

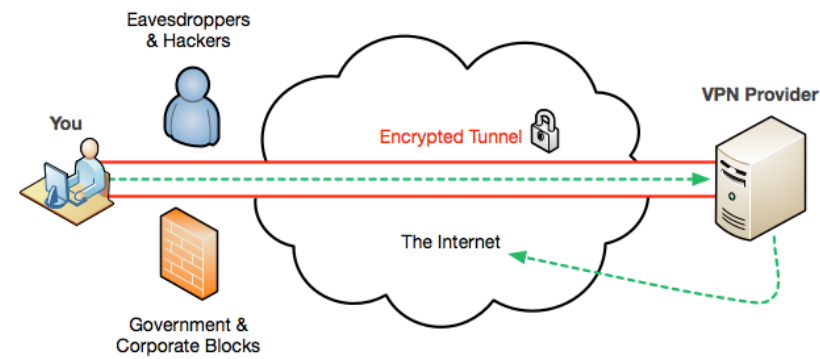
KRESTEN JACOBSEN

VPN (IPSEC+OPENVPN)

Hvad: VPN - Virtual Private Network

Hvorfor:

OVERBLIK: VPN



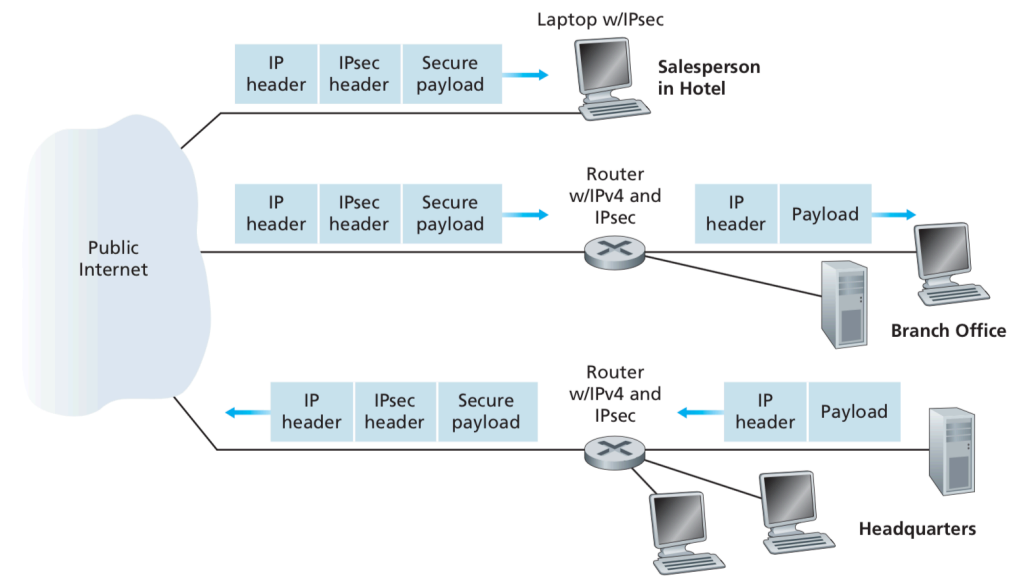
- ▶ Sikre transport af data i mellem to 'endpoints'
- ▶ Indkapsler data i en sikker tunnel, således at man kan bruge et offentligt net som underliggende medie.

Hvorfor bruge det?

Privatliv / konfidentialitet,

Hvorfor ikke bruge det altid? CPU-cykler,

OVERBLIK: VPN



Terminering forskellige steder:

Site-to-site bliver typisk brugt i en cooperative setting til at tilbyde adgang til ressourcer internt i firmaet.

Client / server bliver typisk brugt af private for at højne sikkerheden på et (relativt) lokalt netværk (man-in-the-middle).

TEORI: IPSEC

Host mode with AH	Host mode with ESP
Tunnel mode with AH	Tunnel mode with ESP

AH: *Authentication Header*

Sikrer afsender-autentificering, integritet, men ikke fortrolighed

ESP: *Encapsulating Security Payload* <- Mest brugt, da den også sikrer fortrolighed.

Sikrer afsender-autentificering, integritet OG fortrolighed.

Transport mode:

Genbruger den oprindelige header

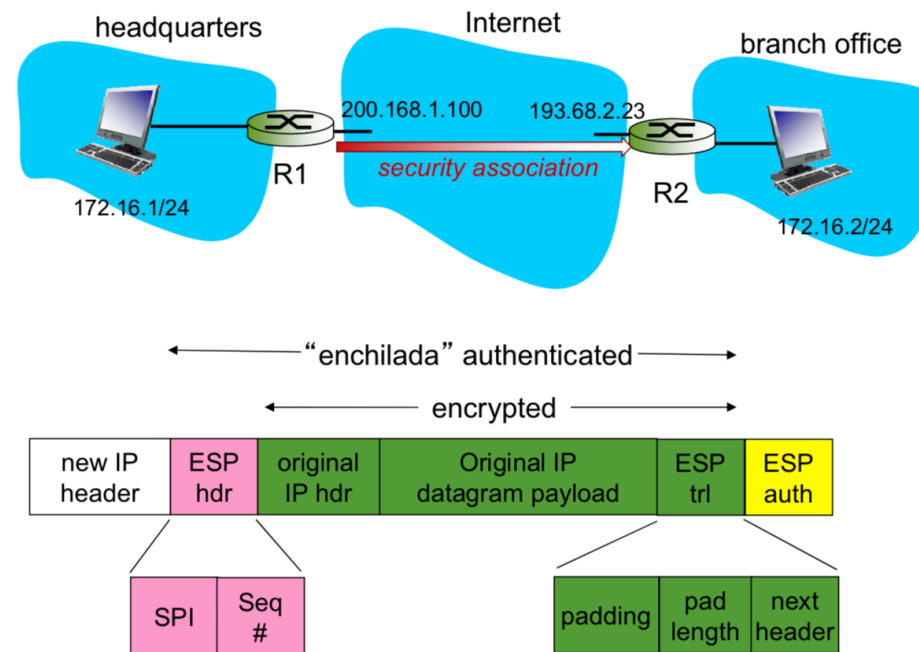
Giver ikke beskyttelse eller kryptering til den originale IP header.

Tunnel mode: <- Mest brugt, da den også sikrer fortrolighed.

Ny header

Giver beskyttelse af hele den originale IP pakke og kryptere den og tilføjer ny header.

TEORI: IPSEC



SA: Security Association
Verificeret envejsforbindelse etableret mellem R1 og R2 (vpn-endpoints)

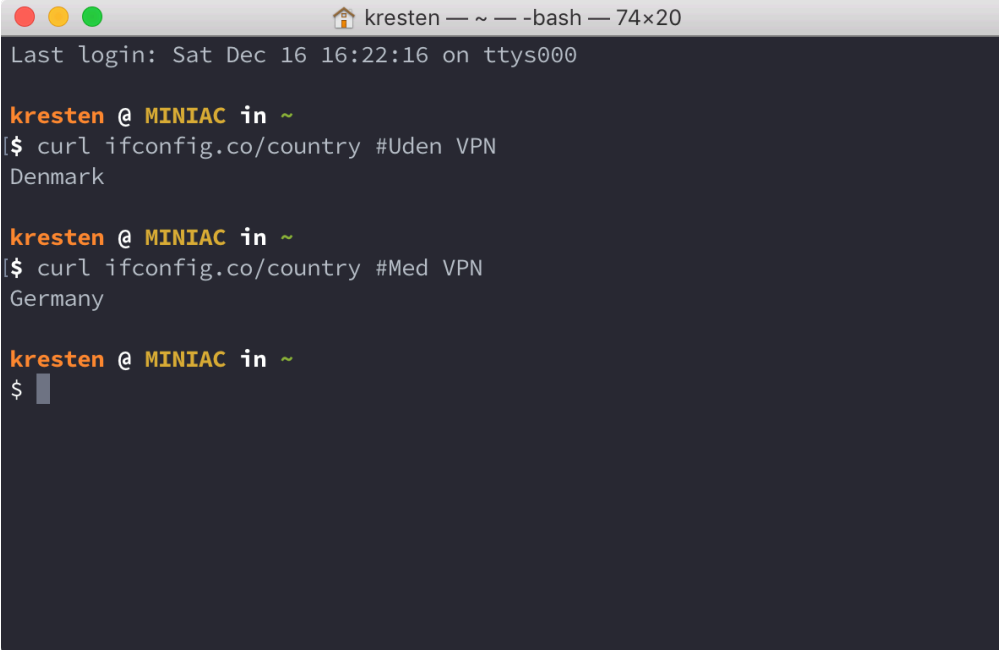
SPI: Security Parameter Index
Specificerer hvilken SA pakken hører til.

Seq #: Sekvensnummer for at forhindre replay-angreb.

ESP trl: ESP trailer: Padding, pad længde, næste header

ESP auth: Verifikationsværdi genereret med delt nøgle

DEMO: TJEK OFFENTLIG IP

A terminal window with a dark background and light text. The window title bar shows 'kresten — ~ — -bash — 74x20'. The terminal content shows a login message, followed by two commands to check the public IP using curl. The first command returns 'Denmark' and the second returns 'Germany'.

```
kresten — ~ — -bash — 74x20
Last login: Sat Dec 16 16:22:16 on ttys000

kresten @ MINIAC in ~
$ curl ifconfig.co/country #Uden VPN
Denmark

kresten @ MINIAC in ~
$ curl ifconfig.co/country #Med VPN
Germany

kresten @ MINIAC in ~
$
```