IN2120 Cybersikkerhet
Høst 2026

Del 09: Kommunikasjonssikkerhet



Nils Petter Wien
Universitetet i Oslo



Foto: Colourbox

Lag- /løkmodellen for sikkerhet

- Alltid flere lag med sikkerhet
- Faller ett – så skal du ha flere igjen



Bildet er ai-generert

Skall- /eggmodellen for sikkerhet

- Hardt skall
- Mykt innhold



Bildet er ai-generert

Zero trust

- «Never trust, always verify»
- Aldri stol på noen, selv om de er på innsiden
  - Valider alle
  - Anta alle er kompromittert
  - Gi minst mulig rettigheter
- Hard på innsiden, hard på utsiden
- «Jo mindre tilgang du har, jo vanskeligere er det å få mer»

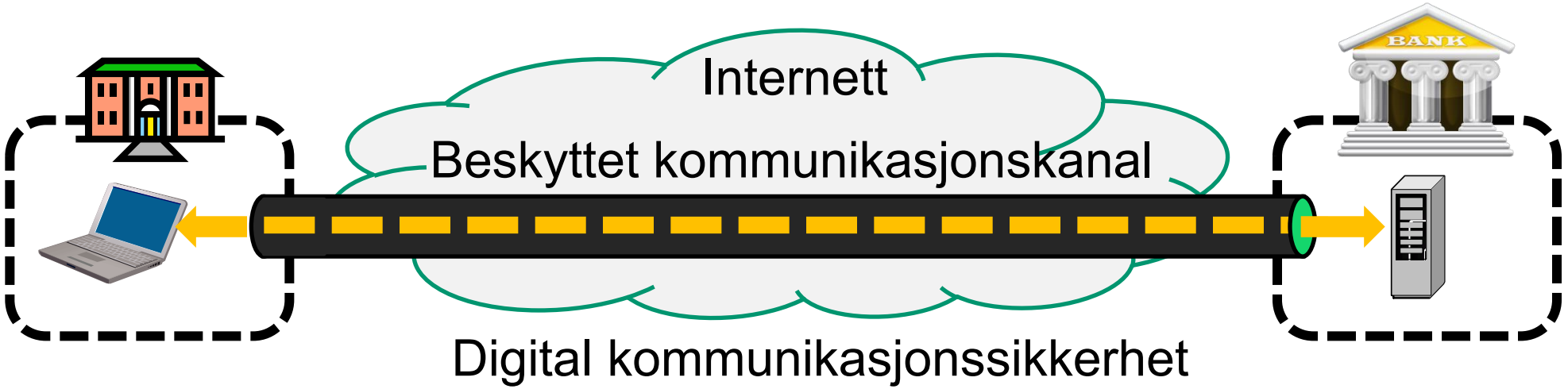


Bildet er ai-generert

Analogi: Transport og kommunikasjonssikkerhet

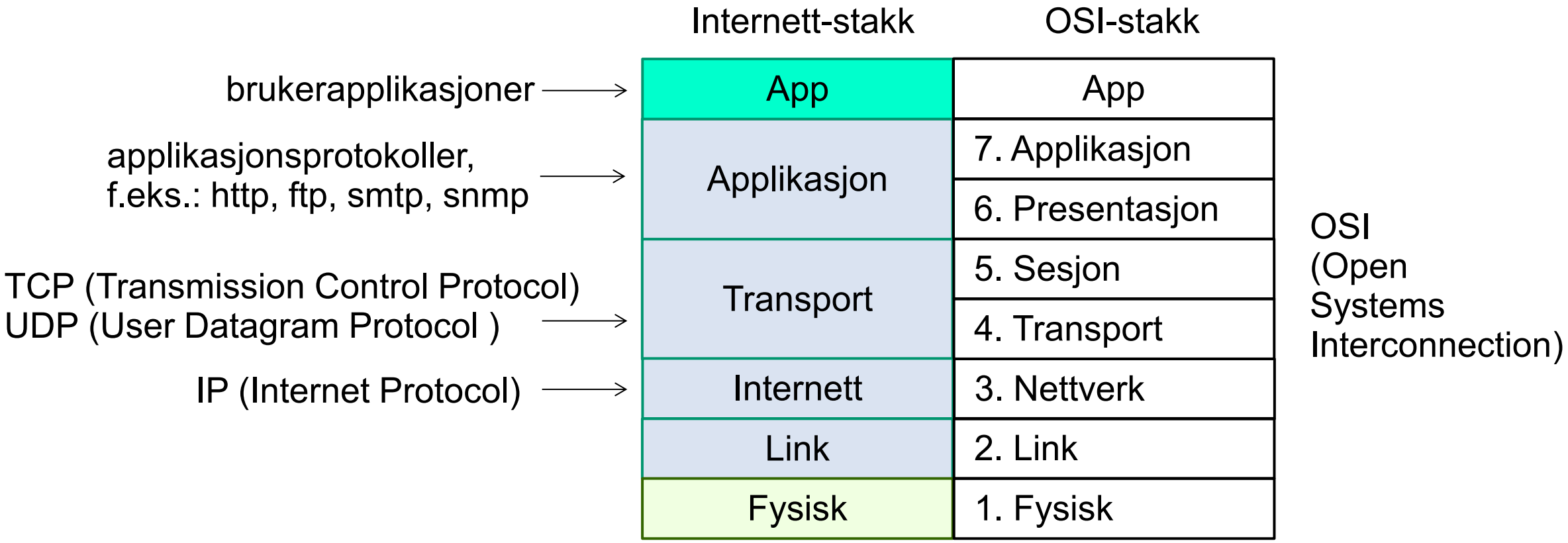


Fysisk transportsikkerhet



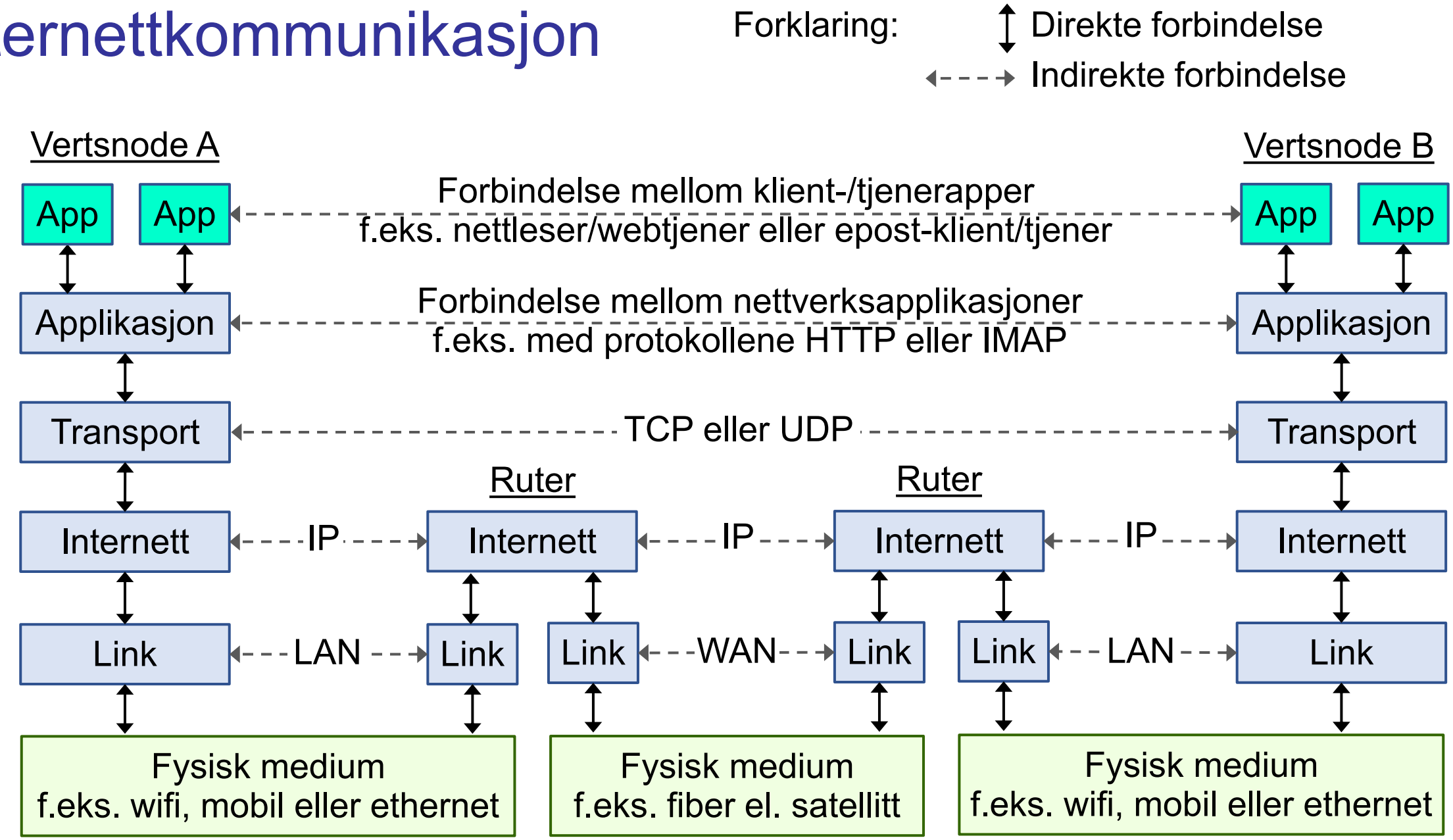
Digital kommunikasjonssikkerhet

Protokollstakk i Internett og tilsvarende i OSI

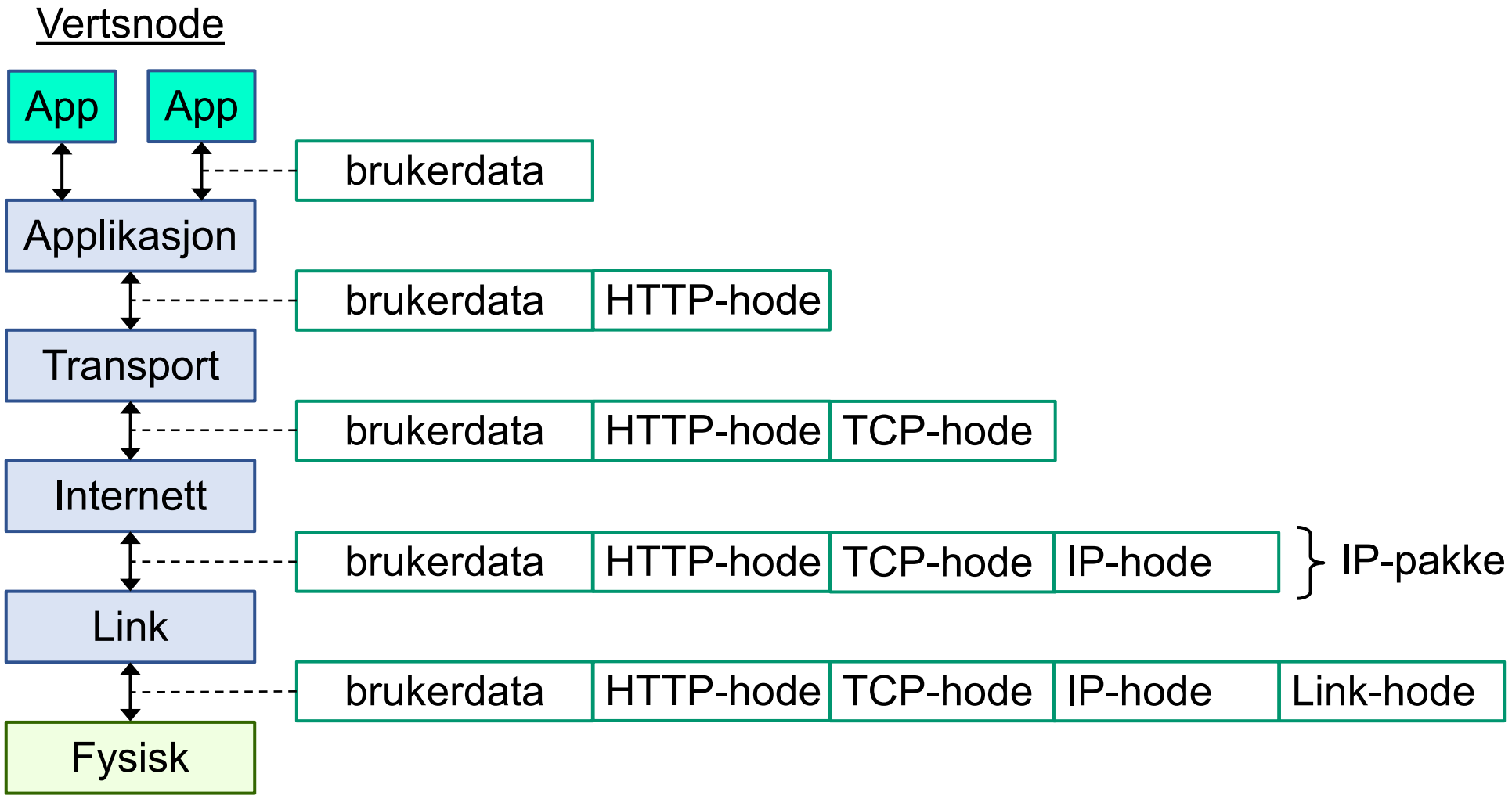


- OSI var en konkurrent til Internettstakken, men Internett vant til slutt

Internettkommunikasjon



Datapakker i protokollstakken



Sikkerhetsprotokoller

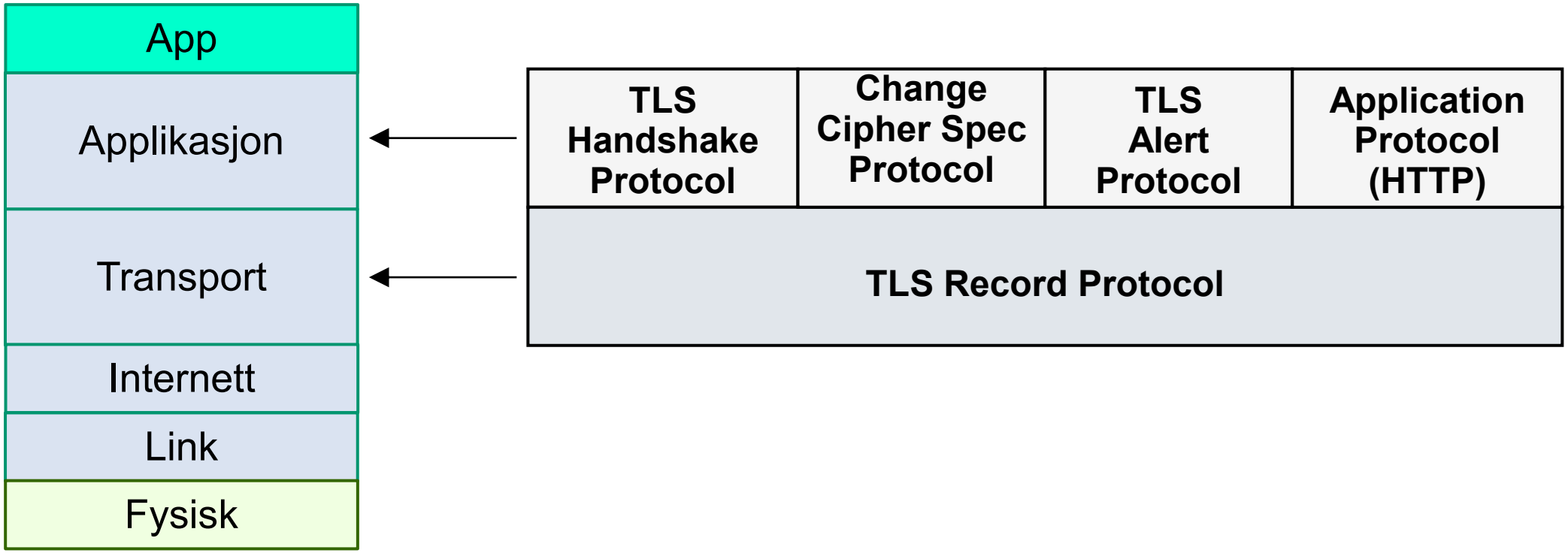
- Mange forskjellige sikkerhetsprotokoller for forskjellige formål
  - autentisering, integritet, konfidensialitet
  - nøkkelutveksling
  - e-valg

- Eksempler: TLS og IPSEC
- Sikkerhetsprotokoller er overraskende vanskelige å designe uten sårbarheter!
  - Mange sårbarheter oppdages år senere
  - ... noen blir aldri oppdaget (eller kanskje bare av angriperne)

TLS: Transport Layer Security

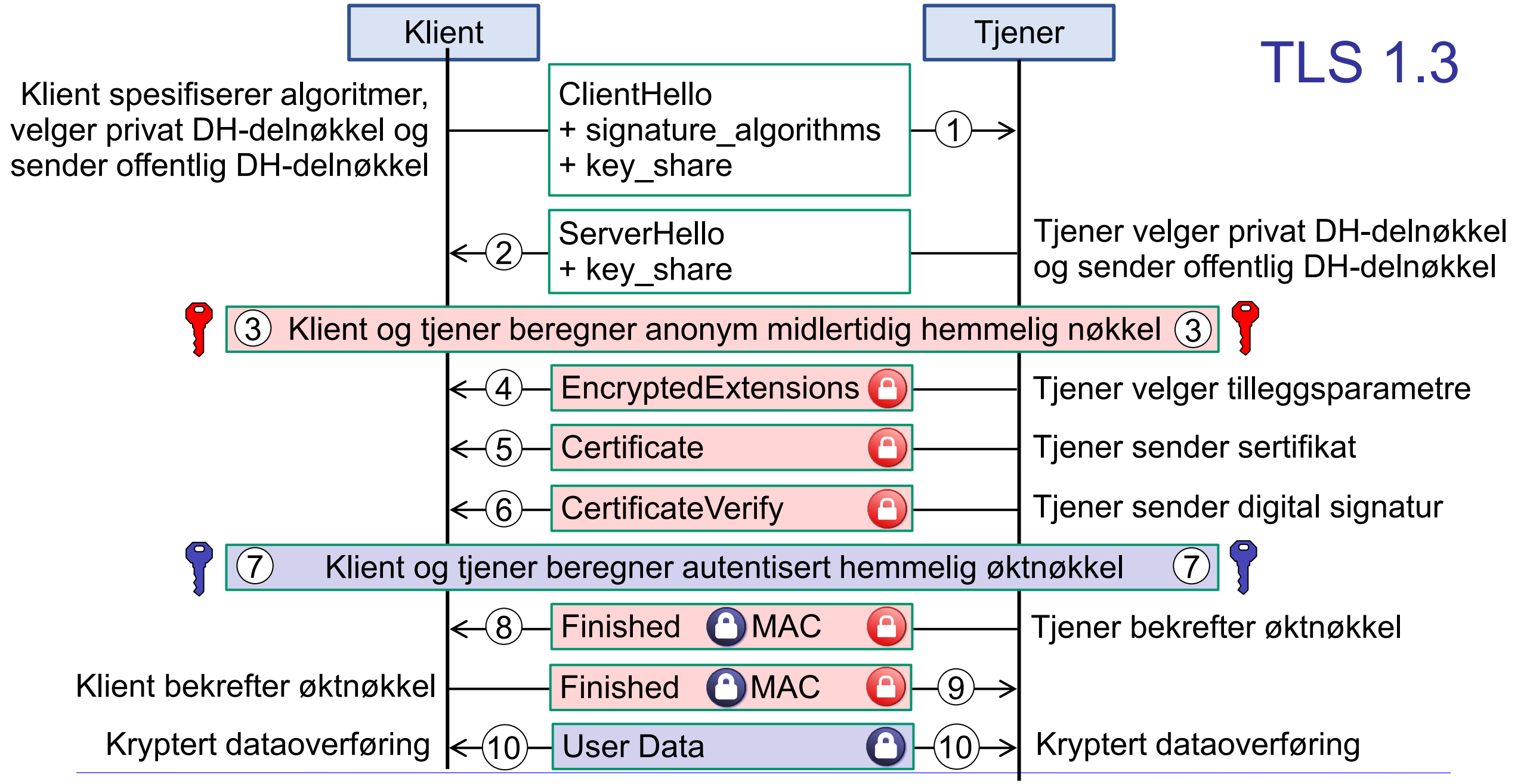
Tidligere kalt SSL (Secure Sockets Layer)

TLS i Internettstakken

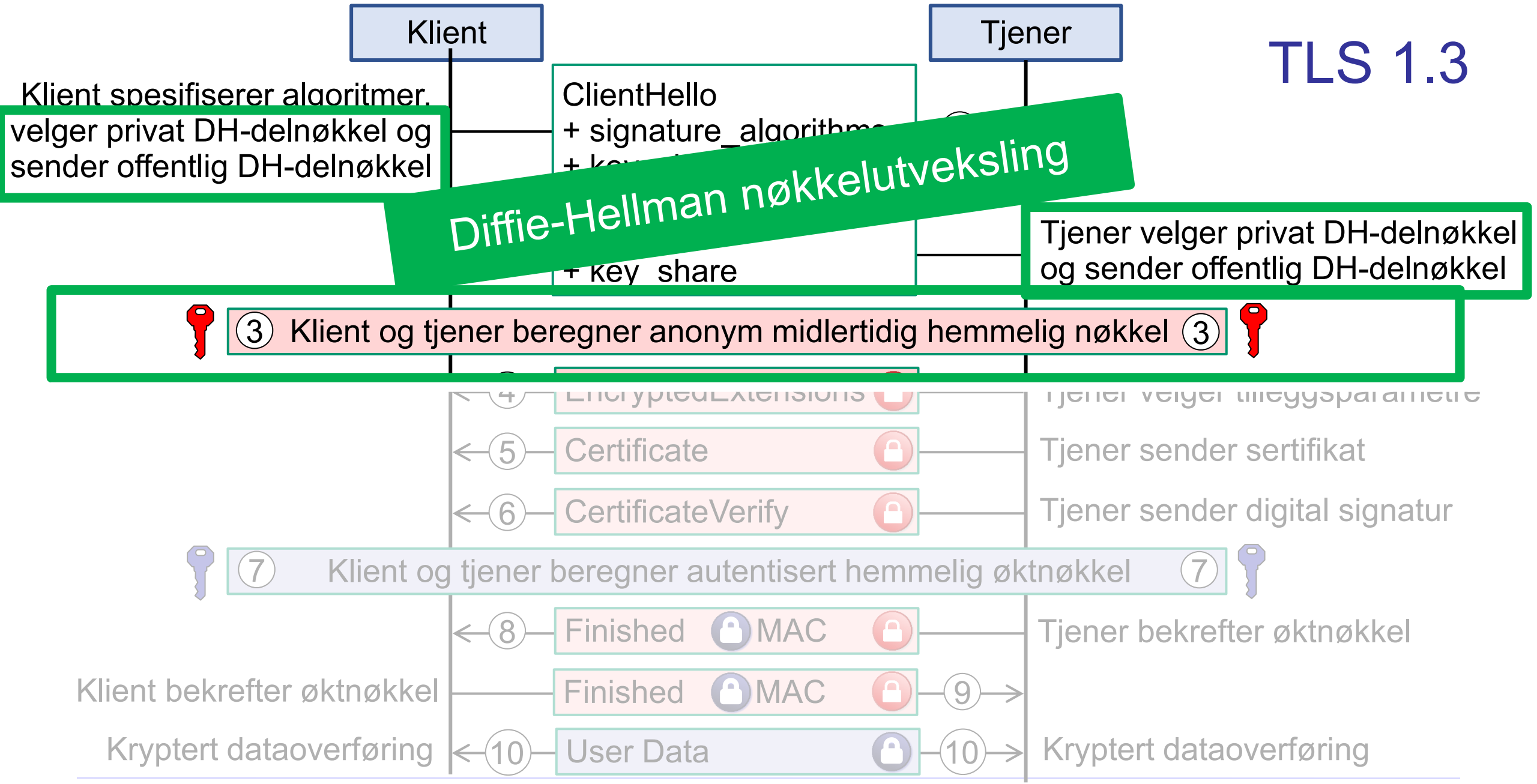


- TLS består egentlig av et sett med protokoller for ulike trinn i økten

TLS 1.3


Klient
Tjener
Klient spesifiserer algoritmer, velger privat DH-delnøkkel og sender offentlig DH-delnøkkel
ClientHello
+ signature_algorithms
+ key_share
1
2
ServerHello
+ key_share
Tjener velger privat DH-delnøkkel og sender offentlig DH-delnøkkel
3 Klient og tjener beregner anonym midlertidig hemmelig nøkkel 3
4
EncryptedExtensions
Tjener velger tilleggsparametre
5
Certificate
Tjener sender sertifikat
6
CertificateVerify
Tjener sender digital signatur
7 Klient og tjener beregner autentisert hemmelig øktnøkkel 7
8
Finished
MAC
Tjener bekrefter øktnøkkel
Klient bekrefter øktnøkkel
Finished
MAC
9
Kryptert dataoverføring
10
User Data
10
Kryptert dataoverføring

TLS 1.3


Klient
Tjener
Klient spesifiserer algoritmer, velger privat DH-delnøkkel og sender offentlig DH-delnøkkel
ClientHello
+ signature_algorithms
+ key_share
Diffie-Hellman nøkkelutveksling
Tjener velger privat DH-delnøkkel og sender offentlig DH-delnøkkel
3 Klient og tjener beregner anonym midlertidig hemmelig nøkkel 3
EncryptedExtensions
Tjener velger tilleggsparametre
5 Certificate
Tjener sender sertifikat
6 CertificateVerify
Tjener sender digital signatur
7 Klient og tjener beregner autentisert hemmelig øktnøkkel 7
8 Finished MAC
Tjener bekrefter øktnøkkel
Klient bekrefter øktnøkkel
Finished MAC
9
Kryptert dataoverføring
10 User Data
10
Kryptert dataoverføring

Repetisjon: Diffie-Hellman nøkkelutveksling





Alice velger privat delnøkkel a

Bob velger privat delnøkkel b

Alice beregner offentlig $g^a \pmod p$

Bob beregner offentlig $g^b \pmod p$

Alice sender til Bob $\longrightarrow$ $g^a \pmod p$

$g^b \pmod p$ $\longleftarrow$ Bob sender til Alice

Alice beregner hemmelig $g^{ab} = (g^b)^a \pmod p$

Bob beregner hemmelig $g^{ab} = (g^a)^b \pmod p$

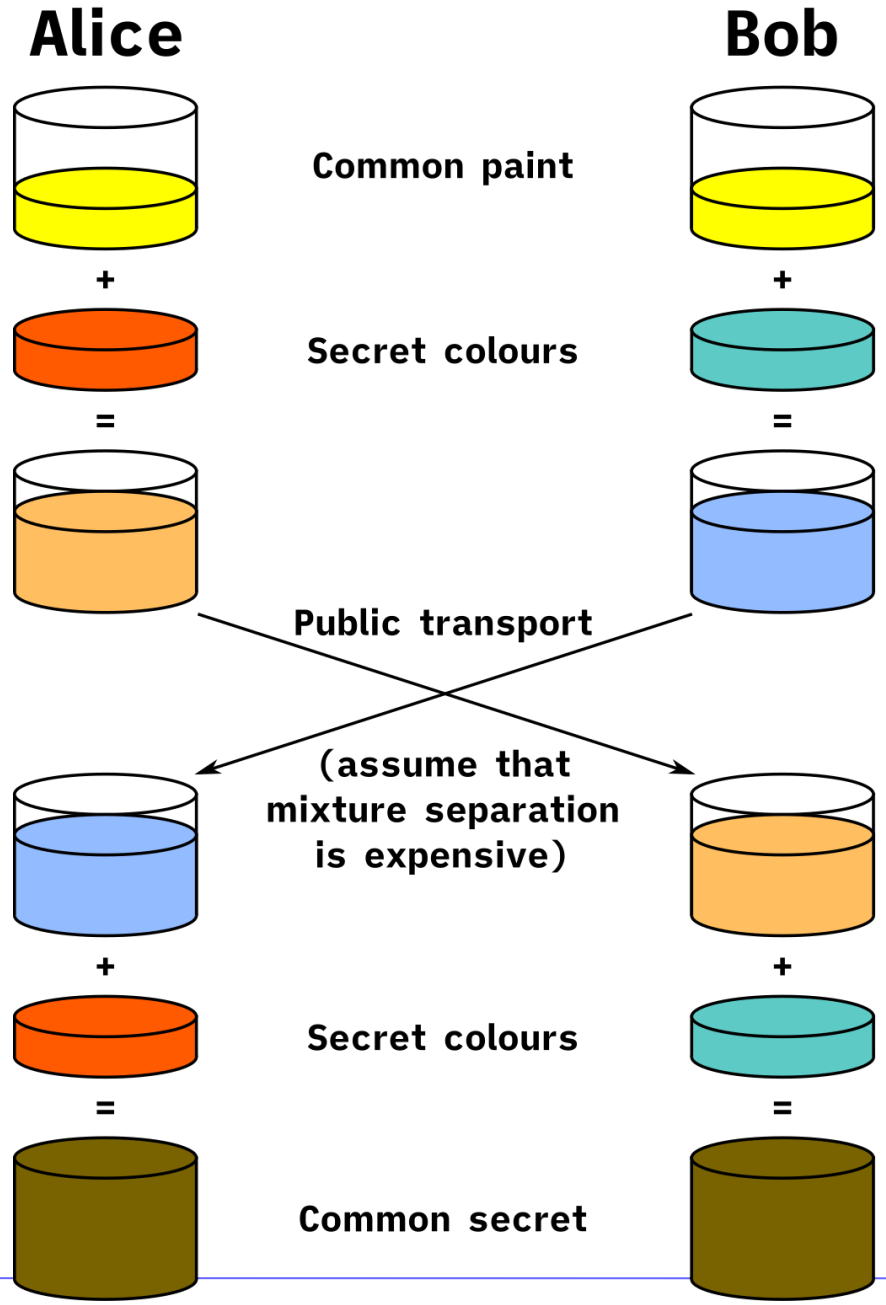


Alice og Bob har utvekslet anonym hemmelig nøkkel g^{ab}



Repetisjon: Diffie-Hellman nøkkelutveksling (analogi)

[Kilde figur: Wikipedia]



Repetisjon: Diffie-Hellman nøkkelutveksling





Alice velger privat delnøkkel a

Bob velger privat delnøkkel b

Alice beregner offentlig $g^a \pmod p$

Bob beregner offentlig $g^b \pmod p$

Alice sender til Bob → $g^a \pmod p$

$g^b \pmod p$ ← Bob sender til Alice

Alice beregner hemmelig $g^{ab} = (g^b)^a \pmod p$

Bob beregner hemmelig $g^{ab} = (g^a)^b \pmod p$

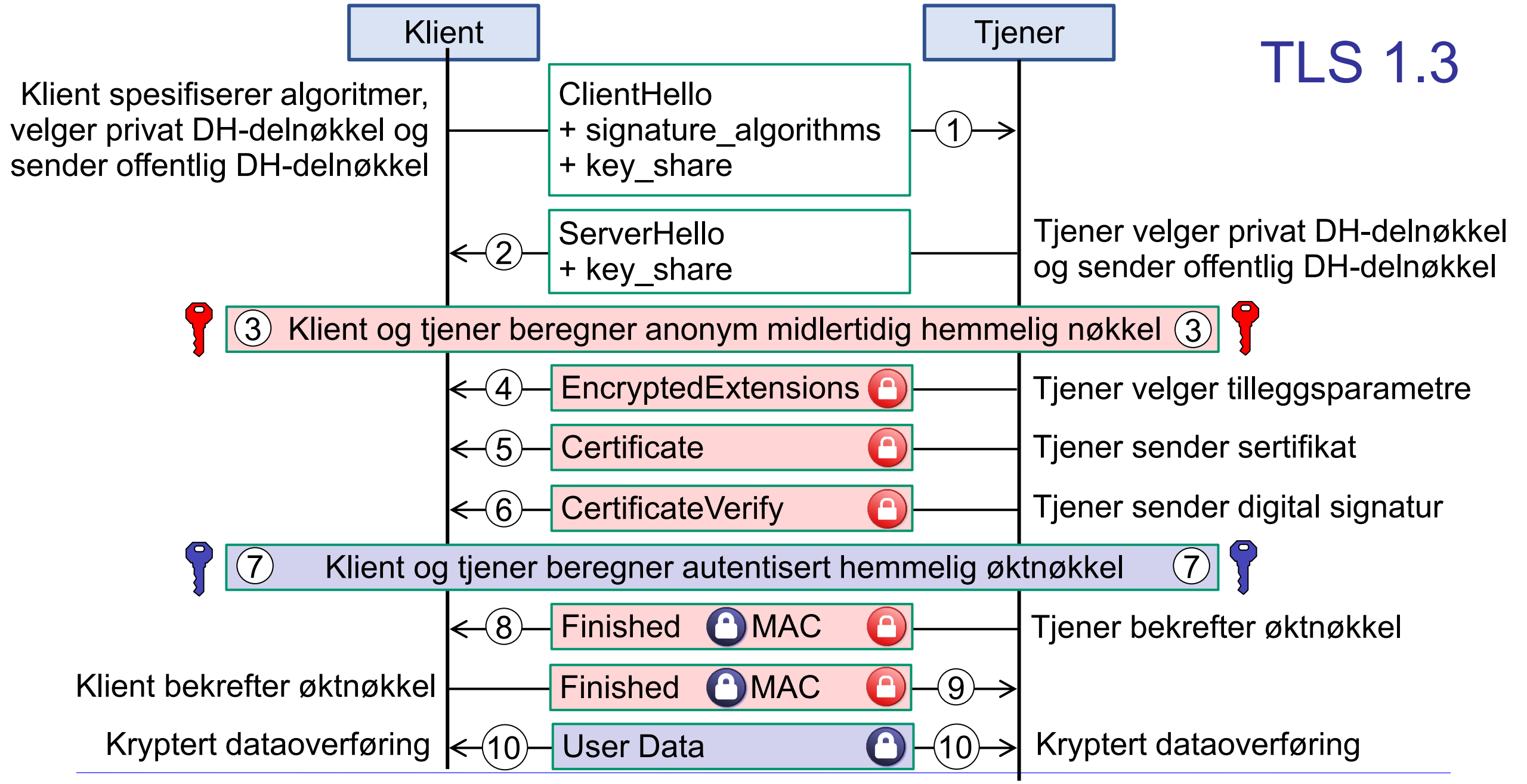


Alice og Bob har utvekslet anonym hemmelig nøkkel g^{ab}

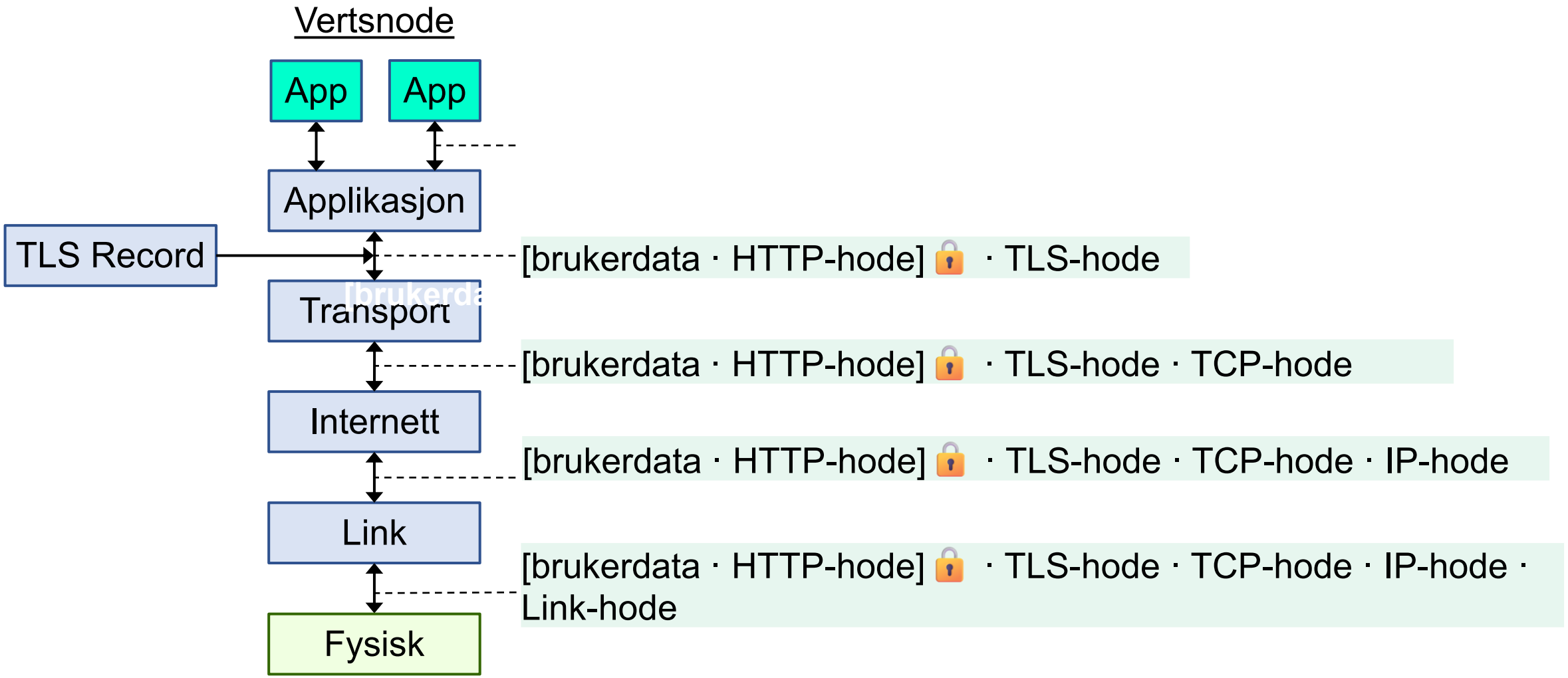


Angripere kan ikke finne de hemmelige delnøklene *a* og *b* fordi beregning av diskret logaritme av store tall er vanskelig. Dermed kan angripere ikke beregne den hemmelige nøkkelen = g^{ab} mod *p*.

TLS 1.3


Klient
Tjener
Klient spesifiserer algoritmer, velger privat DH-delnøkkel og sender offentlig DH-delnøkkel
ClientHello
+ signature_algorithms
+ key_share
1
2
ServerHello
+ key_share
Tjener velger privat DH-delnøkkel og sender offentlig DH-delnøkkel
3 Klient og tjener beregner anonym midlertidig hemmelig nøkkel 3
4
EncryptedExtensions
Tjener velger tilleggsparametre
5
Certificate
Tjener sender sertifikat
6
CertificateVerify
Tjener sender digital signatur
7 Klient og tjener beregner autentisert hemmelig øktnøkkel 7
8
Finished
MAC
Tjener bekrefter øktnøkkel
Klient bekrefter øktnøkkel
Finished
MAC
9
Kryptert dataoverføring
10
User Data
10
Kryptert dataoverføring

Kryptering av brukerdata med TLS



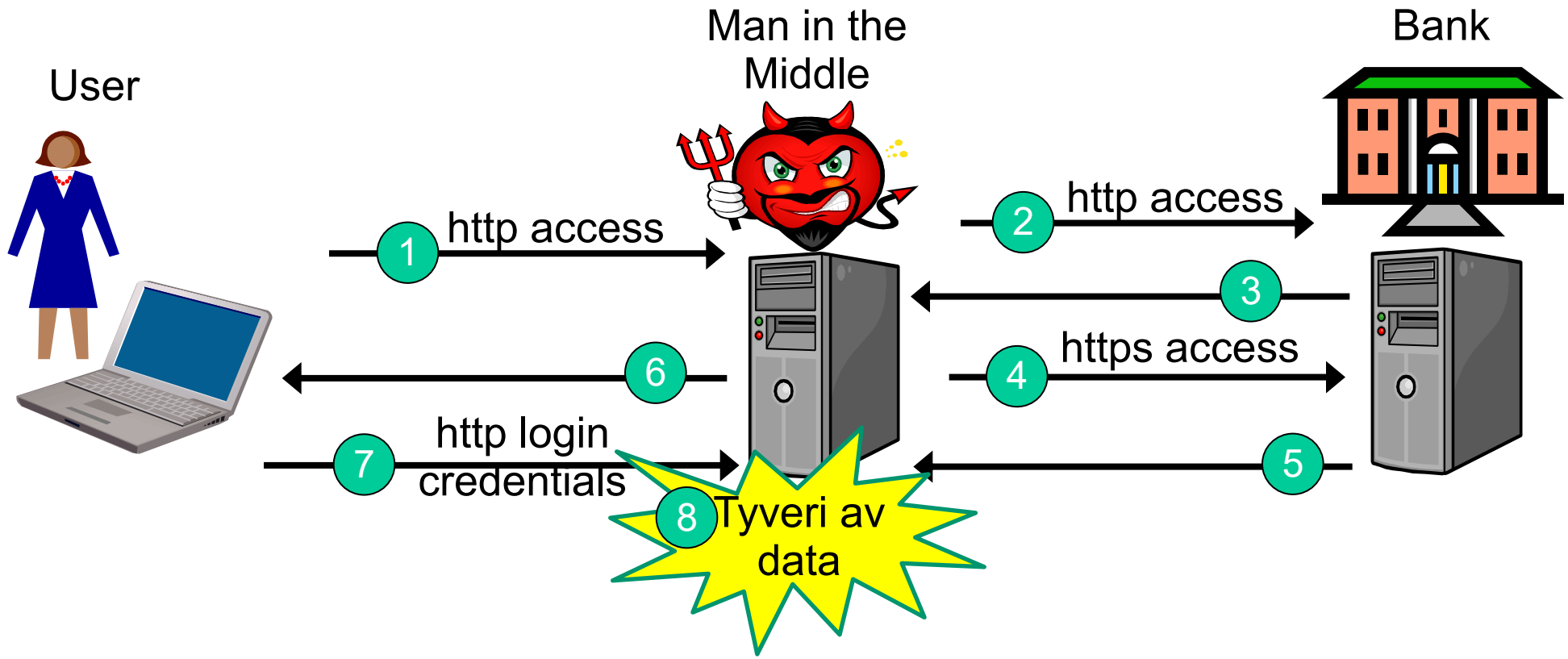
TLS 1.3

- Designet for hurtighet i etableringen av øktnøkkel
- Trenger kun én meldingsrunde (frem og tilbake) for å etablere øktnøkkel
- I TLS er serverens private signeringsnøkkel langsiktig.
- Fremoverhemmelighold oppnås ved bruk av efemær Diffie-Hellman
  - Dvs nye øktnøkler for hver økt

Fremoverhemmelighold

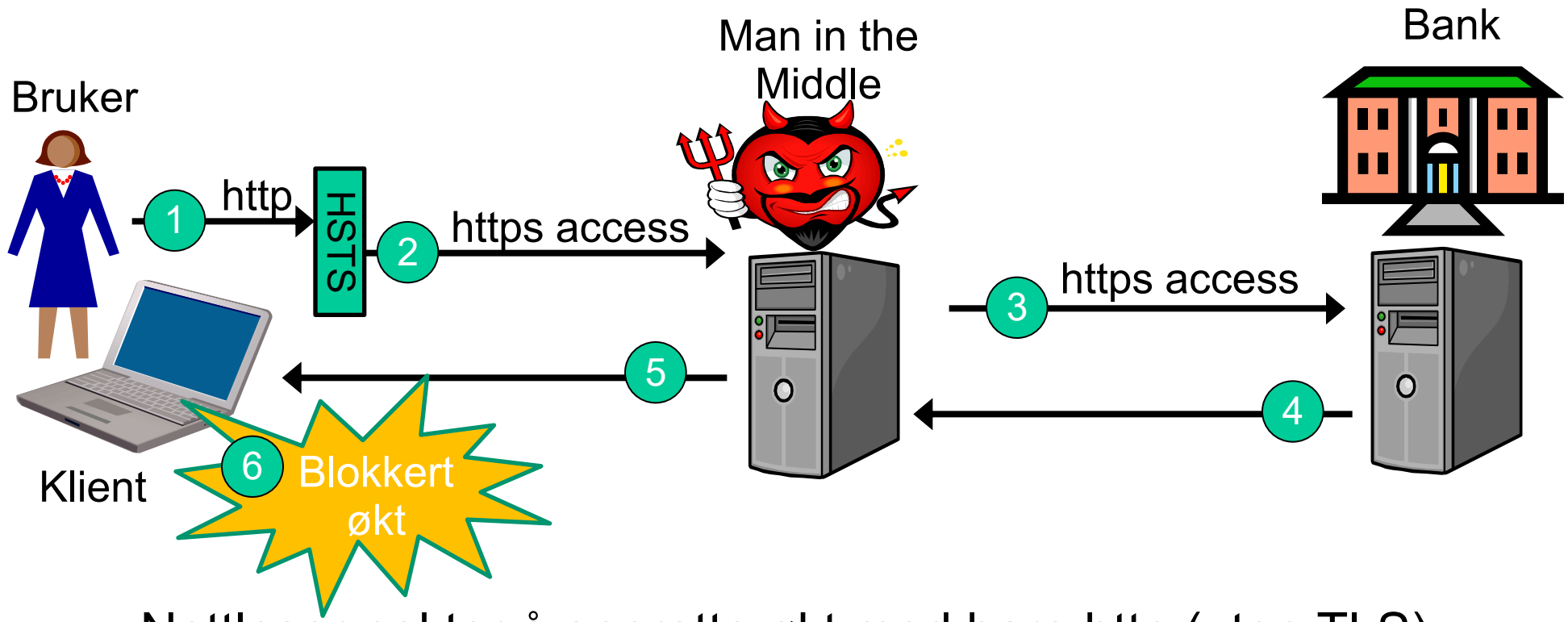
- Fremoverhemmelighold (eng.: forward secrecy)
  - tidligere øktnøkler blir ikke kompromittert selv om en langsiktig kryptonøkkel blir kompromittert en gang i fremtiden.

Angrep med TLS-stripping



- Det fins forskjellige varianter av TLS-stripping

HSTS for å hindre TLS-stripping



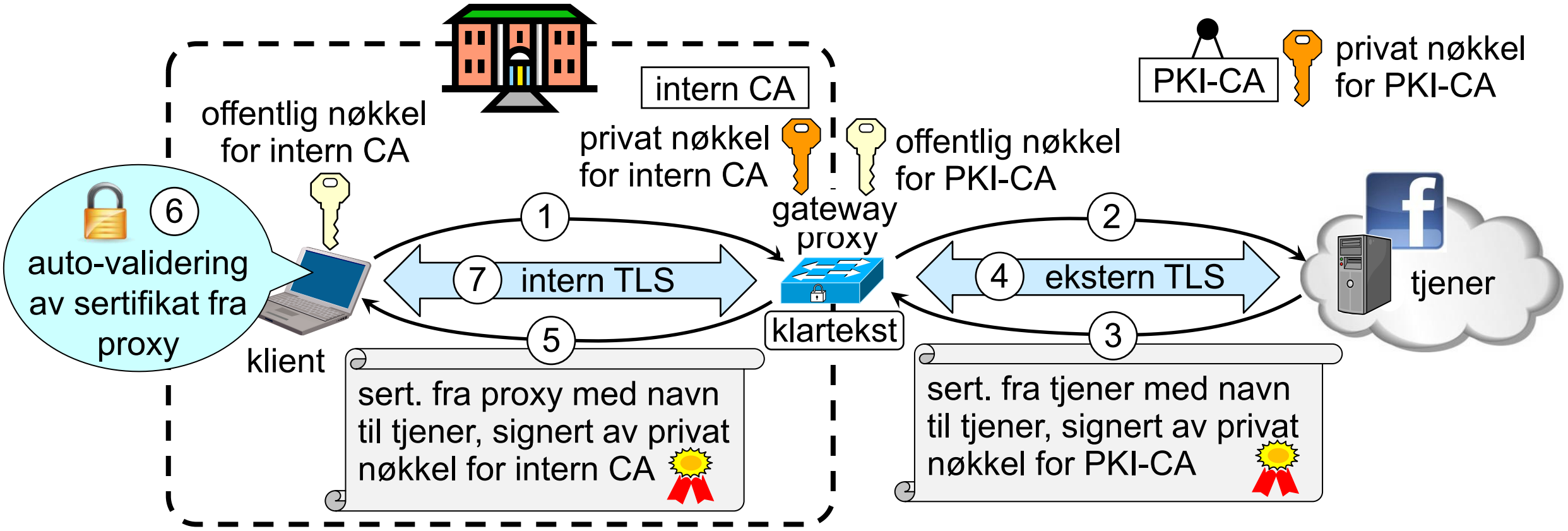
- Nettleser nekter å opprette økt med bare http (uten TLS)
- Nettleser krever https (med TLS)

HSTS - svakhet

- Nettleseren må VITE at HSTS er implementert
- Førstegangs besøk
  - Lagres i nettleseren etter det, så senere besøk er beskyttet
- De fleste større moderne nettlesere har en lang liste over domener og nettsider som krever HSTS
  - (HSTS-preload)

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 tro at han/hun har TLS -tilkobling til den eksterne serveren

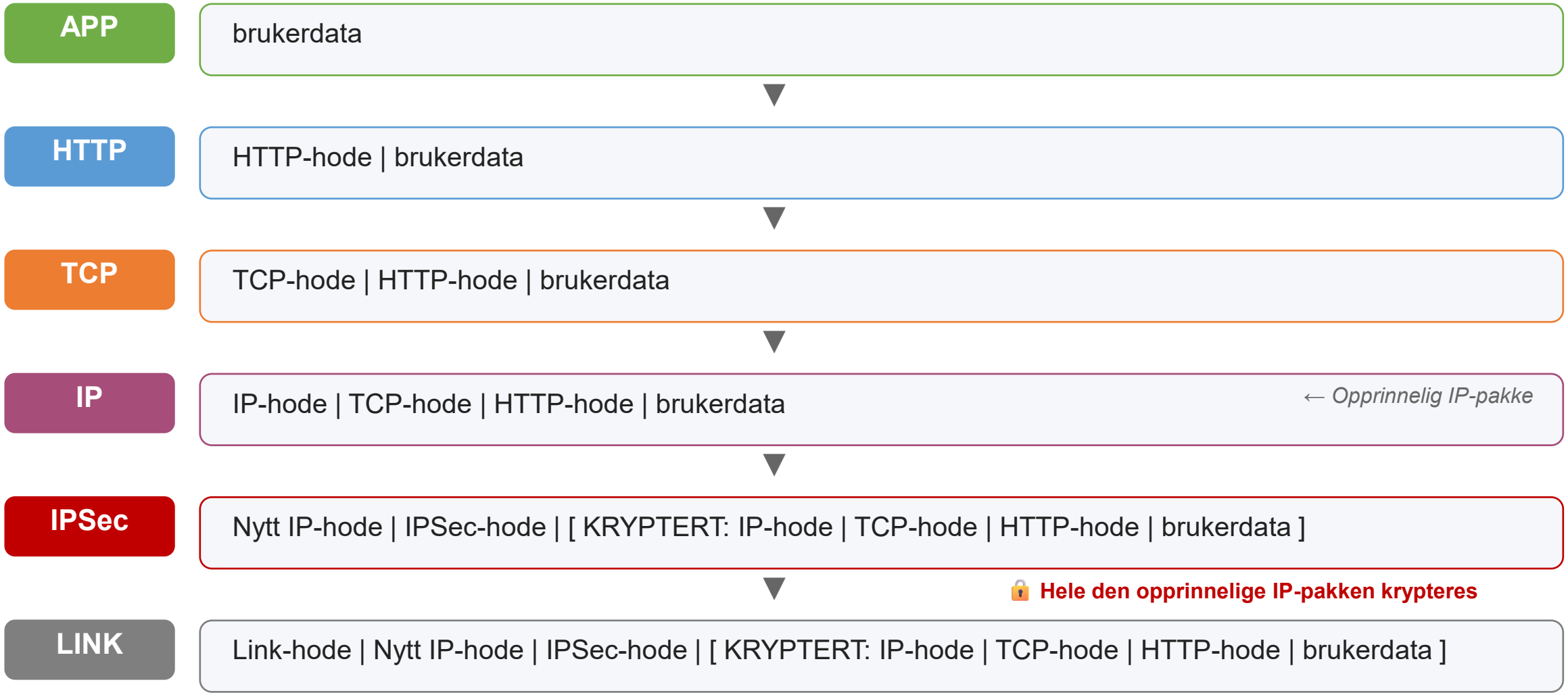


IP Security

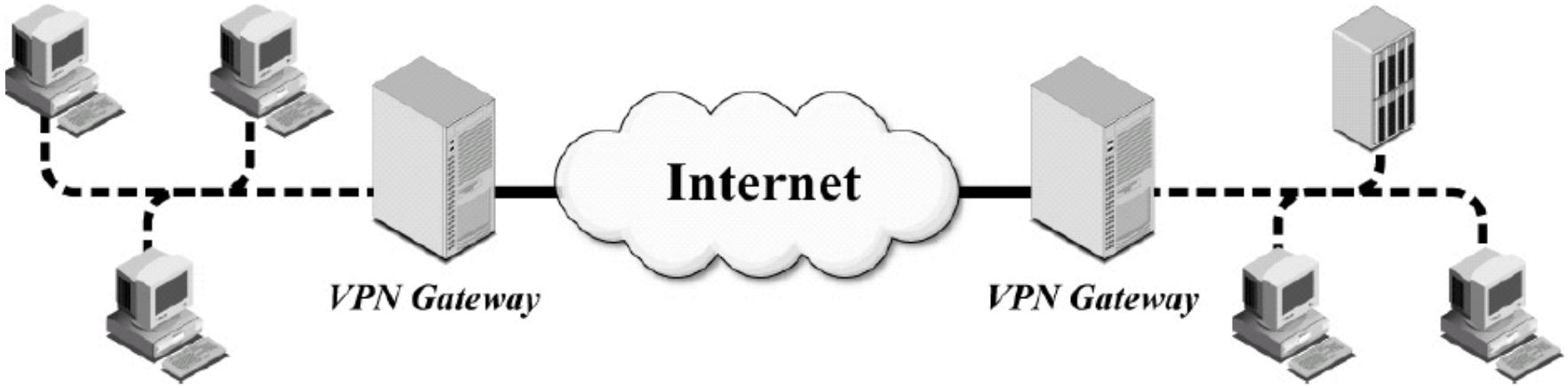
IPsec

- 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.

IPSec Tunnel Mode - Kapsling gjennom lagene

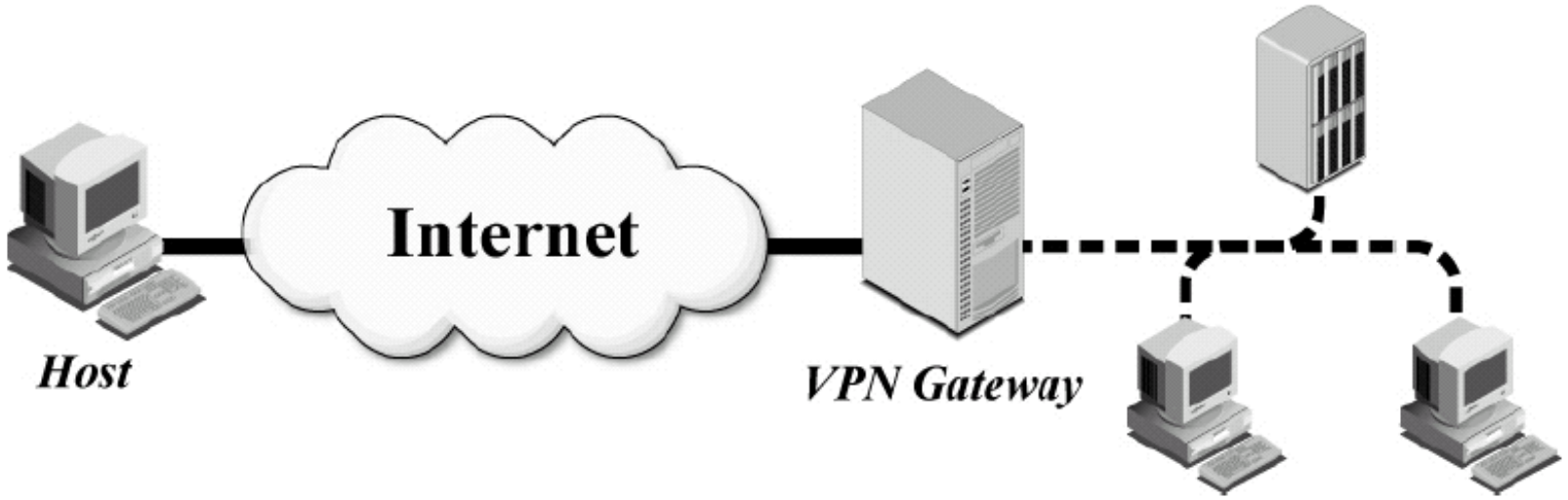


IPsec:
Gateway-to-Gateway Architecture



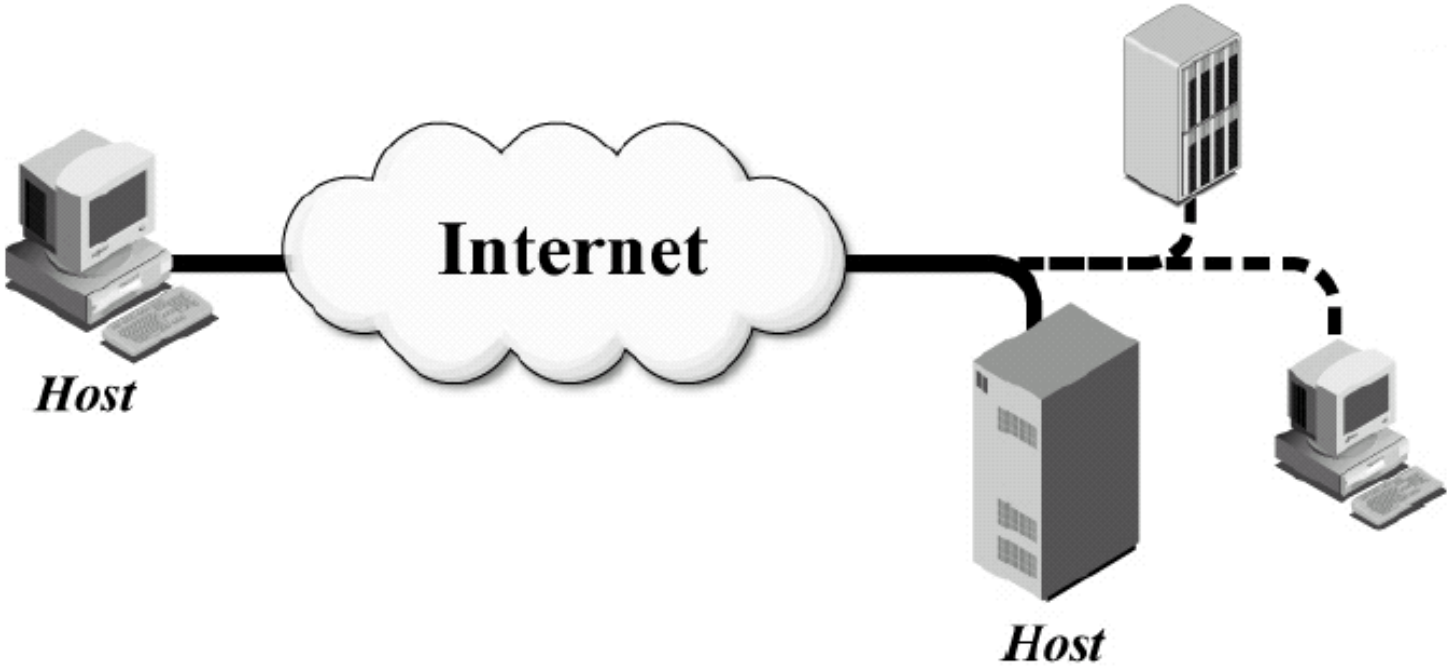
Source: NIST Special Publication 800-77

IPsec:
Host-to-Gateway Architecture



Source: NIST Special Publication 800-77

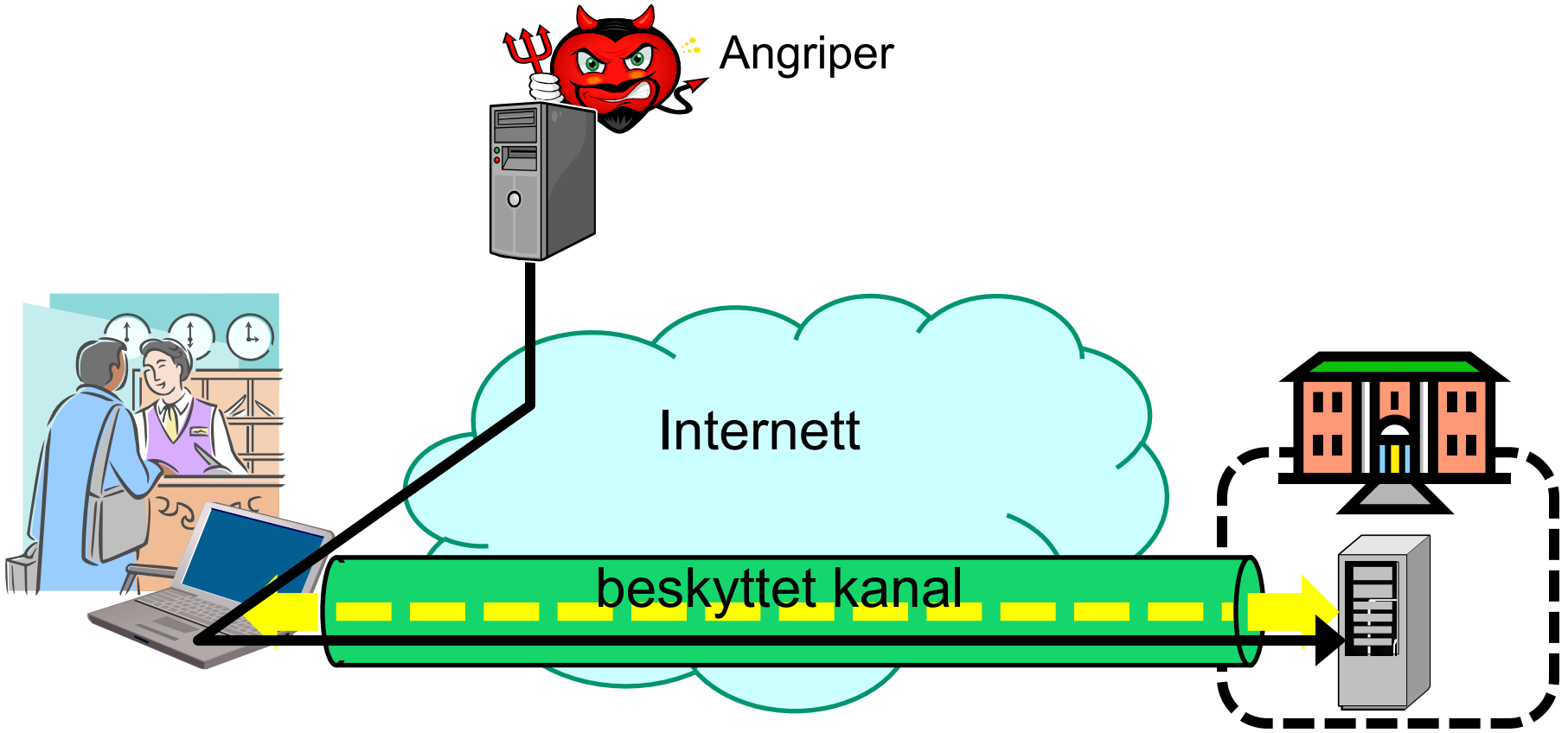
IPsec:
Host-to-Host Architecture



Source: NIST Special Publication 800-77

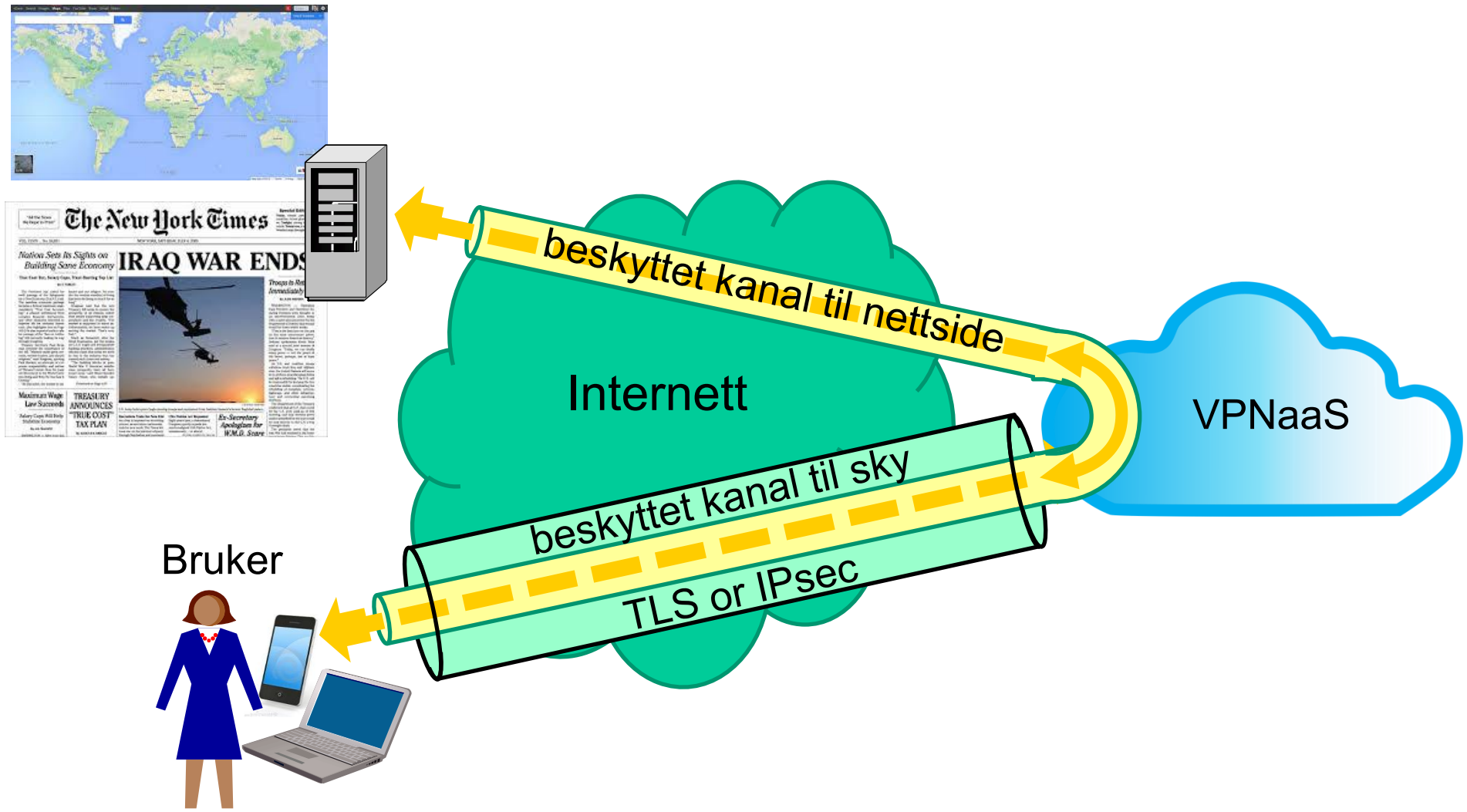
VPN og Tor

VPN for tilgang til hjemme-datanett



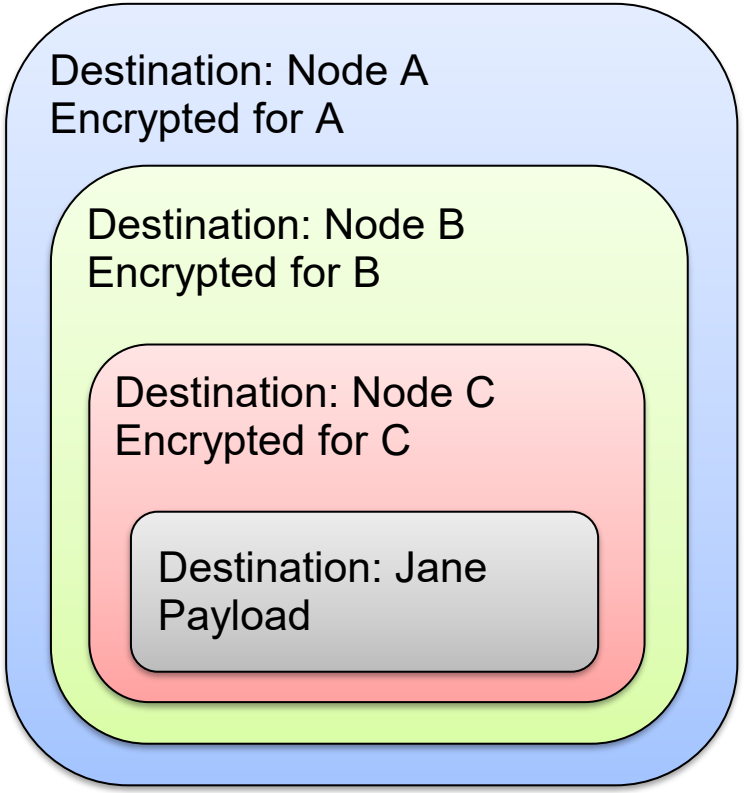
Mulig angrepsvektor gjennom ekstern enhet

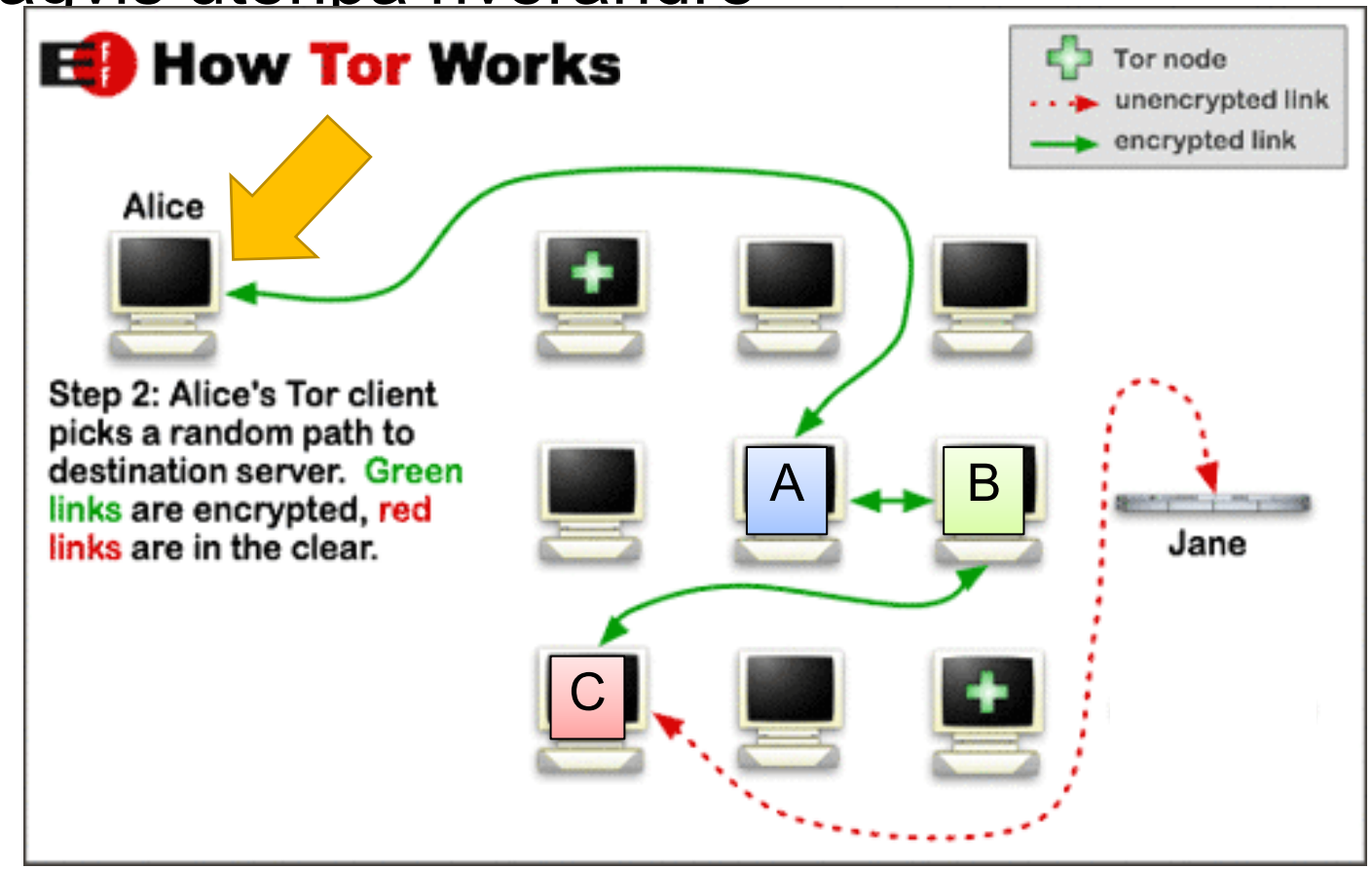
Sky-VPN


Internett-
tjeneste
The New York Times
IRAQ WAR ENDS
beskyttet kanal til nettside
Internett
VPNaaS
beskyttet kanal til sky
TLS or IPsec
Bruker

Tor (The onion router – løkruting)

- Anonymiseringstjeneste som benytter tre separate krypterte forbindelser som ligger lagvis utenpå hverandre



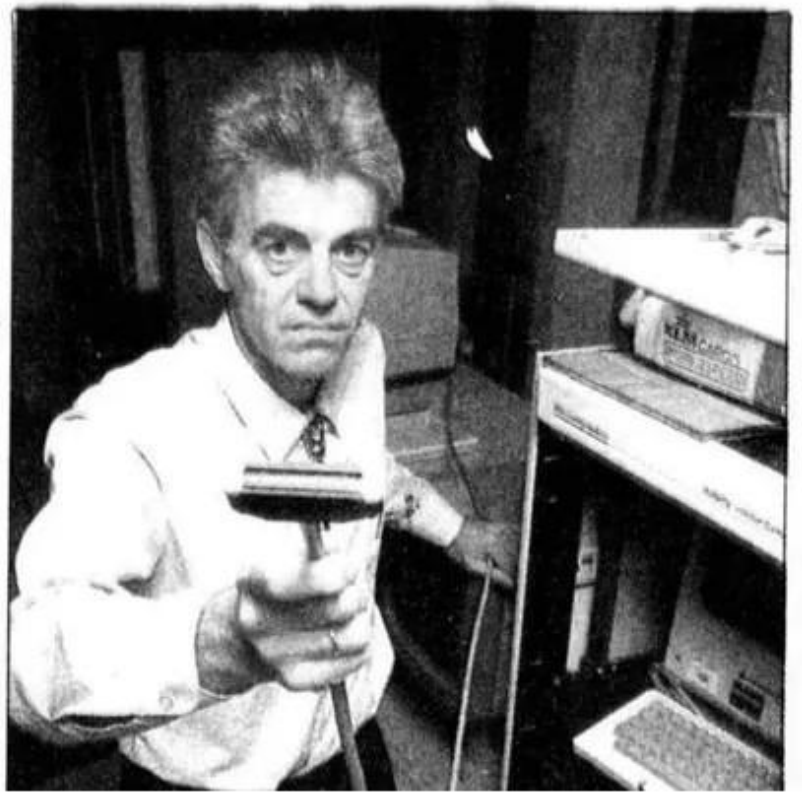


Nettverkssikkerhet

ROLEX
Bjerke
Karl Johansgt. 31 Oslo 02-42 20 44
Prinsensgate 21 Oslo 02-42 60 50
Nedre Torgt. 11 Drammen 03-89 30 77

Aftenposten
Morgenutgave. Tirsdag 8. november 1988. Uke 45. Nr. 518. 129. årg. Kr. 6,00. Fly/ekspr.: Vest-/Midt-Norge kr. 7,00. Nord-Norge kr.

Forhindret norsk data-katastrofe



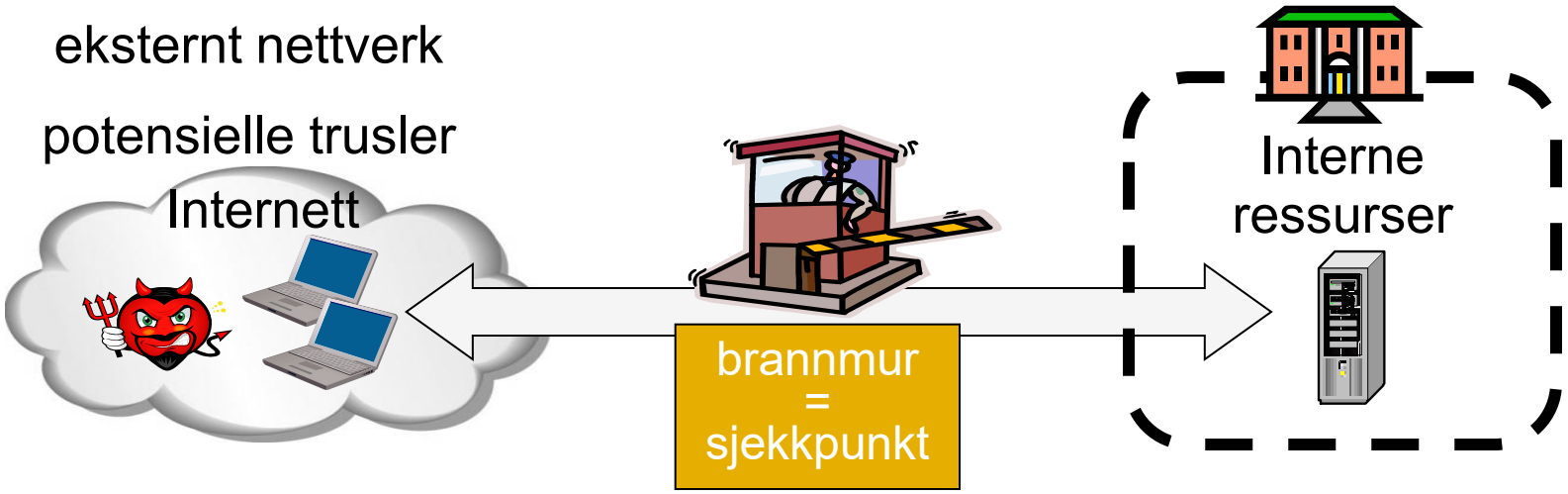
● Han trakk ut kontakten og sparte norske forskningsmiljøer for svarte dataskjermer og millioner i ekstrautgifter.

● «Viruset» er et innsmuglet program som bruker opp maskinenes datakraft slik at de går i stå. Det har lammet

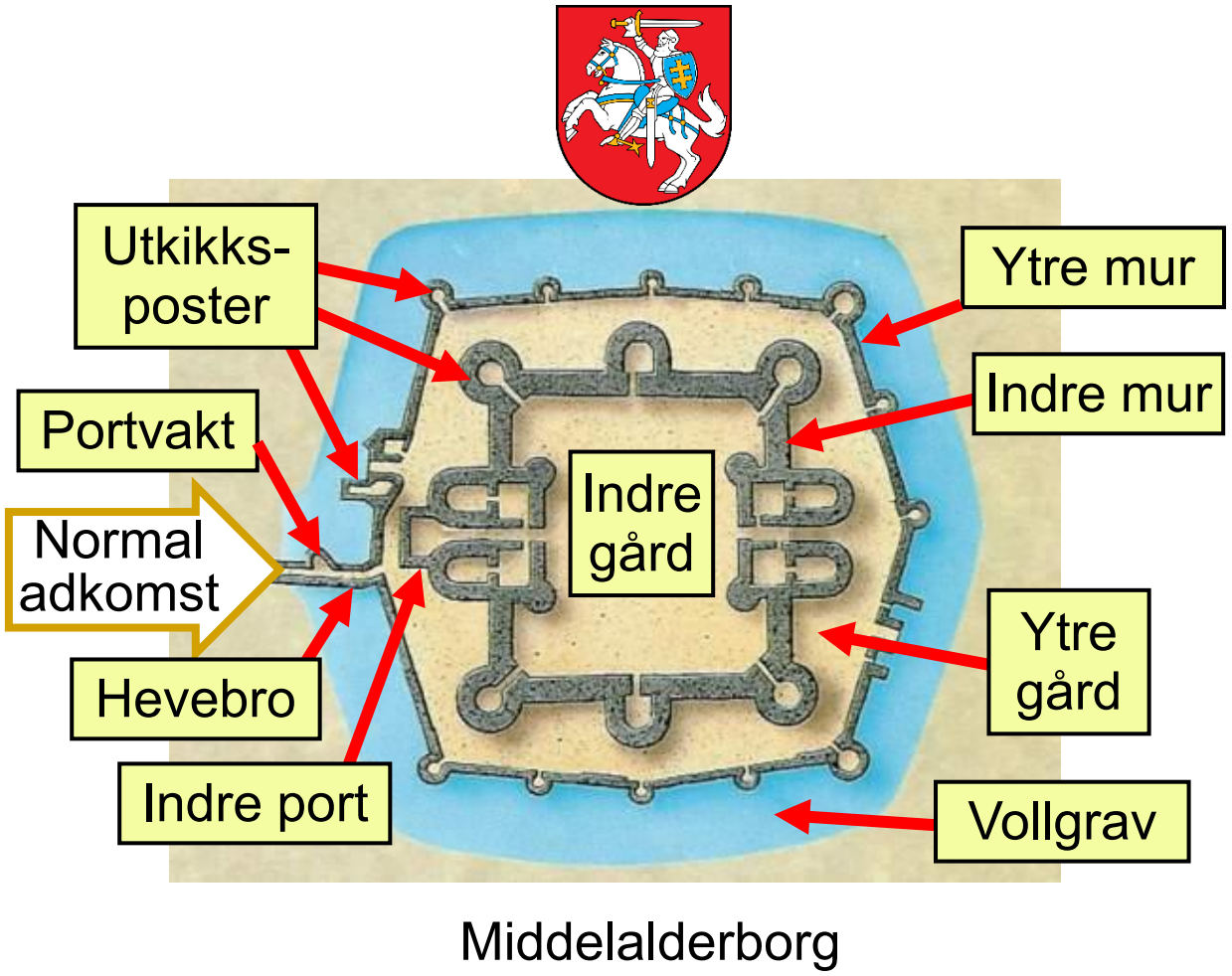
Faksimile: Aftenposten

Datanettsikkerhet med brannmur

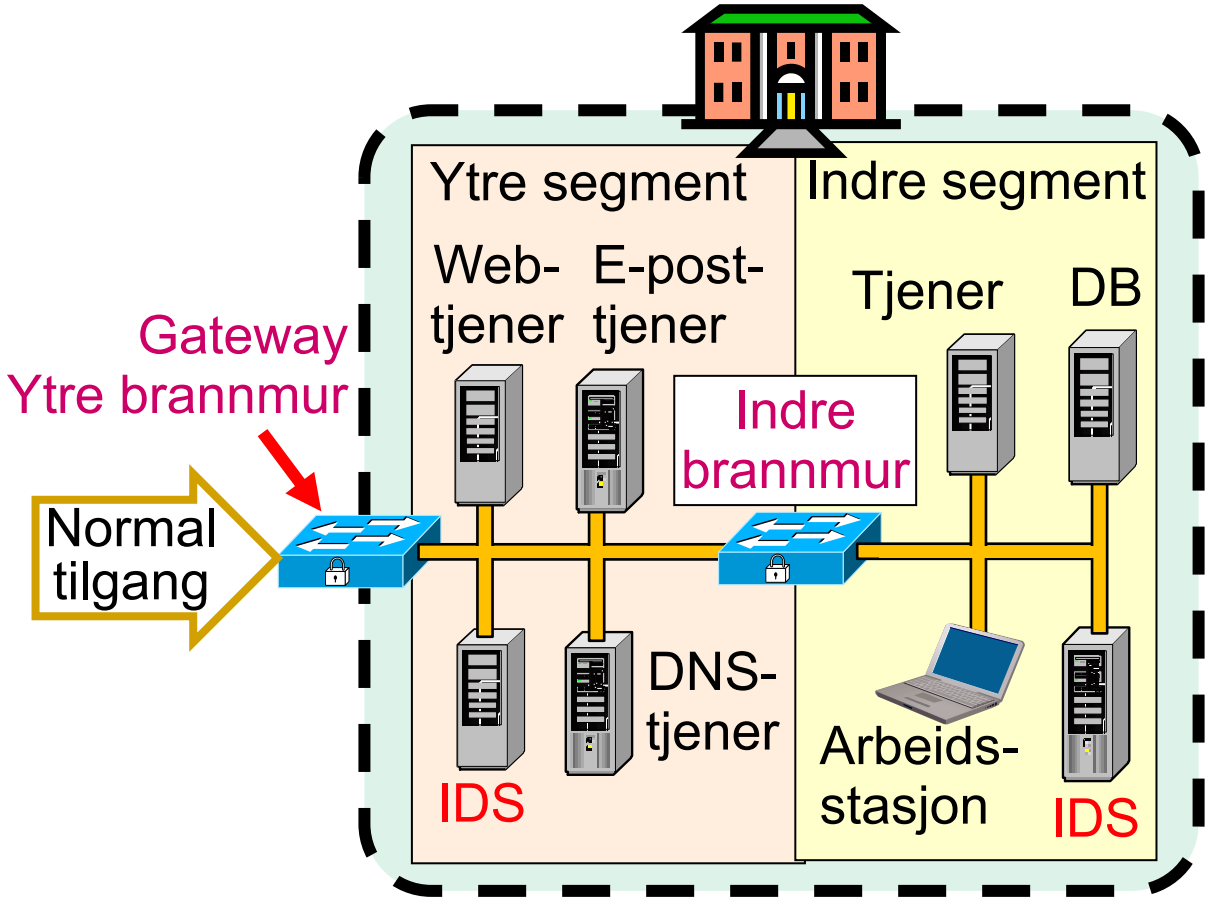
- Sjekkpunkt som beskytter mot angrep fra øvrige nettverk
- Sjekkpunktet bestemmer hvilken trafikk som kan passere inn og ut basert på regler



Analogi: Middelalderborg og datanett



Middelalderborg

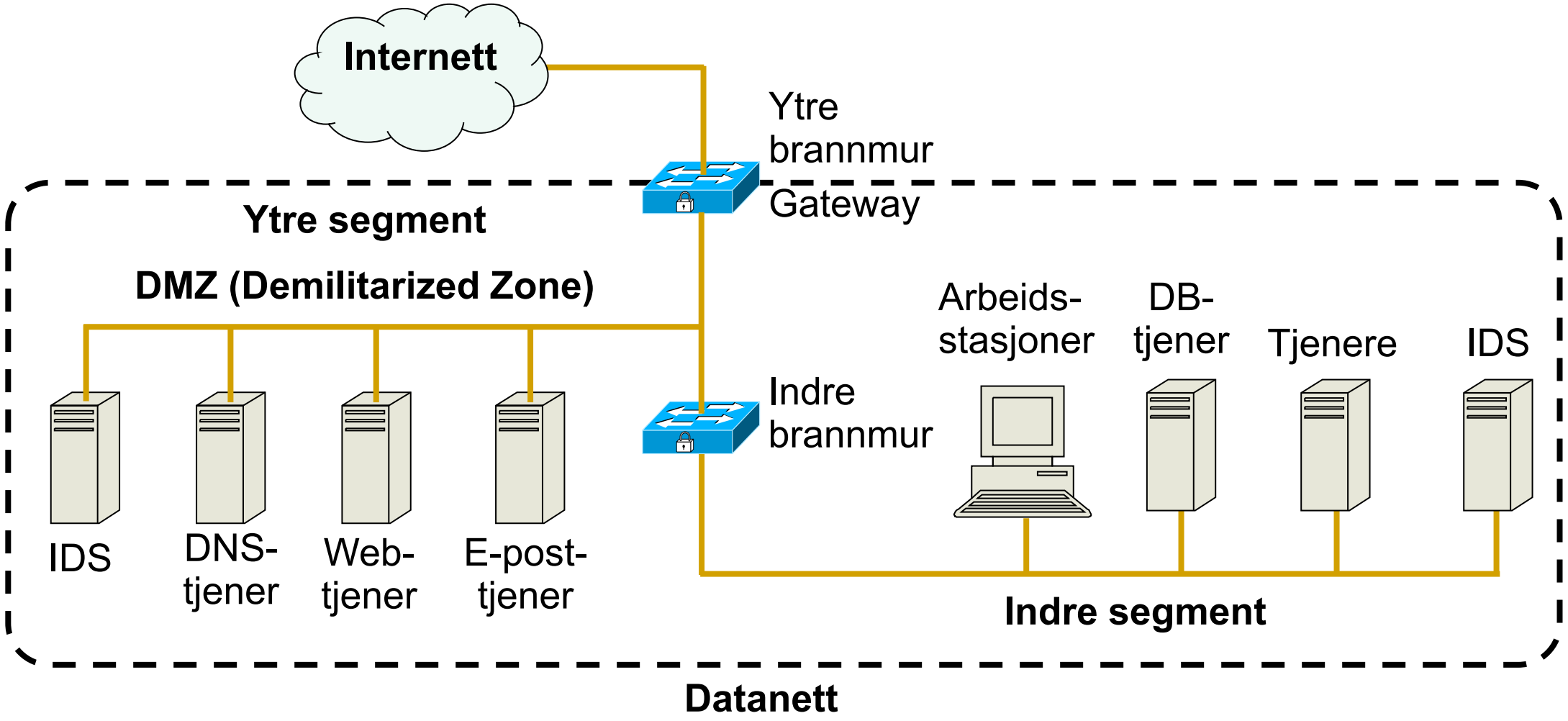


Datanett

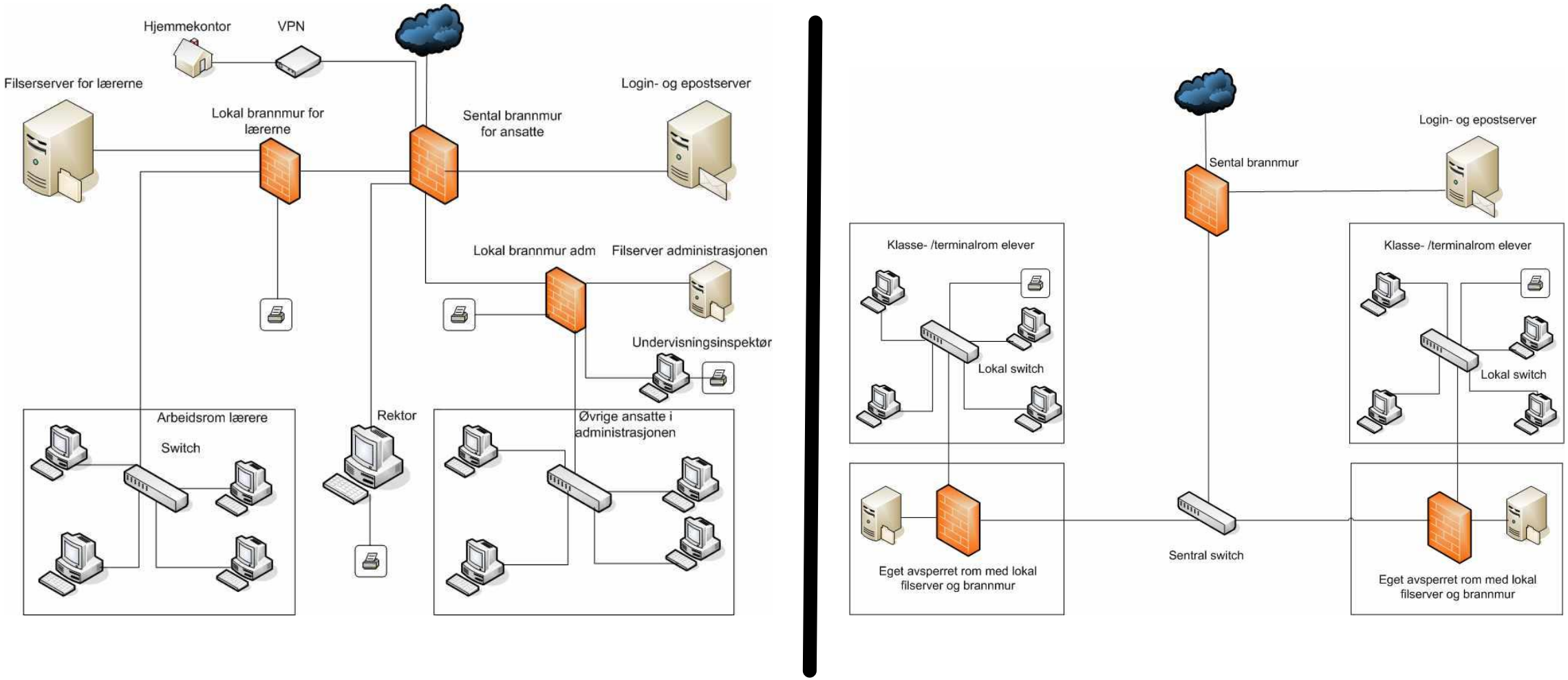
Terminologi

- Nettverkssegment – en spesifikk del av nettverket
- DMZ (demilitarized zone) – eksponert segment, gjerne mot Internett. Evt også mellom ansatt- og indre sikkerhetssoner
- VPN – kryptert virtuell tunnel
- Jumphost
  - Herdet maskin som brukes til å nå et system eller nettverk som ellers ikke er tilgjengelig

Enkel datanettarkitektur med brannmurer

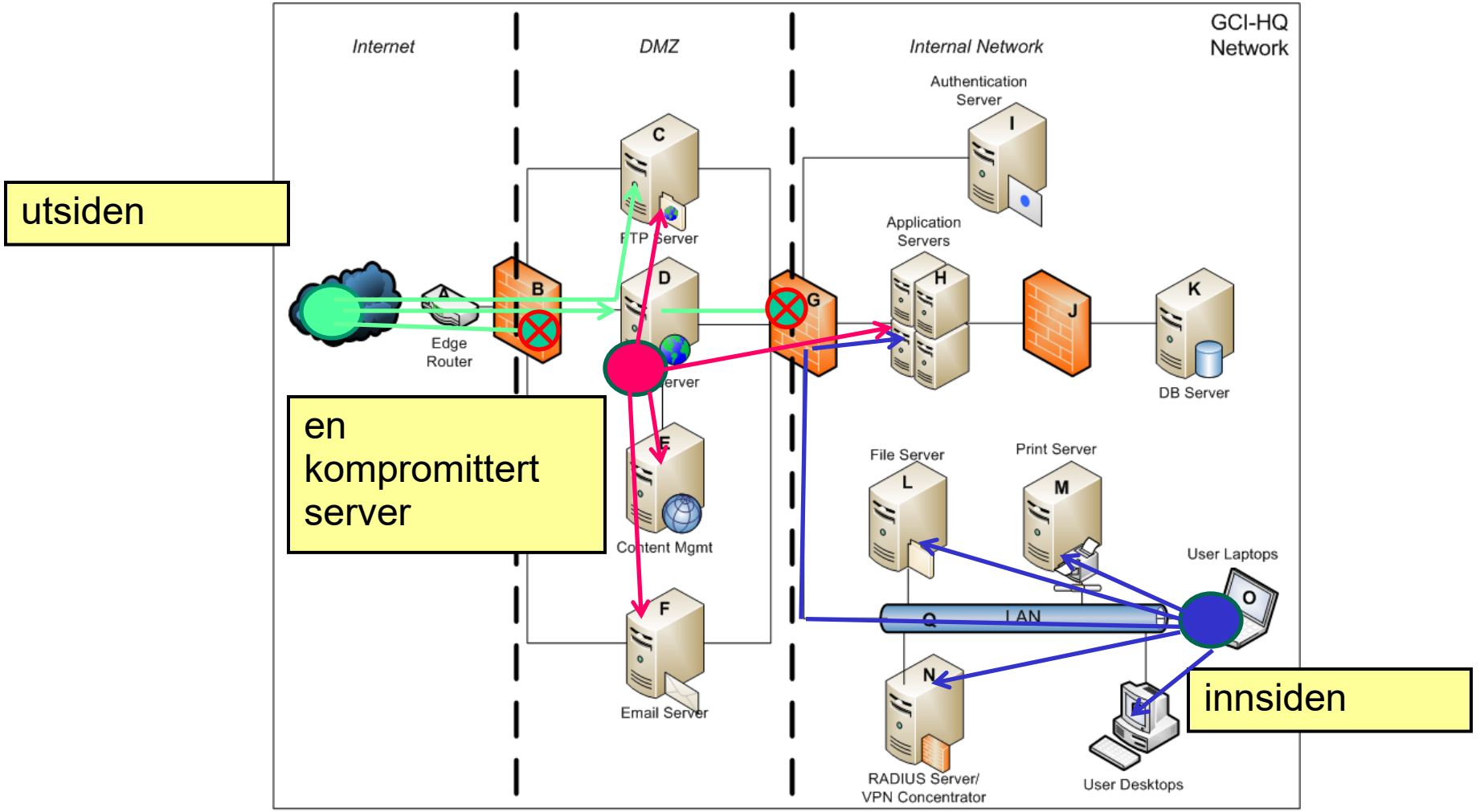


Eksempel på arkitektur for en skole



Kilde: Wien 2005, «En helhetlig sikkerhetsløsning for skolesektoren»

Hvor bør man kartlegge fra?



Standardporter kjente tjenester

- HTTP 80
- HTTPS 443
- SMB 445
- SMTP 25
- SSH 22
- Telnet 23
- RDP 3389
- FTP 21
- DNS 53

Tilstandsløse brannmurer



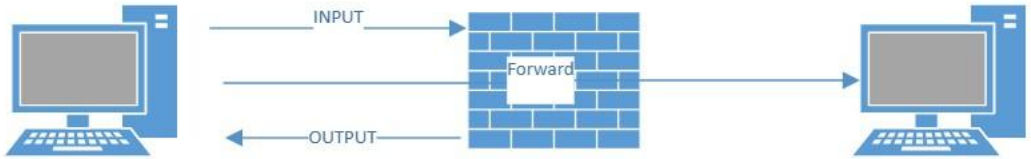
Inspiserer bare pakkehoder

- 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
- Kalles ofte for pakkefilter

iptables –linuxbasert brannmur

- Sett med regler - første treff gjelder

- Input – data inn til selve brannmuren
- Forward – data som skal videresendes
- Output – data ut fra selve brannmuren



Brannmurregler 1

- Prosesseres normalt fra topp til bunn
  - Rekkefølgen er mao avgjørende
  - Sett unntak før hovedregler

- Fordeler
  - Lett å forstå og etterprøve
  - Effektivt – stopper ved første treff

- Enkelte leverandører har andre løsninger
  - Windows Firewall prioriterer alltid blokkering før aksepterende regler

Brannmurregler 2

- Enkelte brannmurer (eks. iptables) har implisitt ACCEPT
  - Slipper igjennom alt som ikke er eksplisitt blokkert
- Anbefaler følgelig eksplisitt DROP all på slutten
  - Blokkerer alt som ikke er eksplisitt tillatt
  - iptables -A INPUT -j DROP
- Eksplisitt DROP er i henhold til prinsippet om minste privilegium
  - Og dermed også Zero Trust.

iptables - eksempel

- 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
- iptables -A INPUT -p tcp -s 131.234.142.33 --dport 21 -j ACCEPT
  - TCP-pakker fra 131.234.142.33 til port 21 direkte til brannmuren aksepteres
- iptables -A OUTPUT -p udp -j DROP
  - UDP-pakker fra brannmuren droppes

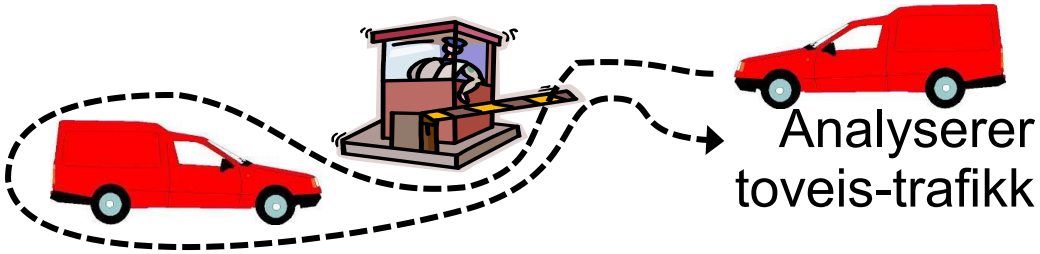
Iptables - eksempel

- iptables -A FORWARD -s 131.234.142.33 -p tcp --dport 80 -j ACCEPT
- iptables -A FORWARD -s 131.234.142.33 -p tcp --dport 22 -j ACCEPT
- iptables -A FORWARD -s 131.234.142.33 -j DROP

  - Hva slipper igjennom fra 131.234.142.33:
  - HTTP
  - HTTPS
  - SSH

  - Hva med HTTP fra 129.240.31.23?

Tilstandsbaserte brannmurer



- Har oversikt over tilstanden i hver forbindelse/økt mellom klient og tjener
- Kan opprette midlertidige regler for spesifikke økter
- Mer fleksibilitet og høy ytelse, men krever minne for å huske tilstand

NAT (Network Address Translation)

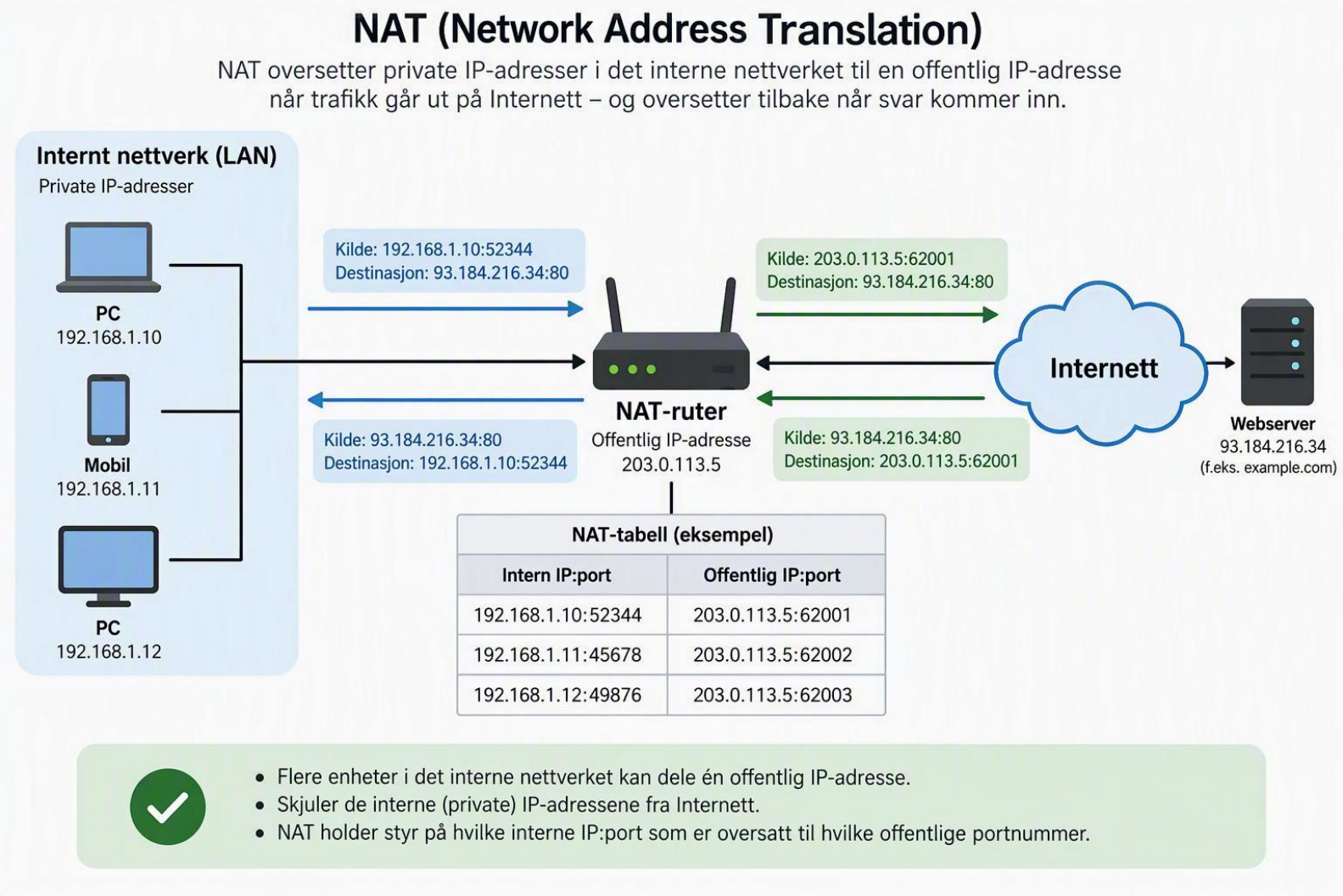
- Enheter i et nettverk kan dele én offentlig IP-adresse når de kommuniserer med Internett.

- Ruter oversetter fra interne til eksterne IP-adresser og portnummer
- Brukes nesten bare på IPv4

- Sparer IPv4-adresser
  - Ikke å regne som en sikkerhetsmekanisme

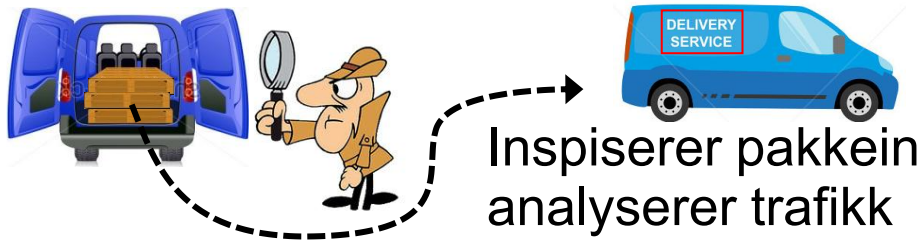
Bildet er AI-generert

NAT



Bildet er AI-generert

Applikasjonsbrannmur



- Inspiserer brukerdata i tillegg til pakkehoder
- Støtter spesifikke applikasjonsprotokoller (HTTP,FTP,…)
- Kan konfigureres for filtrering av spesifikke brukerapplikasjoner (YouTube, Facebook,…)
- Kan filtrere 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 generasjons brannmurer (Next Generation Firewalls)

VLAN (Virtual Local Area Network)

- Logisk segmentering av nettverkssegmenter
  - Programvarebasert
  - Kan for eks dele opp så alle ansatte får eget vlan
- Enkel og billig måte å skille brukere eller utstyr
- NB: trafikk mellom VLAN må filtreres for fungere som tilgangskontroll
- Det finnes angrep – gjerne kalt VLAN-hopping (dere trenger ikke kunne detaljer om disse angrepene).

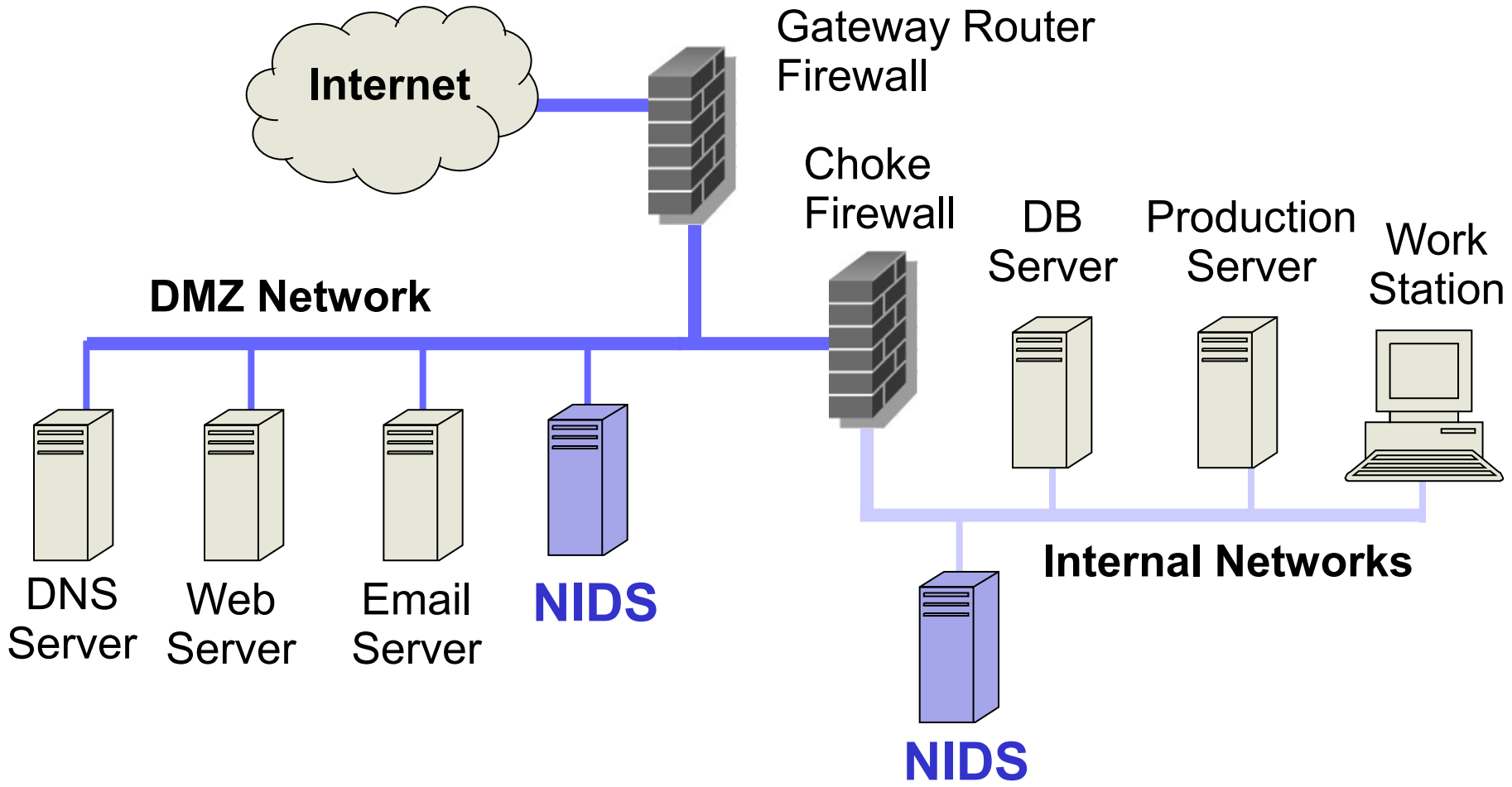
Inntrengingsdeteksjon

Inntrengingsdeteksjonssystemer (IDS) er systemer som forsøker å detektere mistenkelig aktivitet

Inntrengingsdeteksjon

- HIDS (Host-based IDS) forsøker å detektere aktivitet på verten eller systemet den er installert på
  - Overvåker prosesser, filer, filendring, …
- NIDS (Network-based IDS) forsøker å detektere aktivitet på et eller flere nettverkssegment
  - Overvåker nettverkstrafikk

Inntrengingsdeteksjon i nettverk



Merk: Kan også plassere NIDS på utsiden av gateway hvis man ønsker å se all trafikk mot eget nettverk

Signaturbasert inntrengingsdeteksjon

- Kan bare oppdage kjente angrep
  - (som man har signaturer for)
  - Man må (manuelt) utarbeide signaturer
  - Krever ofte at man ser innhold av nettverkspakker (deep packet inspection)
  - Kryptering (gjennom TLS) gjør dem mindre effektive

Signaturbasert Snort og Suricata

- Open source
- Plattformuavhengig

- Kan skrive egne signaturer
  - Begge bruker stort sett samme regelformat

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"; sid:1000001; rev:1;)
```

  - $HOME_NET er en variabel som (typisk) inneholder IP-adresser for eget nett (som skal beskyttes)
  - Genererer alarm ved TCP-trafikk fra $HOME_NET på alle porter til port 22 på IP-adresse 10.0.0.56
  - msg: tekst som vises i alarmen
  - sid: unik ID for regelen (egne regler fra 1 000 000)
  - rev: revisjonsnummer

Eksempel på sårbarhet og Snort-regel

CVE-2017-0147 Detail

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

Source: MITRE
Description Last Modified: 03/16/2017
View Analysis Description



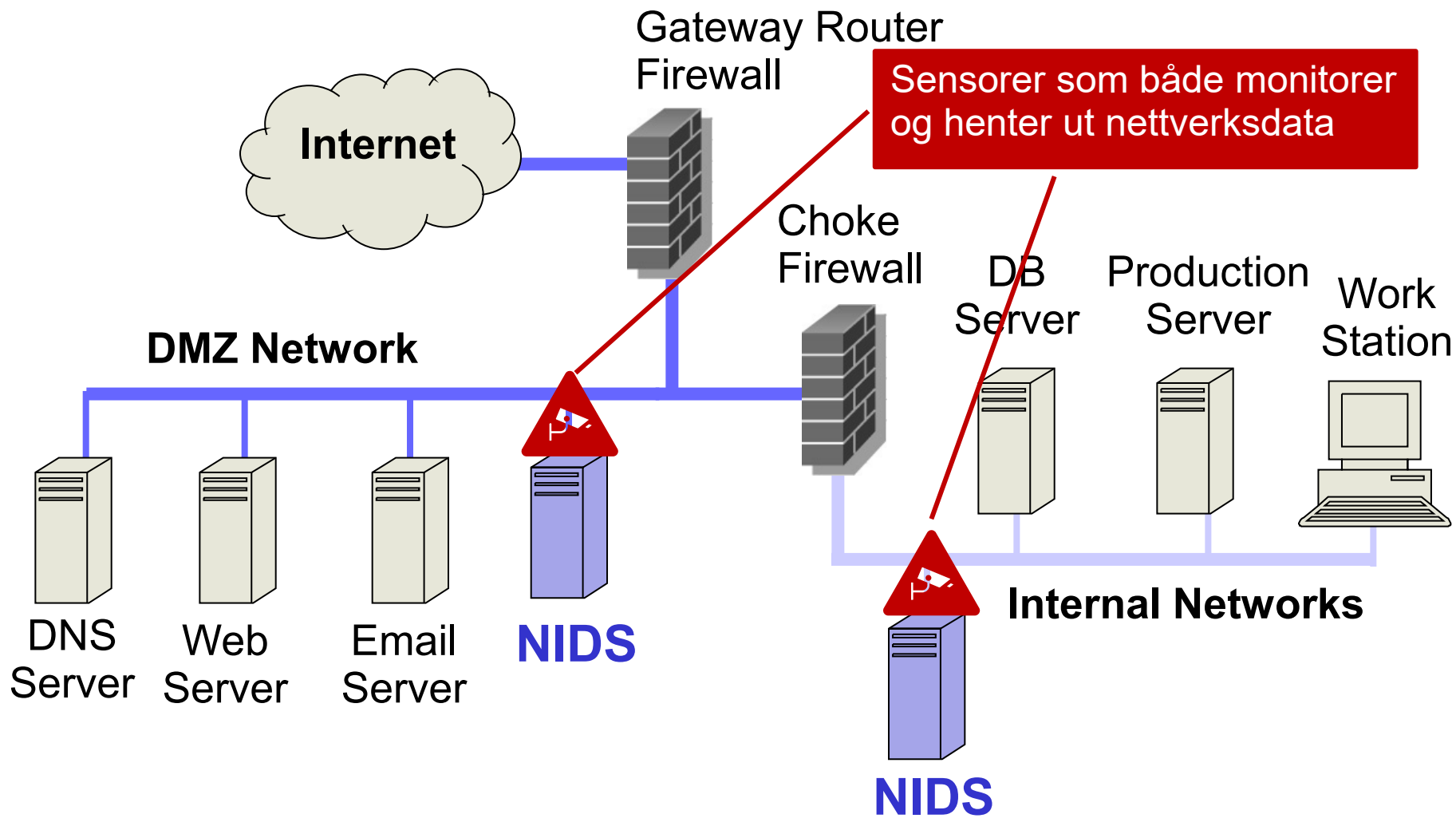

```
alert tcp $HOME_NET 445 -> any any ( msg:"OS-WINDOWS Microsoft Windows SMB possible leak of kernel
heap memory"; flow:to_client,established; content:"Frag",fast_pattern; content:"Free";
content:"|FA FF FF|"; content:"|F8 FF FF|",within 3,distance 5; content:"|F8 FF FF|",within
3,distance 5; metadata:policy balanced-ips alert,policy security-ips drop,ruleset community;
service:netbios-ssn; reference:cve,2017-0147; reference:url,technet.microsoft.com/en-
us/security/bulletin/MS17-010; classtype:attempted-recon; sid:42339; rev:2; )
```

(NB: Denne sliden er et eksempel – trenger ikke å pugges)

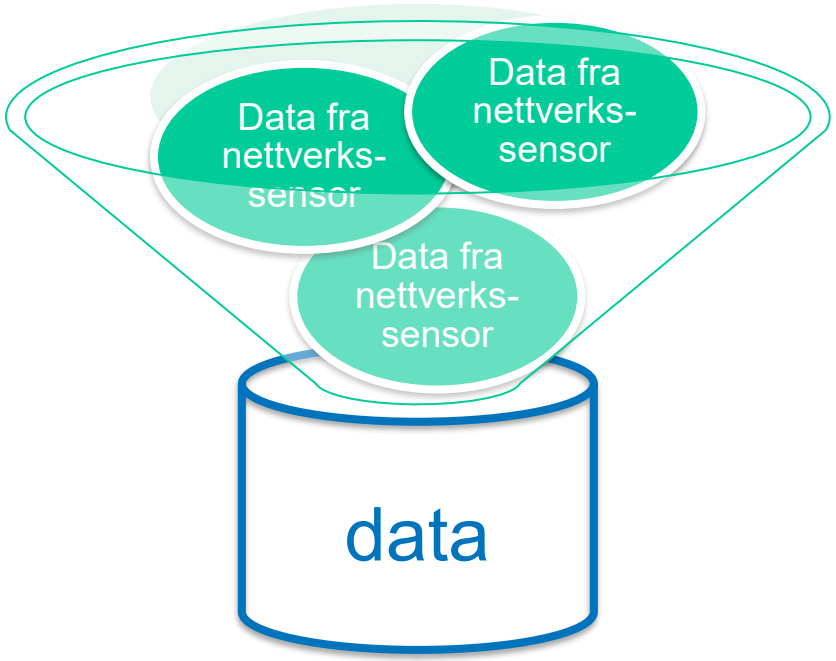
Anomalibasert inntrengingsdeteksjon

- Bruker en modell for normal adferd for å oppdage avvikende adferd
  - For eksempel utløses en alarm når en statistisk sjelden hendelse oppstår
  - Ofte basert på maskinlæring
  - Kan oppdage ukjente angrep
  - ... men vil typisk gi flere falske alarmer

Anomalibasert inntrengingsdeteksjon i nettverk

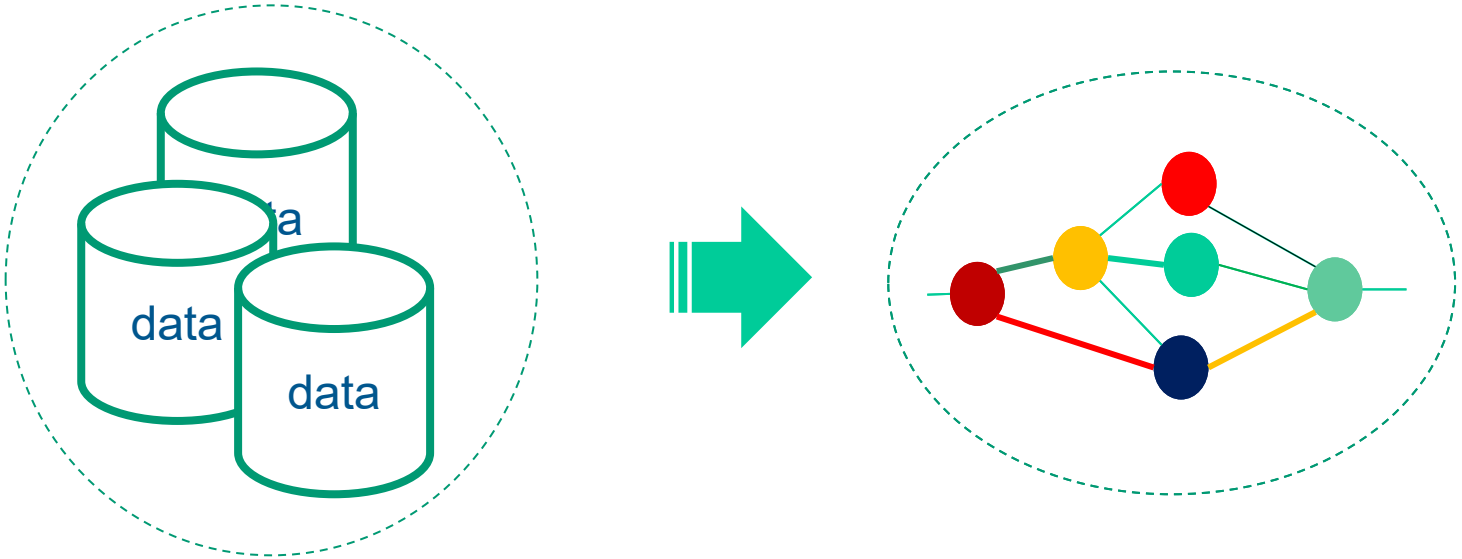


Anomalibasert inntrengingsdeteksjon: maskinlæring



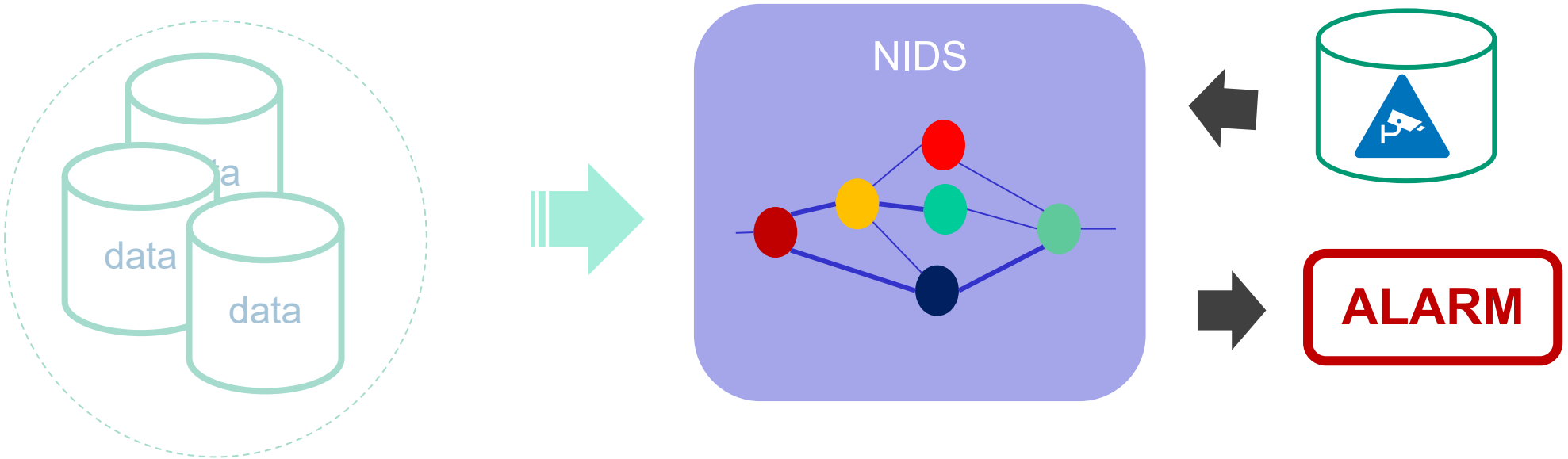
- Henter inn data fra de ulike sensorene fra ulike logger
- For større virksomheter vil det typisk gi veldig store datamengder

Anomalibasert inntrengingsdeteksjon: maskinlæring



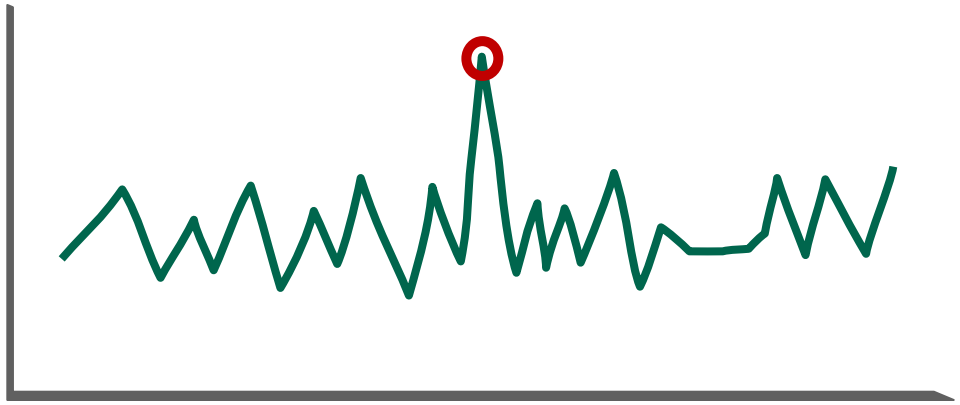
- Data brukes til å trene opp en maskinlæringsmodell
- Typisk har en slik modell mange parametere
  - Maskinlæring bruker data for å finne optimal verdi av parameterne for å kunne bruke maskinlæringsmodellen til deteksjon
  - F.eks. en modell for «normal» adferd

Anomalibasert inntrengingsdeteksjon: maskinlæring



- NIDS bruker maskinlæringsmodellen
- Når systemet overvåker vil NIDS gi alarm basert på svar fra maskinlæringsmodellen
  - Kan for eksempel være at oppførsel observert avviker vesentlig fra normal adferd som maskinlæringsmodellen har lært.

Anomalibasert inntrengingsdeteksjon: eksempel



- Graf over kan for eksempel være nettverkstrafikk mot en tjener
- Rød sirkel indikerer et avvik (en anomali)
  - Med andre ord observeres det vesentlig mer trafikk enn normalen
- Dette kan da resultere i en alarm som må håndteres

Aktiv inntrengingsbeskyttelse (IPS)

- Tilsvarende IDS, men aktiv beskyttelse
  - Automatisk legger inn brannmurregler
  - Automatisk blokkerer tjenester

- Ofte integrert i NGFW
  - Ressurskrevende
  - Falske alarmer kan blokkere legitim trafikk (DoS)
  - Angriper kan spoofe IP-adresser og blokke dem

Honningkrukke (Honeypot)

- Et falskt, men attraktivt mål
  - Gjerne upatchet og usikret
  - All trafikk er illegitim
  - Overvåk all trafikk til og fra
  - Se hva angriperen gjør på maskinen



Bildet er ai-generert

Mørke ip-adresser (Honeypot)

- Avsatte/ubrukte IP-adresser
  - Ikke i bruk
  - All trafikk er illegitim
  - Billig «honeypot»



Bildet er ai-generert

Slutt på presentasjonen