

Kapittel 6: Nettverkssikkerhet

Cybersikkerhet: Teknologier og styring
Audun Jøsang
3. utg. 2025
Universitetsforlaget

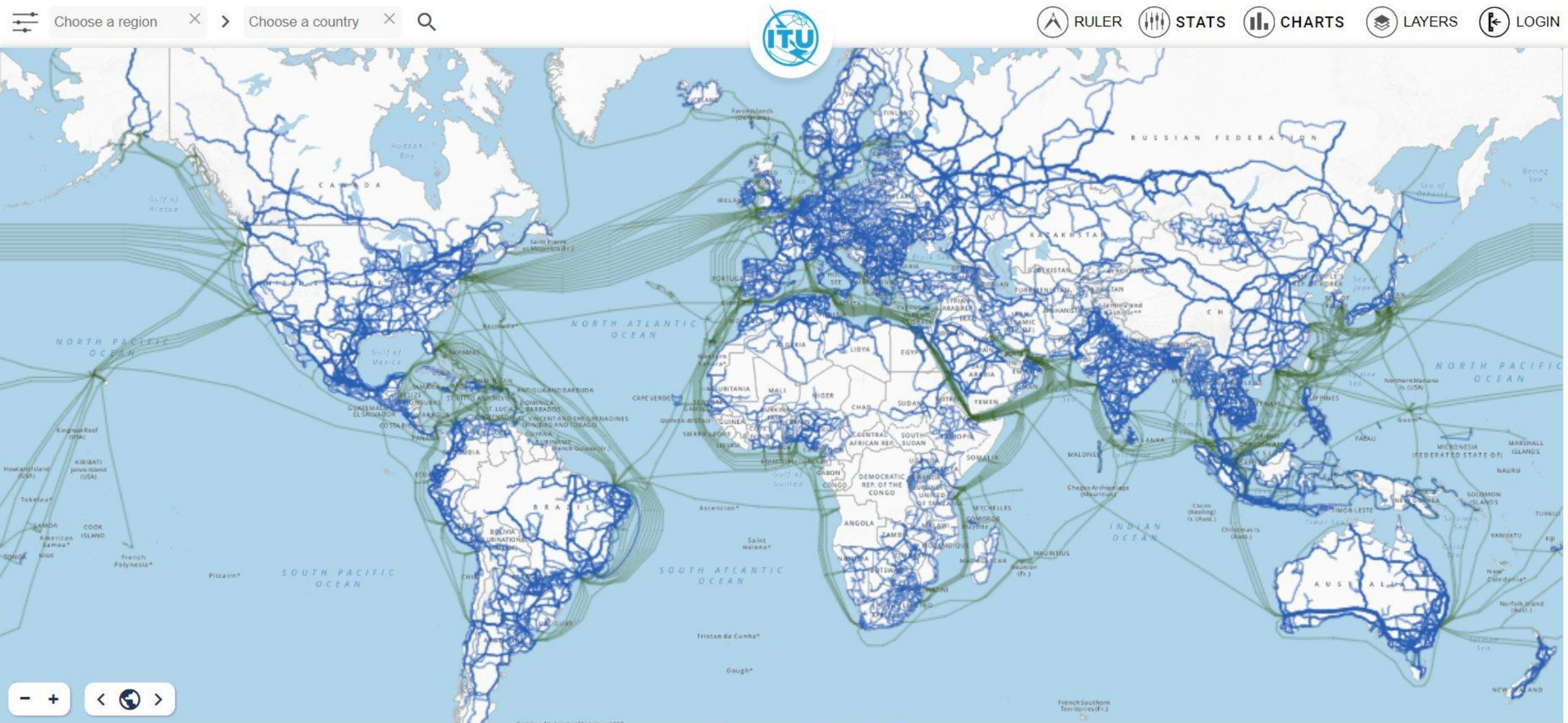


Oversikt

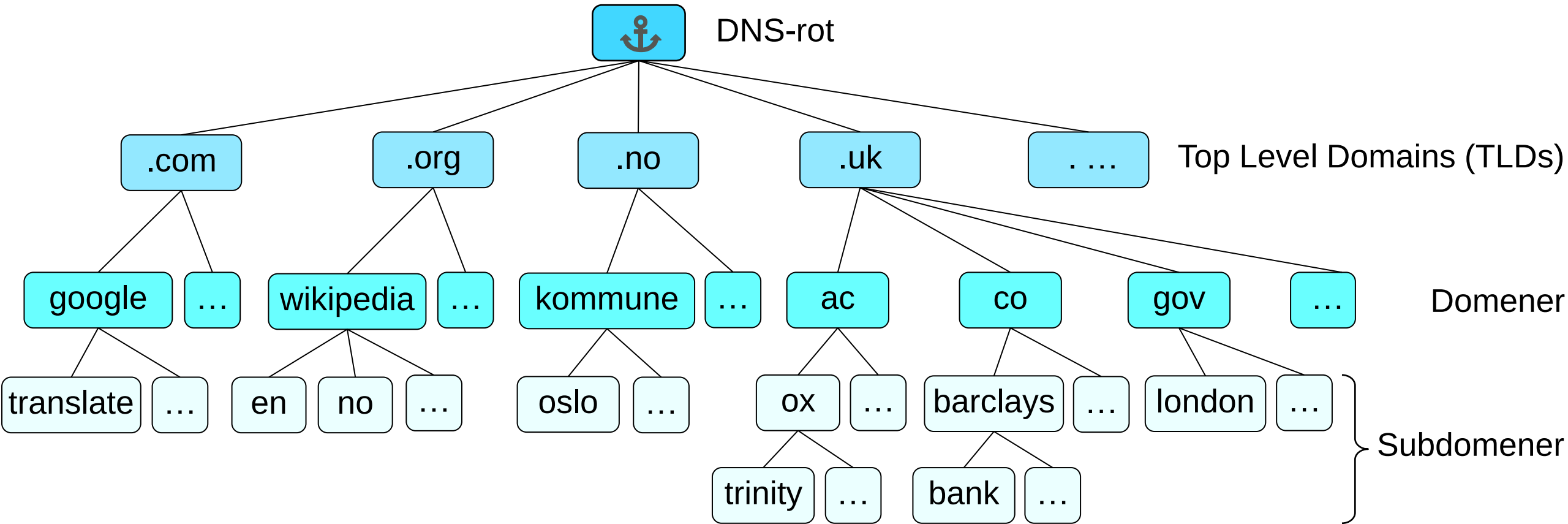
- Internett
 - Strukturen av internett
 - Internettstacken
- Kommunikasjonssikkerhet
 - TLS (Transport Layer Security)
 - IPSec (IP Layer Security)
- Dat넷tsikkerhet
 - Brannmurer
 - Inntrengningsdeteksjon
 - HSTS – HTTP Strict Transport Security
 - TLS-inspeksjon

Det fysiske internett

<https://bbmaps.itu.int/products>



DNS: The Domain Name System



Domenenavn og IP-adresser

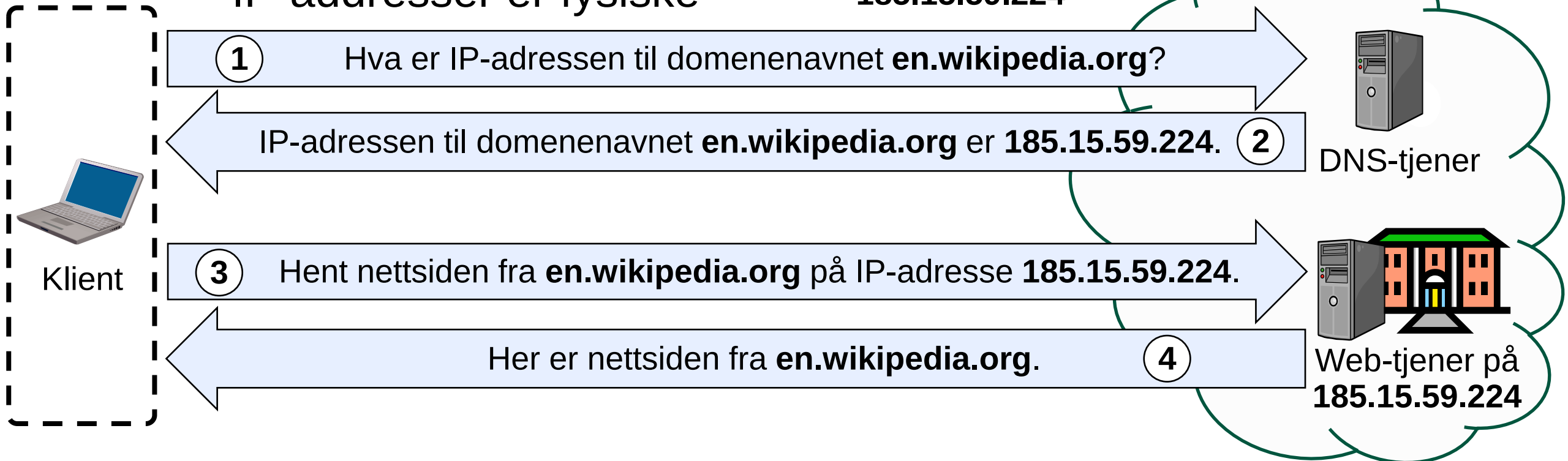
- Domenenavn er virtuelle

en.wikipedia.org

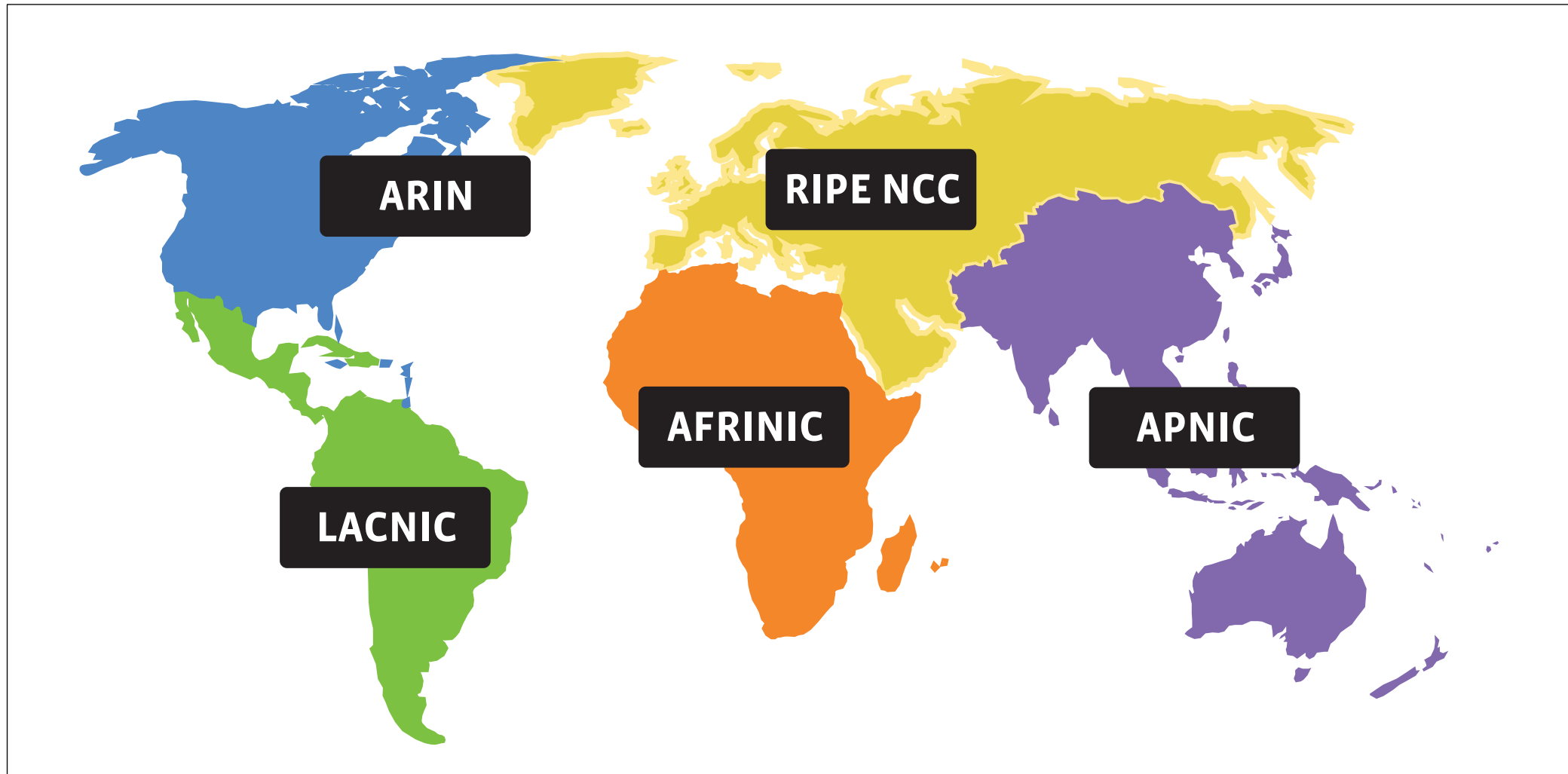
Oversettelse

185.15.59.224

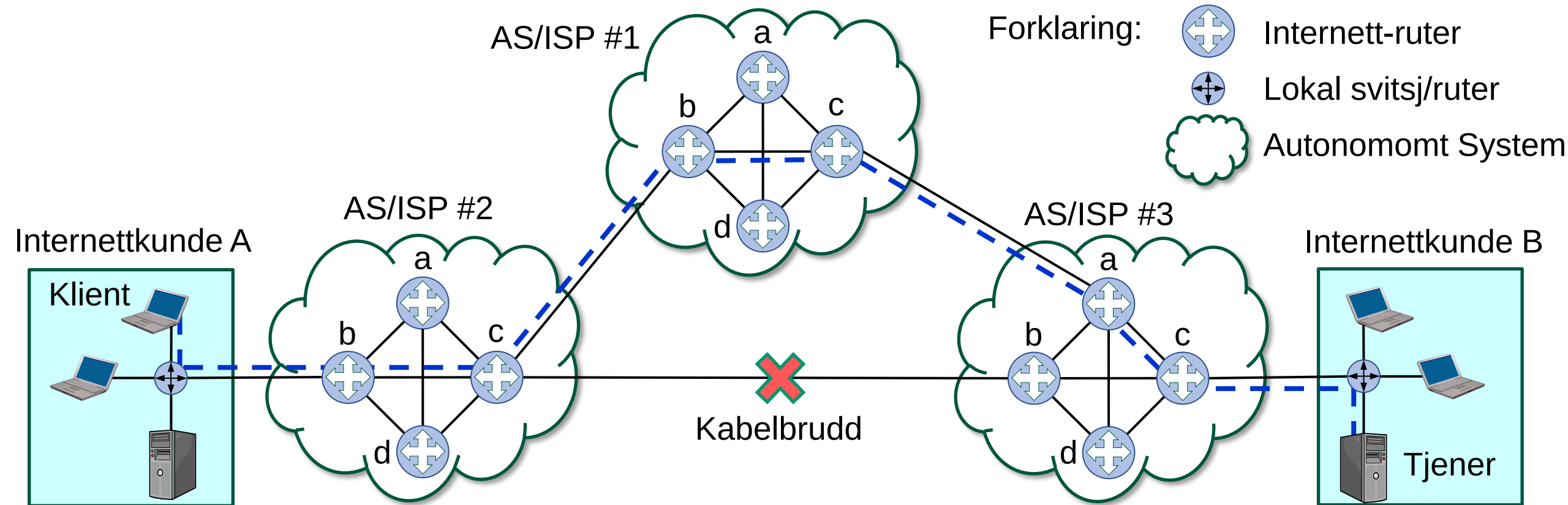
- IP-adresser er fysiske



Global fordeling av IP-adresser



Internettrouting

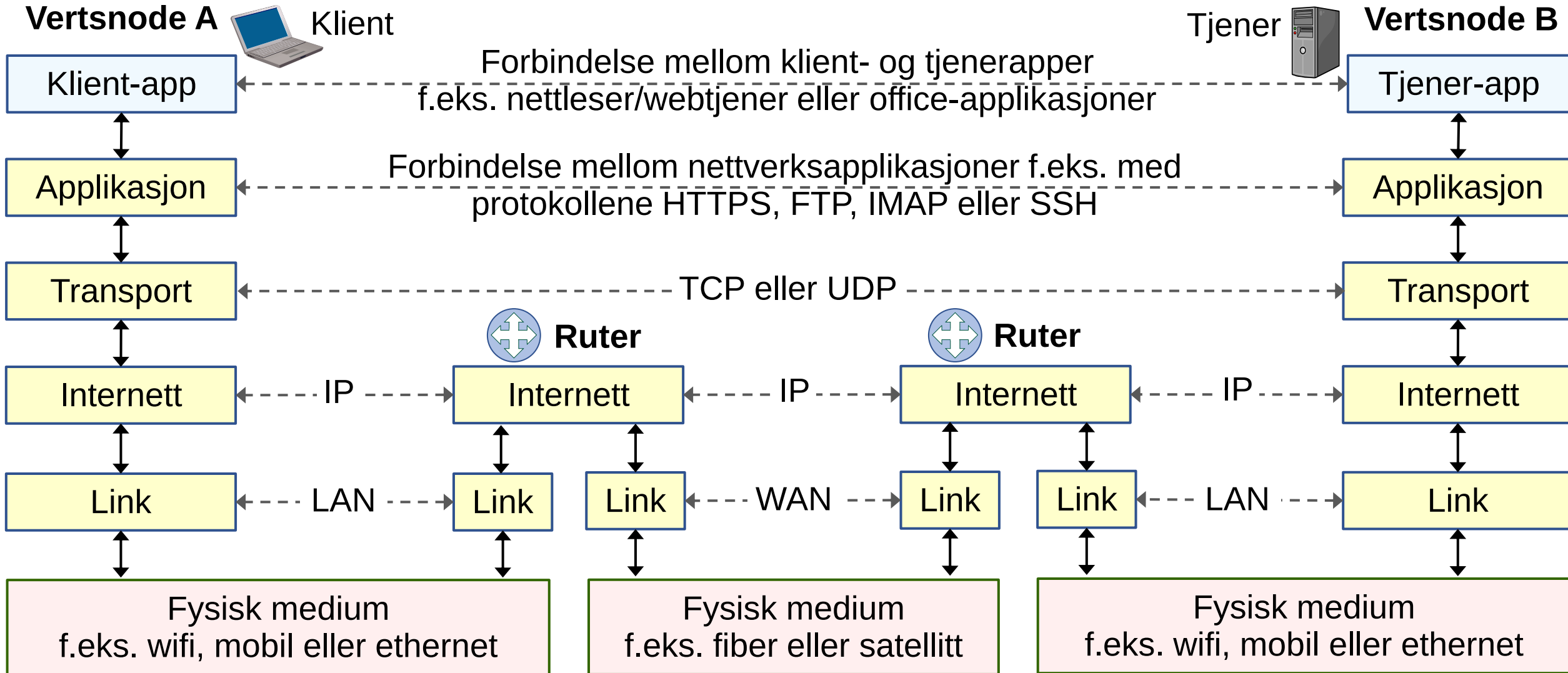


Internettkommunikasjon

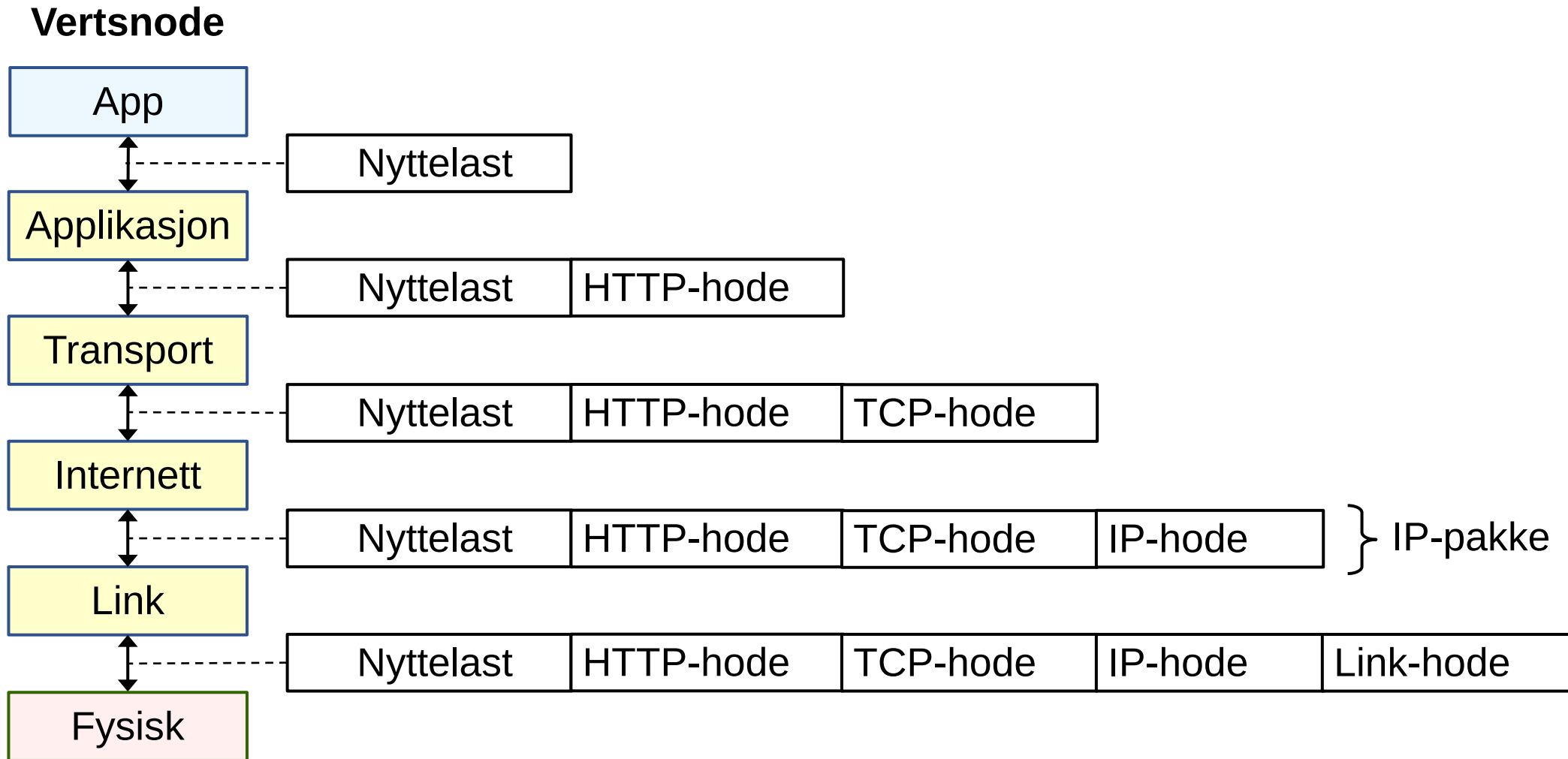
Forklaring:

↕ Grensesnitt innen same node

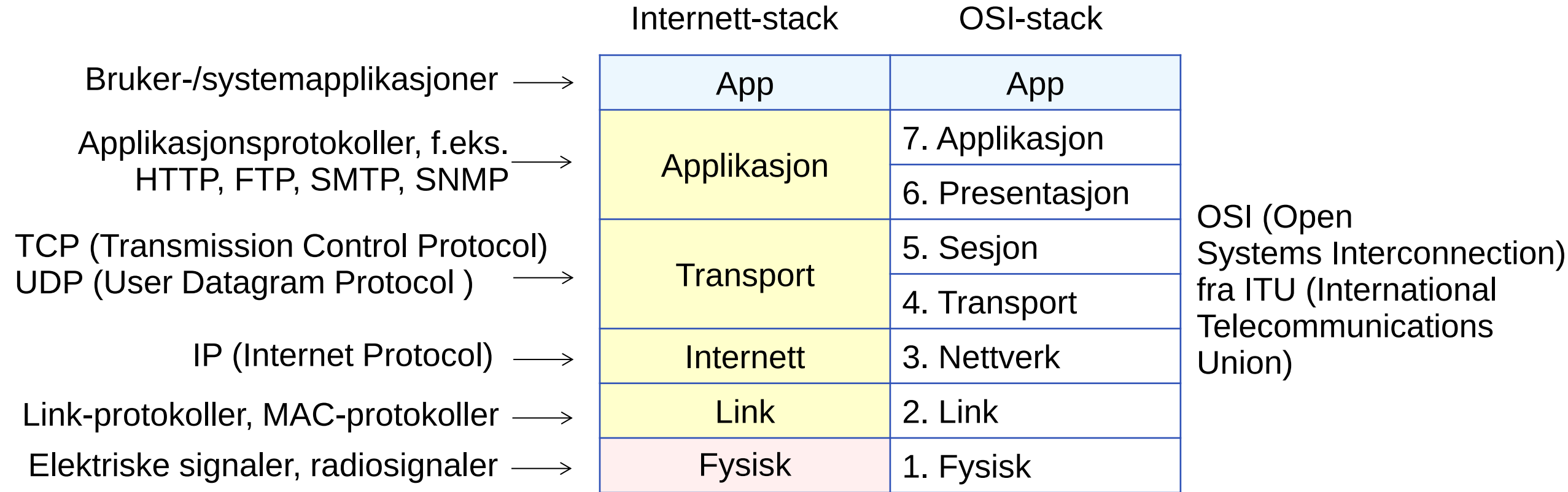
←---→ Virtuell forbindelse gjennom nettverk



Datapakker i protokollstakken

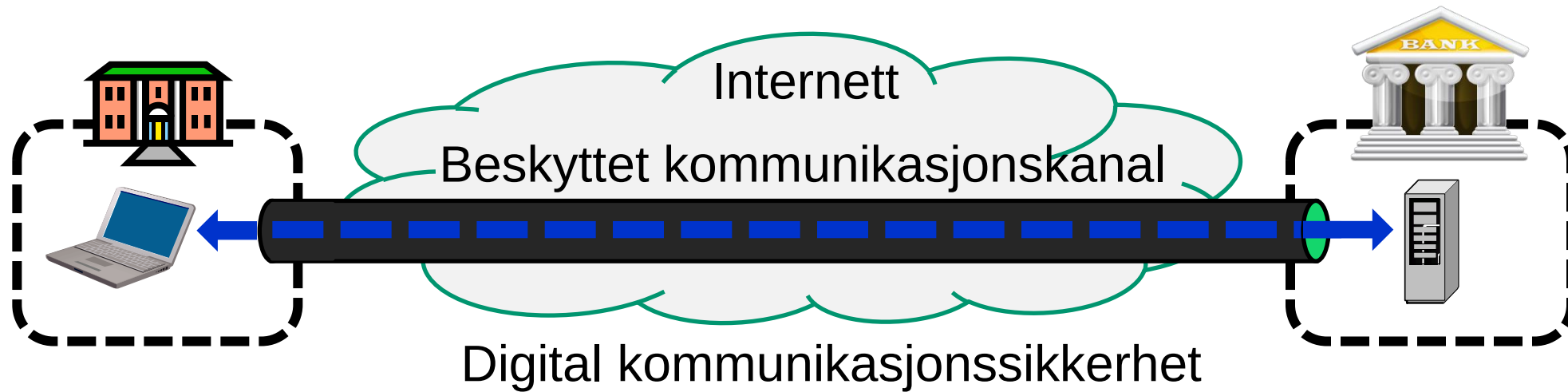


Protokollstakk i internett og tilsvarende i OSI



- OSI var en konkurrent til internett i perioden 1985-1995, men internett vant til slutt

Analogi: Transport og kommunikasjonssikkerhet



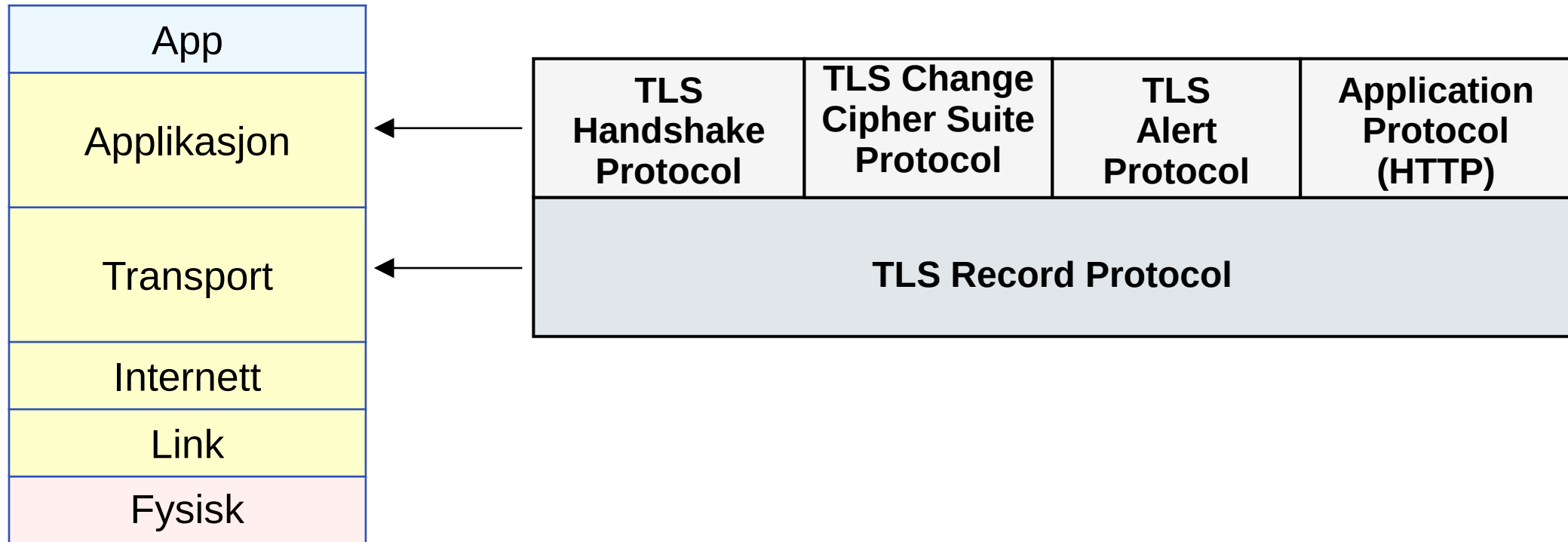
Sikkerhetsprotokoller

- Mange forskjellige sikkerhetsprotokoller for forskjellige formål
 - autentisering, integritet, konfidensialitet
 - nøkkelutveksling
 - e-valg
- Eksempler: TLS og IPSEC
- Sikkerhetsprotokoller er overraskende vanskelig å designe uten sårbarheter!
 - Mange sårbarheter oppdages år senere
 - ... noen blir aldri oppdaget (eller kanskje bare av angriperne)

TLS: Transport Layer Security

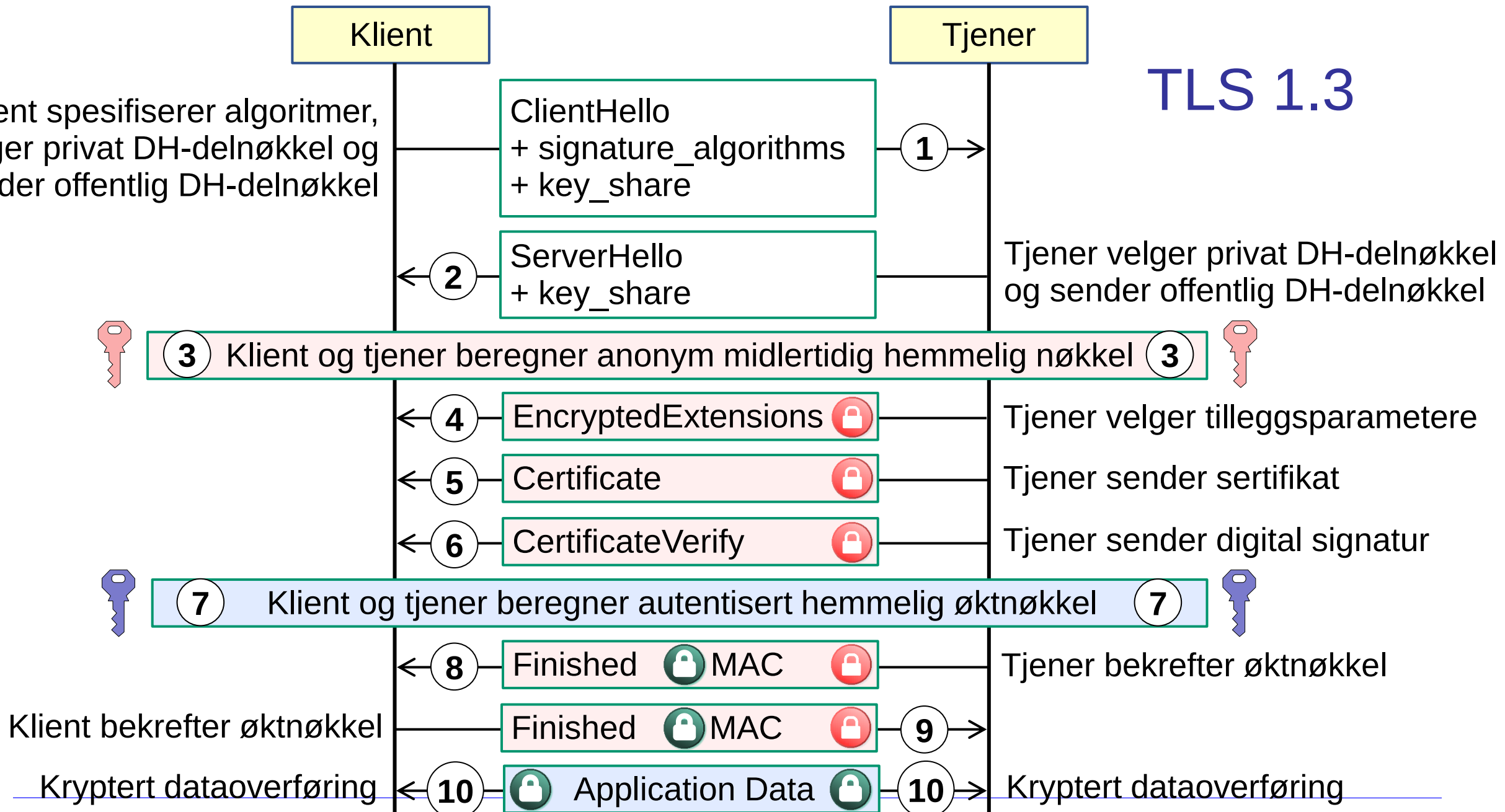
Tidligere kalt SSL (Secure Sockets Layer)

TLS i internettstakken

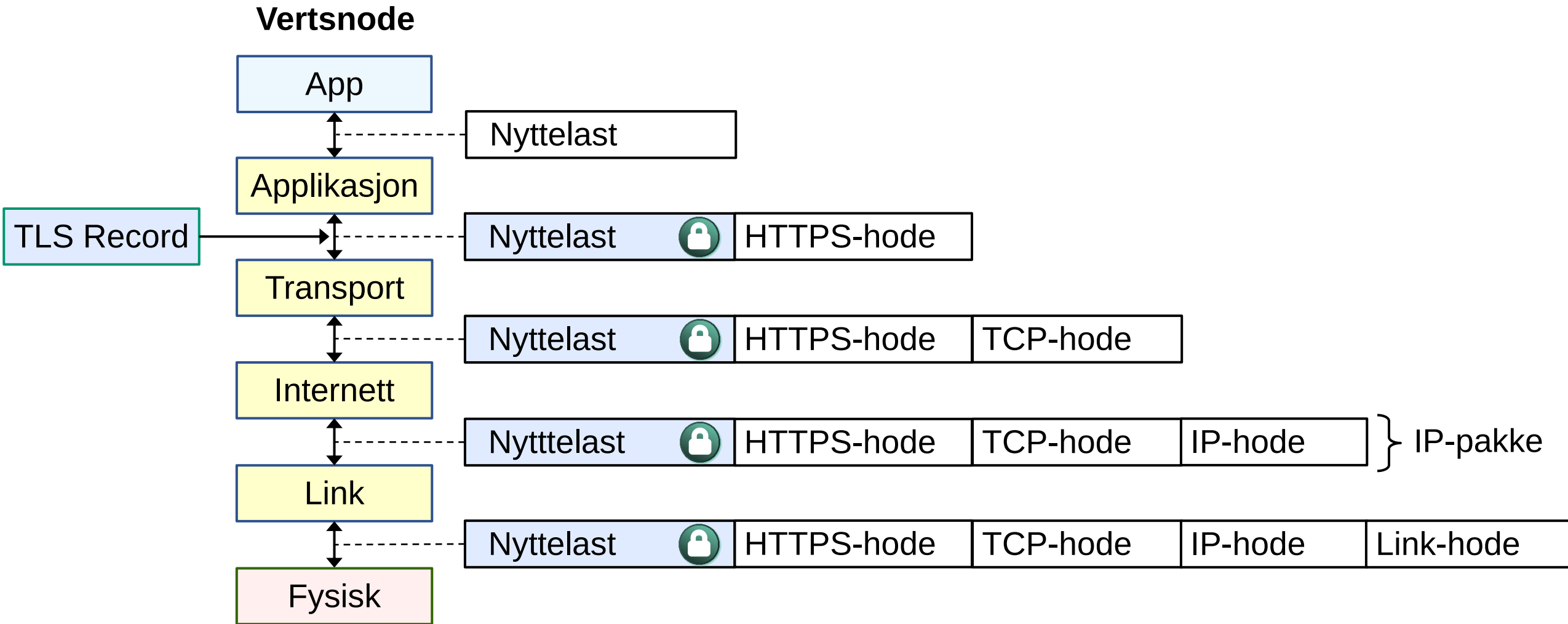


- TLS består egentlig av et sett med protokoller for ulike trinn i økten

TLS 1.3



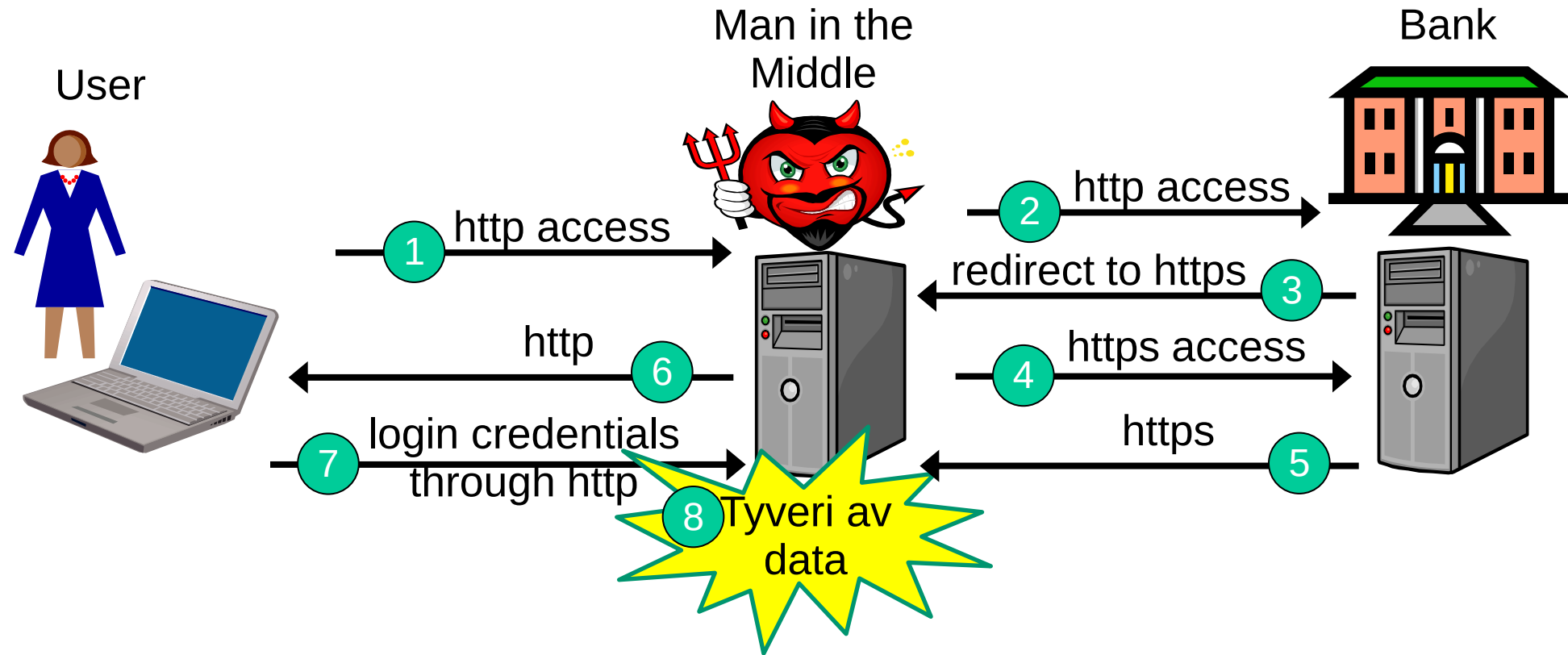
Kryptering av brukerdata med TLS



TLS 1.3

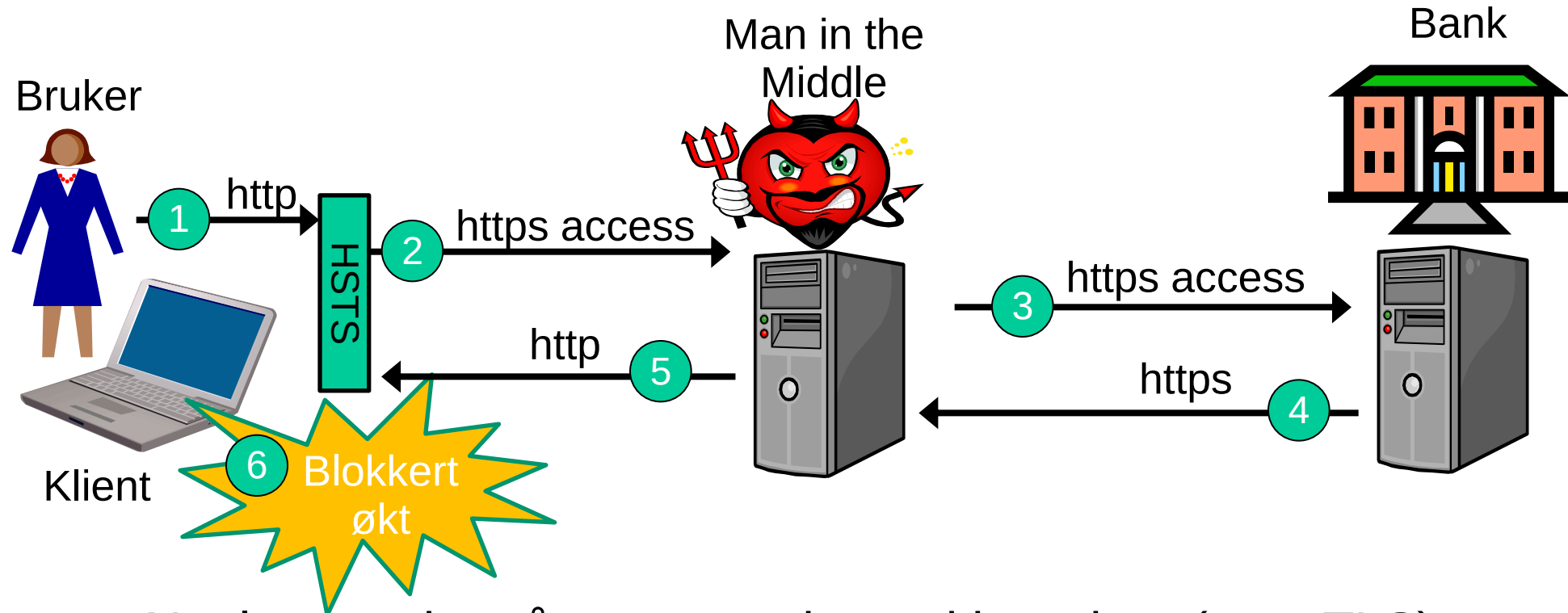
- Designet for hurtighet i etableringen av øktnøkkel
- Trenger kun én meldingsrunde (frem og tilbake) for å etablere øktnøkkel
- Perfekt fremoverhemmelighold (eng.: perfect forward secrecy) betyr at tidligere øktnøkler forblir hemmelige (ikke blir kompromittert) selv om en langsiktig kryptonøkkel blir kompromittert/lekket en gang i fremtiden.
- I TLS er tjenerens private signeringsnøkkel langsiktig.
- Kompromittering av tjeners private nøkkel medføre brudd på autentisitet av tjener fra tidspunktet for kompromittering, som er alvorlig nok.
- Perfekt fremoverhemmelighold oppnås ved bruk av Diffie-Hellman.

Angrep med TLS-stripping



- Det fins forskjellige varianter av TLS-stripping

HSTS for å hindre TLS-stripping



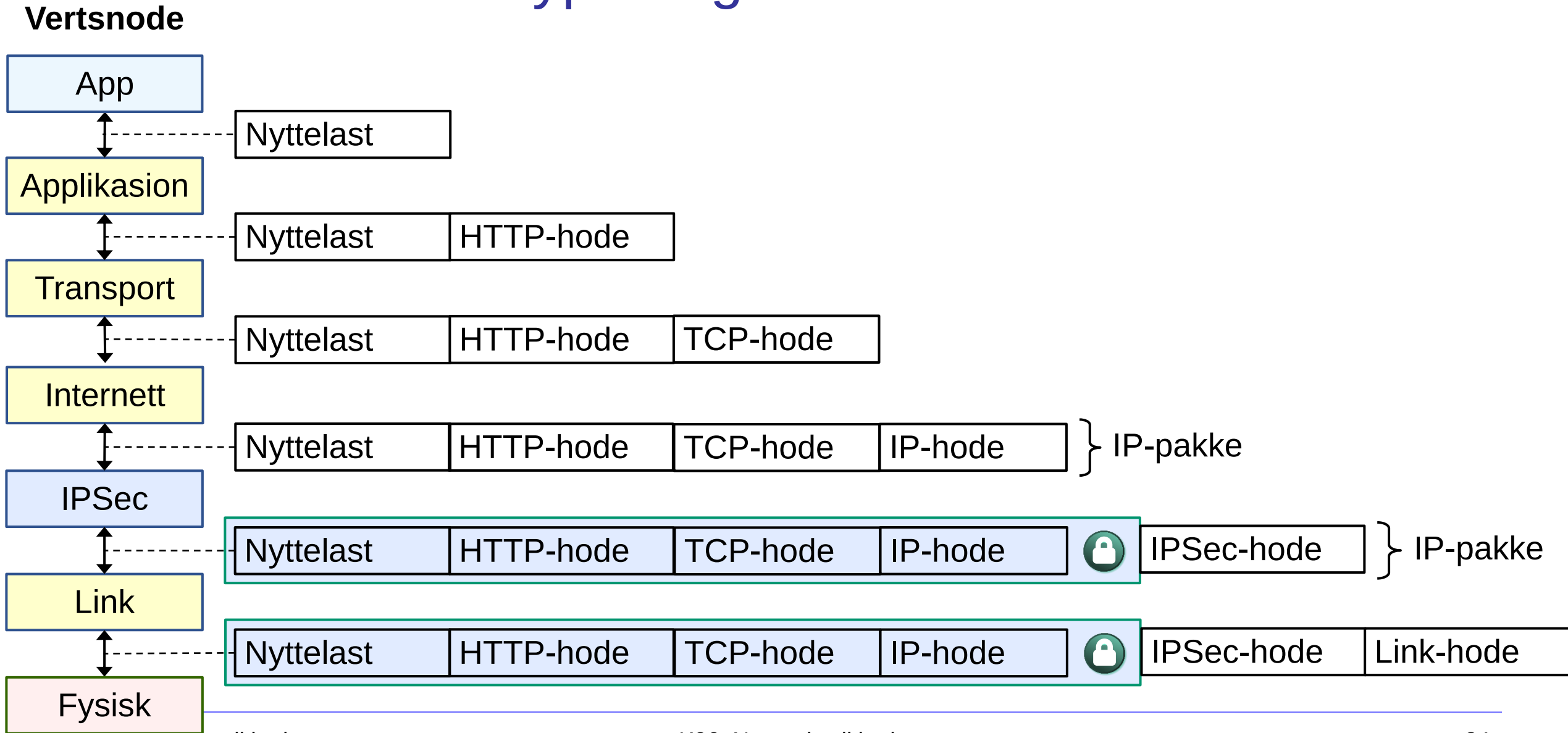
- Nettleser nekter å opprette økt med bare http (uten TLS)
- Nettleser krever https (med TLS)

IP Security

IPSec

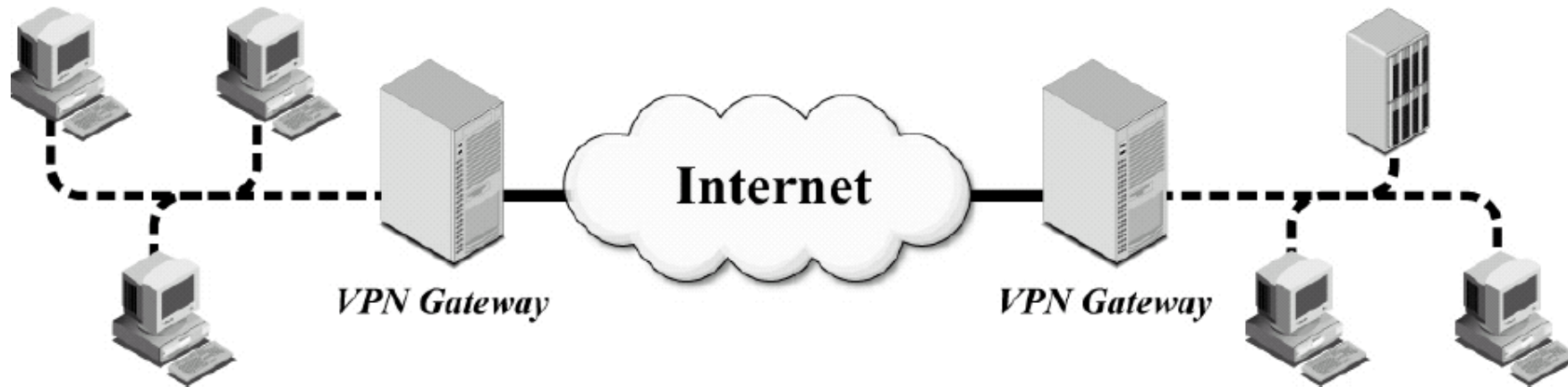
- Internettprotokollsikkerhet (IPSec) er standard for sikker kommunikasjon over internettprotokollen (IP-laget)
 - ved bruk av kryptografiske sikkerhetstjenester.
- Bruker kryptering, autentisering og protokoller for nøkkelutveksling
- Basert på en ende-til-ende-sikkerhetsmodell på IP-laget
- Konfigureres på OS-nivå, ikke i applikasjoner.

Kryptering av brukerdata med IPSec



IPSec:

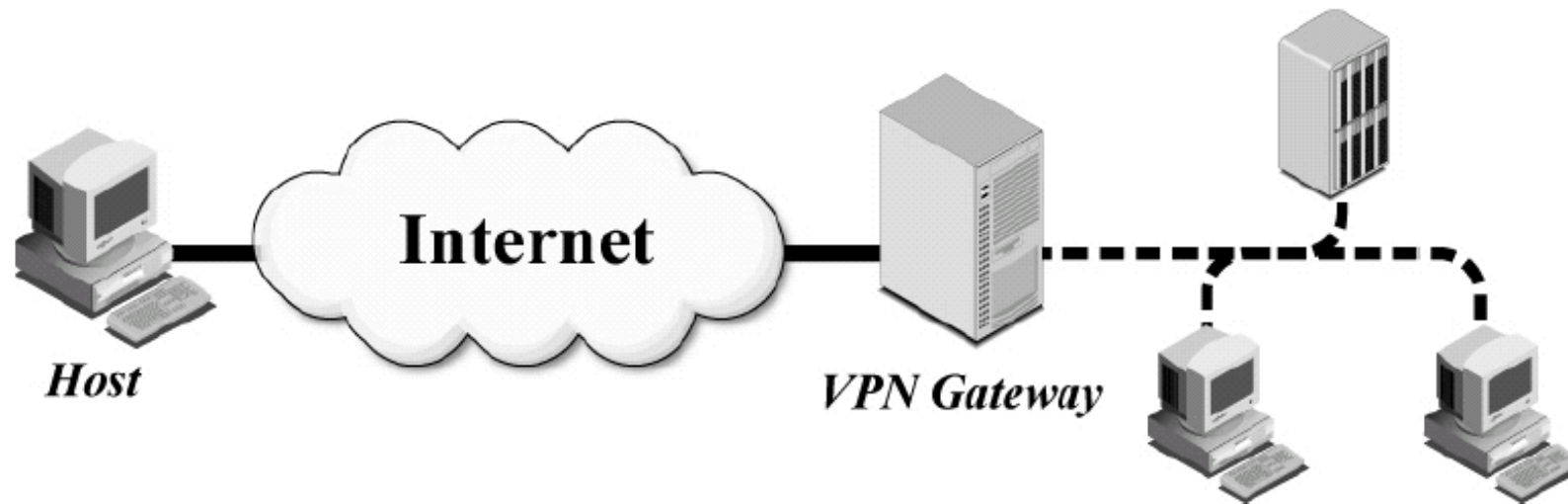
Gateway-to-Gateway Architecture



Source: NIST Special Publication 800-77

IPSec:

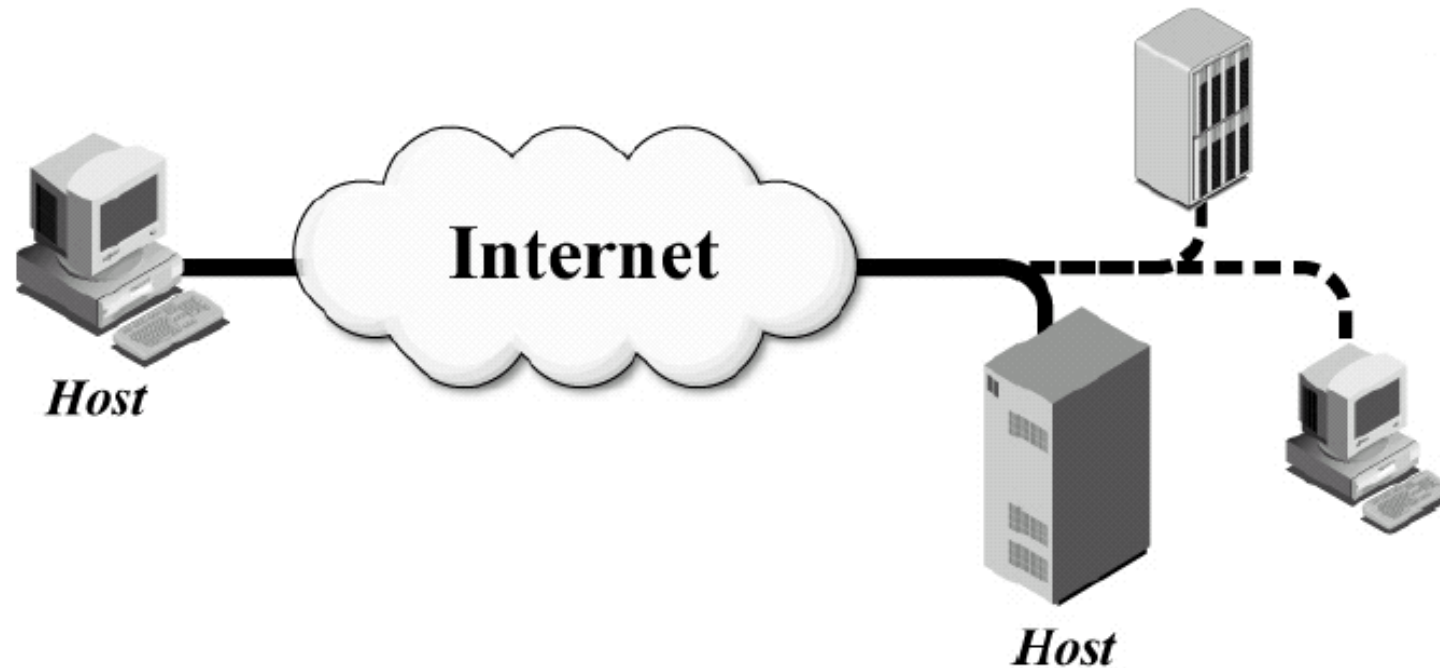
Host-to-Gateway Architecture



Source: NIST Special Publication 800-77

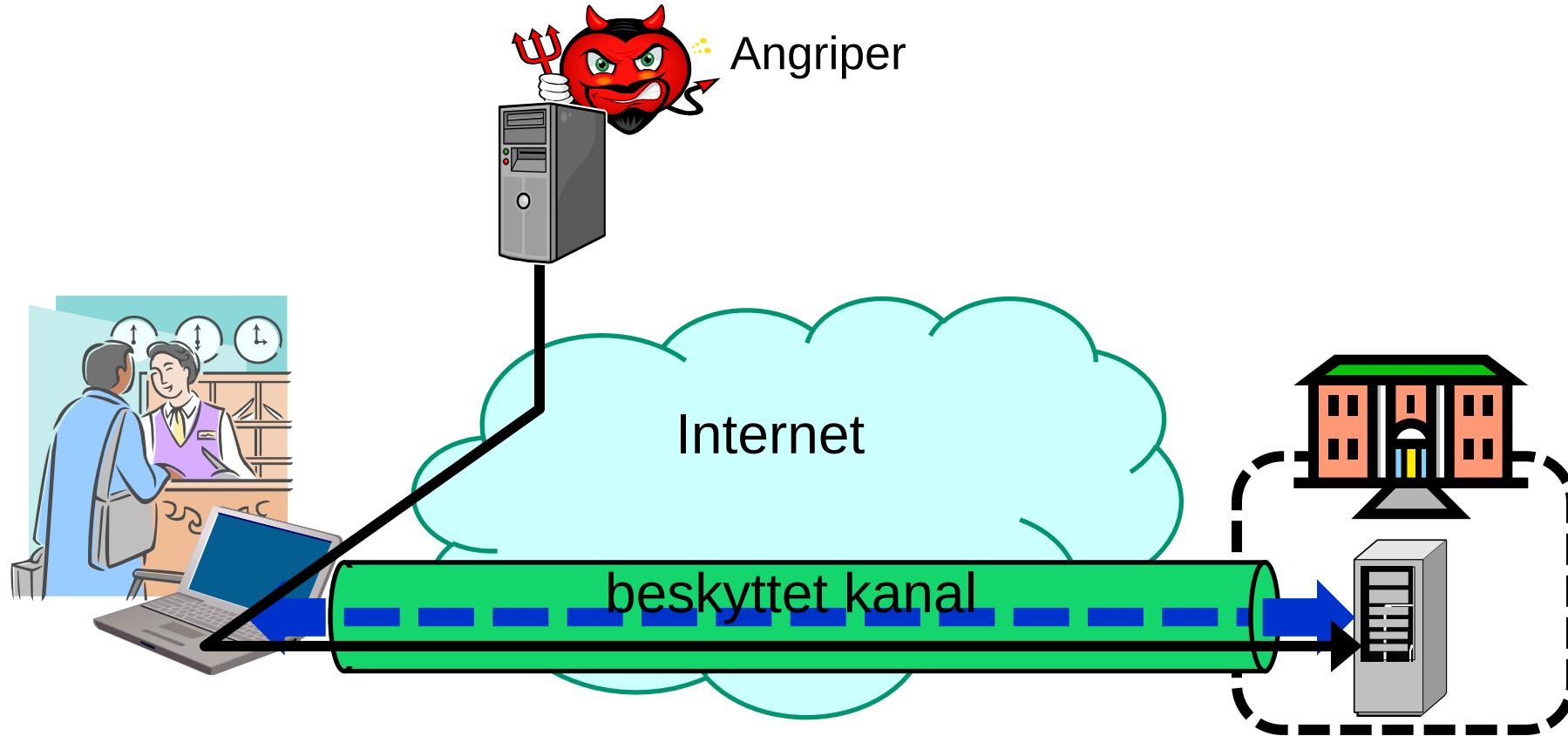
IPSec:

Host-to-Host Architecture



Source: NIST Special Publication 800-77

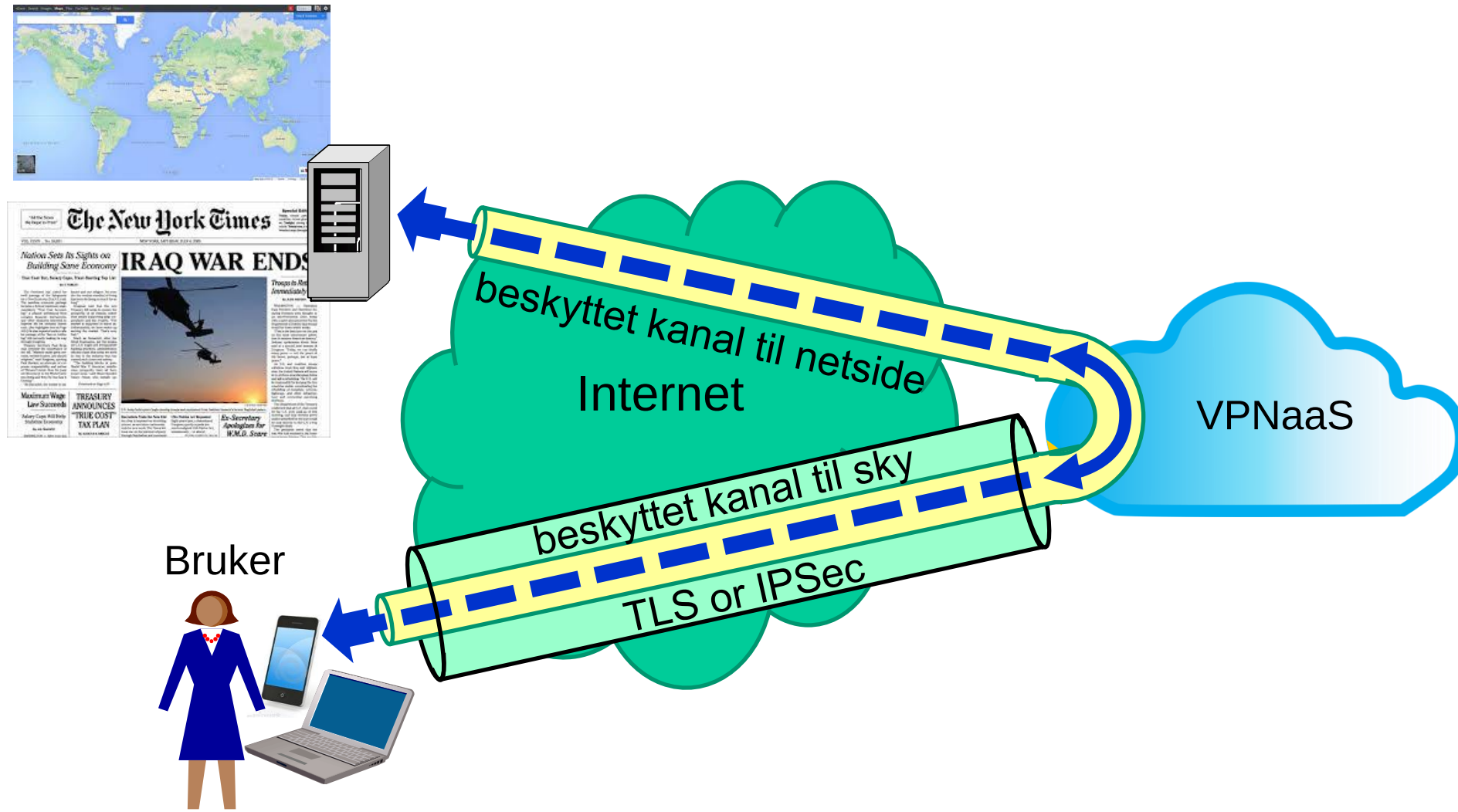
VPN for tilgang til hjemme-datanett



Mulig angrepsvektor gjennom ekstern enhet

Internett-
tjeneste

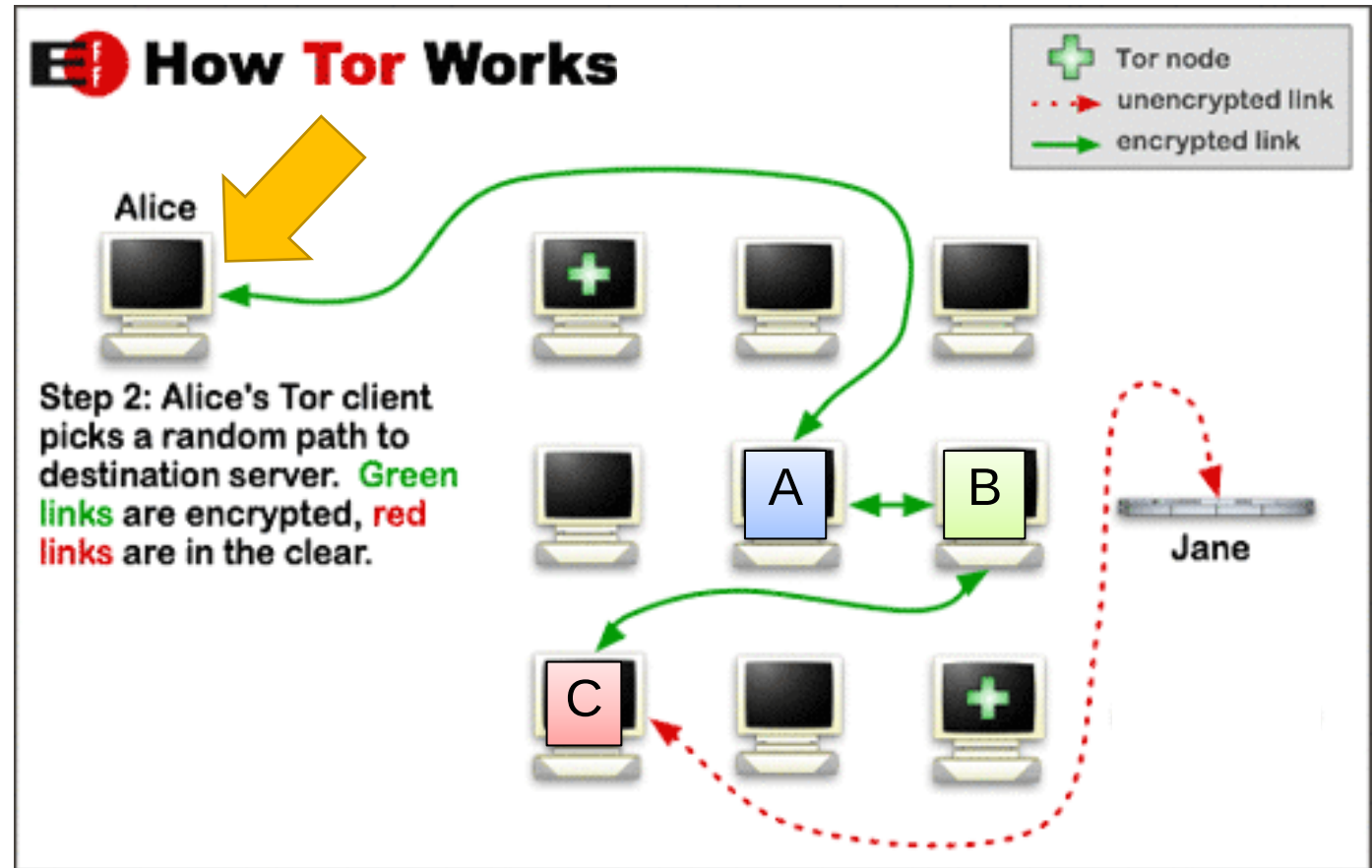
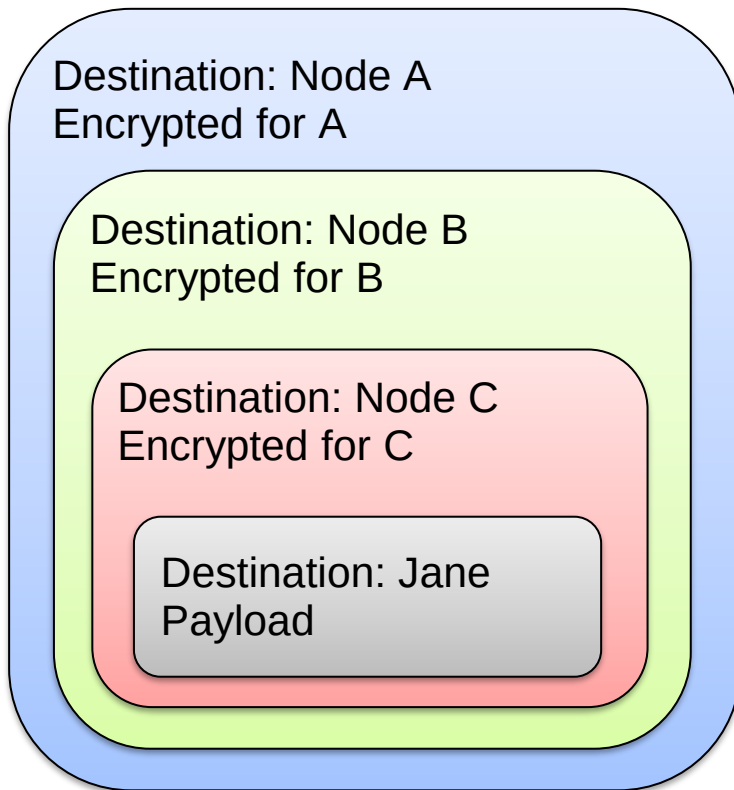
Sky-VPN



Tor (The onion router – løkruting)

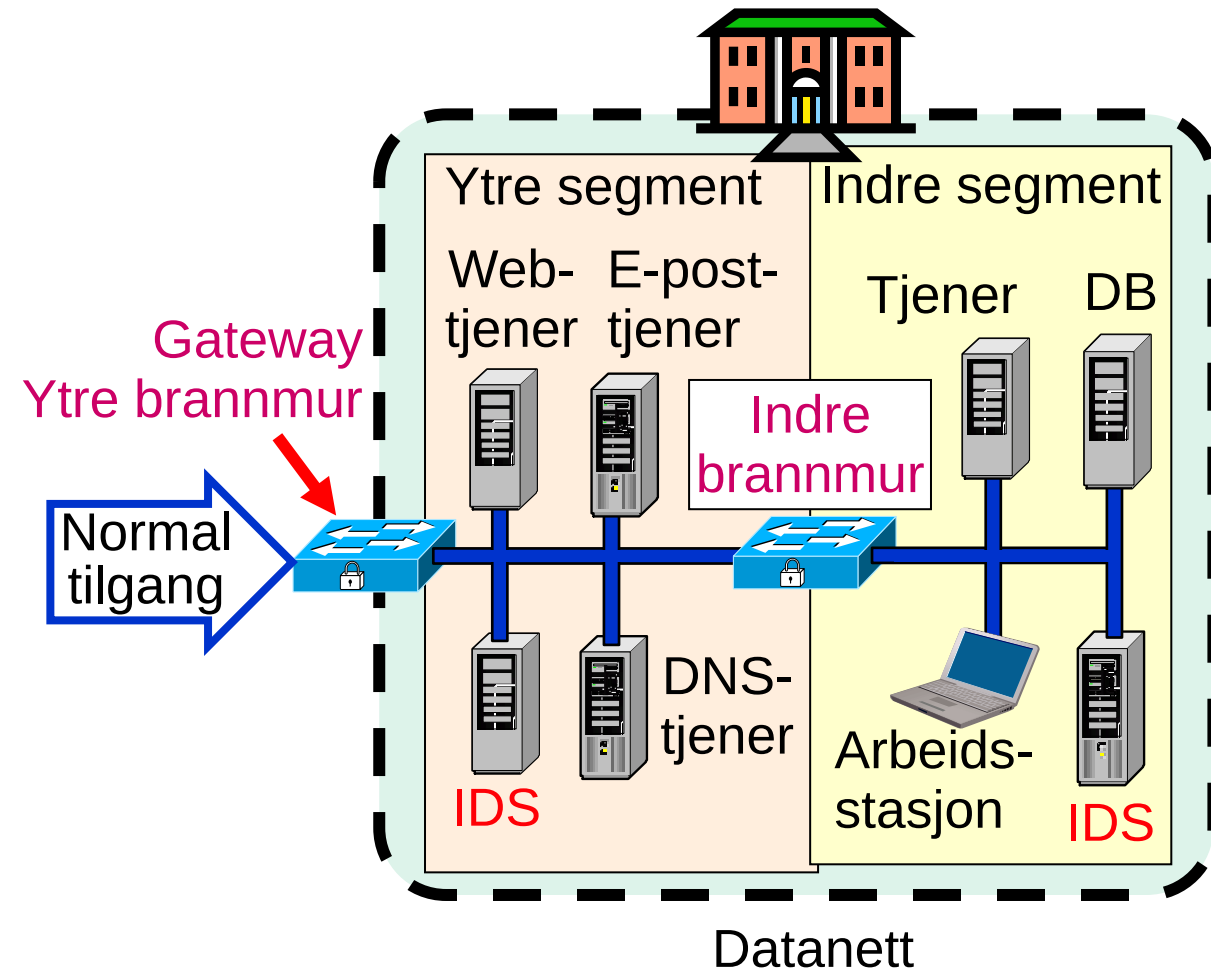
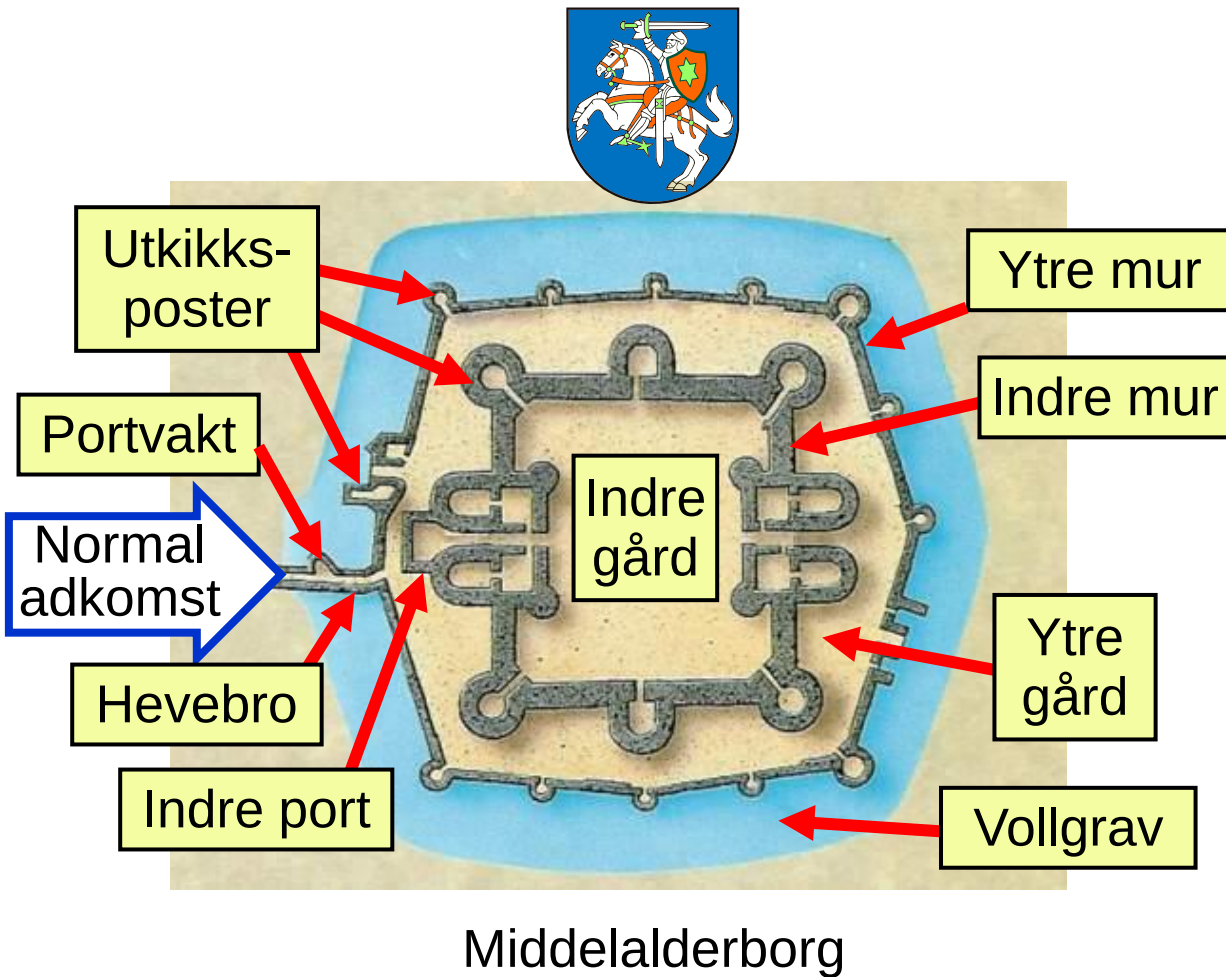


- VPN som benytter 3 enkelte VPN-forbindelser som ligger utenpå hverandre



Datanettsikkerhet

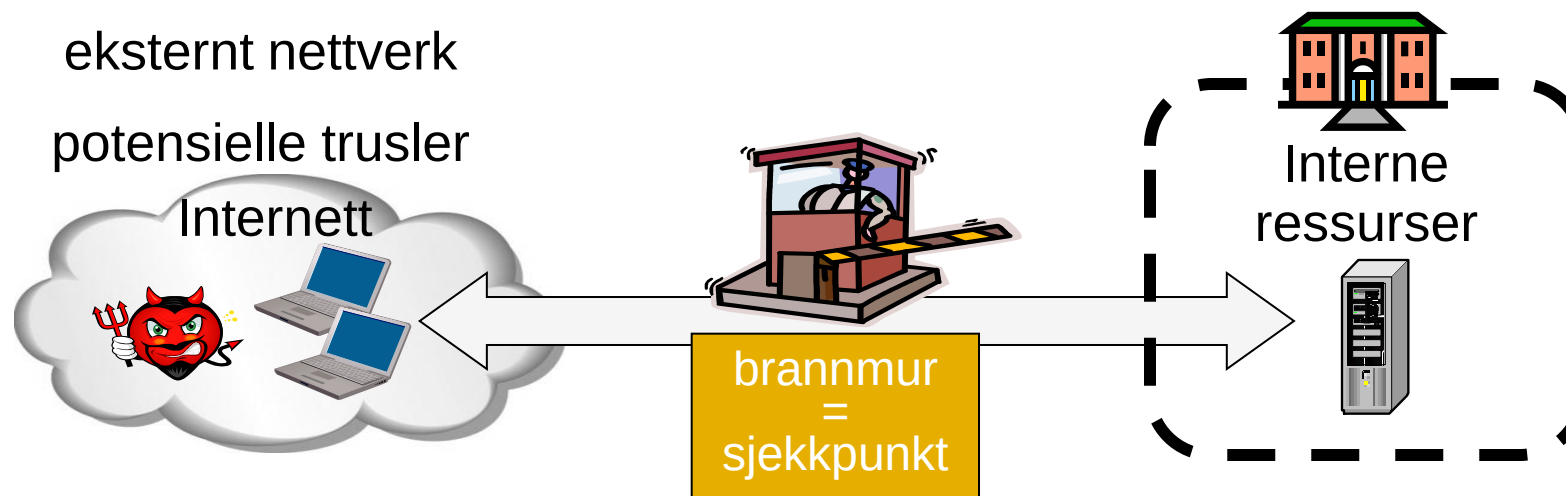
Analogi: Middelalderborg og datanett



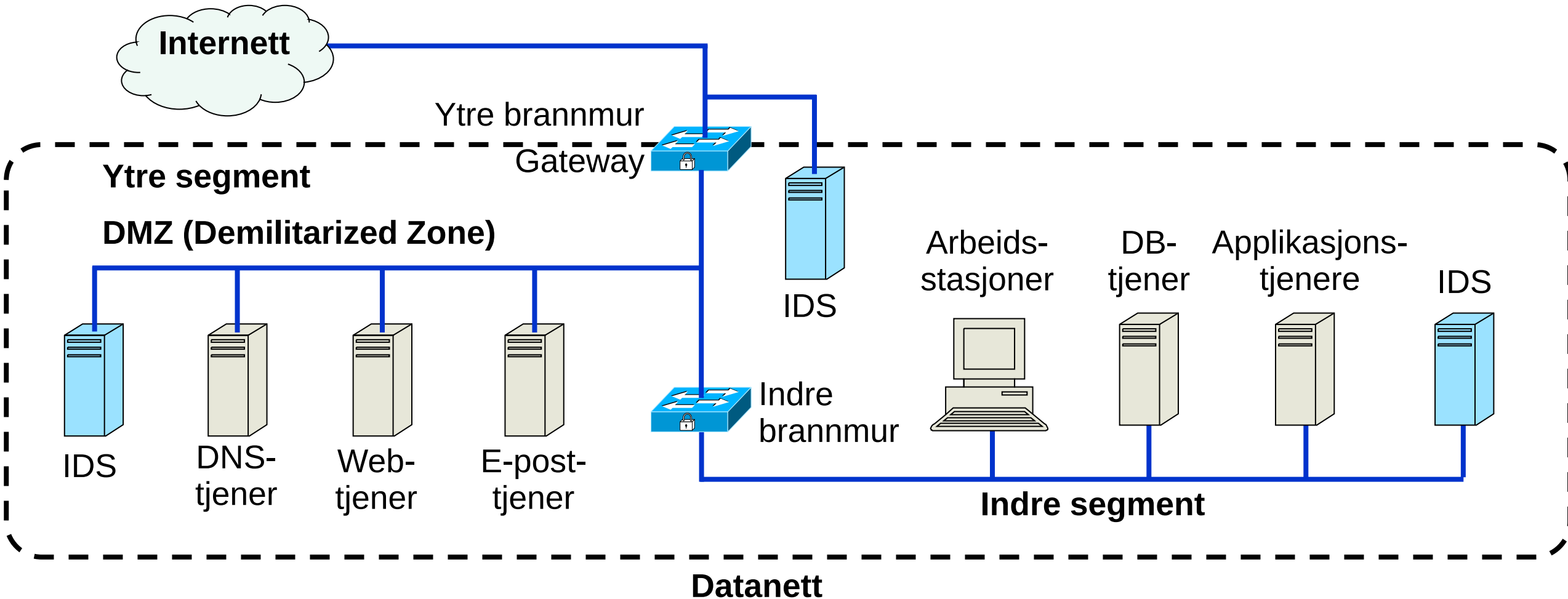
Brannmurer

Datanettsikkerhet med brannmur

- En brannmur er et sjekkpunkt som beskytter de interne nettverkene mot angrep fra eksterne nettverk (internett)
- Sjekkpunktet bestemmer hvilken trafikk som kan passere inn og ut basert på regler



Enkel datanettarkitektur med brannmurer



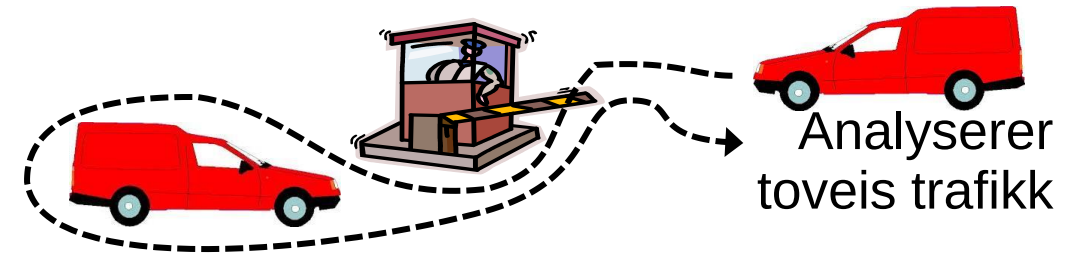
Tilstandsløse brannmurer



Inspiserer bare
pakkehoder

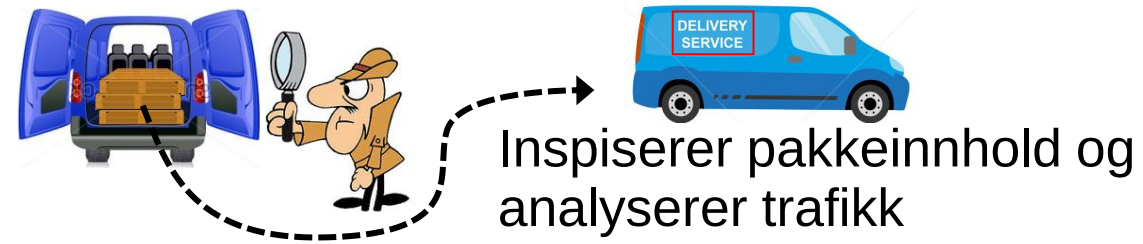
- Enkleste type brannmur som inspiserer pakkehoder på transport- og internett-laget og basert på dette bestemmer om pakke skal godtas eller avvises
- Bruker for eksempel IP-adresse, portnummer, type transportprotokoll
- `iptables` er et mye brukt pakkefilter for Linux
 - `iptables -A FORWARD -s 131.234.142.33 -j ACCEPT`
 - Alle pakker fra (kilde) IP-adresse 131.234.142.33 aksepteres
 - `iptables -A FORWARD -p tcp -d 10.0.0.56 --dport 22 -j ACCEPT`
 - Alle TCP-pakker til (destinasjon) IP-adresse 10.0.0.56 og port 22 aksepteres

Tilstandsbaserte brannmurer



- Har oversikt over tilstanden i hver forbindelse/økt mellom klient og tjener
- Kan opprette midlertidige regler for spesifikt økt
- Mer fleksibilitet og høy ytelse men krever minne for å huske tilstand
- **Eksempel:** `iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT`
 - Aksepterer alle pakker som tilhører en etablert TCP-forbindelse eller er relatert til eksisterende UDP-kommunikasjon

Applikasjonsbrannmur



- An applikasjonsbrannmur kan inspisere brukerdata i tillegg til pakkehoder
- Støtter spesifikke applikasjonsprotokoller (HTTP,FTP,...)
- Kan konfigureres for filtrering av spesifikke brukerapplikasjoner (Youtube, Facebook,...)
- Kan filtrere i ende-til-ende-forbindelse mellom klient og tjener
 - ... eller i 2 deler der brannmuren spiller rollen som proxy
 - Proxy-tjener for klienten og proxy-klient for tjeneren
 - En proxy brannmur kalles ofte en gateway og brukes i VPN som vi har sett
- Applikasjonsbrannmurer med høy ytelse kalles ofte neste generations brannmurer (Next Generation Firewalls)

Avanserte brannmurer

Next Generation Firewalls (NGF)
Web Application Firewall (WAF)



Top Model: PA-7080

Capacity: 200 Gbps

Price from: US\$ 200,000



Top Modelo:

Maestro Hyperscale Orchestrator 175

Capacity from 17,6 Gbps to 850 Gbps

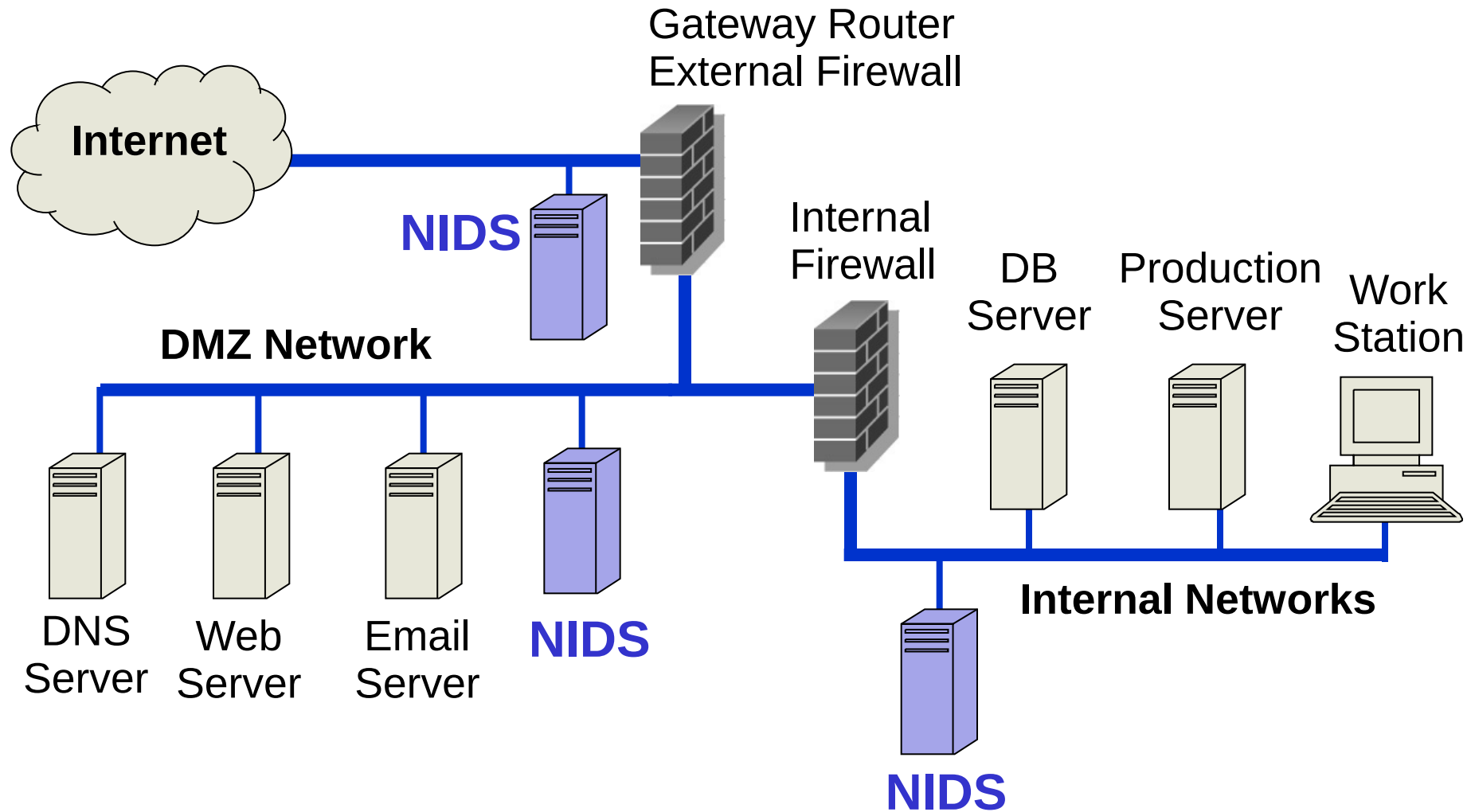
Price from: US\$ 100,000

Inntrengningsdeteksjon

Inntrengningsdeteksjon

- Inntrengningsdeteksjonssystemer (IDS) er systemer som forsøker å detektere mistenkelige aktivitet
- HIDS (Host-based IDS) forsøker å detektere aktivitet på vert/system den er installert
 - Overvåker prosesser, filtendring, ...
- NIDS (Network-based IDS) forsøker å detektere aktivitet på et eller flere nettverkssegment
 - Overvåker nettverkstrafikk
 - Vi fokuserer på NIDS her
- To hovedkategorier: Signaturbaserte og anomalibaserte

Inntrengningsdeteksjon i nettverk



Signaturbasert inntrengningsdeteksjon

- Signaturbasert deteksjon
 - Kjente angrepssignaturer (beskrivelse av kjente angrep)
 - Sekvenser av systemanrop, mønstre for nettverkstrafikk, etc.
 - Kan bare oppdage kjente angrep
- Snort er en mye brukt signaturbasert NIDS
 - Eksempel signatur:

```
alert tcp $HOME_NET any -> 10.0.0.56 22
(msg "SSH til IP-adresse 10.0.0.56")
```

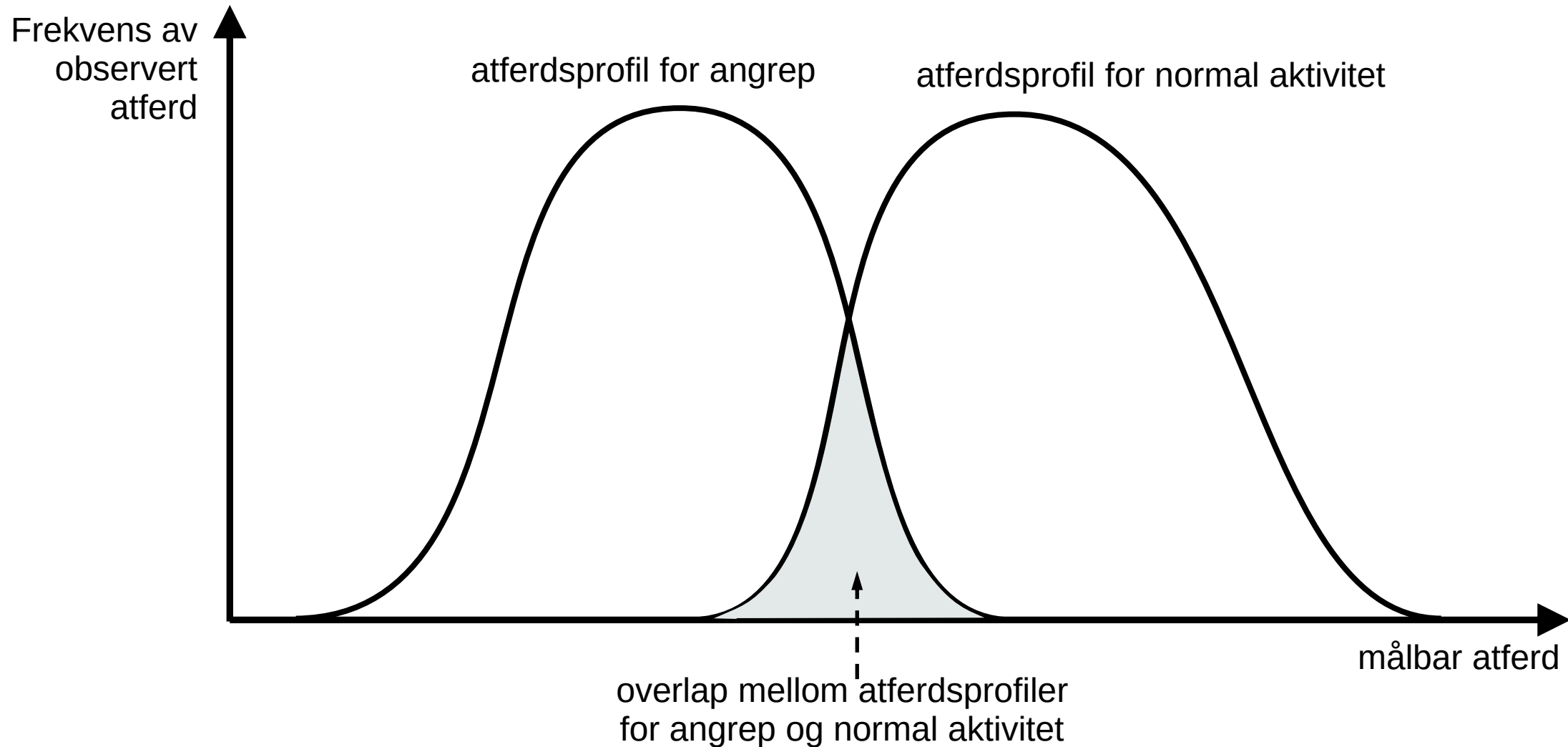
 - Gir alarm dersom eget nett (\$HOME_NET) dersom TCP pakke på 22 til IP-adresse 10.0.0.56 (Port 22 er standardport for SSH)



Anomalibasert inntrengningsdeteksjon

- Signaturbasert deteksjon
 - Kan bare oppdage kjente angrep
 - Man må (manuelt) utarbeide signaturer
 - Krever ofte at man ser innhold av nettverkspakker (deep packet inspection)
 - Kryptering (gjennom TLS) gjør dem mindre effektive
- Anomalibasert deteksjon
 - Bruke en modell for normal systematferd for å oppdage avvikende atferd
 - For eksempel slå en alarm når en statistisk sjelden hendelse oppstår
 - Ofte basert på maskinlæring
 - Kan oppdage ukjente angrep
 - Høyere andel falske alarmer (falske positive) enn signaturbaserte

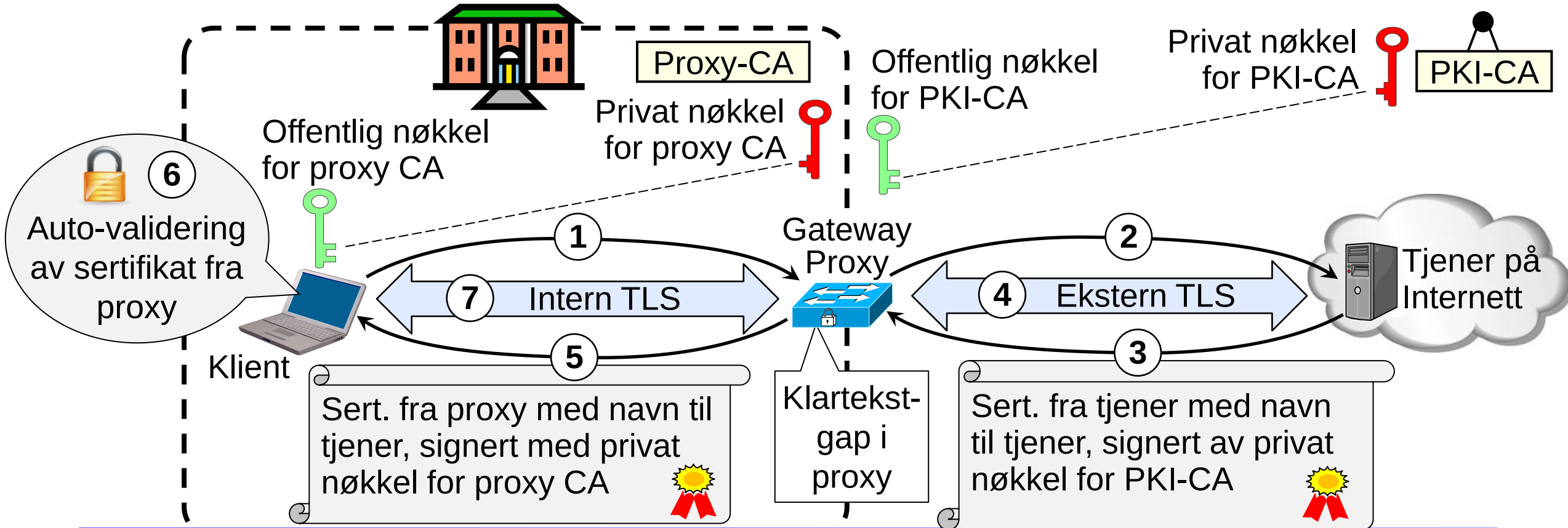
Utfordring med å skille mellom angrep og normal aktivitet



TLS-inspeksjon

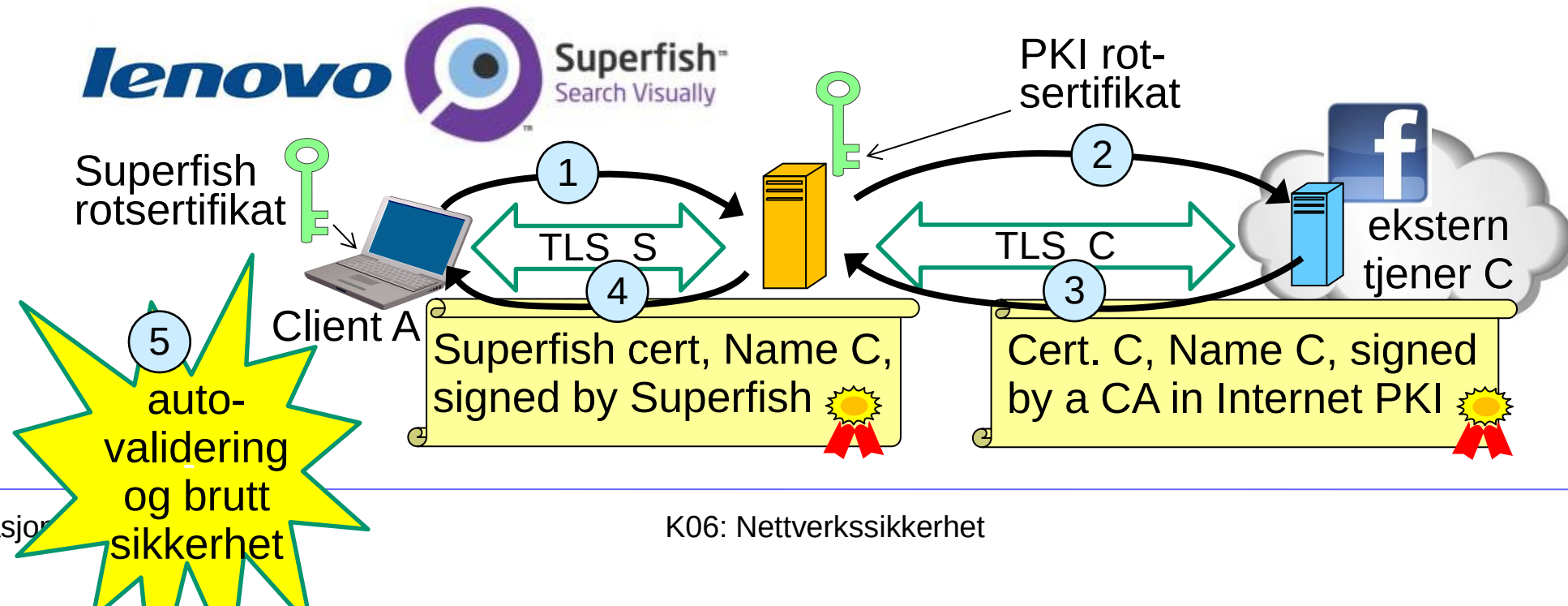
TLS-inspeksjon

- Noen organisasjoner ønsker å kunne lese kryptert https-trafikk fra ansatte
- For å bryte TLS-kryptering må gateway brannmur (proxy) utgi seg for å være ekstern tjener
- Proxy-serversertifikatet valideres automatisk av den lokale klienten, så brukeren kan feilaktig tro at han/hun har kryptert ende-til-ende TLS -tilkobling til den eksterne serveren



Infisering med Lenovo og Superfish

- Superfish rotsertifikat og viderekobling i Lenovo-modeller som ble sendt i løpet av 2014
- Alle HTTPS-tilkoblinger ble viderekoblet til Superfish-serveren for å injisere annonser.
- Superfish opprettet falske serversertifikater med navn på webtjenere (f.eks. Facebook.com), signert av Superfish root private key.
- Falske serversertifikater ble automatisk validert, så brukerne trodde at han/hun hadde en sikker ende-til-ende HTTPS-tilkobling til webserveren.
- Svindel oppdaget i 2015, Superfish cert. slettet og viderekobling fjernet.
- Forlegenhhet for Lenovo. Superfish endret navn til JustVisual.



Slutt på presentasjonen