekter skal indeholde følgende felter, idet de kan være *både interne og eksterne adresser*:

- Netværks objektnavn, f.eks. WEB-DMZ
- Netværk som CIDR
- Kommentar
- Hvilke administratorer der må lave regler for nettet

Heraf følger, at kun *super administratoren* kan oprette nye netværksobjekter der er en delmængde af interne netværk; men det er nok lettere at vedtage det kun er super administratoren der kan oprette netværk overhovedet.

2.6. Status

Opgaver fordelt: Database mv. primært FTH, lidt NTH. Infrastruktur: AMD, Web-gui: KSO. Dokumentation mv. NTH & NIE.

Dato	Ændring
Tir 31 Maj 2016 19:08:06 CEST	Database mv. nogenlunde på plads incl. test data. Netværk og firewall ditto, virtuel maskine oprettet Ubuntu Server LTS 16.04