Arkitekturdokument
Dynamisk Nettverksbrannmur

Espen Gjærde Svein Ove Undal

11.04.2013

Revisjonshistorie

Dato	Versjon	Forklaring	Forfattar
15.04.2013	1.0	Dokumentet oppretta	Espen
16.04.2013	1.0	Diagram og illustrasjonar oppdatert	Espen

Innhald

1 Innleiing

1.1 Hensikta med dokumentet

Dette dokumentet skal beskrive arkitekturen i systemet som blir utvikla. Dokumentet vil gå djupare inn i dei forskjellige systema som vert nytta og korleis desse heng saman. Også her vert det nytta standardiserte logiske modellar for å gje ei betre oversikt over systemet.

1.2 Avgrensingar

Dokumentet skildrar systemet som vert utvikla, og relasjonar til andre system. Det vil ikkje skildre eksterne system som vert nytta.

1.3 Definisjonar og forkortingar

Ord	Forklaring / Definisjon
IPtables	Pakkefilter /-manipulator tilgjengeleg i dei fleste linuxdistribusjonar
Linux-distibusjon	Variant av operativsystemet linux
WebUI	Nettside som kontrollerer eit system/program.
DNF	Systemet som vert utvikla (*Eng: Dynamic Network Firewall*)
Ruting	Sending/Vidaresending av pakkar i eit nettverk
Prerouting	(*Nor: Før-ruting*) behandling av pakkar før dei blir ruta
Daemon	Program som kjører i bakgrunn og utfører oppgaver automatisk.

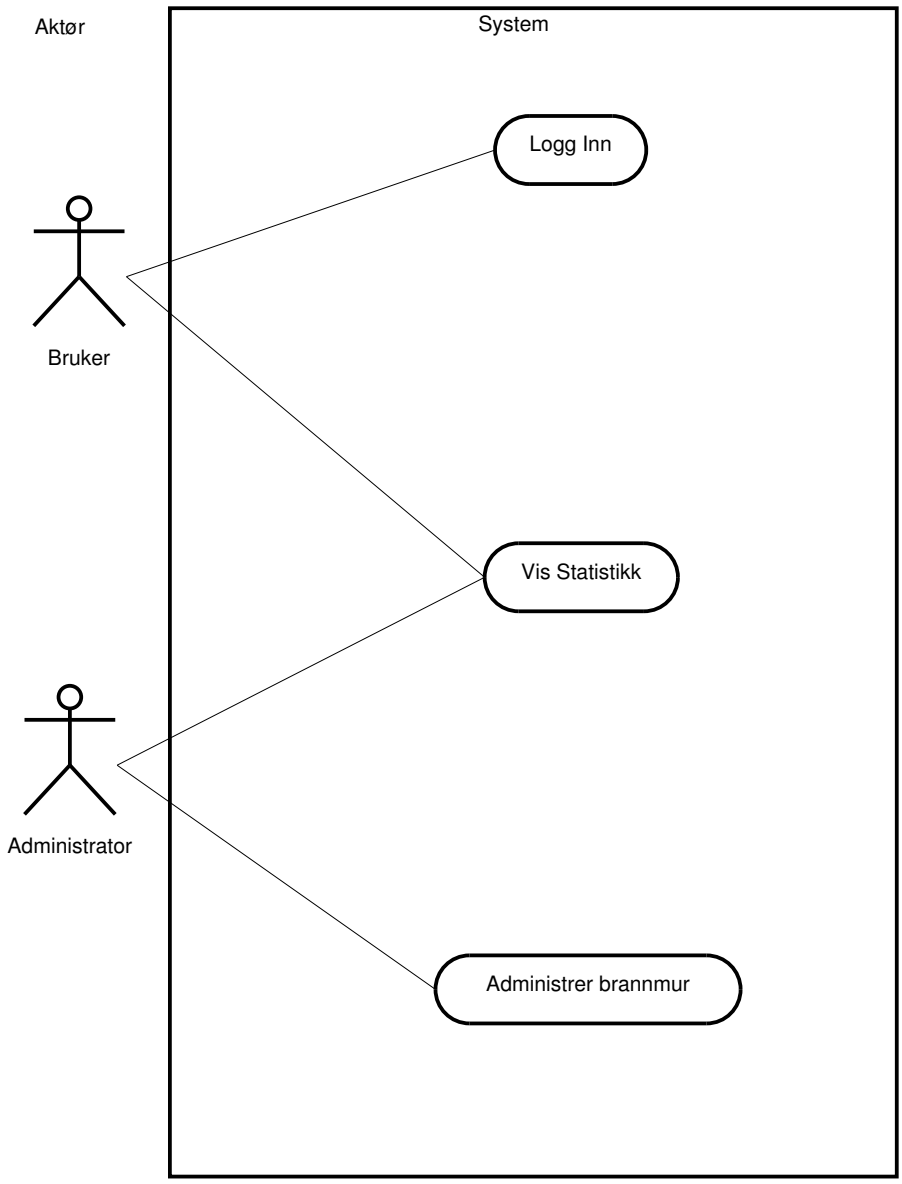
1.4 Oversikt over innhald

Dette dokumentet er av litt meir teknisk art, og inneheld ein modellar for å forklare korleis komponentane i systemet heng saman, og korleis dei kommuniserer med andre komponentar i operativsystemet. Her vil være både UML-standardmodellar, og figurar som bryt noko med UML-standarden. Figurar som bryt litt med standarden vil verte forklart nærmare.

2 Bakgrunn og oversikt

2.1 UseCase modell

UseCase-modellen i figur 1 gir eit bilete av kva funksjonar brukarane av systemet skal ha tilgjeneleg.



Figur 1: UseCase-modell

2.2 Ikkje-funksjonelle krav

Systemet vert utvikla under ein open lisens, og skal være tilgjengeleg for allmennheita. Det vil ikkje følgje nokon garantiar eller krav til service og støtte til systemet.

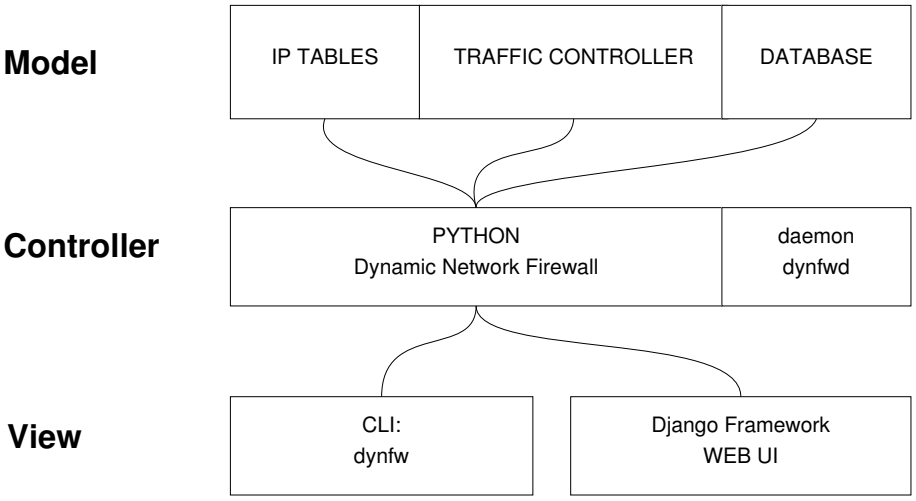
2.3 Vilkår og avhengigheiter

Tjenarside Systemet vert utviklar for Debian Linux, og er avhengig av programmeringsspråket Python, brannmursystemet Iptables og Linux Traffic Control. Alle desse skal være implementert i dei fleste linux-distribusjonar. Vi har også programmert systemet mot ein mySQL-database, men systemet sine grunnfunksjonar kan fungere utan databasen. For authentisering vert linux sitt PAM-system nytta.

Klientside Systemet nyttar webteknologi for å authentisere klientar opp mot systemet. Klientar som skal nytte systemet må derfor ha ein nettlesar. Vi anbefala ein nettlesar av nyare dato.

3 Arkitekturperspektiv

3.1 Logisk

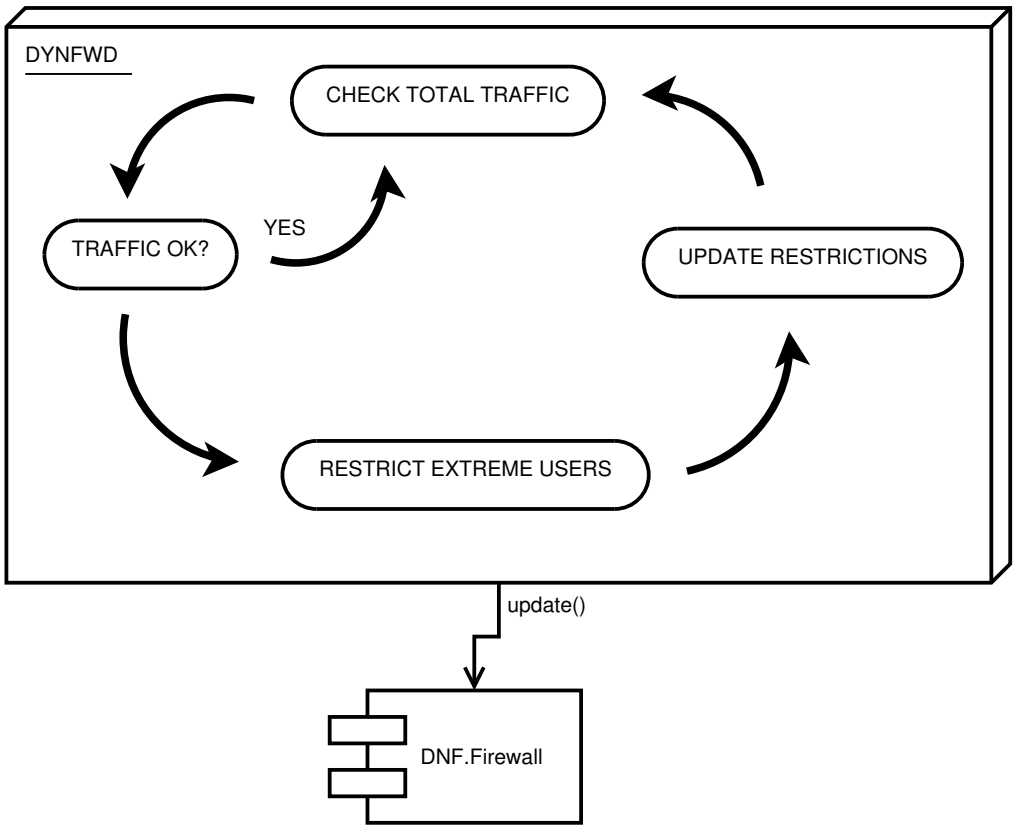


Figur 2: MVC-oppsett av systemet.

3.2 Prosess

3.2.1 Dynfw daemon

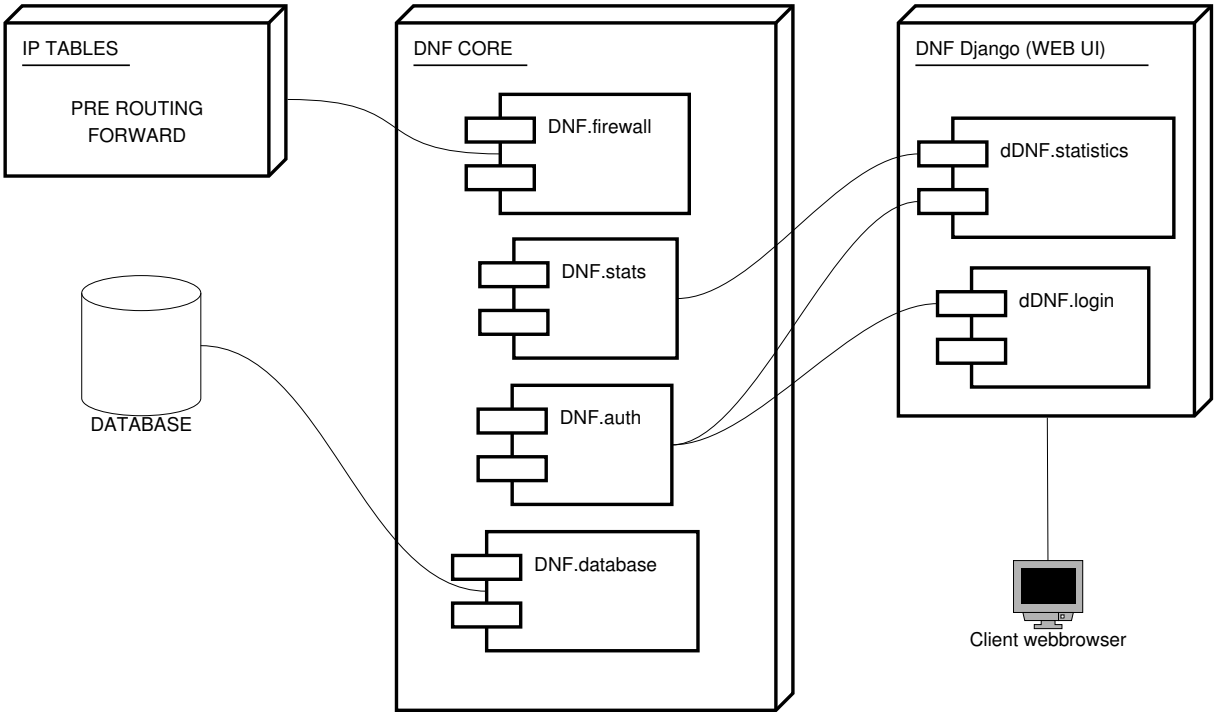
Dynfwd er ein tjeneste (deamon) som kjører i bakgrunnen og automatisk justerer brannmuren og vurderer om nokon av brukarane må avgrensast.



Figur 3: grov skisse over dynfwd si framferd

3.3 Implemetasjon

Vi kan seie at systemet har tre hovuddelar (sjå også figur 2). Figur 4 viser korleis programmvara vi har koda snakkar med dei andre komponentane når nokon nyttar webgrensesnittet. Det gir også ei oversikt over kva pakkar som har ansvar for dei forskjellige linux-komponentane som systemet samarbeider med. Det er verd å merke seg at den automatiske justeringa ikkje kjem til syne i figur 3.

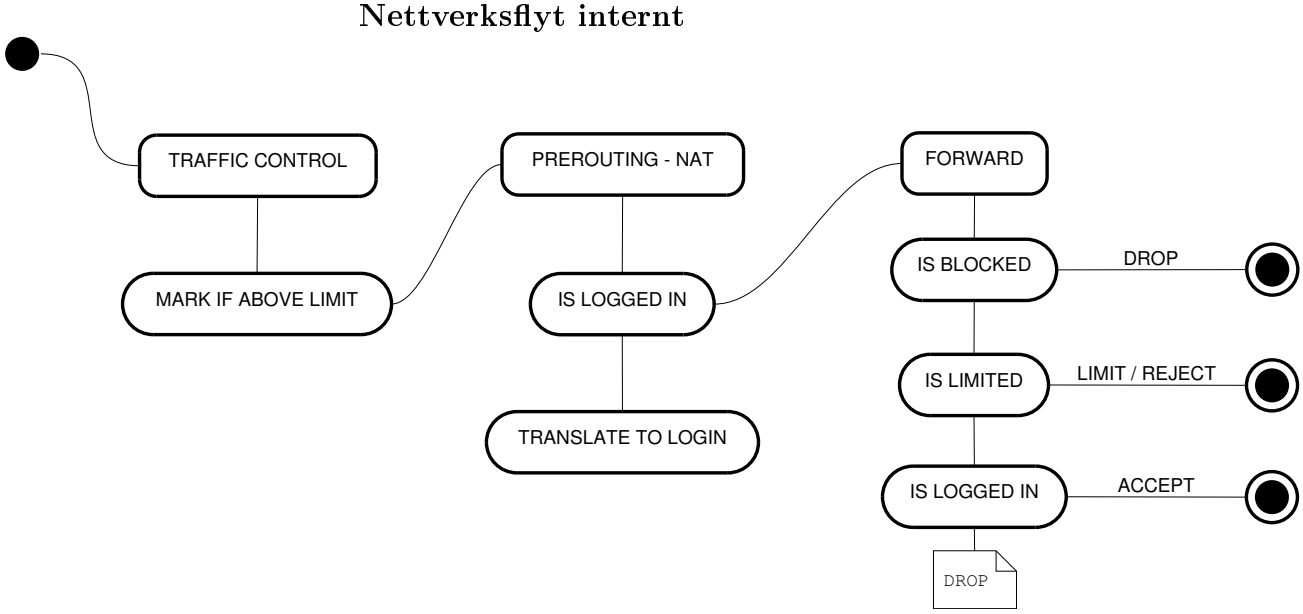


Figur 4: Implementasjonsperspektivet

3.4 Andre perspektiv

3.4.1 Nettverksbehandling

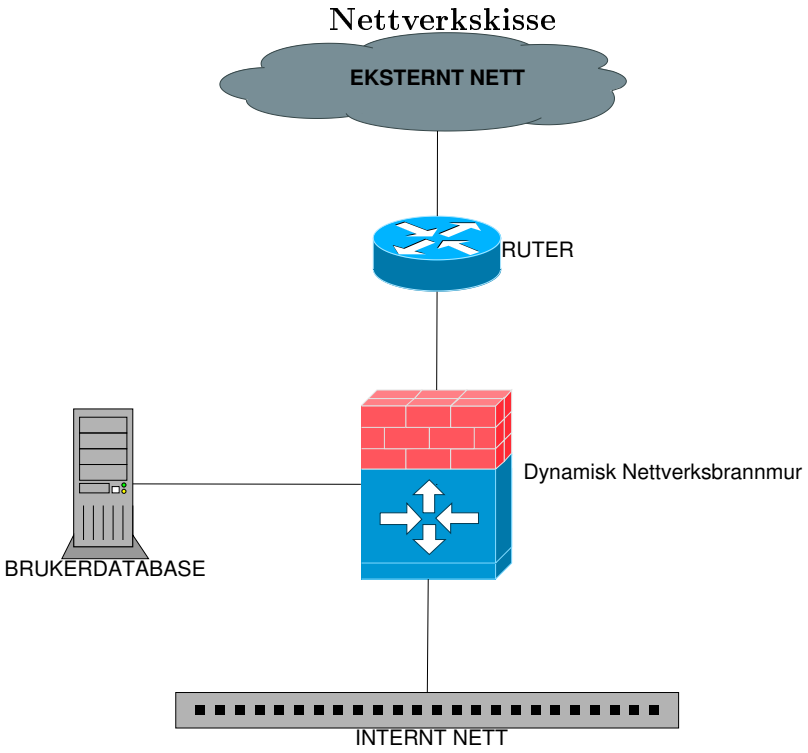
Figur 5 viser korleis trafikken blir behandla internt i systemet. Trafikken går først til linux si mekanisme «Traffic Control», der pakkar som bryt med eit gitt regelverk blir merka. Pakkar går så vidare inn i førruting-regelsettet i Iptables. Her blir det sjekka om ipadressa alt er registrert og logga inn. Om ipadressa ikkje er logga inn, blir trafikken fanga opp og omruta til ei påloggingside. Trafikken blir deretter sendt gjennom ei regelsettet for vidaresending, der det blir sjekka om nokon er svartelista, om trafikken er merka og om personen framleis er pålogga og aktiv.



Figur 5: Skisse over flyt gjennom brannmur

3.4.2 Systemet si plassering i nettverket

Nettverkskissa i figur 6 viser korleis nettverket *kan* settast opp. Det er ikkje naudsynt med ein ekstern brukardatabase, sjølv om det vil være naturleg å ha. Det er også fullt mogleg å ha all rutingfunksjon i same system som dette systemet.



Figur 6: Nettverkskisse