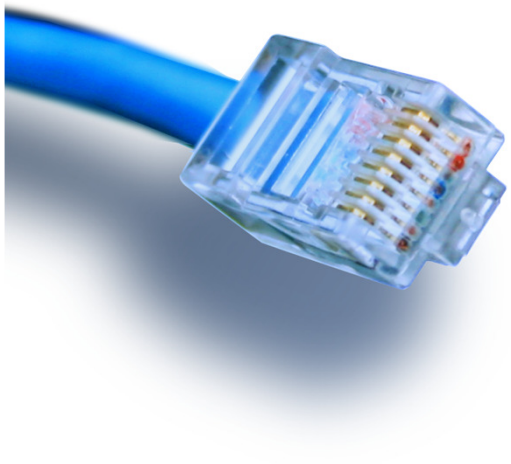
HOUSE OF TECHNOLOGY

– en del af mercantec



Sikkerhed på net

- en introduktion!

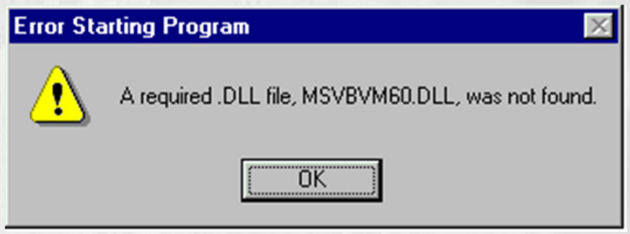
Netteknik

Svage punkter ved IT og net

HOUSE OF TECHNOLOGY

– en del af mercantec

- 'Altid' fejl i helt ny hard- og software!



- Den menneskelige faktor:
  - Sjusk, fejl og dovenskab
- Social hacking:
  - Medarbejdere snydes til udlevering af data
- Mangelfuld organisering af IT-området
  - Mangelfuld uddannelse af brugere og admins
  - Utilstrækkelige retningslinier for sikkerhed
  - IT Sikkerhedsmanual på 800 kedelige sider …

Svage punkter ved IT og net

HOUSE OF TECHNOLOGY

– en del af mercantec

- Upålidelige softwaredesigns
  - Sikkerhed i programmerne er en svær disciplin for mange programmører …
  - Manglende eller mangelfuld kryptering på kommunikation …
- Upålidelige hardwaredesigns / Ubeskyttet hardware
  - Manglende UPS-anlæg (Nødstrømsanlæg)
  - Ubeskyttede tekniske installationer.
    - Fysisk adgang til udstyr giver hackere nem adgang
      - Servere, routere og switche SKAL være i aflåste skabe/rum …
- Problematiske teknologier
  - Trådløse netværk – kan nås af ALLE indenfor radiodækning …
  - Cloud – hvem ejer og hvem tilgår vores data …

Sikkerhed på net er mange ting ...

HOUSE OF TECHNOLOGY

– en del af mercantec

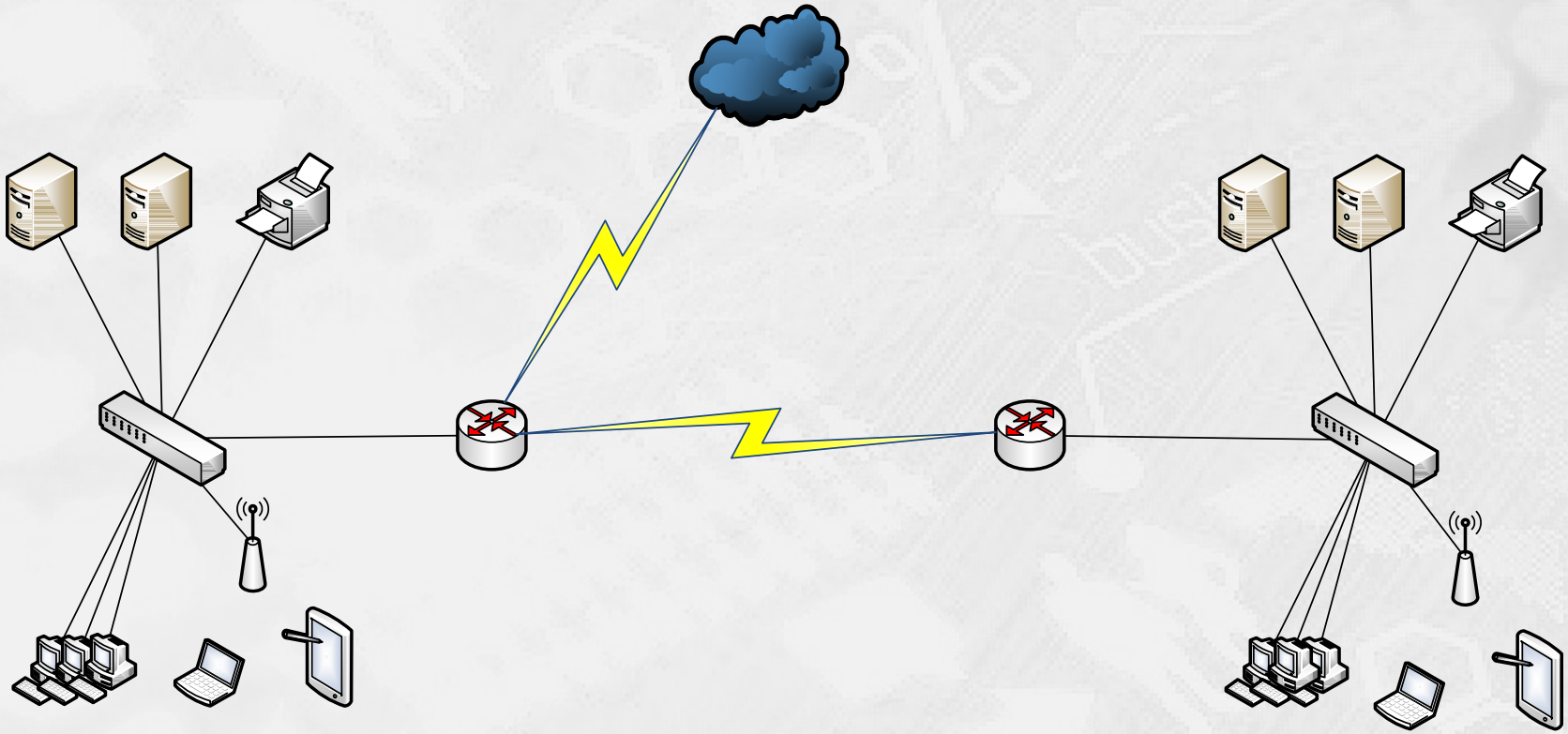
- Prøv at besvare følgende spørgsmål:
  - **Trådløse net** og **mobile enheder** – hvordan sikrer vi det?
  - **Klienter, servere og netværksenheder –** sikkerhedsforskelle?
  - **Datasikkerhed** – hvem har adgang til vores data?
  - **VPN** – er min hjemmearbejdsplads sikker nok?
  - **Kryptering** – bruger jeg en sikker kryptering?
  - **Protokollerne** – hvor godt sikret er de?
  - **Webserveren** – hvordan er 'security best practice'?
  - **Virus og ransomware** – hvordan beskytter jeg firmanettet?
  - **SpyWare, Adware, Pop-ups…** – bliver det bare ved?
  - **Fysisk sikring** – er det virkelig nødvendigt?

Sikkerhed – ja tak, men hvilken?

HOUSE OF TECHNOLOGY

– en del af mercantec

- **Hvilken type sikkerhed skal der til - og hvor?**



Sikkerhed – ja tak, men hvilken?

HOUSE OF TECHNOLOGY

– en del af mercantec

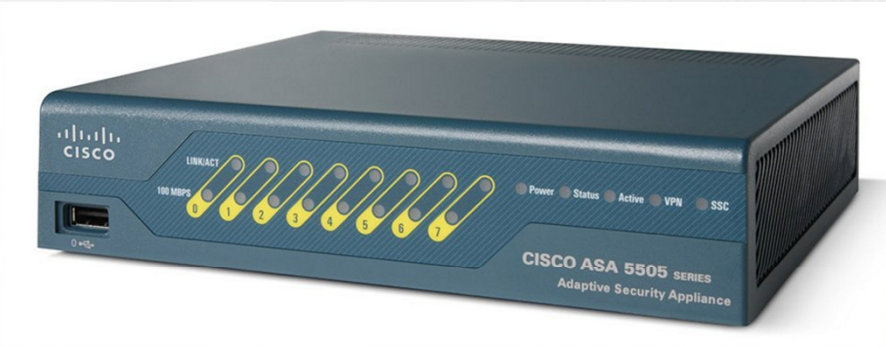
- **Klient-pc'er, Tablets, Smartphones**
  - Opdateringer, Antivirus, E-mail protection, Web browser protection, Firewall, Location service, Anti-theft, Password/Authentication-beskyttelse
- **Servere, f.eks. Microsoft ForeFront 2010**
  - Serveren selv: Opdateringer, Antivirus, E-mail protection, Web browser protection, Firewall, Password/Authentication-beskyttelse
  - Services: Firewall (Application layer, Network layer), Secure Web Access (Proxy, HTTP antivirus/antispyware, URL filter, HTTP Forward Inspection), E-mail protection (Mail-integration, Antivirus, Antispam), Intrusion Prevention (Network Inspection System), Remote Access (VPN med NAP, SSTP integration), Deployment/Management (Tracking, Reporting), Subscription (Malware, URL Filter, IPS), IPsec support

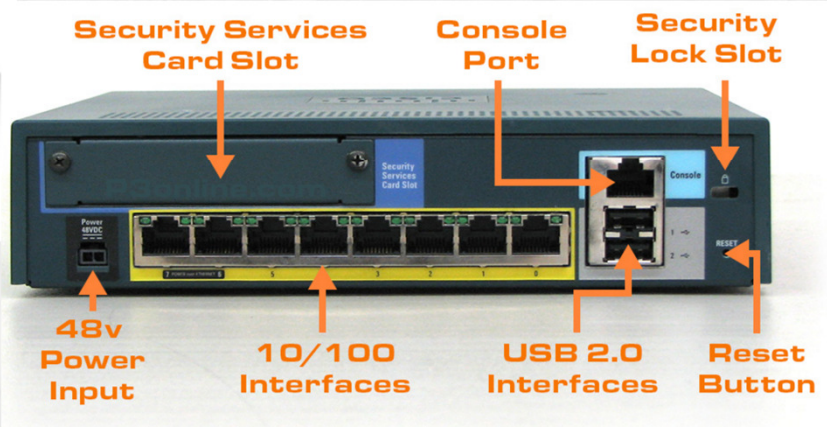
Sikkerhed – ja tak, men hvilken?

HOUSE OF TECHNOLOGY

– en del af mercantec

- Netværksenheder:
  - Firewall enhed, f.eks. Cisco ASA:
    - Enheden selv: Opdateringer, Password/Authentication-beskyttelse
    - Links:
      - http://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-security-appliance/model.html
      - http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733510.html





Styresystemer og sikkerheden

HOUSE OF TECHNOLOGY

– en del af mercantec

- **Angreb på forskellige styresystemer til netværk** kan groft opdeles i følgende typer:
  - **Konto- og adgangskode-angreb**
  - **Netværksangreb**
  - **Angreb ved udnyttelse af applikationer**
  - **Sabotageangreb**
- Af **styresystemer til netværk** kan nævnes
  - UNIX, Linux, Solaris, Novell NetWare, alle Windows Server versionerne osv. ...
  - Kender du navne på flere?

Hackerens primære mål

HOUSE OF TECHNOLOGY

– en del af mercantec

- Hackerens 'største gevinst':
  - En 'overtaget' maskine på et større netværk!
  - En maskine, hvor hackeren kender administrator- eller root - password kan være af stor betydning - og til megen nytte - for en enkelt eller en hel gruppe af hackere
  - Maskinen benyttes (misbruges!) ofte som **server** for gruppens mere eller mindre lyssky foretagender:
    - **Angreb på andre maskiner eller distribution af illegale data**, f.eks. børneporno og hackerværktøjer
    - **Pengeafpresning** ved hjælp af ransomware eller DDOS angreb giver en meget stor indtjening
    - **Politisk eller offentlig indflydelse** ved at fremskaffe og offentliggøre fortrolige dokumenter, f.eks. Edward Snowden

Angrebsformer

HOUSE OF TECHNOLOGY

– en del af mercantec

- **Konto- og adgangskode-angreb**
  - Formålet er helt klart at skaffe sig adgang til hele maskinen eller dele heraf
  - Metoderne varierer fra simpelt gætteri til avancerede hacker-programmer
- **Netværksangreb**
  - Formålet er det samme som ovenstående
  - Metoderne udnytter svaghederne i de anvendte netværksstyresystemer og -protokoller

Svagheder i programmer

HOUSE OF TECHNOLOGY

– en del af mercantec

- Angreb ved **udnyttelse af de svagheder der altid er i programmerne** på maskinen:
  - Formålet varierer fra sabotage over indbrud & overtagelse til lækage af følsomme data.
  - Metoderne her er knyttet til de forskellige programmer.
  - Mest kendt er nok de sikkerhedsproblemer der har været med Microsofts Messenger og lignende programmer som direkte 'annoncerer' sig selv til alle de andre på Internettet.

HOUSE OF TECHNOLOGY

– en del af mercantec

- **Sabotageangreb**
  - Også kaldet Denial of Service (DoS) Attacks
  - Formålet er at gøre modtagersystemet ustabilt - og helst at få det til at gå helt ned!
  - Efterfølgende afpresser man typisk firmaet bag modtagersystemet for at få penge, holdningsændringer eller prøver at få bestemte politiske udtalelser frem
  - Metoderne varierer fra begreber som **Ping of Death**, **SYN Flooding**, **CPU-angreb** og til **SMB-crashes**
  - Der findes en speciel variant af DoS Attacks, nemlig **Distributed DoS Attacks (DDoS)**
    - Mange angriber samtidigt (Evt. via en virus/trojansk hest)

De forskellige typer **vira**

HOUSE OF TECHNOLOGY

– en del af mercantec

- Boot-virus
  - angriber en computers boot-sekvens
  - resultatet er ofte en computer der nægter at starte op
- System-virus (klynge-virus)
  - angriber typisk File Allocation Table
  - resultatet er ofte en computer med rod i filsystemet
- Program-virus
  - den klassiske type, nemlig et program der skjuler sig
  - udfører skumle aktiviteter uden brugeren ved det!
- Polymorfe virus
  - almindelig virus der kan ændre 'udseende' så antivirus programmerne ikke kan finde det
  - angriber computere ganske som andre virus, men de er næsten umulige at udrydde helt
- Stealth-virus
  - almindelig virus der kan 'skjule sig' i f.eks. Boot- eller filområdet på en harddisk
  - angriber computere ganske som andre virus, men de er svære at udrydde helt
- Retro virus
  - almindelig virus der målrettet går efter at slette antivirus programmerne!
- Data-virus
  - en nyere type virus, der typisk udnytter makrokommandoer eller PostScript, begge programmeringssprog, der ofte findes på Pc'er
  - Resultaterne spænder fra uskyldig selvkopiering til sletning af systemfiler!
- Trojanske heste
  - når et angreb lykkes bliver Pc'en, som navnet antyder, angrebet indefra! Der installeres diskret et lille spion-program på maskinen.
  - resultatet kan være at der diskret indsamles kodeord og andre login informationer, som efterfølgende elegant sendes til hackeren med en e-mail!
- Worms
  - en bestemt type virus der kan 'formere' sig over datanetværk
  - er ofte i brug før et større 'angreb' af f.eks. DoS

Beskyttelse mod vira

HOUSE OF TECHNOLOGY

– en del af mercantec

- Virksomheder bør oprette en **virus-handlingsplan,** og gennem den
  - få styr på alle fjern-dataforbindelser, f.eks. Internet og Dial-Back
  - få styr på alle softwarekilder
  - få styr på gæsteindgange og samarbejdspartnere
  - installere antivirus software
  - have effektiv backup!
  - kunne fjerne vira hurtigt og effektivt (beredskab)

SpyWare is watching you!

HOUSE OF TECHNOLOGY

– en del af mercantec

- Det er næsten umuligt at surfe rundt på Internettet med en Browser i dag uden at **få installeret en masse uønskede spion-programmer**, også kaldet Spyware, på sin maskine
- Spywaren **opsamler informationer om brugerne adfærd** på nettet, og denne information sælges herefter til en masse forskellige firmaer verden over som f.eks. sælger varer via webshops på nettet
- Der er **millioner af kroner på spil her** og det er umuligt at helt at stoppe det
  - Brug **uddannelse af brugerne** som effektivt middel til at mindske problemet – det er overraskende effektivt!
  - **Fjern alle unødvendige hjælpeprogrammer,** f.eks. Java og Adobe Shockwave, som f.eks. benyttes af ransomware programmerne
  - Brug **en effektiv opdateringsservice**, f.eks. WSUS / Windows Update til at holde maskinerne opdateret – dette forbedrer sikkerheden klart

Adware, Malware & Ransomware

HOUSE OF TECHNOLOGY

– en del af mercantec

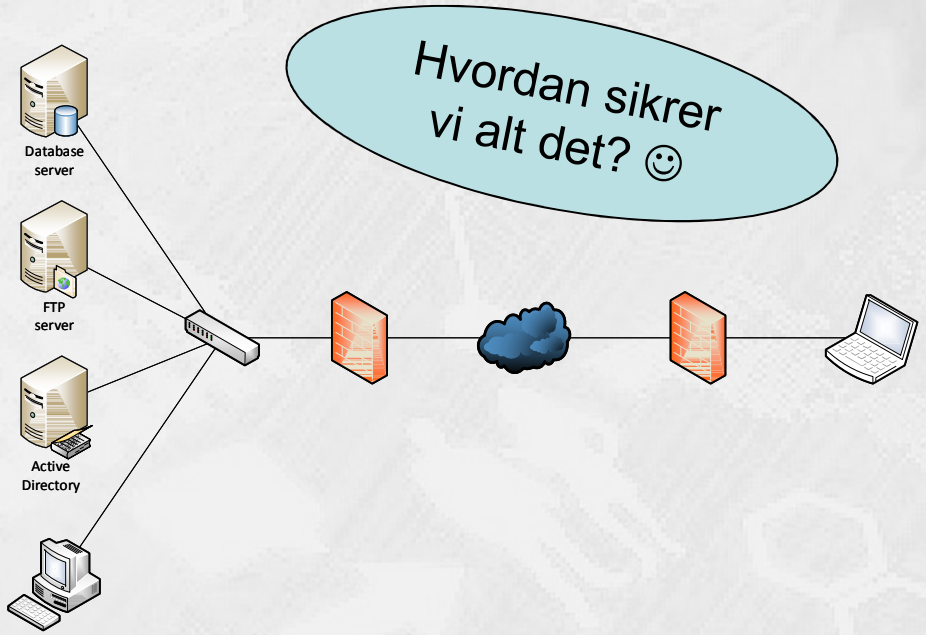
- Begrebet **adware** anvendes om programmer, som viser reklamer.
- Begrebet **malware** anvendes om programmer, som f.eks. ødelægger andre programmer på pc'en.
- Begrebet **ransomware** anvendes om programmer, som f.eks. overtager/krypterer alle data på pc'en, hvorefter hackeren afpresser brugeren for penge mod at få udleveret krypteringsnøglen, så man kan få adgang til sine data igen.
  - Desværre meget effektivt, og ofte er det svært at få adgang til data selvom man betaler et par gange ☹
- ***Derfor: Husk at tage backup - ofte!***

Datasikkerhed – hvad er det?

HOUSE OF TECHNOLOGY

– en del af mercantec

- Ifølge den engelske wiki er datasikkerhed defineret som:
  - "Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users."
- Det er vigtigt at huske at data også kan være
  - På netværk på vej mellem en medarbejder-pc og en arbejdsplads
  - På en bærbar glemt i toget
  - På en smartphone tabt i bussen …
  - I luften, som radiobølger, mellem en bærbar og AP'et
  - Osv… ;-)



Datasikkerhed – og begreberne

HOUSE OF TECHNOLOGY

– en del af mercantec

- **Confidentiality - Fortrolighed**
  - Kun tiltænkte modtagere ser indhold
- **Authentication – Pålidelighed**
  - Sikkerhed for at afsenderen/modtageren er - og forbliver - den rigtige afsender/modtager.
- **Integrity Checking – Helheds check**
  - At data ikke er blevet ændret mellem afsender og modtager
- **Non-Repuditation – Ikke fornægtelse**
  - Afsender kan ikke senere nægte at have sendt data

Datasikkerhed – IPsec begreber

HOUSE OF TECHNOLOGY

– en del af mercantec

- Indenfor IPsec dukker der et par ekstra begreber op:

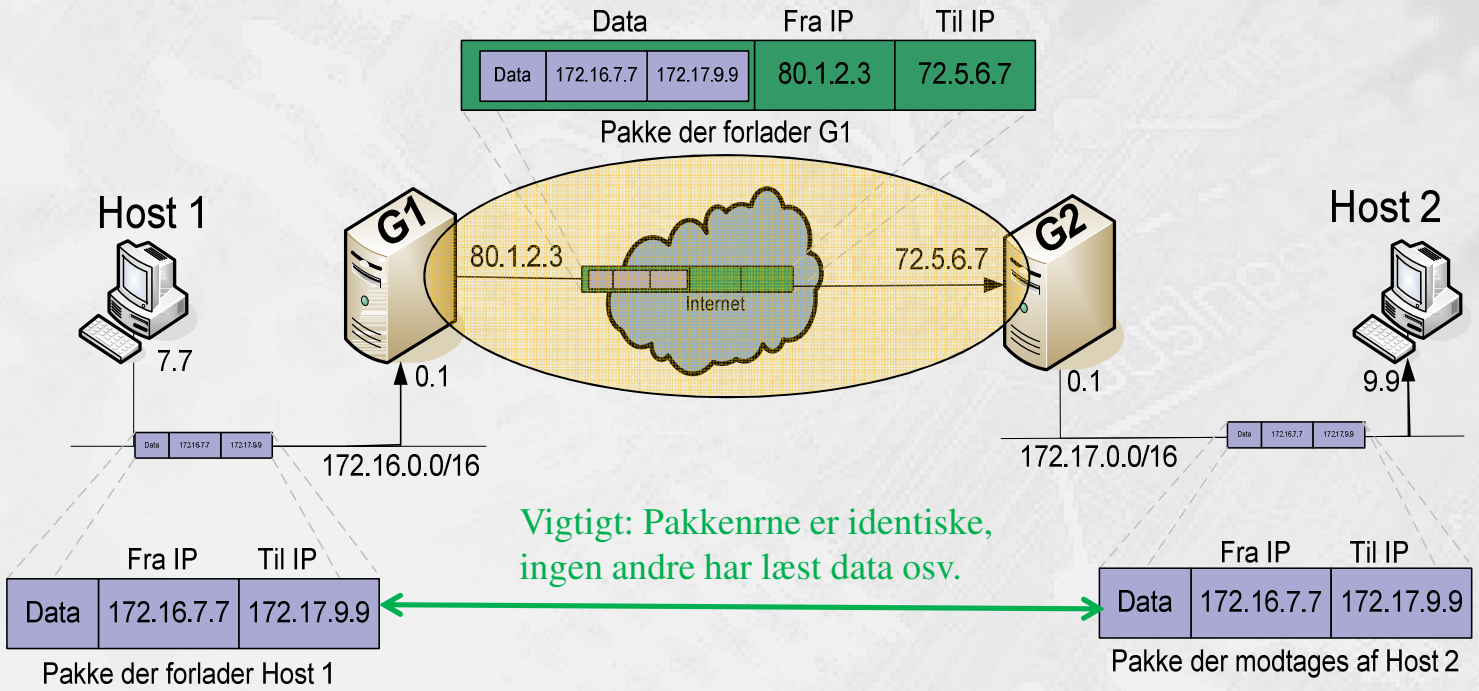
- **Anti-replay protection – Data kan ikke gengives i transport**
  - Kun tiltænkte modtagere ser indholdet

- **Key management – Håndtering af kryptonøgler**
  - Et feature som på en sikker måde udveksler og håndterer alle nødvendige kryptonøgler i systemet

VPN – en introduktion

HOUSE OF TECHNOLOGY

– en del af mercantec



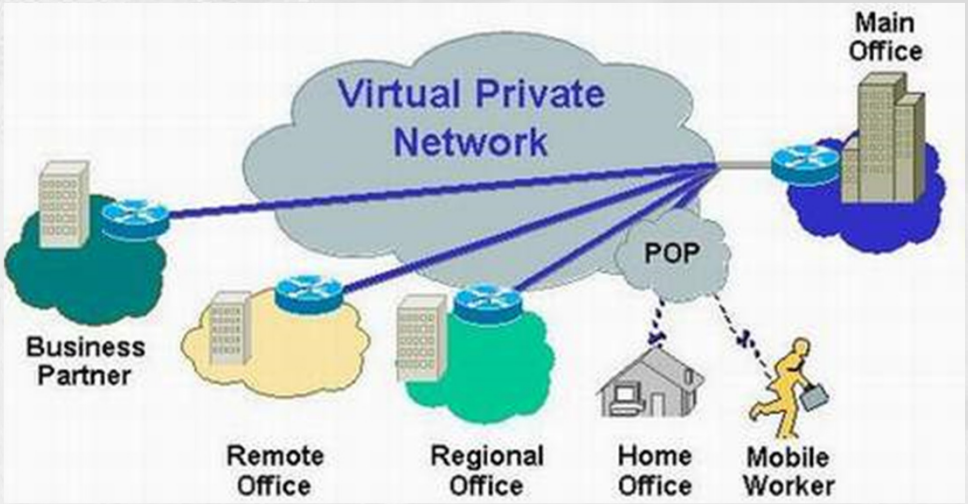
- - datasikkerhed på tværs af usikre netværk

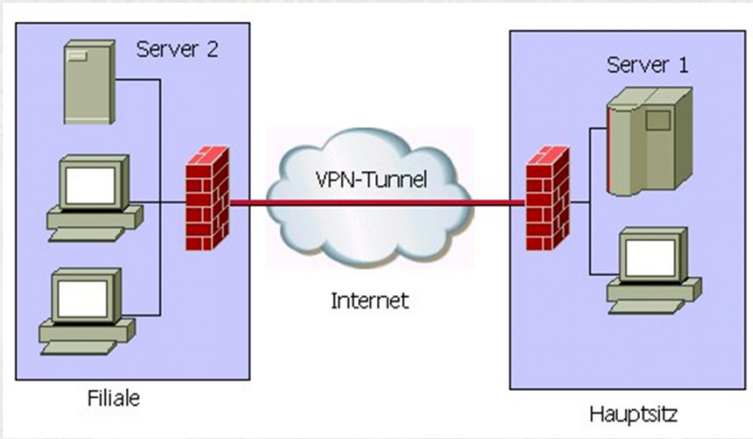
Hvad er et VPN?

HOUSE OF TECHNOLOGY

– en del af mercantec

- VPN - Virtual Private Network
- Et privat net (tunnel) gennem et offentligt net, fx Internettet
- Et VPN er et antal tilslutninger til et Backbone net som må udveksle trafik.
- Medlemmerne i et VPN må ikke udveksle trafik med andre.
- Et VPN er defineres af et sæt regler der
  - Definerer connectivitet og QoS mellem tilslutninger i VPN'et.

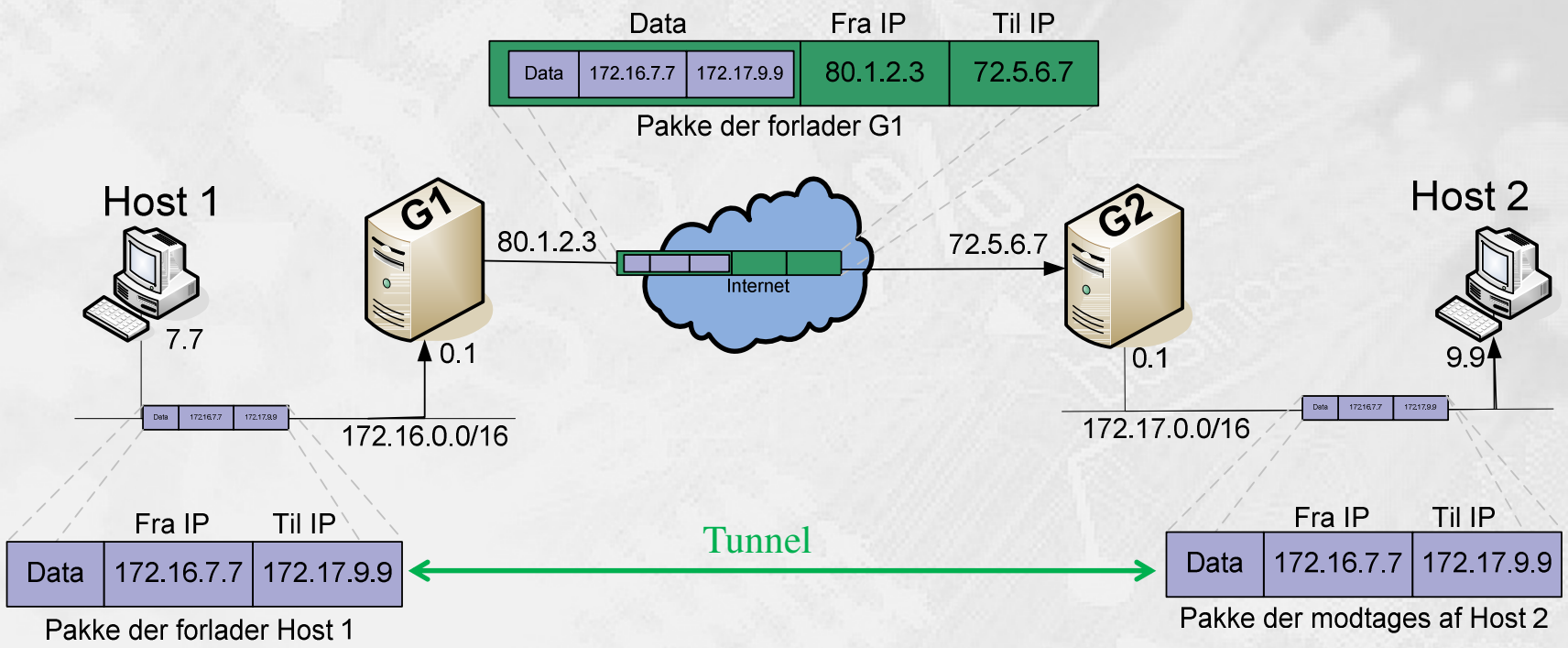




VPN Tunneling

HOUSE OF TECHNOLOGY

– en del af mercantec



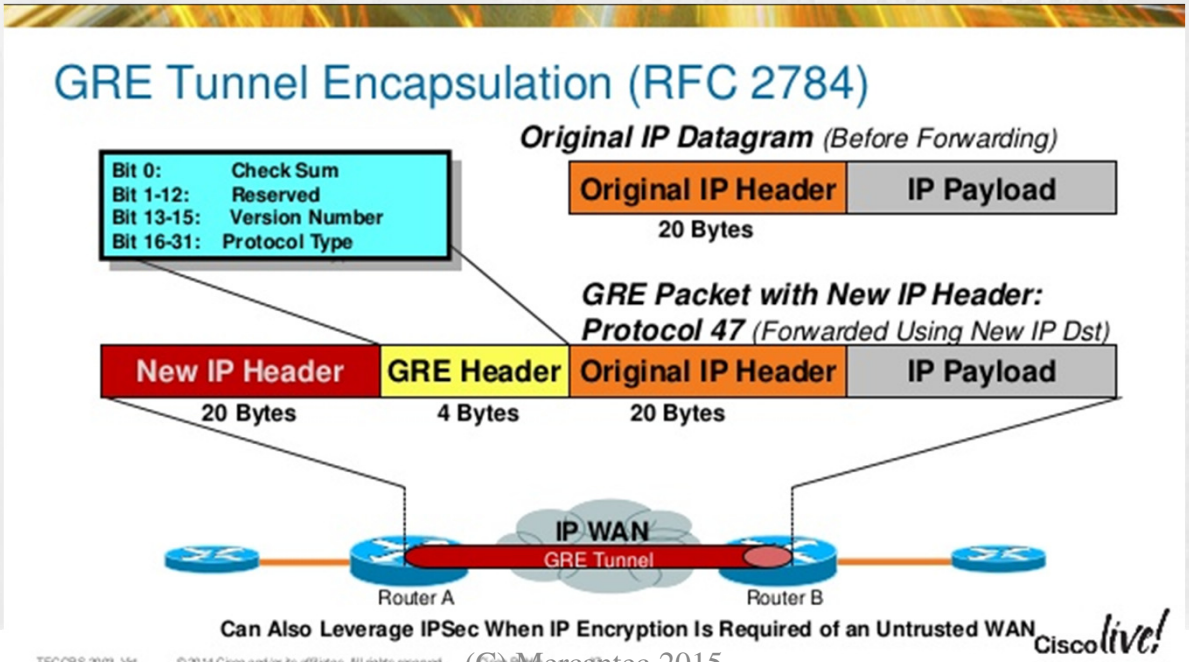
- Definition: En tunnel er **en vej mellem to enheder** – typisk to Gateways (G1 & G2) – hvorigennem trafik **kan passere uændret**

Tunneling protokoller

HOUSE OF TECHNOLOGY

– en del af mercantec

- Tunneling (uden kryptering) kræver 3 forskellige protokoller:
  - En passager protokol – dvs. de **originale data** (**IP**, NetBEUI, IPX) som overføres
  - Encapsulation (indpakning) protokol – Protokollen som de originale data er pakket ind i (fx **GRE**, IPSec, L2F, PPTP, L2TP)
  - En bærer protokol (fx. **IP**) som anvendes til at transportere informationen



Tunneling protokoller

HOUSE OF TECHNOLOGY

– en del af mercantec

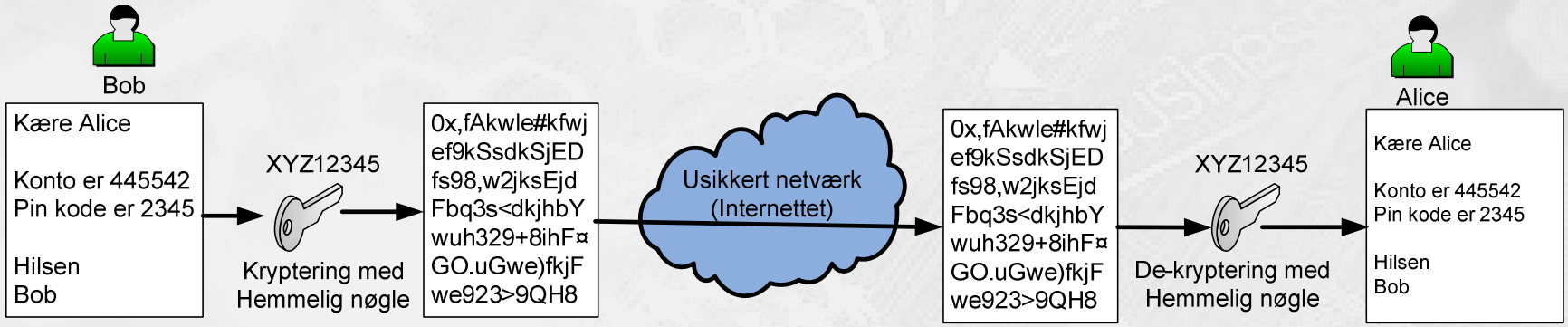
- Et eksempel på en '**netværks lag over netværks lag**' tunnel:
  - **GRE** (generic routing encapsulation)
    - Traditionel tunneling - beskrevet i RFC1701 og 1702.
- Et eksempel på en '**datalink lag over netværk lag**' tunnel:
  - **L2TP** (layer 2 tunneling protocol)
    - Client-Server protokol som kombinerer mange faciliteter fra PPTP og L2F (layer 2 forwarding)
  - **PPTP** (point to point tunneling protocol)
    - Client-Server protokol som er meget benyttet i forbindelse med Microsoft klienter
    - Understøttes af næsten alle Windows operativ- og filsystemer
    - Benytter Microsoft MPPE kryptering
  - **L2F** (Layer 2 Forwarding)
    - Udviklet af Cisco og L2F kan bruge alle type authentication som understøttes i PPP

Kryptering

HOUSE OF TECHNOLOGY

– en del af mercantec

- At kryptere en besked er at *prøve* at gøre beskeden umulig at læse mellem afsender og modtager
- At de-kryptere en besked er at gøre den læselig igen.



HOUSE OF TECHNOLOGY

– en del af mercantec

- Symmetrisk nøgle
  - Samme nøgle anvendes til kryptering og dekryptering
  - Udveksling af hemmelige nøgler en sikkerheds risiko

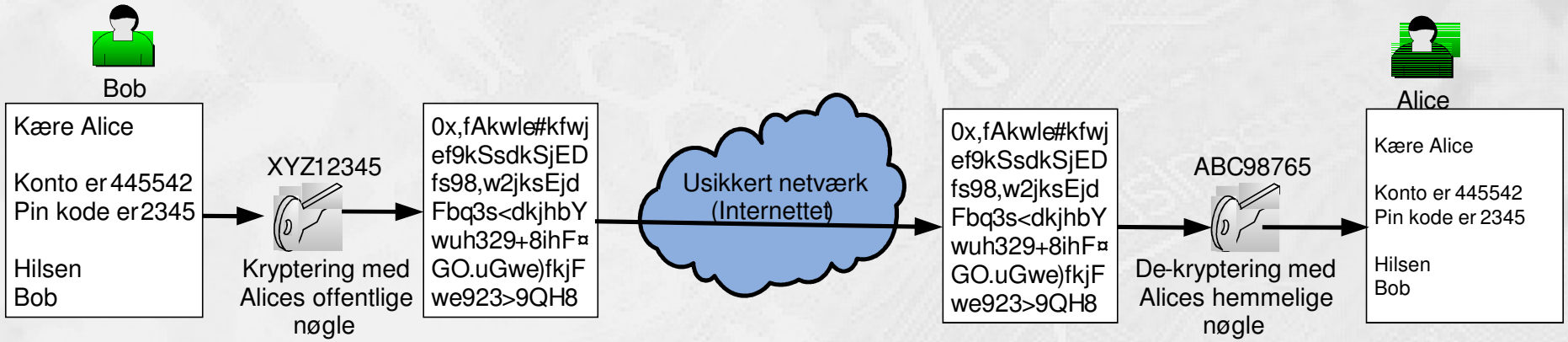
- Asymetriske nøgler
  - Forskellige nøgler - en privat *og* en offentlig - anvendes til kryptering og dekryptering
  - Udveksling af offentlige nøgler *ingen* sikkerheds risiko.

Asymmetriske nøgler

HOUSE OF TECHNOLOGY

– en del af mercantec

- Alice sender Bob sin offentlige nøgle i en almindelig mail

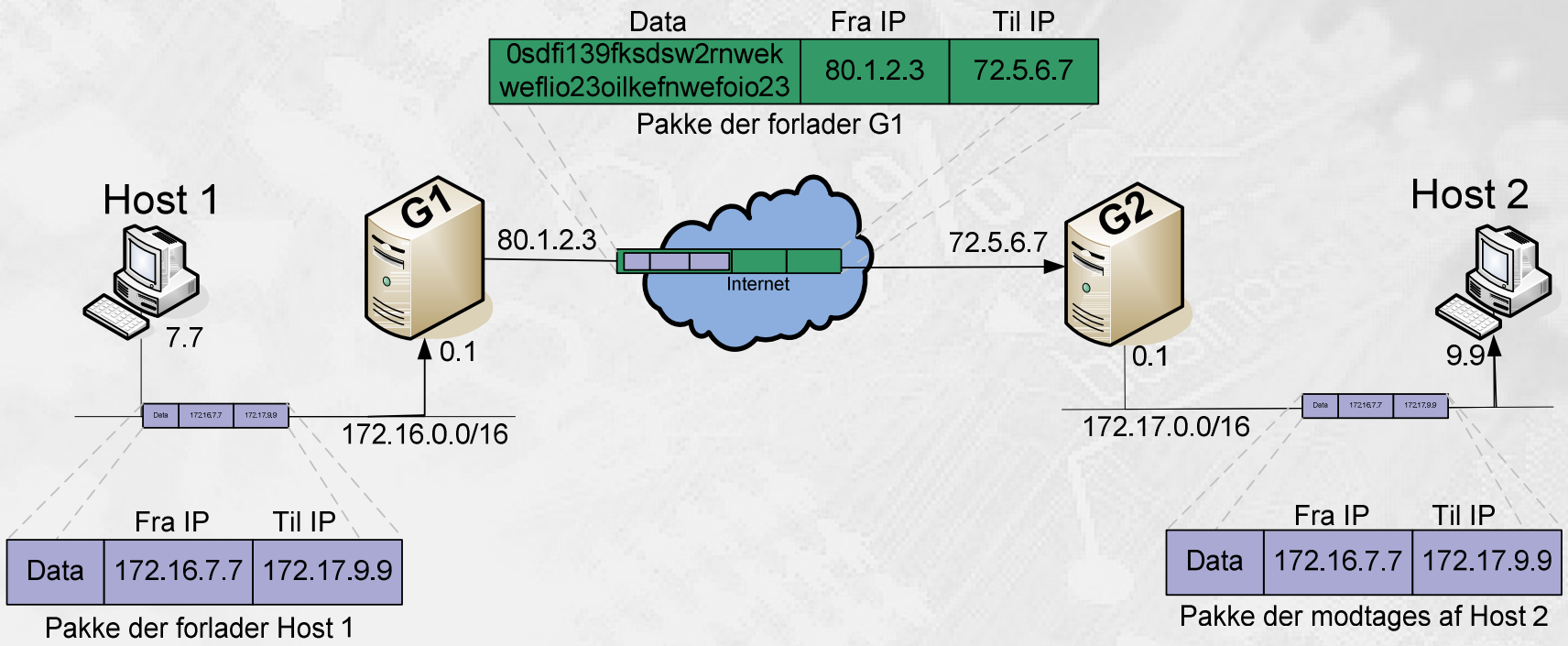


- Nøglerne fungerer matematisk ved at anvende meget store primtal. (200 cifre eller mere)
- Alice kan sende data til Bob, ved at få hans offentlige nøgle

Kryptering og Tunneling

HOUSE OF TECHNOLOGY

– en del af mercantec



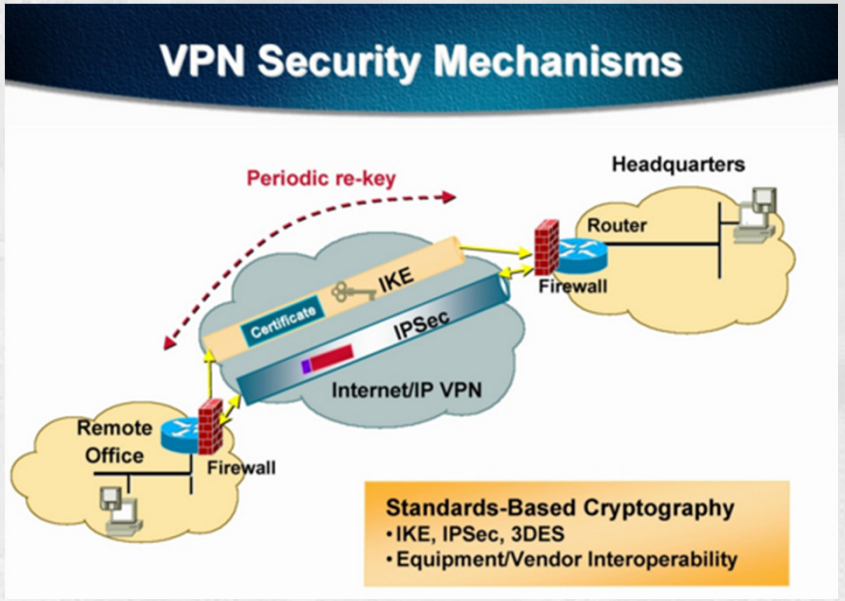
- Kryptering sikrer at uvedkommende ikke tyder data
- Kryptering af hele IP pakken sikrer hemmeligholdelse af identitet på afsender og modtager (Originale IP adresser)

IPsec - Internet Protocol Security

HOUSE OF TECHNOLOGY

– en del af mercantec

- IPsec er:
  - **Ikke** en transportprotokol, men en **sikkerheds protokol suite** …
  - En **tilføjelse til IPv4**
    - **Suiten installeres separat**
  - **Indbygget i IPv6** som standard
- IPsec giver:
  - 'Per IP pakke' beskyttelse
  - **Authentication** og **Encryption** på forbindelserne, dvs. fra:
    - IP host til IP host
    - Netværk til netværk
      - Mellem to **Security gateways**
    - IP host til netværk
      - F.eks. en software-VPN

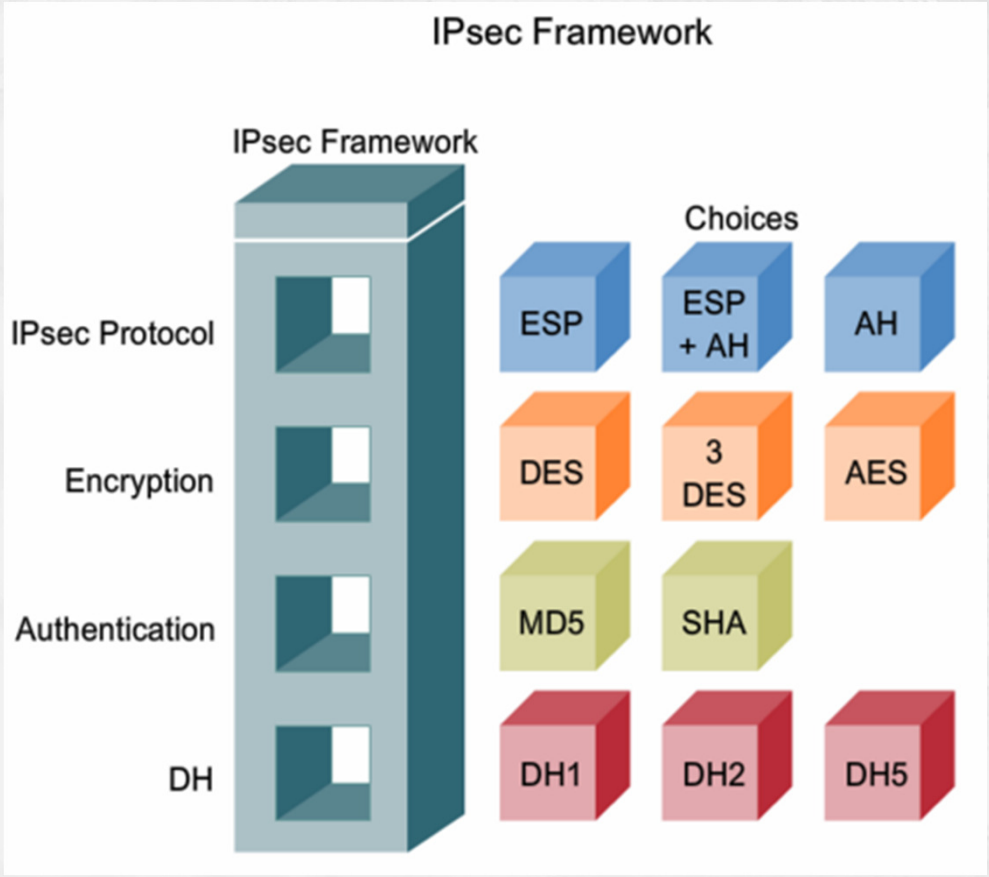


- IPsec **opererer på netværkslaget**, hvilket giver højere sikkerhed end systemer på de højere lag, f.eks. SSH, TLS eller SSL systemerne

IPsec - Internet Protocol Security

HOUSE OF TECHNOLOGY

– en del af mercantec



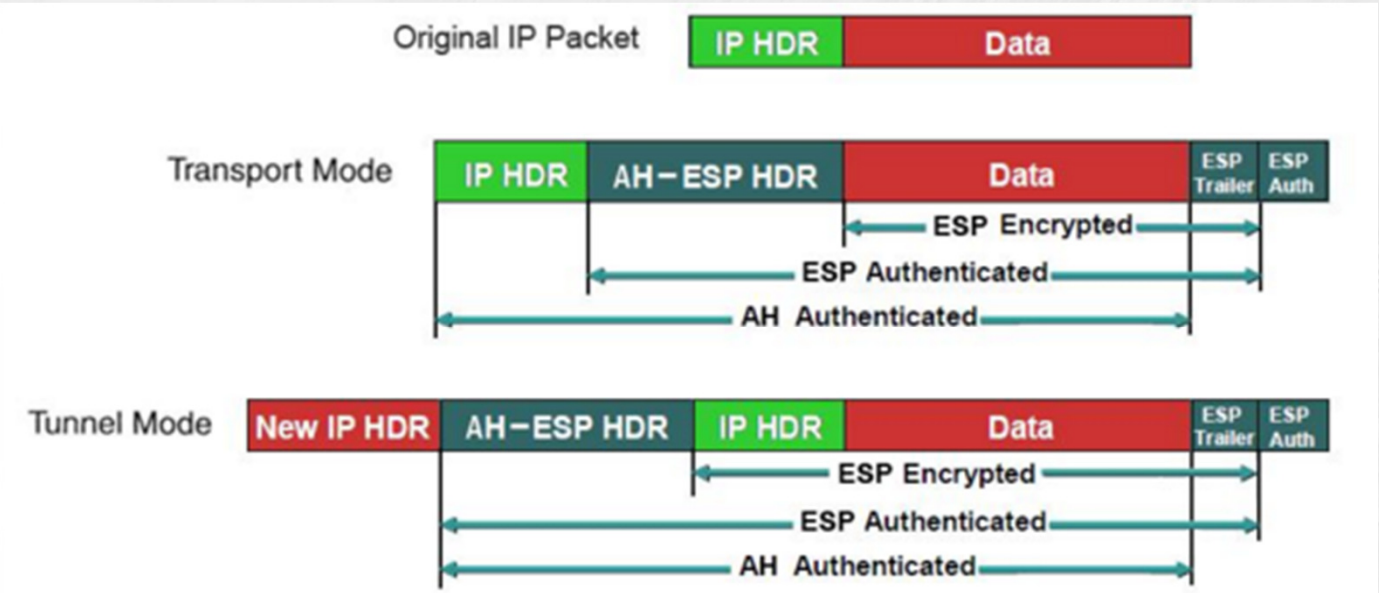
- **IPsec modulerne:**
  - **Protokollerne AH og ESP** giver authentication og integritet
    - AH er ukrypteret
    - ESP benytter kryptering
  - **Krypteringen DES, 3DES og AES** giver confidentiality på dataudvekslingen
  - **Authentication MD5 og SHA** giver via en sikker HASH funktionalitet både integrity protection og authenticity
  - **Diffie-Hellman** giver mulighed for at udveksle kryptonøgler sikkert over et usikkert netværk

IPsec – de to 'modes'

HOUSE OF TECHNOLOGY

– en del af mercantec

- IPsec kan benyttes i to 'modes':
  - **Transport mode –** IPsec headeren lægges ind i den originale pakke
    - Bruges ofte til **Remote access VPN løsninger**
  - **Tunnel mode –** hele pakken krypteres og bliver en del af en ny, større pakke
    - Bruges ofte til **Site-to-site VPN**



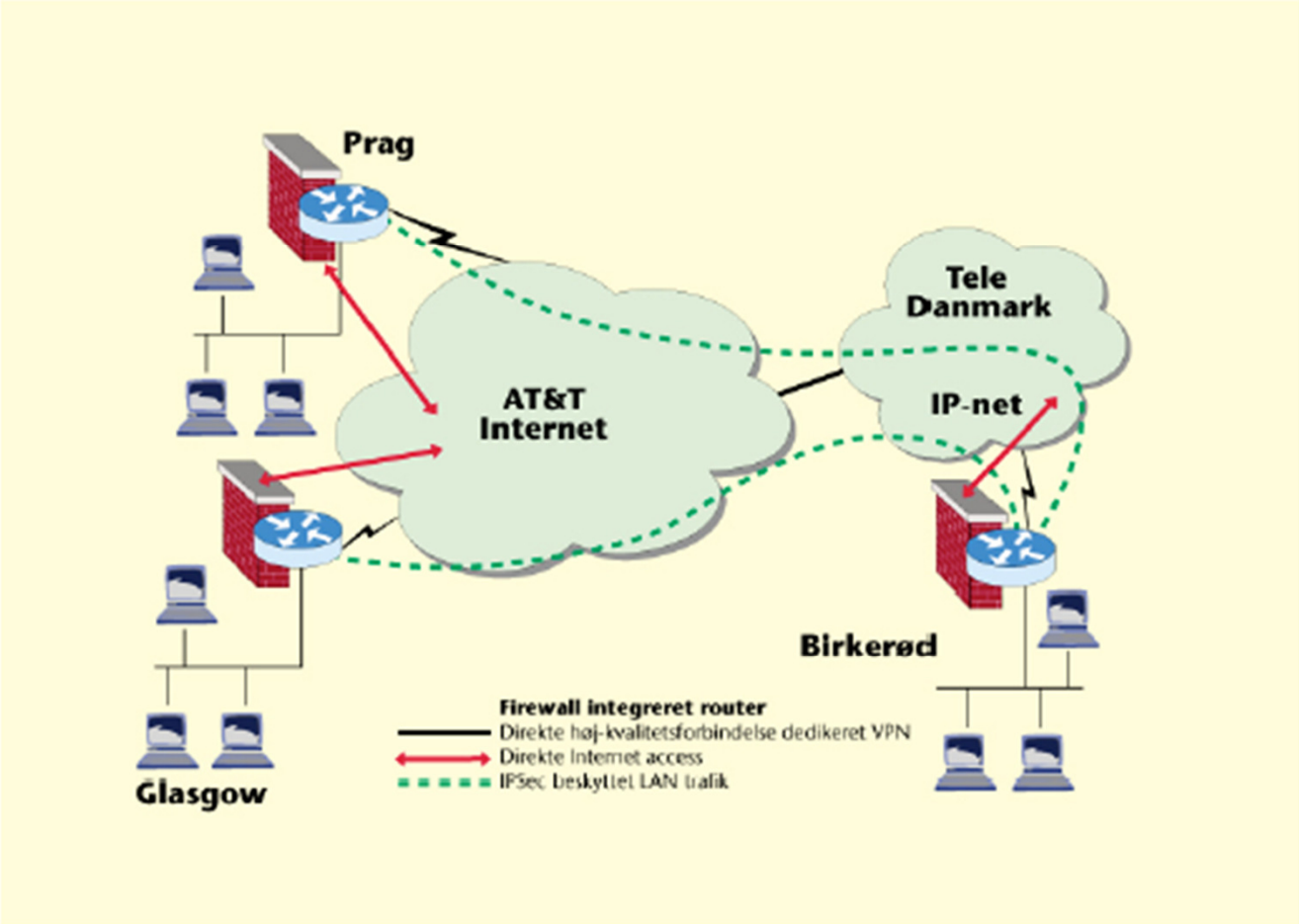
IPSec Architecture

Eksempel - Internationalt VPN

HOUSE OF TECHNOLOGY

ercantec+

IVPN med internet access. Routeren er installeret og konfigureret med IP-Sec SW. samt en Cisco IOS firewall med lokal tilgang til internettet via AT&T nettet og der er opsat de ønskede tuneller.



Eksemplet viser et Internationalt VPN med tre lokationer, hvor der samtidig er etableret direkte internet-adgang. Trafikken mellem de tre lokationer er beskyttet af IPSec. mans downloading m.m. fra internettet sikres gennem firewall.

Eksempel - TDC VPN løsninger

HOUSE OF TECHNOLOGY

– en del af mercantec

- **Routerbaseret VPN**
  - VPN forbindelsen etableres imellem CPE (Costumer Premises Equipment) routerne dvs. kunde routere.
  - Kan anvendes på alle tilslutninger til Internet
- **Netbaseret VPN**
  - Anvender MPLS VPN mellem kundens sites
  - Giver større sikkerhed

Mere information

HOUSE OF TECHNOLOGY

– en del af mercantec

- Hvis du vil finde mere information om sikkerhed, vira mv. kan du prøve følgende hjemmesider:
  - http://www.icsalabs.com/ og
  - http://www.symantec.com/avcenter/

- Her kan du også følge med i den aktuelle situation omkring sikkerhedstruslerne på 'nettet'