

1.5 Interne og Eksterne integrasjoner

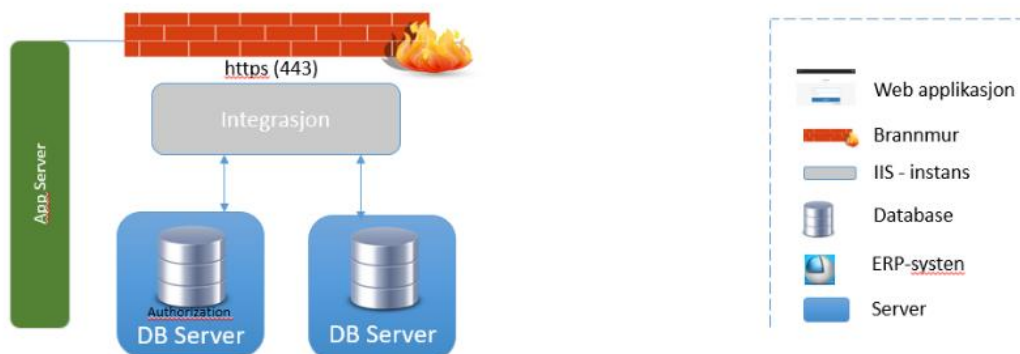
Overgang fra interne til eksterne integrasjoner, hvor trafikken går via internett, med tilhørende krav til sikkerhet

Interne integrasjoner

Hvis system som skal integreres står i samme drift/server-miljø, dvs på innsiden av brannmur, vil en kunne ha direkte tilgang til databasene eller API, uten å måtte ivareta sikkerhet og trafikk som kreves ved datatrafikk via internett. Hente/lese data fra SQL-baser fungerer bra, men skal en oppdatere bør det skje via integrasjonsgrensesnitt (API/Service-lag) som ivaretar forretningslogikk og versjoner av systemet.

Integrasjoner er installert lokalt, gjerne direkte mot databasen, er ofte svært sårbare, vanskelig å vedlikeholde og lite tilgjengelige. De er også lite ønskelig rent driftsmessig da det fordrer at utvikler eller integrert system har direkte tilgang til servermiljøet. Slike løsninger er gjerne lite standardisert og skaper avhengighet til utvikler eller tredjepart. Hva som skjer ved en oppgradering er usikkert, krever mye testing og integrasjonen kan fort bli glemt inntil løsningen stopper ved for eksempel en oppgradering.

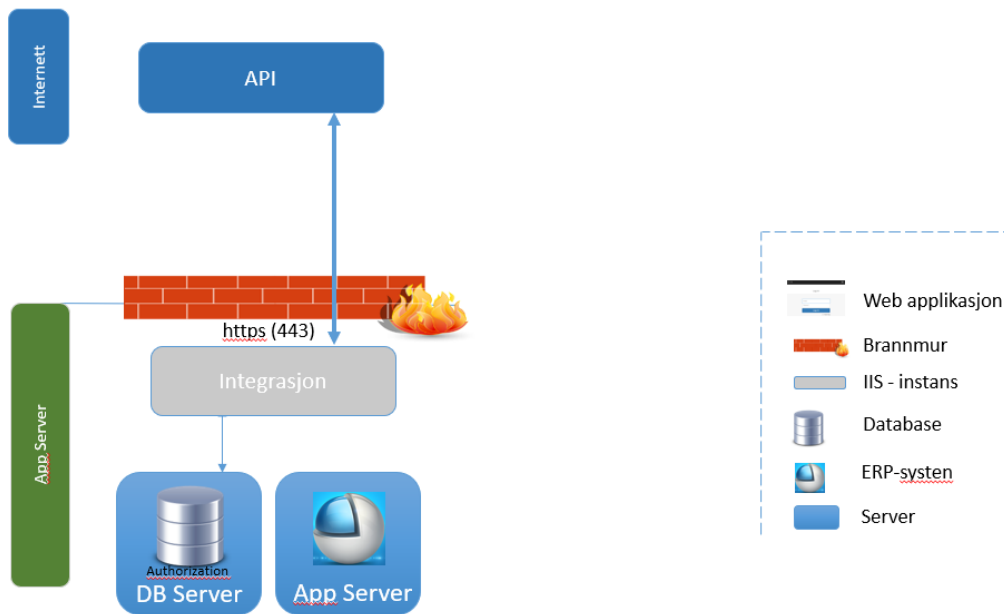
Intern



Internt mot eksternt

En mellomting mellom lokale løsninger på serveren og API-baserte løsninger, er at integrasjonen er basert på et program som kjører repeterende internt på serveren, koblet til eksternt API. Også betegnet som «*snurre på innsiden*». Programmet leser og skriver da direkte mot vertssystemet, mens koblingen mot eksternt integrert system går direkte mot et tilgjengelig API via internett. Programmer av denne typen, plassert sammen med applikasjon/database, blir mindre og mindre aktuelle ettersom applikasjoner og API-er blir skybaserte (nå kun via Internett). Løsningen vil ha mye av de samme svakhetene som rene interne integrasjoner.

Intern - Ekstern



Eksterne integrasjoner

Digitale telelinjer (ISDN) og etter hvert Internett åpnet muligheter for at applikasjoner i prinsippet kan ligge hvor som helst, hvor brukergrensesnittet enten da nås via WEB-grensesnitt eller via Terminalserver («Citrix»). Det samme gjelder integrasjonsgrensesnitt, hvor API (soup/rest) er å regne som standard. Skal du lage eller sette opp integrasjon mot eksisterende API, trenger du som utvikler stort sett bare endpoint (url), brukernavn og passord. Trafikken går normalt kryptert (https) via web-server eller proxy, men kan i tillegg sikres med en lukket ende til ende kobling vi kaller VPN ([virtual privat network](#)).

Sikkerhetsmessig vil en fil eller meldingsbasert integrasjonen i prinsippet bli det samme, hvor meldinger og filer sendes via samme infrastruktur, men må da behandles i en avsender/mottaker-mottaker applikasjon som skal eksportere eller importere dataene til eller fra ekstern kilde.

Applikasjoner og databaser som er lagret på tilgjengelige servermiljø, hos kunden eller driftsleverandør, kalles «On Premis System» eller «OnPrem». API er da også lagret på lokal server sammen med applikasjonen, men kan da nås på tilsvarende måte som API for rene Skybaserte system hvor hele løsningen ligger hos systemleverandør. Selv om systemene gradvis blir skybaserte, vil vi av ulike årsaker oppleve at OnPrem-løsningene har lang levetid, selv med Windows-baserte grensesnitt vs WEB-basert.

Server-arkitektur og sikkerhet for «OnPrem» er beskrevet i [kap x.x](#)

Ekstern - Reversed Proxy

